08/09/2024

Bloc2 - sem3-4 - atelier 01 Configuration avancée du routage

**Document de l’atelier :**

* [Bloc2\_sem3-4\_activite-2-Configuring.pka](Bloc2_sem3-4_activite-2-Configuring%20Floating%20Static%20Routes.pka)
* [Bloc2\_sem3-4\_activite-3-EIGRP-convergence.pka](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-3-EIGRP-convergence.pka)
* [Bloc2\_sem3-4\_activite-4-GNS3.gns3](Bloc2_sem3-4_activite-4-GNS3/Bloc2_sem3-4_activite-4-GNS3.gns3)
* [Bloc2\_sem3-4\_activite-5-EIGRP-redistribution-debut.pkt](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-5-EIGRP-redistribution-debut.pkt)
* [Bloc2\_sem3-4\_activite-6-OSPF-debut.pkt](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-6-OSPF-debut.pkt)
* [Bloc2\_sem3-4\_activite-7-ospfmultiarea\_debut.pkt](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-7-ospfmultiarea_debut.pkt)
* [Bloc2\_sem3-4\_activite-8\_DR.pkt](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-8_DR.pkt)
* [Bloc2\_sem3-4\_activite-9-Redistribution-des-routes-entre-EIGRP-et-OSPF.pkt](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-9-Redistribution-des-routes-entre-EIGRP-et-OSPF.pkt)
* [Bloc2\_sem3-4\_activite-10-Redistribution\_de\_route\_statique.pkt](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-10-Redistribution_de_route_statique.pkt)
* [Bloc2\_sem3-4\_activite-11-Decouverte-OSPF-HSRP-1-Depart.pka](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-11-Decouverte-OSPF-HSRP-1-Depart.pka)
* [Bloc2\_sem3-4\_activite-12-Decouverte-OSPF-HSRP-1-Depart-partie-2.pkt](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-12-Decouverte-OSPF-HSRP-1-Depart-partie-2.pkt)
* [Bloc2\_sem3-4\_activite-13-configure\_and\_Verify\_eBGP.pka](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-13-introduction_au_protocole_BGP.pkt)
* [Bloc2\_sem3-4\_activite-14-configure\_and\_Verify\_eBGP.pka](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-14-configure_and_Verify_eBGP.pka)
* [Bloc2\_sem3-4\_activite-15-bgp-debut.pkt](file:///E:\B2%20SIO2%20Infrastructure%20réseau\Routage%20avencee%20actuelle\atelier%2001\Bloc2_sem3-4_activite-15-bgp-debut.pkt)

Table des matières

[1 Introduction : 2](#_Toc178416871)

[2 Un peu de théorie 3](#_Toc178416872)

[2.1 Classification des protocoles de routage 3](#_Toc178416873)

[2.2 Les protocoles à état de liens 3](#_Toc178416874)

[2.3 Algorithme SPF 3](#_Toc178416875)

[2.4 Le protocole OSPF 4](#_Toc178416876)

[2.5 Encapsulation de message OSPF 4](#_Toc178416877)

[2.6 Protocole Hello 4](#_Toc178416878)

[2.7 Mise à jour d’état de liens OSPF 4](#_Toc178416879)

[2.8 Algorithme OSPF 4](#_Toc178416880)

[2.9 Authentification et Chiffrement dans OSPF 5](#_Toc178416881)

[3 Prérequis 5](#_Toc178416882)

[4 Enoncé 1 : Configuration d’une adresse IP de routage statique flottante 5](#_Toc178416883)

[4.1 Contexte : 5](#_Toc178416884)

[4.2 Partie 1 : Configurer une route statique flottante IPv4 5](#_Toc178416885)

[4.2.1 Étape 1 : configurez une route statique par défaut IPv4. 5](#_Toc178416886)

[4.2.2 Étape 2 : configurez une route statique flottante IPv4. 6](#_Toc178416887)

[4.2.3 Partie 2 : Tester le basculement vers la route statique flottante IPv4 8](#_Toc178416888)

[4.3 Partie 3 : Configurer et tester le basculement vers une route statique flottante IPv6 9](#_Toc178416889)

[4.3.1 Étape 1 : configurez une route statique flottante IPv6. 9](#_Toc178416890)

[4.3.2 Étape 2 : testez le basculement vers la route statique flottante IPv6. 9](#_Toc178416891)

[4.3.3 Énoncé 2 : Présentation du protocole EIGRP 11](#_Toc178416892)

[4.3.4 Énoncé 3 : Étude d’un fichier pka et protocole EIGRP 1](#_Toc178416893)

[4.3.5 Énoncé 4 : Configuration d’un tunnel GRE et routage EIGRP 3](#_Toc178416894)

[4.3.6 Énoncé 5 : Redistribution de routes via le protocole EIGRP 8](#_Toc178416895)

[4.3.7 Énoncé 6 : Configuration OSPF avec VLSM 9](#_Toc178416896)

[4.3.8 Énoncé 7 : Configuration OSPF Multi-Area Virtual Link 24](#_Toc178416897)

[4.3.9 Énoncé 8  : Modification du coût OSPF et élection du routeur DR et du routeur BDR 28](#_Toc178416898)

[4.3.10 Énoncé 9 : Redistribution des routes entre EIGRP et OSPF 35](#_Toc178416899)

[4.3.11 Énoncé 10 : Redistribution de route statique 39](#_Toc178416900)

[4.3.12 Énoncé 11 : OSPF et la redondance via HSRP 41](#_Toc178416901)

[4.3.13 Énoncé 12 : Introduction au protocole BGP 54](#_Toc178416902)

[4.3.14 Énoncé 13 : Packet Tracer – Configuration et vérification du routage eBGP 56](#_Toc178416903)

[4.3.15 Énoncé 14 : Atelier BGP Configuration du protocole BGP avec un routage par défaut 64](#_Toc178416904)

[5 Conclusion : 73](#_Toc178416905)

[6 Webographie : 74](#_Toc178416906)

# Introduction :

L'atelier présenté les protocoles de routage utilisés dans les réseaux informatiques, en se concentrant sur les protocoles EIGRP, OSPF, et BGP, ainsi que sur les concepts de redistribution et de redondance. Ce parcours d'apprentissage permet d'explorer les mécanismes de routage statique, les techniques de redistribution des routes entre différents protocoles, et la configuration avancée des tunnels GRE. L'atelier met également en lumière des aspects essentiels comme la gestion des réseaux multi-zones avec OSPF Multi-Area, ainsi que l'optimisation des routes à travers les protocoles HSRP et BGP.

À travers des fichiers Packet Tracer et GNS3, l'atelier cadre des pratiques pour configurer et tester ces technologies, en abordant des sujets comme la convergence des routes, l'authentification et le chiffrement dans OSPF, et la mise en place de routes redondantes pour garantir la disponibilité du réseau.

# Un peu de théorie

## Classification des protocoles de routage

Les protocoles de routage se divisent en deux catégories : ceux pour les petits réseaux (RIP, OSPF, IGRP, EIGRP) et ceux pour les grands réseaux (BGP). OSPF est le protocole par défaut pour les réseaux internes, tandis que BGP est utilisé pour les très grands réseaux comme l'Internet.

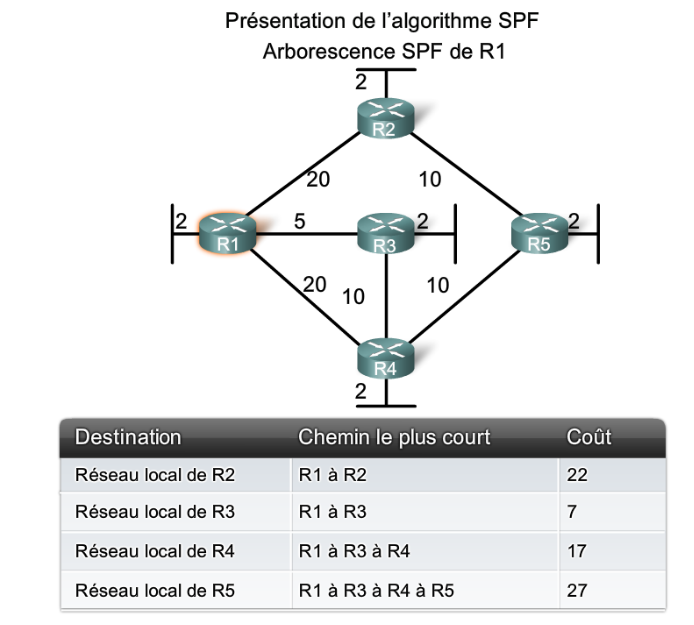
## Les protocoles à état de liens

Les protocoles à état de liens, comme OSPF, utilisent l'algorithme SPF (Shortest Path First) pour déterminer les chemins les plus efficaces dans un réseau. La commande show ip route permet de vérifier les tables de routage.

## Algorithme SPF

L'algorithme SPF a été créé par Edsger Dijkstra, un mathématicien et informaticien néerlandais. Il est surtout connu pour son algorithme de calcul du plus court chemin dans les graphes, essentiel dans les protocoles de routage modernes.

Présentation de l’algorithme



Exercices : Faites pour chacun des autres routeurs la table SPF.

|  |  |  |
| --- | --- | --- |
| Destination | Chemin le plus court | Cout |
| Réseau local de R1 | R2 à R1 | 22 |
| Réseau local de R3 | R2 à R1 à R3 | 27 |
| Réseau local de R4 | R2 à R 5 à R4 | 24 |
| Réseau local de R5 | R2 à R5 | 12 |

|  |  |  |
| --- | --- | --- |
| Destination | Chemin le plus court | Cout |
| Réseau local de R1 | R3 à R1 | 7 |
| Réseau local de R2 | R3 à R1 à R2 | 27 |
| Réseau local de R4 | R3 à R4 | 12 |
| Réseau local de R5 | R3 à R4 à R5 | 24 |
| Destination | Chemin le plus court | Cout |
| Réseau local de R1 | R4 à R1 | 22 |
| Réseau local de R2 | R4 à R1 à R2 | 37 |
| Réseau local de R3 | R4 à R3 | 12 |
| Réseau local de R5 | R4 à R5 | 12 |
| Destination | Chemin le plus court | Cout |
| Réseau local de R1 | R5 à R2 à R1 | 32 |
| Réseau local de R2 | R5 à R2 | 12 |
| Réseau local de R3 | R5 à R4 à R3 | 22 |
| Réseau local de R4 | R5 à R4 | 12 |

## Le protocole OSPF

OSPF (Open Shortest Path First) est un protocole de routage à état de liens qui utilise l'algorithme SPF pour calculer les chemins les plus courts dans un réseau. Il est adapté aux grands réseaux internes, divise ceux-ci en zones pour optimiser la gestion et les mises à jour. OSPF converge rapidement et est largement utilisé pour sa précision et son efficacité dans les environnements complexes.

## Encapsulation de message OSPF

Les messages OSPF sont encapsulés directement dans les paquets IP sans utilisation de TCP ou UDP. OSPF utilise le protocole IP 89 pour la transmission de ses messages. Chaque message contient des informations essentielles comme les identifiants des routeurs et les données de topologie du réseau, permettant aux routeurs d'échanger efficacement les états de lien et de calculer les meilleures routes.

## Protocole Hello

Le protocole Hello est utilisé par OSPF pour établir et maintenir les relations de voisinage entre routeurs. Il envoie régulièrement des paquets Hello pour découvrir les routeurs voisins et vérifier leur disponibilité. Ce mécanisme permet de détecter les changements de topologie rapidement et de s'assurer que les routes entre routeurs restent fiables et à jour.

## Mise à jour d’état de liens OSPF

Les mises à jour d'état de liens OSPF (Link-State Update) sont utilisées pour diffuser les changements dans la topologie du réseau. Lorsque la topologie change (ajout/suppression de routeurs, changement de liens), OSPF envoie des Link-State Advertisements (LSA) à tous les routeurs du réseau. Ces LSAs permettent à chaque routeur de mettre à jour sa base de données d'état de lien et de recalculer les meilleures routes via l'algorithme SPF. Ce processus garantit une convergence rapide et une cohérence des tables de routage.

## Algorithme OSPF

L'algorithme OSPF (Open Shortest Path First) repose sur le calcul du plus court chemin grâce à l'algorithme SPF (Shortest Path First), également connu sous le nom d'algorithme de Dijkstra. Chaque routeur OSPF maintient une base de données de l'état de liens, représentant la topologie du réseau. À partir de ces informations, OSPF calcule les chemins les plus courts vers chaque destination, en attribuant un coût à chaque lien. OSPF optimise ainsi l'acheminement des paquets en fonction de la métrique la plus faible, permettant une convergence rapide et un routage efficace.

## Authentification et Chiffrement dans OSPF

OSPF utilise l'authentification et le chiffrement pour sécuriser les échanges entre routeurs. L'authentification garantit que les messages proviennent de routeurs légitimes, avec des options comme l'authentification simple ou l'authentification MD5. Le chiffrement protège les messages contre les interceptions, assurant la confidentialité et la sécurité des communications réseau.

# Prérequis

*Pour valider les prérequis nécessaires avant d’aborder l’atelier, indiquez si les affirmations suivantes sont vraies ou fausses.*

1. Les systèmes autonomes représentent des entités administratives de gestion des réseaux : Vrai

Les systèmes autonomes (AS) sont des entités administratives qui gèrent un ensemble de réseaux sous une même politique de routage.

1. Le protocole OSPF est un protocole à vecteur de distance : Faux, c'est un protocole à état de lien.
2. BGP est un EGP (Exterior Gateway Protocol) : Vrai (mais peut avoir des trames inter-AS).

BGP est effectivement un protocole de passerelle extérieure utilisé pour échanger des informations de routage entre systèmes autonomes, avec possibilité de communication inter-AS.

1. EIGRP est un protocole à état de liens : Vrai et Faux, EIGRP est un protocole hybride, combinant des éléments de vecteur de distance et d'état de lien.
2. OSPF supporte la mise en place d’authentification : Vrai

OSPF prend en charge l'authentification pour sécuriser les échanges entre routeurs.

1. EIGRP est un protocole défini par l’IETF : Faux, EIGRP est un protocole propriétaire de Cisco.

# Enoncé 1 : Configuration d’une adresse IP de routage statique flottante

Vous utiliserez le fichier [Bloc2\_sem3-4\_activite-2-Configuring](Bloc2_sem3-4_activite-2-Configuring%20Floating%20Static%20Routes.pka) Floating Static Routes.pka et vous répondrez aux questions posées. Voici le texte de l’activité.

## Contexte :

Dans cette activité, vous configurerez des routes statiques flottantes IPv4 et IPv6. Ces routes sont manuellement configurées avec une distance administrative supérieure à celle de la route principale et, par conséquent, ne seront pas inscrites dans la table de routage jusqu’à l’échec de la route principale. Vous testerez le basculement vers les routes de sauvegarde, puis vous restaurerez la connectivité à la route principale.

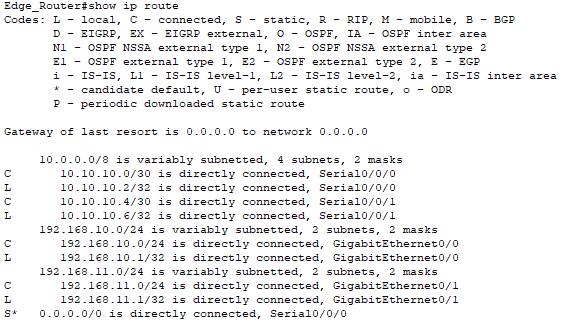
## Partie 1 : Configurer une route statique flottante IPv4

### Étape 1 : configurez une route statique par défaut IPv4.

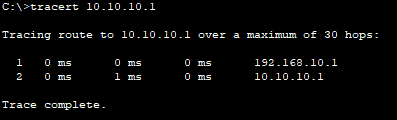
1. Configurez une route statique par défaut connectée directement depuis le routeur Edge\_Router vers Internet. La route principale par défaut doit traverser FAI1.

Edge\_Router(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/0

1. Affichez le contenu de la table de routage. Montrez que la route par défaut est visible dans la table de routage.



1. Depuis PC-A, tracez la route vers Serveur Web. La route doit démarrer à la passerelle par défaut 192.168.10.1 et passer par l’adresse 10.10.10.1. Si ce n’est pas le cas, montrez votre configuration de route statique par défaut.



### Étape 2 : configurez une route statique flottante IPv4.

1. Quelle est la distance administrative d’une route statique ?

La distende administrative et de 1 car une route statique est toujours à 1 par défaut.

1. Configurez une route statique flottante par défaut avec une distance administrative de 5. La route doit pointer sur ISP2.



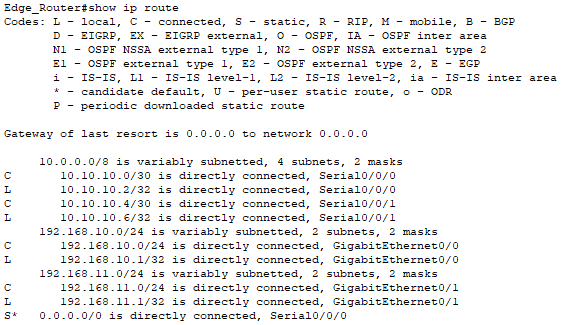
1. Consultez la configuration en cours et montrez que la route statique flottante par défaut IPv4 y est, tout comme la route statique par défaut IPv4.

Edge\_Router#show r



Affichez le contenu de la table de routage. Est-ce que la route statique flottante IPv4 est présente dans la table de routages ? Expliquez votre réponse

La table de routage montre une route statique par défaut indiquée par S/… mais il n'est pas précisé si elle est flottante car ils manquent la priorité administrative. Pour s’avoir s'il s'agit d'une route statique flottante il faut vérifier la configuration avec show r.



Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

### Partie 2 : Tester le basculement vers la route statique flottante IPv4

1. Sur le routeur Edge\_Router, demandez à l’administrateur de désactiver l’interface de sortie de la route principale.

Edge\_Router(config)#interface serial 0/0/1

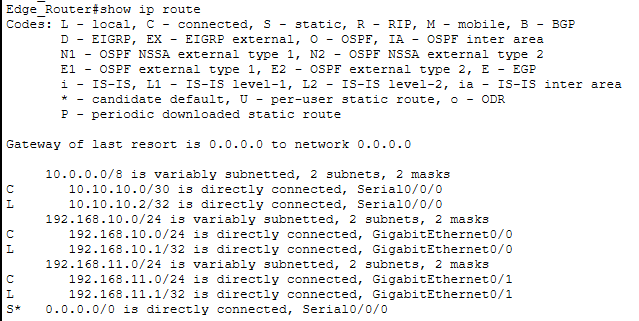
Edge\_Router(config-if)#shutdown

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

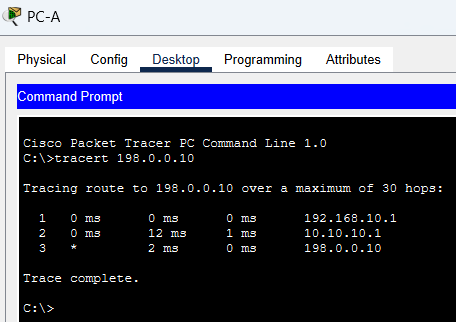
Description générée automatiquement

1. Montrez que la route statique flottante IPv4 est désormais dans la table de routage.

Il n’y a rien de plus qu’avant mais la route S\* 0.0.0.0/0 is directly connected, Serial0/0/0 et probablement la route statique flottante IPv4.



1. Tracez la route entre le PC-A et le serveur Web.



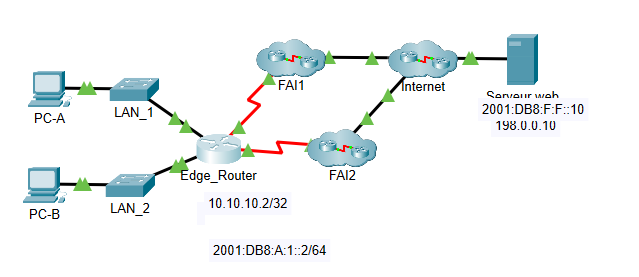
1. La route de secours a-t-elle fonctionné ? Si ce n’est pas le cas, attendez encore quelques secondes pour la convergence, puis testez à nouveau. Si la route de secours ne fonctionne toujours pas, étudiez votre configuration de route statique flottante.

Oui, la route de secours a fonctionné. De plus, le temps de réponse a été un peu plus long car il a tenté d'abord de passer par le même chemin qu'il avait emprunté la première fois avant de passer par l'autre route.

1. Restaurez la connectivité vers la route principale.

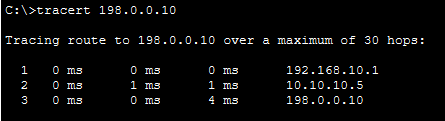
Edge\_Router(config)#interface serial 0/0/0

Edge\_Router(config-if)#no shutdown



1. Tracez la route entre le PC-A et le serveur Web pour vérifier que la route principale est restaurée.

Nous pouvons d'abord constater que le temps de réponse est bien plus court avec la route principale, mais également que l'adresse IP est différente car elle ne passe pas par le même FAI.



## Partie 3 : Configurer et tester le basculement vers une route statique flottante IPv6

### Étape 1 : configurez une route statique flottante IPv6.

1. La route statique flottante IPv6 vers le routeur ISP1 est déjà configurée. Configurez une route statique flottante par défaut IPv6 avec une distance administrative de 5. La route doit se diriger vers l’adresse IPv6 (2001:DB8:A:2::1) du routeur ISP2.



1. Consultez la configuration en cours pour vérifier que la route statique flottante IPv6 par défaut est désormais répertoriée sous la route statique par défaut IPv6.



### Étape 2 : testez le basculement vers la route statique flottante IPv6.

Sur le routeur Edge\_Router, demandez à l’administrateur de désactiver l’interface de sortie de la route principale.

Edge\_Router(config)# interface Serial0/0/0

Edge\_Router(config-if)# shutdown

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

Description générée automatiquement

Montrez que la route statique flottante IPv6 est désormais dans la table de routage.

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

Description générée automatiquement

c.     Tracez la route entre le PC-A et le serveur Web.

La route de secours a-t-elle fonctionné ? Si ce n’est pas le cas, attendez encore quelques secondes pour la convergence, puis testez à nouveau. Si la route de secours ne fonctionne toujours pas, étudiez votre configuration de route statique flottante.

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

Description générée automatiquement

Oui la route de secours a bien fonctionné nous pouvons le voir avec la capture d’écran, qui nous montre le ping entre PC-A et serveur web qui a réussis « Successful »

Restaurez la connectivité vers la route principale.

Edge\_Router(config)#interface s0/0/0

Edge\_Router(config-if)#no shutdown

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

Description générée automatiquement

e.     Tracez la route entre le PC-A et le serveur Web pour vérifier que la route principale est restaurée.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Nous pouvons voir avec cette capture d’écran que la route principale a bien été restauré car il passe par le premier Fai qui et en 10.10.10.1

### Énoncé 2 : Présentation du protocole EIGRP

EIGRP est un protocole propriétaire à Cisco, il ne fonctionne que sur les routeurs Cisco et a une distance administrative de 90 (5 pour les routes EIGRP summary), il utilise l’algorithme DUAL (Diffusing Update Algorithm) pour améliorer la convergence. EIGRP est le seul protocole de routage qui utilise un chemin de secours pour la transmission lors de l’inaccessibilité du chemin principale ou bien le successeur.

EIGRP est un protocole de routage hybride. C’est-à-dire qu’il n’est ni un protocole à vecteur de distance (RIP, RIPv2) ni un protocole à état de liens (type OSPF), il supporte aussi le VLSM (Variable Length Subnet Mask).

Pourquoi utiliser EIGRP (Avantages) ?

EIGRP est un protocole de routage propriétaire Cisco qui offre plusieurs avantages. Il supporte le VLSM, permettant une gestion flexible des sous-réseaux. Sa convergence rapide est assurée grâce à l'algorithme DUAL, qui évite les interruptions lors d'une panne. EIGRP utilise des mises à jour déclenchées pour prévenir les boucles de routage. Il est compatible avec tous les protocoles de couche liaison de données (PPP, NBMA, BMA). De plus, il prend en charge le load balancing, répartissant la charge sur plusieurs chemins, et utilise l'unicast et le multicast au lieu du broadcast, optimisant ainsi l'efficacité du réseau.

Six avantages ont été énoncés précédemment, mais êtes-vous capable d’associer un commentaire plus long concernant certains termes évoqués ci-dessus ?

En premier le VLSM permet d'optimiser l'utilisation des adresses IP en ajustant la taille des sous-réseaux selon les besoins réels, ce qui est essentiel pour des réseaux de tailles variables. Pour l’algorithme DUAL utilisé par EIGRP permet de recalculer rapidement les meilleures routes en cas de changement de topologie, réduisant ainsi le temps d'interruption du réseau. Cela assure une haute disponibilité et réactivité. De plus contrairement aux protocoles à vecteur de distance traditionnels, EIGRP envoie des mises à jour uniquement lorsqu'un changement se produit, limitant ainsi les risques de boucles et réduisant la consommation de bande passante pour les échanges inutiles. Il est plus compatibilité avec d’autre protocolaire car EIGRP fonctionne avec différents types de protocoles de la couche liaison de données, comme PPP, NBMA, et BMA, ce qui le rend adaptable à divers environnements réseau. Il y a également le Load balancing. Ce protocole permet de répartir le trafic sur plusieurs chemins de même coût ou avec des coûts différents, augmentant ainsi la performance et la fiabilité du réseau. En ce qui concerne l’utilisation de multicast et unicast. L’EIGRP évite le broadcast, qui peut inonder le réseau, en préférant l'unicast et le multicast pour la transmission d'informations, ce qui réduit la surcharge sur les ressources réseau et améliore l'efficacité.

Qu’est-ce que le VLSM ?

Le VLSM est une technique de sous-réseautage qui permet d'utiliser des masques de sous-réseau de longueurs variables au sein d'un même réseau. Cela optimise l'utilisation des adresses IP en attribuant des tailles de sous-réseaux adaptées aux besoins spécifiques. Le VLSM réduit le gaspillage d'adresses et offre une flexibilité dans la gestion des réseaux, facilitant ainsi la planification et l'organisation des adresses IP.

En quoi consiste la convergence ?

La convergence dans les réseaux informatiques est le processus par lequel tous les routeurs atteignent une vision cohérente et à jour de la topologie du réseau après un changement, comme une panne ou l'ajout d'un routeur. Cela implique la mise à jour des tables de routage par l'échange d'informations. Un temps de convergence rapide est crucial pour minimiser les interruptions de service et assurer la fiabilité du routage. En résumé, la convergence est essentielle pour maintenir la performance et la stabilité d'un réseau.

Qu’est-ce que le load-balancing ?

Le load balancing, ou équilibrage de charge, est une technique qui répartit le trafic ou les demandes sur plusieurs ressources, comme des serveurs ou des liens réseau. Cela optimise l'utilisation des ressources, évitant la surcharge d'un seul élément et améliorant la performance globale. En redirigeant le trafic en cas de défaillance d'une ressource, le load balancing assure également la haute disponibilité des services. En résumé, il est essentiel pour garantir l'efficacité et la continuité des services dans un réseau.

Terminologie d’EIGRP et description du mécanisme

* Table de voisinage
* Table de topologie
* Table de routage
* Successeur
* Successeur potentiel
* Distance Administrative

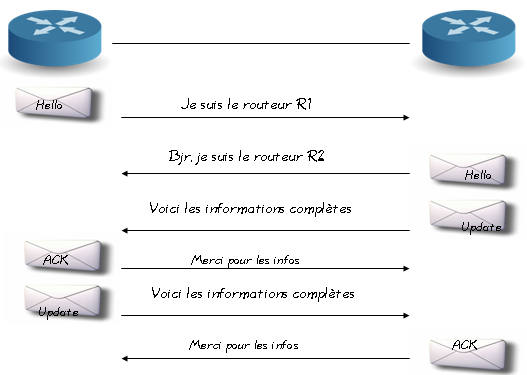


Figure 1 : EIGRP, découverte du réseau

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

Description générée automatiquementLe protocole EIGRP est un protocole de routage dynamique développé par Cisco, qui calcule les routes en fonction de la bande passante, du délai, de la fiabilité, de la charge, et du MTU. Ce projet consiste à configurer EIGRP dans un réseau simulé sous GNS3, avec un numéro de système autonome 100.

**Étapes de configuration :**

1. **Accéder au mode de configuration** :

Router2#configure terminal

1. **Activer EIGRP pour ASN 100** :

Router2(config)#router eigrp 100

1. **Déclarer les réseaux** :

Router2(config-router)#network 192.168.0.0

Router2(config-router)#network 192.168.2.0

Router2(config-router)#network 172.16.0.0

1. **Vérifier la configuration** :
   * Afficher les voisins EIGRP :

show ip eigrp neighbors

Afficher les routes EIGRP :

show ip route eigrp

### Énoncé 3 : Étude d’un fichier pka et protocole EIGRP

Vous utiliserez le fichier <Bloc2_sem3-4_activite-3-EIGRP-convergence.pka> vous répondrez aux questions posées. Voici le texte de l’activité.

Observation de la convergence du réseau

Connecter et configurer les connexions WAN

Configurer le protocole EIGRP pour annoncer des réseaux spécifiques

Observer la convergence du réseau dans la fenêtre de l’environnement ILC lors de l’arrêt et de la réactivation d’une interface

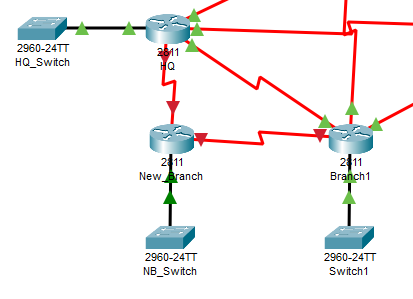
Examiner les paquets EIGRP en mode Simulation lors de la convergence du réseau

#### Contexte/Préparation

Le système vous a fourni une topologie dans laquelle HQ, Branch1, Branch2 et Branch3 sont préconfigurés. Un nouveau routeur a été ajouté à la topologie (New\_Branch) ; sa configuration est partielle. Vous devrez connecter New\_Branch à HQ et à Branch1, terminer la configuration du nouveau routeur, puis examiner la convergence du réseau.

#### Étape 1 : connexion et configuration de la connexion WAN sur le routeur New\_Branch

Connectez l’interface S0/0/0 sur New\_Branch à S0/1/1 sur HQ (DCE).



Connectez l’interface S0/0/1 sur New\_Branch à l’interface S0/1/1 sur Branch1 (DCE).

Configurez l’interface S0/0/0 avec l’adresse IP 172.16.3.218/30.



Configurez l’interface S0/0/1 avec l’adresse IP 172.16.3.221/30.



#### Étape 2 : configuration du protocole EIGRP pour annoncer un réseau spécifique sur le routeur New\_Branch

Configurez New\_Branch avec le protocole EIGRP et 3 comme numéro de système autonome.

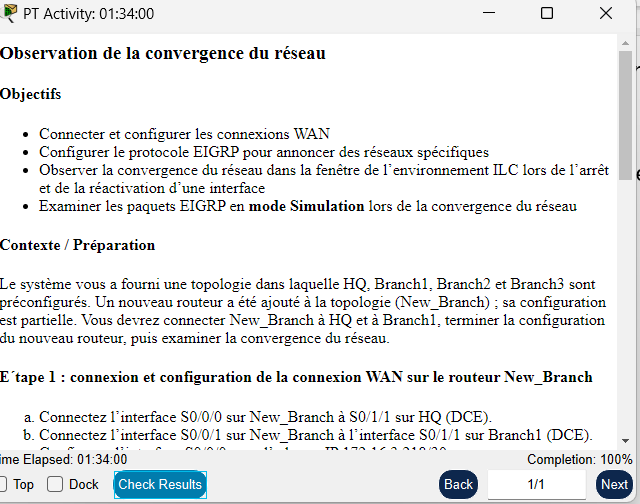
Annoncez spécifiquement les réseaux connectés directement.

New\_Branch(config)#route eigrp 3

New\_Branch(config-router)#network 172.16.3.160 0.0.0.31

New\_Branch(config-router)#network 172.16.3.216 0.0.0.3

New\_Branch(config-router)#network 172.16.3.220 0.0.0.3



#### Étape 3 : observation de la convergence du réseau en mode Temps réel

Dans la fenêtre CLI de New\_Branch, vous pouvez observer la convergence en mode Temps réel. Lors de la convergence du réseau, le protocole EIGRP développe des contiguïtés.

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

Description générée automatiquement

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

Description générée automatiquement

Après la convergence du réseau, arrêtez l’interface S0/0/0 sur New\_Branch.

New\_Branch(config)#interface Serial0/0/0

New\_Branch(config-if)#shutdown

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

Description générée automatiquement

Observez les modifications du réseau.

En arrêtant l'interface Serial0/0/0, EIGRP a détecté la perte de contiguïté avec le voisin 172.16.3.217 et a mis à jour la table de routage en conséquence, supprimant les routes associées. Seules les routes via Serial0/0/1 sont désormais présentes.

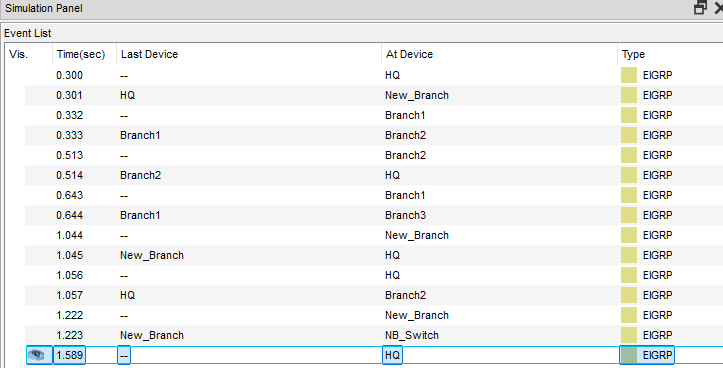
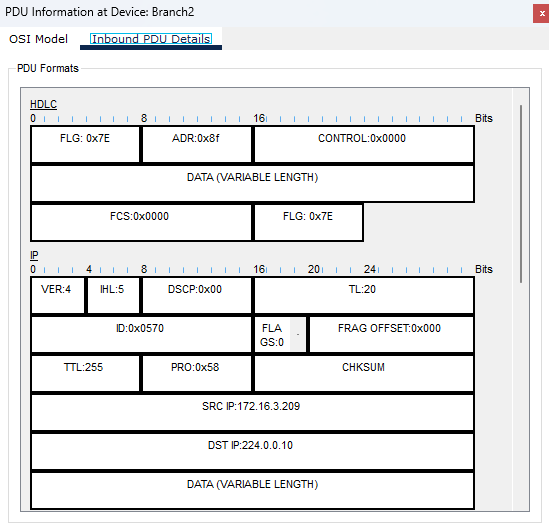
Réactivez l’interface S0/0/0.

New\_Branch(config)#interface Serial0/0/0

New\_Branch(config-if)#no shutdown

#### Étape 4 : observation de la convergence du réseau en mode Simulation

Cliquez sur Simulation Mode.

Définissez les filtres de la liste d’évènements pour afficher uniquement les paquets EIGRP.

Accédez à la fenêtre d’interface CLI de New\_Branch.

Arrêtez l’interface S0/0/1.

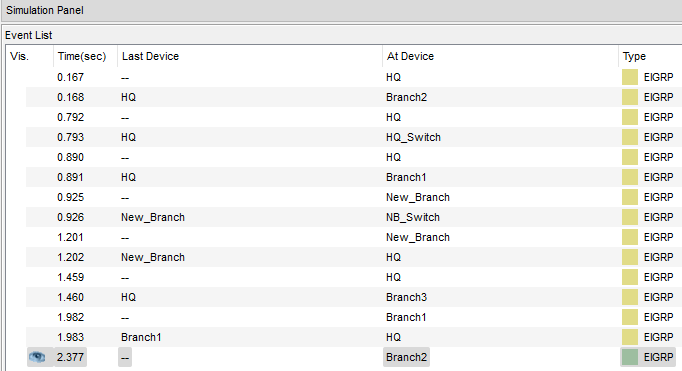


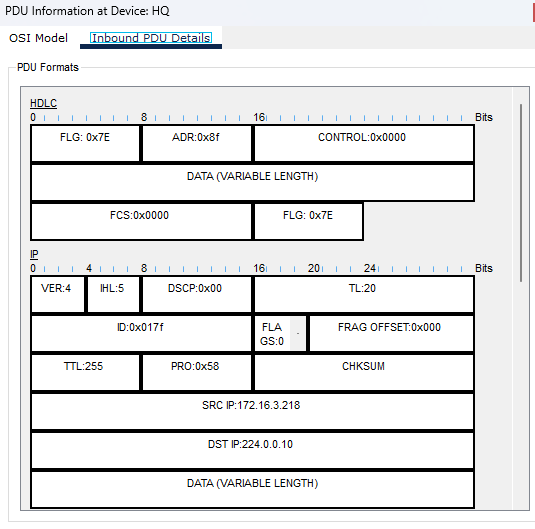
Cliquez sur le bouton Auto Capture/Play pour lancer la simulation.

Rouvrez la fenêtre CLI et observez les effets.

Laissez la simulation s’exécuter un bref instant, puis cliquez sur le bouton Auto Capture/Play pour l’interrompre.

Examinez certains paquets dans Event List.





En arrêtant l'interface S0/0/1 du routeur New\_Branch, je constate que la communication directe avec Branch1 est interrompue. Cela force le routeur à passer par HQ pour acheminer le trafic, puisque le lien direct entre New\_Branch et Branch1 est coupé.

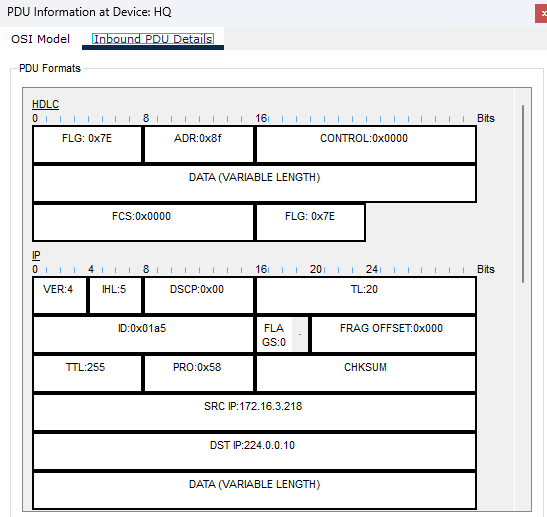
Avec l'arrêt de l'interface, l'adresse IP utilisée pour communiquer avec les autres branches changée, car le routeur d'exploiter les autres interfaces disponibles. Cependant, la désactivation de S0/0/1 modifie la topologie du réseau et change le chemin emprunté pour les communications, rendant le routeur dépendant de HQ pour atteindre Branch1.

#### Étape 5 : observation des effets liés à l’activation d’une interface

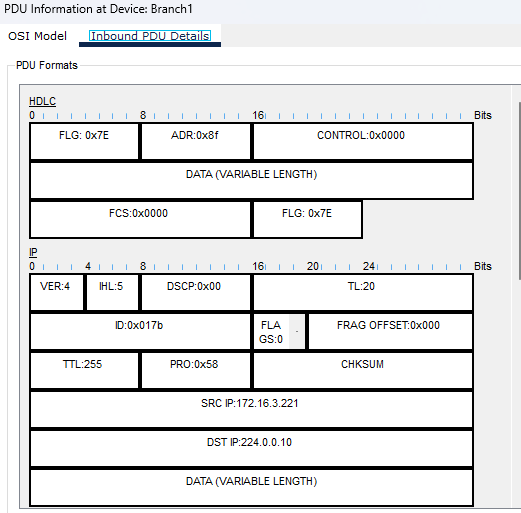
Relancez la simulation en cliquant de nouveau sur le boutonAuto Capture/Play.

Réactivez l’interface S0/0/1 et observez la convergence dans la fenêtre CLI, la liste d’évènements et la topologie.

Arrêtez la simulation.







##### Remarques générales et questions

Quelles informations s’affichent dans la fenêtre CLI après la convergence du protocole EIGRP ? Faites-en une analyse circonstanciée.

Après la convergence d'EIGRP, la CLI affiche les voisins découverts et les adjacences établies, avec des messages comme "Neighbor X is up: new adjacency." La table de routage se met à jour, montrant des routes marquées par D (pour EIGRP). Des messages de stabilité, tels que "EIGRP: Convergence achieved", apparaissent, indiquant que le routage est stable. La table de topologie, accessible via show ip eigrp topology, liste les routes passives (stables) et leurs successeurs. Des paquets Hello sont régulièrement échangés pour maintenir les adjacences.

On peut donc voir que les routeurs utilisant le protocole EIGRP tentent de rétablir tous les chemins afin que les paquets puissent arriver à destination par l'interface qui n'est pas désactivée.

Qu’est-il advenu des paquets EIGRP sur le nouveau réseau local lorsque la liaison de réseau étendu a été rompue entre HQ et New\_Branch ?

Lorsque la liaison entre HQ et New\_Branch est rompue, les voisins EIGRP perdent leur adjacence, et les routes dépendant de cette connexion sont supprimées. EIGRP réévalue la topologie et tente de trouver des chemins alternatifs. Si aucun n'est disponible, les paquets destinés à New\_Branch sont abandonnés. Des messages d'état, comme "stuck-in-active" (SIA), peuvent apparaître si le recalcul prend trop de temps. Les paquets EIGRP cessent donc de circuler entre les deux sites jusqu'à rétablissement de la liaison.

### Énoncé 4 : Configuration d’un tunnel GRE et routage EIGRP

Document : [Bloc2\_sem3-4\_activite-4-GNS3.gns3](Bloc2_sem3-4_activite-4-GNS3/Bloc2_sem3-4_activite-4-GNS3.gns3)

On pourra utiliser ici aussi le simulateur GNS3.

Quel est l’objectif de l’implantation de tunnels ?

L'implantation de tunnels réseau, vise à permettre le transport sécurisé de données entre deux réseaux distants via un tunnel logique. Cela permet d'encapsuler des protocoles ou des paquets non routables sur un réseau public ou incompatible. Les tunnels facilitent également la création de réseaux privés virtuels (VPN), permettant ainsi de relier des sites distants de manière sécurisée et efficace.

Qu’est-ce qu’un tunnel GRE ?

Un tunnel GRE (Generic Routing Encapsulation) est une technologie d'encapsulation qui permet d'encapsuler des protocoles réseau dans un autre protocole, généralement IP, pour transporter des données sur des réseaux hétérogènes. GRE est souvent utilisé pour créer des tunnels point-à-point entre deux routeurs sur un réseau public, permettant le transport de différents types de trafic réseau (IP, IPv6, multicast, etc.) à travers des réseaux qui ne supportent normalement que l'IP.

Réaliser sous GNS3 le schéma de réseau dont la figure est ci-dessous. Le tunnel GRE est entre les routeurs R2 et R3 et aura comme adresse réseau 172.16.1.0/24.

Vous montrerez par des captures réseau appropriées que le tunnel est bien utilisé lors d’un ping entre le poste PC1 et le poste PC2.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Description générée automatiquement

On peut voir avec ces captures d’écran que le tunnel a bien fonctionné, car les deux PC sont considérés comme faisant partie du même réseau alors qu’ils sont connectés à des routeurs différents et ont des adresses IP différentes. On peut également voir avec les trames capturées à l’aide de Wireshark que toutes les informations passent d’un pc à l’autre comment s’il n’y avait pas de routeur entre les différent pc ce qui fait que dans les trame capture on ne voit pas le routeur 1, qui fait office de passerelle entre les deux réseaux.

En arrêtant l’interface du tunnel sur R3, vous montrerez qu’un recalcul de la table de routage se fait. Il sera bon à cet effet de la présenter dans un premier temps puis de la présenter après la manipulation. Vous étudierez alors les modifications qui y ont été apportées.

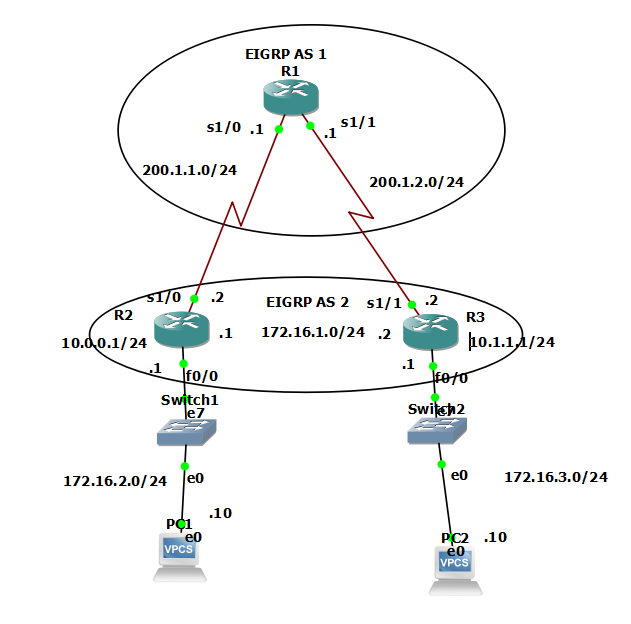
Une image contenant texte, capture d’écran, Police

Description générée automatiquementUne image contenant texte, capture d’écran, Police

Description générée automatiquement

Dans la table de routage après l’extinction du tunneling, R3 possède des routes connectées directement (10.1.1.0/24, 172.16.1.0/24, etc.) et des routes apprises via EIGRP (172.16.1.0/24, 200.1.2.0/24). Après la remis en état de l'interface Tunnel0, de nouvelles routes apparaissent, comme 172.16.1.2/32 et 172.16.1.0/24, maintenant connectées via le tunnel. Cela modifie les chemins utilisés par le routeur. Lorsque le tunnel est désactivé (shutdown sur Tunnel0), ces routes sont supprimées de la table. Le routeur recalculera alors les chemins et reviendra aux routes précédentes, notamment celles apprises via EIGRP, sur des interfaces physiques comme Serial1/1. Cela montre la capacité du routage à s'adapter aux changements dans la topologie du réseau en temps réel.

Une image contenant texte, diagramme, ligne, cercle

Description générée automatiquementPrésentation : Mon réseaux :

Voici les éléments permettant d’effectuer la configuration demandée

PC1 :

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

PC2 :

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

Description générée automatiquement

**Routeur R2 :**

R2(config)# interface loopback 0

R2(config-if)# ip address 10.0.0.1 255.255.255.0

R2(config-if)# no shutdown

R2(config-if)# interface serial 1/0

R2(config-if)# ip address 200.1.1.2 255.255.255.0

R2(config-if)# clockrate 128000

R2(config-if)# no shutdown

R2(config-if)# interface fa0/0

R2(config-if)# ip address 172.16.2.1 255.255.255.0

R2(config-if)# no shutdown

R2(config)# int tunnel0

R2(config-if)# tunnel source serial 1/0

R2(config-if)# tunnel destination  200.1.2.2

R2(config-if)# ip address 172.16.1.1 255.255.255.0

R2(config-if)# no shutdown

R2(config)# router eigrp 1

R2(config-router)# no auto-summary

R2(config-router)# network 200.1.1.0

R2(config-router)# network 172.16.2.0

R2(config)# router eigrp 2

R2(config-router)# no auto-summary

R2(config-router)# network 172.16.1.0

Une image contenant texte, capture d’écran

Description générée automatiquement

**Routeur R1 :**

R1(config)# interface serial 1/0

R1(config-if)# ip address 200.1.1.1 255.255.255.0

R1(config-if)# clockrate 128000

R1(config-if)# no shutdown

R1(config-if)# interface serial 1/1

R1(config-if)# ip address 200.1.2.1 255.255.255.0

R1(config-if)# clockrate 128000

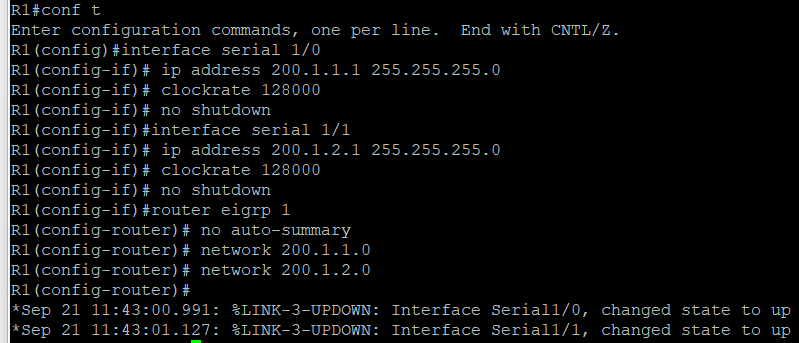
R1(config-if)# no shutdown

R1(config)# router eigrp 1

R1(config-router)# no auto-summary

R1(config-router)# network 200.1.1.0

R1(config-router)# network 200.1.2.0



**Routeur R3 :**

R3(config)# interface loopback 0

R3(config-if)# ip address 10.1.1.1 255.255.255.0

R3(config-if)# no shutdown

R3(config-if)# interface serial 1/1

R3(config-if)# ip address 200.1.2.2 255.255.255.0

R3(config-if)# clockrate 128000

R3(config-if)# no shutdown

R3(config-if)# interface fa0/0

R3(config-if)# ip address 172.16.3.1 255.255.255.0

R3(config-if)# no shutdown

R3(config)# int tunnel0

R3(config-if)# tunnel source serial 1/1

R3(config-if)# tunnel destination  200.1.2.2

R3(config-if)# ip address 172.16.1.2 255.255.255.0

R3(config-if)# no shutdown

R3(config)# router eigrp 1

R3(config-router)# no auto-summary

R3(config-router)# network 200.1.2.0

R3(config-router)# network 172.16.3.0

R3(config-router)# network 10.1.1.0

R3(config)# router eigrp 2

R3(config-router)# no auto-summary

R3(config-router)# network 172.16.1.0Une image contenant texte, capture d’écran

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

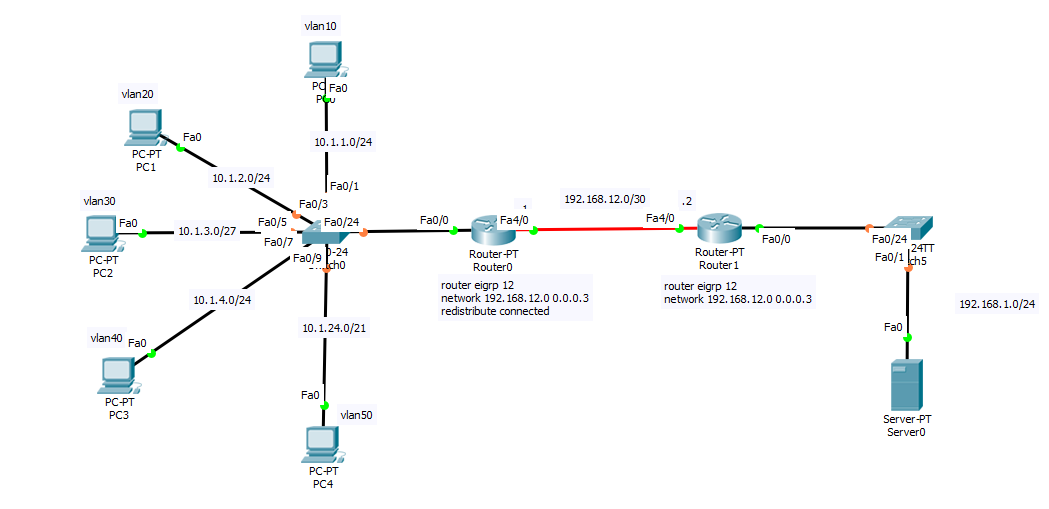
Description générée automatiquement  
Une image contenant capture d’écran, texte, Police

Description générée automatiquement

On peut voir avec toutes ces configurations que le tunnel a bien été mis en place et, grâce au ping et à Wireshark, que les PC arrivent bien à communiquer.

### Énoncé 5 : Redistribution de routes via le protocole EIGRP

Utiliser le fichier : <Bloc2_sem3-4_activite-5-EIGRP-redistribution-debut.pkt>



Lorsque vous utilisez EIGRP comme protocole de routage, vous avez deux options pour filtrer les routes annoncées :

Distribuer des listes ;

Redistribuer - déclaration avec route-map.

Le but de cet exercice est de montrer comment filtrer les routes annoncées sur EIGRP en utilisant différents moyens et méthodes, les méthodes les plus populaires utilisent les commandes

1. **Distribute-list** : Permet de filtrer les routes en utilisant une liste de contrôle d'accès (ACL). Cela contrôle quelles routes sont annoncées ou acceptées.
2. **Redistribute-list** : Similaire à distribute-list, mais utilisé lors de la redistribution de routes entre différents protocoles de routage.
3. **Route-map** : Offre une méthode plus flexible pour filtrer les routes en utilisant des conditions spécifiques. Les route-maps peuvent être associées à des ACL ou des prefix-lists pour un filtrage plus granulaire.

Toutes ces commandes doivent être associées à des ACL ou un prefix-list.

Nous avons deux routeurs R0 et R1 exécutant le processus EIGRP 12.

R0 possède cinq sous-réseaux et redistribue cette connaissance auprès de R1. Quelle est la commande permettant cette redistribution ?

Pour redistribuer les sous-réseaux de R0 vers R1 dans EIGRP, utilisez la commande suivante dans la configuration de R0 : redistribute connected. Cette commande permet à R0 de partager ses routes connectées avec R1, à condition que R1 soit également configuré pour EIGRP.

Faites les recherches permettant au moyen d’une ACL d’annoncer tous les réseaux 10.1.0.0/21. Quelles seraient les commandes que vous utiliseriez avec une Access List 1 ?

Pour annoncer tous les réseaux 10.1.0.0/21 avec une ACL, utilisez les commandes suivantes :

**Créer l'ACL :**

access-list 1 permit 10.1.0.0 0.0.7.255

access-list 1 deny any

**Appliquer l'ACL dans EIGRP :**

router eigrp 12

redistribute connected

network 10.1.0.0 0.0.7.255

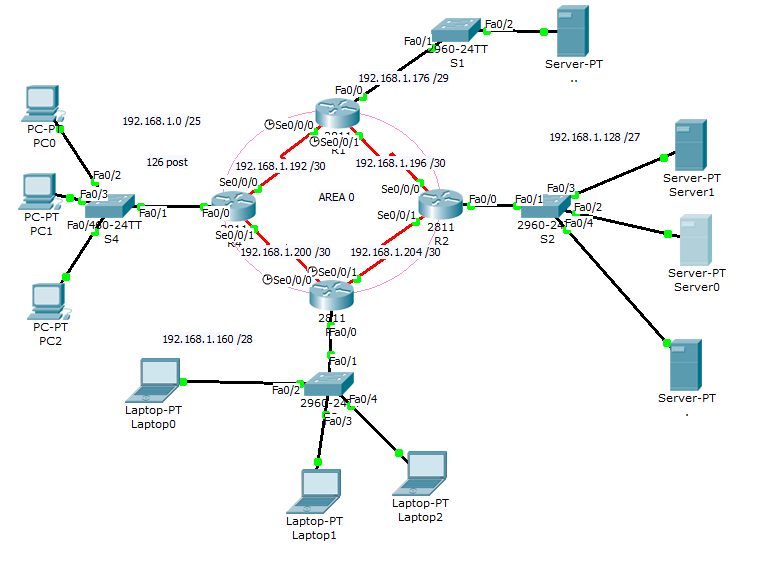
### Énoncé 6 : [Configuration OSPF avec VLSM](http://www.networking-space.com/2011/05/configuration-ospf-avec-vlsm.html)

On utilisera le fichier : <Bloc2_sem3-4_activite-6-OSPF-debut.pkt>

OSPF (Open Shortest Path First) est un protocole de routage à état de liens, son développement est public, ce qui permet de le trouver sur de nombreux systèmes. Ce protocole présente les avantages de converger rapidement et d’être très adaptable. Cependant, il est assez complexe à mettre en œuvre. Il est utilisé dans les réseaux de taille moyenne.

Concepts de zone unique OSPF : OSPF est un protocole à état de liens. Il peut être utilisé et configuré en tant que zone unique pour les petits réseaux. Les grands réseaux OSPF utilisent une conception hiérarchique, plusieurs zones se connectent à une zone de distribution, la zone0, appelée également Backbone.

|  |  |
| --- | --- |
| Avantages : | Désavantages |
| Réduit la charge de routage | Ne supporte que la pile de protocoles TCP/IP |
| Accélère la convergence | Demandes significatives sur la mémoire et le CPU |
| Améliore les performances | Nécessite un administrateur réseau ayant des compétences en routage à état de liens… |



Appliquer les commandes de configuration de l’OSPF suivantes

Configuration d’OSPF :

Routeur 1 :

Router(config)#host R1

R1(config)#int fa 0/0

R1(config-if)#ip add 192.168.1.177 255.255.255.248

R1(config-if)#no sh

R1(config-if)#in se 0/0/0

R1(config-if)#ip add 192.168.1.194 255.255.255.252

R1(config-if)#clo r 64000

R1(config-if)#in se 0/0/1

R1(config-if)#ip add 192.168.1.197 255.255.255.252

R1(config-if)#clo r 64000

R1(config-if)#no sh

R1(config)#router ospf 1

R1(config-router)#net 192.168.1.176 0.0.0.7 area 0

R1(config-router)#net 192.168.1.192 0.0.0.3 area 0

R1(config-router)#net 192.168.1.196 0.0.0.3 area 0

Routeur 2 :

Router(config)#host R2

R2(config)#int fa 0/0

R2(config-if)#ip add 192.168.1.129 255.255.255.224

R2(config-if)#no sh

R2(config-if)#

R2(config-if)#int se 0/0/0

R2(config-if)#ip add 192.168.1.198 255.255.255.252

R2(config-if)#no sh

R2(config)#router ospf 1

R2(config-router)#net 192.168.1.204 0.0.0.3 area 0

R2(config-router)#net 192.168.1.196 0.0.0.3 area 0

R2(config-router)#net 192.168.1.128 0.0.0.31 area 0

Routeur 3 :

Router(config)#host R3

R3(config)#int fa 0/0

R3(config-if)#ip add 192.168.1.161 255.255.255.240

R3(config-if)#no sh

R3(config-if)#in se 0/0/0

R3(config-if)#ip add 192.168.1.202 255.255.255.252

R3(config-if)#clo r 64000

R3(config-if)#no sh

R3(config-if)#in se 0/0/1

R3(config-if)#ip add 192.168.1.206 255.255.255.252

R3(config-if)#clo r 64000

R3(config-if)#no sh

R3(config-if)#exit

R3(config)#router ospf 1

R3(config-router)#net 192.168.1.200 0.0.0.3 area 0

R3(config-router)#

00:44:08: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

R3(config-router)#net 192.168.1.204 0.0.0.3 area 0

R3(config-router)#net 192.168.1.160 0.0.0.15 area 0

00:44:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.198 on Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-router)#end

Routeur 4 :

R4(config)#int fa 0/0

R4(config-if)#ip add 192.168.1.1 255.255.255.128

R4(config-if)# no sh

R4(config-if)#in se 0/0/0

R4(config-if)#ip add 192.168.1.193 255.255.255.252

R4(config-if)#no sh

R4(config-if)#int se 0/0/1

R4(config-if)#ip add 192.168.1.201 255.255.255.252

R4(config-if)#no sh

R4(config-if)#in lo

R4(config-if)#ip add 172.16.1.1 255.255.255.255

R4(config-if)#no sh

R4(config-if)#router ospf 1

R4(config-router)#net 192.168.1.0 0.0.0.127 area 0

R4(config-router)#net 192.168.1.200 0.0.0.3 area 0

R4(config-router)#net 172.16.1.0 0.0.0.0 area 0

Vérifier le bon fonctionnement du réseau et que toutes les interfaces sont bien configurées. Si ce n’est pas le cas faire les modifications nécessaires.

Pour pouvons fair fonctionne le réseau correctement j’ai dû utiliser plusieurs commandes

En premier le routeur 1 n’avais pas son interface Serial0/0/0 qui été activer j’ai donc utilisé les commandes suivantes :

R1(config)#interface Serial0/0/0

R1(config-if)# no shutdown

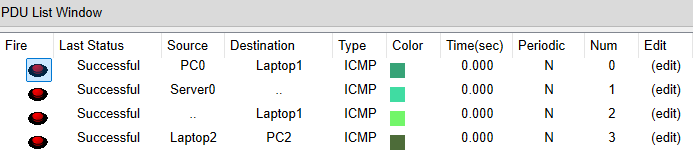
Demême pour le routeur 2 sont interface Serial0/0/1 ne fonctionner pas et elle n’avait pas d’adresse ip.

R2(config)#interface Serial0/0/1

R2(config-if)#ip address 192.168.1.205 255.255.255.252

R2(config-if)#no shutdown

Avec c’est ping j’ai pu confirmer que tout le réseau fonctionner



L’objectif final est de créer un cœur de réseau fortement maillé utilisant le routage OSPF avec une authentification md5 usant du mot de passe CISCO.

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

Description générée automatiquementUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquementUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquementL’authentification permet d’accroître la sécurité des routeurs et en l’occurrence du protocole de routage, en s’assurant que les annonces reçues proviennent de routeurs connus.

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

Description générée automatiquement

Sur chaque routeur, montrez les commandes saisies à l’aide des instructions show running-config et show ip route (affiche la table de routage du routeur).

**Routeur 1 :**

hostname R1

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

--More--

%SYS-5-CONFIG\_I: Configured from console by console

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface FastEthernet0/0

ip address 192.168.1.177 255.255.255.248

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 192.168.1.194 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

clock rate 64000

!

interface Serial0/0/1

ip address 192.168.1.197 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

clock rate 64000

!

interface Serial0/2/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/2/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

network 192.168.1.176 0.0.0.7 area 0

network 192.168.1.192 0.0.0.3 area 0

network 192.168.1.196 0.0.0.3 area 0

!

ip classless

!

ip flow-export version 9

!

!

!

no cdp run

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end

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

Description générée automatiquement

**Routeur 2 :**

R2#show running-config

Building configuration...

Current configuration : 1240 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R2

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface FastEthernet0/0

ip address 192.168.1.129 255.255.255.224

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 192.168.1.198 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

!

interface Serial0/0/1

ip address 192.168.1.205 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

!

interface Serial0/2/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/2/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

network 192.168.1.204 0.0.0.3 area 0

network 192.168.1.196 0.0.0.3 area 0

network 192.168.1.128 0.0.0.31 area 0

!

ip classless

!

ip flow-export version 9

!

!

!

no cdp run

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

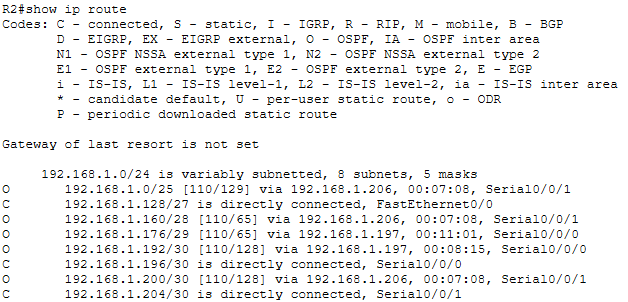
login

!

!

!

end



**Routeur 3 :**

R3#show running-config

Building configuration...

Current configuration : 1276 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname R3

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface FastEthernet0/0

ip address 192.168.1.161 255.255.255.240

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 192.168.1.202 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

clock rate 64000

!

interface Serial0/0/1

ip address 192.168.1.206 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

clock rate 64000

!

interface Serial0/2/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/2/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

network 192.168.1.200 0.0.0.3 area 0

network 192.168.1.204 0.0.0.3 area 0

network 192.168.1.160 0.0.0.15 area 0

!

ip classless

!

ip flow-export version 9

!

!

!

no cdp run

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end

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

Description générée automatiquement

**Routeur 4 :**

Router#show running-config

Building configuration...

Current configuration : 1238 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Router

!

!

!

!

!

!

!

!

ip cef

no ipv6 cef

!

!

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface FastEthernet0/0

ip address 192.168.1.1 255.255.255.128

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Serial0/0/0

ip address 192.168.1.193 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

!

interface Serial0/0/1

ip address 192.168.1.201 255.255.255.252

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 CISCO

!

interface Serial0/2/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/2/1

no ip address

clock rate 2000000

shutdown

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

network 192.168.1.0 0.0.0.127 area 0

network 192.168.1.200 0.0.0.3 area 0

network 172.16.1.0 0.0.0.0 area 0

!

ip classless

!

ip flow-export version 9

!

!

!

no cdp run

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end

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

Description générée automatiquement

Pour vérifier l’authentification, utilisez la commande de débogage debug ip ospf adj.



Montrez les différents évènements associés au protocole OSPF sur un des routeurs. Quelles sont les trames échangées ?

Le protocole OSPF utilise plusieurs types de messages pour établir et maintenir des adjacences entre routeurs et échanger des informations de routage. Les étapes clés incluent l'envoi de paquets Hello pour découvrir les voisins, suivi de paquets Database Description (DBD) pour résumer la base de données de routage. Les routeurs échangent ensuite des Link State Request (LSR) pour demander des informations manquantes, et répondent avec des Link State Update (LSU) contenant les données requises. Après réception des LSU, des accusés de réception (LSAck) sont envoyés pour confirmer la réception. OSPF maintient également l'adjacence par l'envoi régulier de paquets Hello et s'adapte aux changements de topologie en mettant à jour la base de données de routage.

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

Description générée automatiquementUne image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Choisir une des trames constitutives de l’échange préalable et en présenter le contenu en l’analysant.

Analyse de la trame OSPF Hello :

Version : 2  
Cela correspond à la version 2 du protocole OSPF, qui est la version standard utilisée dans les réseaux IPv4.

Type : 1  
Le type de paquet est Hello, utilisé pour découvrir et maintenir la communication entre routeurs voisins.

Packet Length : 48 octets  
Cela représente la taille totale de la trame OSPF Hello, incluant tous les champs du paquet.

Router ID : 192.168.1.198  
L'adresse IP 192.168.1.198 est le Router ID de l'expéditeur du paquet Hello. Le Router ID est un identifiant unique pour chaque routeur dans le processus OSPF.

Area ID : 0.0.0.0  
L'Area ID indique que ce paquet Hello appartient à l'aire OSPF 0, souvent utilisée comme l'aire de backbone dans une topologie OSPF.

Checksum : 0  
Le checksum vérifie l'intégrité des données du paquet. Ici, il semble que le checksum soit calculé comme nul, ce qui peut être dû à la capture en laboratoire ou à une simplification dans l'outil utilisé pour l'analyse.

Auth Type : 2  
Ce champ indique que l'authentification est de type 2, ce qui correspond à une authentification basée sur des mots de passe (en texte clair ou MD5).

Network Mask : 255.255.255.252  
Le masque de sous-réseau utilisé par le routeur est un masque de 30 bits, correspondant à un sous-réseau permettant uniquement deux adresses IP utilisables (généralement dans une liaison point-à-point).

Hello Interval : 10  
Ce champ indique que le routeur envoie des paquets Hello toutes les 10 secondes pour vérifier la disponibilité des voisins.

Router Dead Interval : 40  
Si un routeur ne reçoit pas de paquets Hello de son voisin dans un intervalle de 40 secondes, il considère que le voisin est injoignable.

Options : 0  
Le champ Options peut contenir des informations sur les capacités du routeur (comme la prise en charge de certaines fonctionnalités OSPF), mais ici il est à 0.

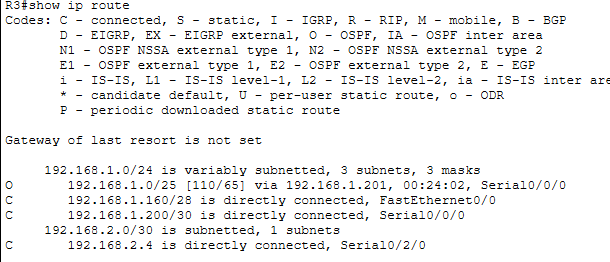
Ce paquet Hello est utilisé pour établir ou maintenir une relation de voisinage entre le routeur R1 (192.168.1.198) et d'autres routeurs connectés au même sous-réseau. Les paramètres comme le Hello Interval et le Router Dead Interval permettent de déterminer la périodicité des échanges et la tolérance aux pannes de communication. Le routeur opère dans l'aire 0, souvent désignée comme l'aire de backbone OSPF, et utilise une authentification de type 2.

Simuler un problème réseau en déconnectant un câble puis montrez les changements de routage à partir des clients à l’aide des commandes tracert ou traceroute ou bien avec la commande show ip route, sur les routeurs.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

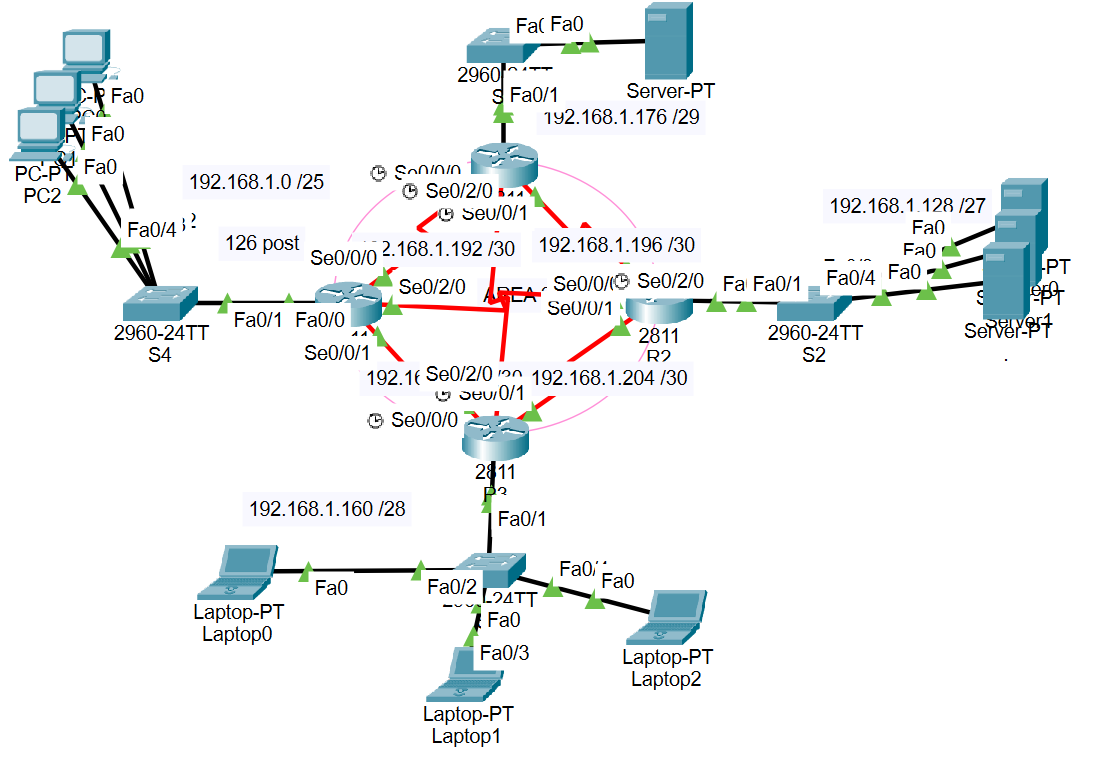
Description générée automatiquement

Grâce à OFPS, même avec une liaison coupée, le protocole parvient à faire en sorte que les trames arrivent à destination en suivant un autre chemin que celui considéré comme le plus court, puisque le chemin n'existe plus.



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

Description générée automatiquement



Présenter vos commandes ayant permis la configuration et montrer que les échanges entre les routeurs sont bien cryptés.

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

Description générée automatiquement

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

Description générée automatiquement

R2(config)#interface Serial0/2/0

R2(config-if)#ip address 192.168.2.1 255.255.255.252

R2(config-if)#ip ospf authentication message-digest

R2(config-if)#ip ospf message-digest-key 1 md5 CISCO

OSPF: Key 1 already exists

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#

R2(config)#router ospf 1

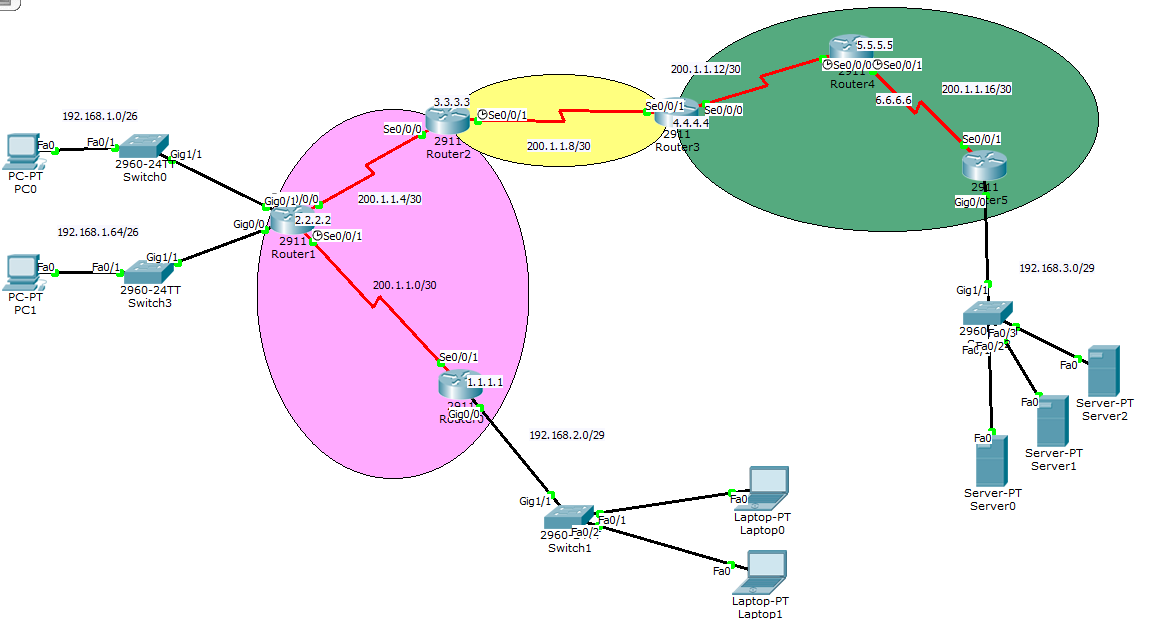
R2(config-router)#network 192.168.2.0 0.0.0.3 area 0

### Énoncé 7 : Configuration OSPF Multi-Area Virtual Link

On utilisera le fichier : <Bloc2_sem3-4_activite-7-ospfmultiarea_debut.pkt>

Objectifs : utiliser les liens virtuels pour connecter plusieurs zones OSPF

Le réseau utilisé sera le suivant :



Configuration des Routeurs :

Routeur 0 :

r0(config)#router ospf 1

r0(config-router)#area 1 virtual-link 3.3.3.3

r0(config-router)#net 200.1.1.0 0.0.0.3 area 1

r0(config-router)#net 192.168.2.0 0.0.0.7 area 1

r0(config-router)#net 1.1.1.1 0.0.0.0 area 1

r0(config-router)#

Routeur 1 :

r1(config)#router ospf 1

r1(config-router)#net 192.168.1.64 0.0.0.63 area 1

r1(config-router)#net 192.168.1.0 0.0.0.63 area 1

r1(config-router)#net 200.1.1.4 0.0.0.3 area 1

r1(config-router)#net 200.1.1.0 0.0.0.3 area 1

r1(config-router)#net 2.2.2.2 0.0.0.0 area 1

Routeur 2 :

R2(config)#router ospf 1

R2(config-router)#area 1 virtual-link 1.1.1.1

R2(config-router)#net 200.1.1.4 0.0.0.3 area 1

R2(config-router)#net 200.1.1. 8 0.0.0.3 area 0

R2(config-router)#net 3.3.3.3 0.0.0.0 area 0

R2(config-router)#exit

Routeur 3 :

r3(config)#router ospf 1

r3(config-router)#area 2 virtual-link 6.6.6.6

r3(config-router)#net 200.1.1.8 0.0.0.3 area 0

r3(config-router)#net 200.1.1.12 0.0.0.3 area 2

r3(config-router)#net 4.4.4.4 0.0.0.0 area 0

r3(config-router)#exit

Routeur 4 :

R4(config)#router ospf 1

R4(config-router)#net 200.1.1.12 0.0.0.3 area 2

R4(config-router)#net 200.1.1.16 0.0.0.3 area 2

R4(config-router)#net 5.5.5.5 0.0.0.0 area 2

R4(config-router)#exit

Routeur 5 :

r5(config)#router ospf 1

r5(config-router)#area 2 vir

r5(config-router)#area 2 virtual-link 4.4.4.4

r5(config-router)#net 200.1.1.16 0.0.0.3 area 2

r5(config-router)#net 6.6.6.6 0.0.0.0 area 2

r5(config-router)#net 192.168.3.0 0.0.0.7 area 2

r5(config-router)#

Il manque les adresse IP sur tous les routeurs et laptops je les ses donc rajouter.

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

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquementPour les laptops j’ai modifié la default Gateway car elle été en 192.168.2.7 qui est l’adresse de diffusion je les donc passer en 192.168.2.6 qui est la dernière adresse se IP utilisable.

De plus dans la configuration donner les virual link ne sont pas les bonnes pour chaque routeur j’ai donc modifier également cette partie.



Donner les tables de routage des différents routeurs et fournir une explication détaillée de la table de routage de R5.

r5#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/26 is subnetted, 1 subnets

S 192.168.1.0/26 [1/0] via 200.1.1.17

192.168.2.0/29 is subnetted, 1 subnets

S 192.168.2.0/29 [1/0] via 200.1.1.17

192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.3.0/29 is directly connected, GigabitEthernet0/0

L 192.168.3.6/32 is directly connected, GigabitEthernet0/0

200.1.1.0/24 is variably subnetted, 3 subnets, 2 masks

O 200.1.1.12/30 [110/128] via 200.1.1.17, 00:02:02, Serial0/0/1

C 200.1.1.16/30 is directly connected, Serial0/0/1

L 200.1.1.18/32 is directly connected, Serial0/0/1

Explication détaillée de la table de routage de Router5 (R5) :

1. Routes statiques :

192.168.1.0/26 et 192.168.2.0/29 sont des routes statiques configurées manuellement. Ces routes statiques permettent à Router5 d'envoyer du trafic vers les réseaux 192.168.1.0/26 (probablement connectés à Router3) et 192.168.2.0/29 via 200.1.1.17 (le next-hop qui correspond à l'interface de Router3). La distance administrative par défaut pour les routes statiques est de 1, ce qui signifie qu'elles seront préférées par rapport à d'autres types de routes, sauf les routes directement connectées.

2. Routes directement connectées :

192.168.3.0/29 est directement connecté à l'interface GigabitEthernet0/0 de Router5. Ce réseau est local pour Router5, et il peut donc envoyer le trafic directement vers les hôtes de ce sous-réseau sans passer par un autre routeur.

200.1.1.16/30 est également directement connecté à l'interface Serial0/0/1 de Router5. Ce sous-réseau est utilisé pour interconnecter Router5 et Router3, ce qui permet de transporter le trafic entre les deux routeurs.

3. Routes OSPF :

200.1.1.12/30 est une route apprise via OSPF (Open Shortest Path First), avec une distance administrative de 110 et un coût de 128. Cette route permet à Router5 de rejoindre un réseau de transit entre Router3 et un autre routeur via l'adresse 200.1.1.17. Cela montre que OSPF est actif sur Router5 et qu'il peut propager et apprendre des routes dynamiques à travers le réseau.

4. Routes locales :

192.168.3.6/32 et 200.1.1.18/32 sont des adresses IP locales directement assignées aux interfaces de Router5. Ces routes locales indiquent que ces adresses sont directement associées à l'interface concernée et ne nécessitent pas de routage supplémentaire.

Montrer que votre réseau est en état de fonctionner

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

Description générée automatiquement

Une image contenant capture d’écran, texte, Police

Description générée automatiquement

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

Description générée automatiquement

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

Description générée automatiquement

### Énoncé 8  : [Modification du coût OSPF](http://www.networking-space.com/2011/05/global-knowledge-11.html) et élection du routeur DR et du routeur BDR

Document : <Bloc2_sem3-4_activite-8_DR.pkt>

DR/BDR et la Métrique OSPF

DR et BDR en OSPF

• DR (Designated Router) et BDR (Backup Designated Router) sont élus dans les réseaux multiaccès (comme Ethernet) pour faciliter l'échange des informations de routage.

• Élection basée sur :

- Priorité d'interface (modifiable avec ip ospf priority).

- Si priorité égale, l'adresse IP la plus élevée est choisie.

Métrique OSPF (Coût)

• OSPF utilise le coût pour choisir le meilleur chemin. Le coût est calculé par :

Coût = 10^8 / Bande passante (kbps)

• Plus le coût est bas, meilleur est le chemin.

Modification du Coût

• Commande bandwidth : Modifie la bande passante d'une interface.

Exemple : R1(config-if)# bandwidth 10000 # 10 Mbps

• Commande ip ospf cost : Spécifie directement le coût OSPF.

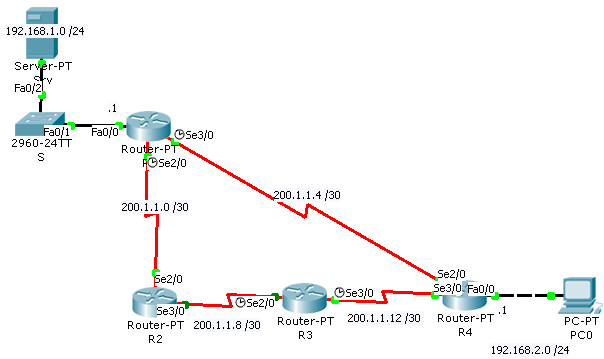
Exemple : R1(config-if)# ip ospf cost 1562

Ajustement Global de la Bande Passante de Référence

• La commande auto-cost reference-bandwidth permet de modifier la bande passante de référence (par défaut 100 Mbps).

Exemple : R1(config-router)# auto-cost reference-bandwidth 1000 # 1 Gbps

Topographie à réaliser



Configuration

Routeur 1

Router(config)#host R1

R1(config)#int fa 0/0

R1(config-if)#ip add 192.168.1.1 255.255.255.0

R1(config-if)#no sh

R1(config-if)#int se 2/0

R1(config-if)#ip add 200.1.1.1 255.255.255.252

R1(config-if)#bandwidth 1000000

R1(config-if)#clo r 64000

R1(config-if)#no sh

R1(config-if)#int se 3/0

R1(config-if)#ip add 200.1.1.5 255.255.255.252

R1(config-if)#clo r 64000

R1(config-if)#no sh

R1(config-if)#

R1(config-if)#router ospf 1

R1(config-router)#net 192.168.1.0 0.0.0.255 area 0

R1(config-router)#net 200.1.1.0 0.0.0.3 area 0

R1(config-router)#net 200.1.1.4 0.0.0.3 area 0

Routeur 2

Router(config)#host R2

R2(config)#int se 2/0

R2(config-if)#ip add 200.1.1.2 255.255.255.252

R2(config-if)#bandwidth 1000000

R2(config-if)#no sh

R2(config-if)#int se 3/0

R2(config-if)#ip add 200.1.1.10 255.255.255.252

R2(config-if)#bandwidth 1000000

R2(config-if)#no sh

R2(config-if)#exit

R2(config)#router ospf 1

R2(config-router)#net 200.1.1.0 0.0.0.3 area 0

00:12:57: %OSPF-5-ADJCHG: Process 1, Nbr 200.1.1.5 on Serial2/0 from LOADING to FULL, Loading Done

R2(config-router)#net 200.1.1.8 0.0.0.3 area 0

Routeur 3

Router(config)#host R3

R3(config)#int se 2/0

R3(config-if)#ip add 200.1.1.9 255.255.255.252

R3(config-if)#bandwidth 1000000

R3(config-if)#clo r 64000

R3(config-if)#no sh

R3(config-if)#int se 3/0

R3(config-if)#ip add 200.1.1.13 255.255.255.252

R3(config-if)#bandwidth 1000000

R3(config-if)#clo r 64000

R3(config-if)#no sh

R3(config)#router ospf 1

R3(config-router)#net 200.1.1.8 0.0.0.3 area 0

R3(config-router)#net 200.1.1.12 0.0.0.3 area 0

Routeur4

Router(config)#host R4

R4(config)#int se 3/0

R4(config-if)#ip add 200.1.1.14 255.255.255.252

R4(config-if)#bandwidth 1000000

R4(config-if)#no sh

R4(config-if)#int se 2/0

R4(config-if)#ip add 200.1.1.6 255.255.255.252

R4(config-if)#no sh

R4(config-if)#int fa 0/0

R4(config-if)#ip add 192.168.2.1 255.255.255.0

R4(config-if)#no sh

R4(config)#router ospf 1

R4(config-router)#net 192.168.2.0 0.0.0.255 area 0

R4(config-router)#net 200.1.1.12 0.0.0.3 area 0

R4(config-router)#net 200.1.1.4 0.0.0.3 area 0

00:22:05: %OSPF-5-ADJCHG : Process 1, Nbr 200.1.1.13 on Serial3/0 from LOADING to FULL, Loading Done

Concevoir le réseau, montrer dans une première phase.

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

Description générée automatiquement

Il faut bien penser à utiliser des câble serial DCE et pas des DTE

Quel est le routeur DR ? Les commandes show· ip ospf neighbor detail ou show ip ospf neighbor permettent de voir le résultat de l’élection.

R1#show ip ospf neighbor detail

Neighbor 200.1.1.14, interface address 200.1.1.6

In the area 0 via interface Serial3/0

Neighbor priority is 0, State is FULL, 7 state changes

DR is 0.0.0.0 BDR is 0.0.0.0

Options is 0x00

Dead timer due in 00:00:35

Neighbor is up for 00:08:35

Index 1/1, retransmission queue length 0, number of retransmission 0

First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)

Last retransmission scan length is 0, maximum is 0

Last retransmission scan time is 0 msec, maximum is 0 msec

R2#show ip ospf neighbor detail

R2#

R3#show ip ospf neighbor detail

Neighbor 200.1.1.14, interface address 200.1.1.14

In the area 0 via interface Serial3/0

Neighbor priority is 0, State is FULL, 7 state changes

DR is 0.0.0.0 BDR is 0.0.0.0

Options is 0x00

Dead timer due in 00:00:33

Neighbor is up for 00:09:16

Index 1/1, retransmission queue length 0, number of retransmission 0

First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)

Last retransmission scan length is 0, maximum is 0

Last retransmission scan time is 0 msec, maximum is 0 msec

R4#show ip ospf neighbor detail

Neighbor 200.1.1.5, interface address 200.1.1.5

In the area 0 via interface Serial2/0

Neighbor priority is 2, State is FULL, 6 state changes

DR is 0.0.0.0 BDR is 0.0.0.0

Options is 0x00

Dead timer due in 00:00:31

Neighbor is up for 00:09:38

Index 1/1, retransmission queue length 0, number of retransmission 0

First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)

Last retransmission scan length is 0, maximum is 1

Last retransmission scan time is 0 msec, maximum is 0 msec

Neighbor 200.1.1.13, interface address 200.1.1.13

In the area 0 via interface Serial3/0

Neighbor priority is 0, State is FULL, 6 state changes

DR is 0.0.0.0 BDR is 0.0.0.0

Options is 0x00

Dead timer due in 00:00:32

Neighbor is up for 00:09:37

Index 2/2, retransmission queue length 0, number of retransmission 0

First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)

Last retransmission scan length is 0, maximum is 1

Last retransmission scan time is 0 msec, maximum is 0 msec

Dans les informations affichées, il est mentionné que pour tous les routeurs dans la topologie, les adresses du DR (Designated Router) et du BDR (Backup Designated Router) sont toutes deux à 0.0.0.0. Cela indique qu'il n'y a pas de DR ou de BDR élus sur ces segments spécifiques.

Cela peut arriver dans des réseaux point-à-point ou dans des interfaces avec priorité définie à 0 pour OSPF. Dans ce cas, il n'y a pas d'élection de DR ou de BDR, et les routeurs fonctionnent en mode point-à-point ou dans un environnement où cette fonctionnalité n'est pas nécessaire.

Avant toute modification du coût quelle est la route prise par les trames de PC0 vers Srv. Puis dans un second temps modifier le coût afin de faire transiter les trames par l’autre chemin possible.

Avant la motivation des couts le PC0 passer par 2 routeurs avant d’arriver au serveur

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Après la modification des couts pour passer de l’autre cotter il y a aussi deux routeurs

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

Description générée automatiquement

Pour vérifier la redondance, j'ai donc désactivé une interface afin de m'assurer qu'elle passe de l'autre côté. On peut voir sur la capture d’écran que cela a bien marcher.

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

Description générée automatiquement

Après modification des coûts y-a-t-il des modifications dans l’élection du routeur DR ?

La modification des coûts OSPF n'affecte pas l'élection du DR/BDR. L'élection du DR dépend uniquement de la priorité OSPF et de l'adresse IP la plus élevée en cas d'égalité de priorité. Si tu souhaites influencer l'élection du DR, tu dois modifier la priorité OSPF de l'interface concernée, mais pas le coût.

Il est possible de forcer l’élection en utilisant la commande d’interface ip ospf priority Priorité. Par exemple : ip ospf priority 2

On peut forcer l'élection du DR/BDR en utilisant la commande ip ospf priority [valeur] sur une interface. Le routeur avec la priorité la plus élevée devient le DR, et le second devient le BDR. Une priorité de 0 exclut un routeur de l'élection.

La priorité par défaut est 1, une priorité de 0 annule la participation du routeur à l’élection.

Choisissez le routeur que vous voulez élire comme racine et forcer l’élection.

Justifiez votre choix et montrer que cela a bien eu lieu.

Pour forcer l'élection d'un routeur comme DR (Designated Router) dans OSPF, il faut modifier la priorité des routeurs. Par défaut, la priorité est 1, et une priorité de 0 annule la participation du routeur à l'élection.

Je choisis R4 comme routeur désigné (DR). La raison de ce choix est que R4 a déjà une priorité de 2, ce qui est plus élevé que les autres routeurs, et il est bien positionné dans la topologie pour centraliser les mises à jour OSPF.

R4(config)# interface Serial2/0

R4(config-if)# ip ospf priority 200

R3(config)# interface Serial3/0

R3(config-if)# ip ospf priority 1

R2(config)# interface Serial3/0

R2(config-if)# ip ospf priority 1

R1(config)# interface Serial3/0

R1(config-if)# ip ospf priority 1

J'ai essayé de forcer R4 à être DR, mais c'est impossible, même en supprimant toutes les tables OSPF plusieurs fois sur tous les routeurs. Voici ce qu'il m'affiche : le routeur veut bien faire ce que je lui dis, il passe soit par le haut, soit par le bas, mais il est impossible de le faire devenir DR.

R4#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface

200.1.1.5 0 2WAY/DROTHER 00:00:36 200.1.1.5 Serial2/0

200.1.1.13 0 FULL/ - 00:00:31 200.1.1.13 Serial3/0

R1#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface

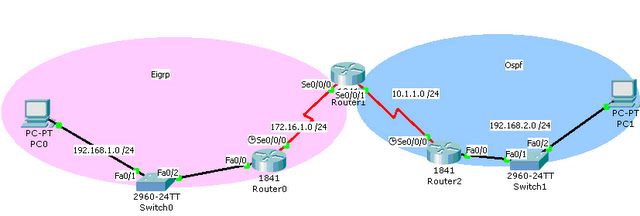
200.1.1.10 0 FULL/ - 00:00:33 200.1.1.2 Serial2/0

200.1.1.14 0 EXSTART/ - 00:00:34 200.1.1.6 Serial3/0

### Énoncé 9 : [Redistribution des routes entre EIGRP et OSPF](http://www.networking-space.com/2011/04/redistribution-des-routes-entre-eigrp.html)

On utilisera le fichier : <Bloc2_sem3-4_activite-9-Redistribution-des-routes-entre-EIGRP-et-OSPF.pkt>

Le principe de la redistribution de route consiste à collecter les informations relatives aux routes apprises via un protocole de routage et à les injecter dans un autre domaine de routage. Les routes statiques ou connectées peuvent aussi être redistribuées. Lorsqu’un routeur OSPF utilise des routes apprises via un autre protocole de routage et les rend disponibles pour les autres routeurs OSPF avec lesquels il est en communication, ce routeur devient un Autonome System Border Gateway.



Nous allons faire en sorte que le routeur ROUTER1 soit capable de redistribuer dans la zone EIGRP les routes apprises avec OSPF. Pour cela, dans la configuration du protocole EIGRP, vous allez utiliser la commande (config-router)# redistribute ospf 1 metric 10000 100 255 1 1500

Voilà comment configurer la redistribution sur le réseau :

Routeur 0

interface FastEthernet0/0

ip address 192.168.1.1 255.255.255.0

!

interface Serial0/0/0

ip address 172.16.1.1 255.255.255.0

clock rate 64000

!

router eigrp 100

network 192.168.1.0

network 172.16.1.0 0.0.0.255

auto-summary

Routeur 1

interface Serial0/0/0

ip address 172.16.1.2 255.255.255.0

!

interface Serial0/0/1

ip address 10.1.1.1 255.255.255.0

!

router eigrp 100

redistribute ospf 1 metric 10000 100 255 1 1500

network 172.16.1.0 0.0.0.255

auto-summary

!

router ospf 1

log-adjacency-changes

redistribute eigrp 100 subnets

network 10.1.1.0 0.0.0.255 area 0

Routeur 2

interface FastEthernet0/0

ip address 192.168.2.1 255.255.255.0

!

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.0

clock rate 64000

!

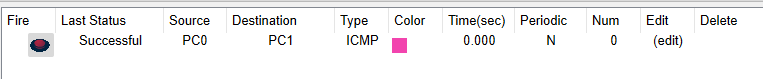
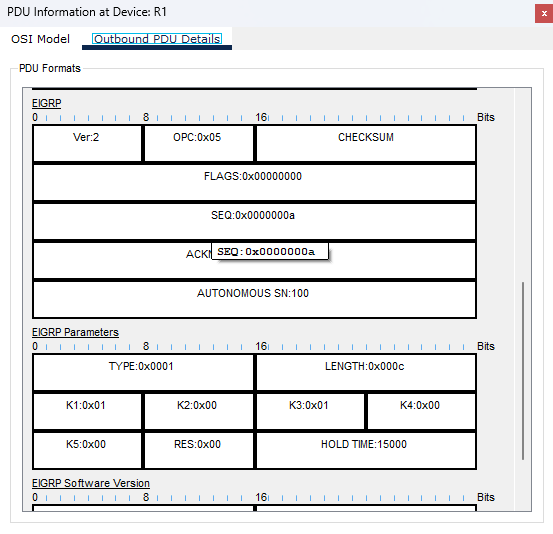
router ospf 1

log-adjacency-changes

network 10.1.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0





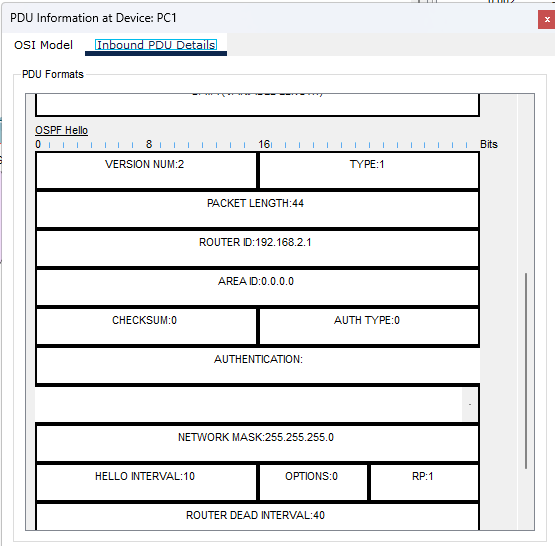


Image 1 :

On observe des échanges de paquets sur plusieurs appareils avec OSPF et EIGRP. Les routeurs R2, Switch1, et PC1 communiquent via OSPF, tandis que les routeurs R1 et R0 échangent des informations via EIGRP. Les délais minimums pour ces échanges sont affichés, montrant la réactivité des routeurs.

Image 2 :

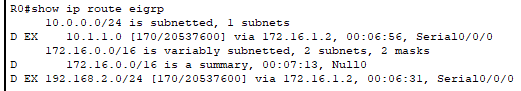
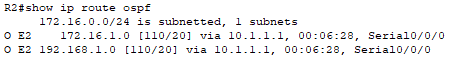
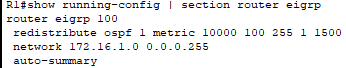
Un paquet OSPF Hello est envoyé par Router2 à PC1. Ce paquet fait partie du processus d’établissement et de maintien de la relation OSPF dans l'Area 0. Le Router ID est 192.168.2.1, avec un intervalle de Hello de 10 secondes et un Router Dead Interval de 40 secondes.

Image 3 :

Un paquet EIGRP de type ACK est envoyé par Router1. Ce paquet appartient à l’AS 100 avec des paramètres K-values configurés pour que la bande passante et le délai soient utilisés dans le calcul des métriques.

Les capture d’écran montrent des communications simultanées sur un réseau utilisant OSPF et EIGRP. OSPF est utilisé pour maintenir des adjacences, tandis qu’EIGRP gère la distribution des routes dans l'AS 100, avec une bonne gestion des métriques.

Montrer à l’aide de commandes pertinentes que vous permettez la redistribution des routes.



Router1 OSPF Configuration : La redistribution des routes EIGRP dans OSPF est configurée avec la commande redistribute eigrp 100 subnets.

Router1 EIGRP Configuration : La redistribution des routes OSPF dans EIGRP est configurée avec la commande redistribute ospf 1 metric 10000 100 255 1 1500, définissant les métriques spécifiques pour EIGRP.

Table de routage EIGRP sur Router1 : Le réseau 192.168.1.0/24 est appris via EIGRP, ce qui confirme que la redistribution fonctionne.

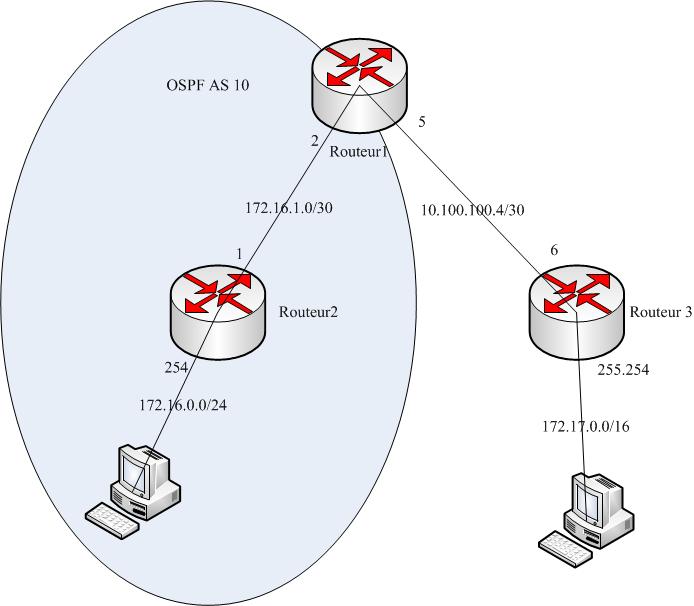
Table de routage OSPF sur Router1 : Le réseau 192.168.2.0/24 est appris via OSPF, ce qui prouve que la redistribution des routes EIGRP dans OSPF est active.

Table de routage OSPF sur Router2 : Router2 apprend correctement les réseaux EIGRP via OSPF, confirmant que la redistribution fonctionne bien.

Table de routage EIGRP sur Router0 : Router0 a appris des routes OSPF via EIGRP, prouvant la redistribution bidirectionnelle entre OSPF et EIGRP.

### Énoncé 10 : Redistribution de route statique

Document : <Bloc2_sem3-4_activite-10-Redistribution_de_route_statique.pkt>

Sur des réseaux de taille importante, plusieurs systèmes de routage peuvent cohabiter, cependant, ils ne partagent pas directement leurs informations de routage (à part EIGRP et IGRP). En conséquence, il est possible de configurer les routeurs pour qu’ils redistribuent leurs routes dans d’autres protocoles de routage.

Après avoir mis en place l’atelier, assurez-vous que chaque périphérique communique avec son ou ses voisins proches.

Mettez en place le protocole de routage OSPF sur les routeurs 1 et 2, configurez le routage statique sur les routeurs 1 et 3, activez la redistribution de route puis montrez que l’ordinateur 1 communique avec l’ordinateur 2.

Router(config)#hostname R0

interface GigabitEthernet0/1

ip address 172.16.0.254 255.255.255.0

no shutdown

interface GigabitEthernet0/0

ip address 172.16.1.1 255.255.255.252

no shutdown

router ospf 10

network 172.16.0.0 0.0.0.255 area 0

network 172.16.1.0 0.0.0.3 area 0

end

write memory

Router(config)#hostname R1

interface GigabitEthernet0/0

ip address 172.16.1.2 255.255.255.252

no shutdown

interface GigabitEthernet0/1

ip address 10.100.100.5 255.255.255.252

no shutdown

router ospf 10

network 172.16.1.0 0.0.0.3 area 0

redistribute static subnets

ip route 172.17.0.0 255.255.0.0 10.100.100.6

end

write memory

Router(config)#hostname R3

R3(config)#ip route 172.16.0.0 255.255.255.0 10.100.100.5

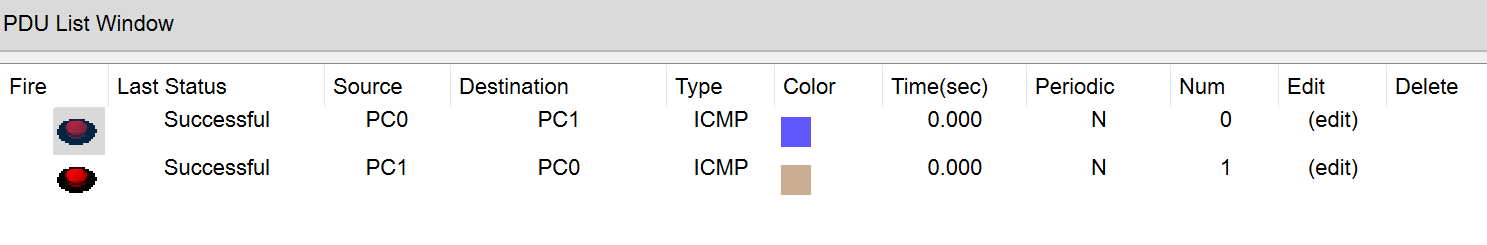
R3(config)#

R3(config)#

R3(config)#interface GigabitEthernet0/0

R3(config-if)#no shutdown

Montrez à l’aide de commandes pertinentes que la redistribution de routes se fait bien

****

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

Description générée automatiquement**

### Énoncé 11 : OSPF et la redondance via HSRP

#### Objectifs

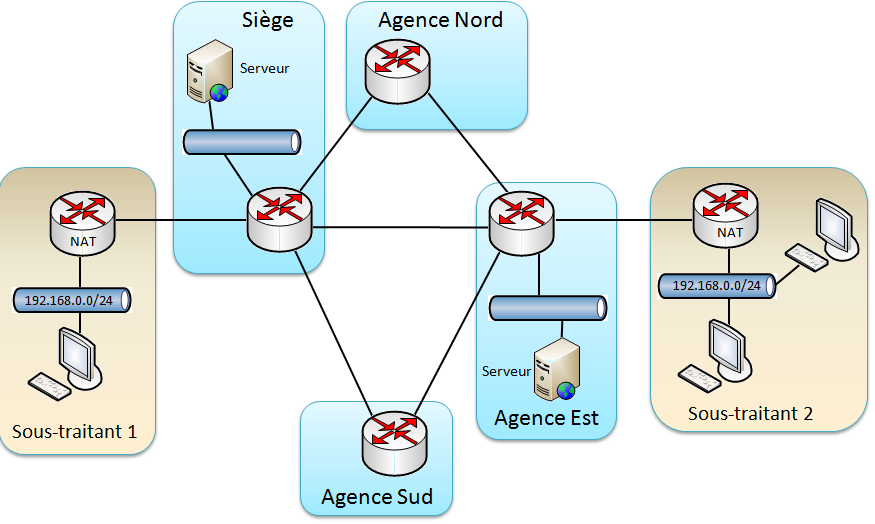
Mettre en place du routage dynamique au sein d’un réseau de routeurs de liaison connectés à deux sites distants de sous-traitants, avec le protocole OSPF. Les sites distants utilisent un même plan d’adressage en 192.168.0.0/24.

Sur un des sites terminaux, mettre en place une redondance de routeurs, permettant une tolérance de panne, avec le protocole HSRP.

A noter qu’il ne s’agit ici que d’un cas d’école permettant de mettre en œuvre les protocoles OSPF et HSRP et que chacun de ces protocoles peut être implémenté indépendamment.

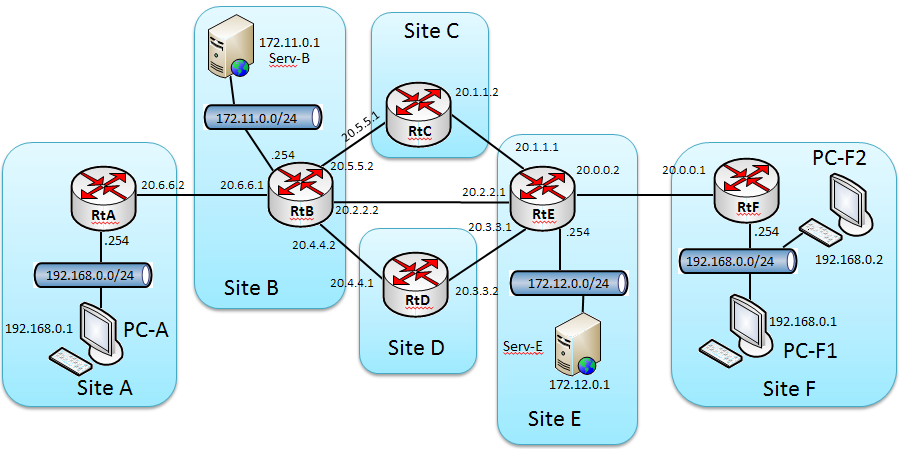
#### Situation de départ

Une entreprise comprend quatre sites - un siège et trois agences régionales - reliés les uns aux autres. Deux sous-traitants accèdent à ce réseau en mode NAT. Ces sous-traitants peuvent accéder à des ressources présentes sur les sites de l’entreprise.



Par la suite, pour des raisons pédagogiques, les deux sites des sous-traitants et les quatre sites de l’entreprise ci-dessus seront nommés de gauche à droite par les lettres A, B, C, D, E, F.

Le service NAT et la route par défaut sont configurés sur les deux routeurs des sites terminaux des sous-traitants.



#### Tableau des réseaux de connexion entre routeurs

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Du routeur vers le routeur | RtA | RtB | RtC | RtD | RtE | RtF |
| RtA | - | 20.6.6.0/30 | - | - | - | - |
| RtB | 20.6.6.0/30 | - | 20.5.5.0/30 | 20.4.4.0/30 | 20.2.2.0/30 | - |
| RtC | - | 20.5.5.0/30 | - | - | 20.1.1.0/30 | - |
| RtD | - | 20.4.4.0/30 | - | - | 20.3.3.0/30 | - |
| RtE | - | 20.2.2.0/30 | 20.1.1.0/30 | 20.3.3.0/30 | - | 20.0.0.0/30 |
| RtF | - | - | - | - | 20.0.0.0/30 | - |

#### Plan d’adressage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Périphérique | Interface | Adresse IP | Masque de sous-réseau | Passerelle par défaut |
| Router A | Fa0/1 | 192.168.0.254 | 255.255.255.0 | N/A |
| S0/0/0 | 20.6.6.2 | 255.255.255.252 | N/A |
| Router B | Gi0/1 | 172.11.0.254 | 255.255.255.0 | N/A |
| S0/0/0 | 20.6.6.1 | 255.255.255.252 | N/A |
| S0/0/1 | 20.5.5.2 | 255.255.255.252 | N/A |
| S0/1/0 | 20.4.4.2 | 255.255.255.252 | N/A |
| S0/1/1 | 20.2.2.2 | 255.255.255.252 | N/A |
| Router C | S0/0/0 | 20.1.1.2 | 255.255.255.252 | N/A |
| S0/0/1 | 20.5.5.1 | 255.255.255.252 | N/A |
| Router D | S0/0/0 | Partie 4 | 255.255.255.252 | N/A |
| S0/0/1 | 20.3.3.2 | 255.255.255.252 | N/A |
| S0/1/0 | 20.4.4.1 | 255.255.255.252 | N/A |
| Router E | Gi0/1 | 172.12.0.254 | 255.255.255.0 | N/A |
| S0/0/0 | 20.0.0.2 | 255.255.255.252 | N/A |
| S0/0/1 | 20.3.3.1 | 255.255.255.252 | N/A |
| S0/1/0 | 20.1.1.1 | 255.255.255.252 | N/A |
| S0/1/1 | 20.2.2.1 | 255.255.255.252 | N/A |
| Router F | Fa0/0 | 192.168.0.254 | 255.255.255.0 | N/A |
| S0/0/0 | 20.0.0.1 | 255.255.255.252 | N/A |

Mise en place du routage OSPF

Ressource : fiche technique OSPF en annexe 1.

Première étape : vérifications

On utilisera le fichier : <Bloc2_sem3-4_activite-11-Decouverte-OSPF-HSRP-1-Depart.pka>

Vérifier la connectivité des postes vers leur passerelle et la connectivité de chaque routeur avec son – ou ses – voisin(s). Vérifier également l’absence de connectivité dès lors qu’il s’agit de traverser les routeurs de liaison.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

On peut voir que les PC on bien put communique avec leur passerait par défaut.

Une image contenant texte, logiciel, Icône d’ordinateur, nombre

Description générée automatiquement

On peut également voir que les routeurs arrives a communique entre eux donc la configuration est correcte.

Vérifier le fonctionnement du service NAT sur les routeurs terminaux.

Routeur-A#show ip nat statistics

Total translations: 0 (0 static, 0 dynamic, 0 extended)

Outside Interfaces: Serial0/0/0

Inside Interfaces: FastEthernet0/1

Hits: 1 Misses: 12

Expired translations: 2

Dynamic mappings:

Routeur-A#

Routeur-F#show ip nat statistics

Total translations: 0 (0 static, 0 dynamic, 0 extended)

Outside Interfaces: Serial0/0/0

Inside Interfaces: FastEthernet0/0

Hits: 1 Misses: 3

Expired translations: 1

Dynamic mappings:

Routeur-F#

Il y a eu une bonne traduction NAT (un hit) sur chaque routeur, ce qui signifie qu'au moins un paquet a été correctement traduit et transmis. Cependant, cela reste très limité par rapport au nombre de paquets échoués. Donc oui le NAT fonctionne.

Deuxième étape : routage dynamique

Mettre en place le routage OSPF sur les routeurs de liaison.

RA :

router ospf 1

log-adjacency-changes

network 192.168.0.0 0.0.0.255 area 0

network 20.6.6.0 0.0.0.3 area 0

RB :

router ospf 1

log-adjacency-changes

network 20.6.6.0 0.0.0.3 area 0

network 20.5.5.0 0.0.0.3 area 0

network 20.4.4.0 0.0.0.3 area 0

network 172.11.0.0 0.0.0.255 area 0

network 20.2.2.0 0.0.0.3 area 0

RC :

router ospf 1

log-adjacency-changes

network 20.5.5.0 0.0.0.3 area 0

network 20.1.1.0 0.0.0.3 area 0

RD :

router ospf 1

log-adjacency-changes

network 20.4.4.0 0.0.0.3 area 0

network 20.3.3.0 0.0.0.3 area 0

RE :

router ospf 1

log-adjacency-changes

network 20.3.3.0 0.0.0.3 area 0

network 20.1.1.0 0.0.0.3 area 0

network 20.0.0.0 0.0.0.3 area 0

network 172.12.0.0 0.0.0.255 area 0

network 20.2.2.0 0.0.0.3 area 0

Mettre en place une batterie de tests et de « preuves » de fonctionnement du routage.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Tous ces tests montrent que le routage fonctionne bien, car s'il ne fonctionnait pas, il y aurait des problèmes de communication entre les différents appareils, ce qui n'est pas le cas ici.

Troisième étape : mode dégradé

Vous allez démontrer le fonctionnement du routage dynamique en mode dégradé, c’est-à-dire en modifiant l’état de l’infrastructure amenant le protocole à changer de route pour faire aboutir une requête.

Routeur-B(config)#interface Serial0/1/0

Routeur-B(config-if)#shutdown

Montrer les effets d’une rupture de lien sur le fonctionnement du protocole OSPF.

Routeur-B#show ip route

Gateway of last resort is not set

20.0.0.0/8 is variably subnetted, 9 subnets, 2 masks

O 20.0.0.0/30 [110/128] via 20.2.2.1, 00:48:04, Serial0/1/1

O 20.1.1.0/30 [110/128] via 20.2.2.1, 00:48:04, Serial0/1/1

[110/128] via 20.5.5.1, 00:48:04, Serial0/0/1

C 20.2.2.0/30 is directly connected, Serial0/1/1

L 20.2.2.2/32 is directly connected, Serial0/1/1

O 20.3.3.0/30 [110/128] via 20.2.2.1, 00:21:52, Serial0/1/1

C 20.5.5.0/30 is directly connected, Serial0/0/1

L 20.5.5.2/32 is directly connected, Serial0/0/1

C 20.6.6.0/30 is directly connected, Serial0/0/0

L 20.6.6.1/32 is directly connected, Serial0/0/0

172.11.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.11.0.0/24 is directly connected, GigabitEthernet0/1

L 172.11.0.254/32 is directly connected, GigabitEthernet0/1

172.12.0.0/24 is subnetted, 1 subnets

O 172.12.0.0/24 [110/65] via 20.2.2.1, 00:48:04, Serial0/1/1

O 192.168.0.0/24 [110/129] via 20.2.2.1, 00:17:29, Serial0/1/1

Routeur-B#show ip route

Gateway of last resort is not set

20.0.0.0/8 is variably subnetted, 11 subnets, 2 masks

O 20.0.0.0/30 [110/128] via 20.2.2.1, 00:48:37, Serial0/1/1

O 20.1.1.0/30 [110/128] via 20.2.2.1, 00:48:37, Serial0/1/1

[110/128] via 20.5.5.1, 00:48:37, Serial0/0/1

C 20.2.2.0/30 is directly connected, Serial0/1/1

L 20.2.2.2/32 is directly connected, Serial0/1/1

O 20.3.3.0/30 [110/128] via 20.2.2.1, 00:22:25, Serial0/1/1

C 20.4.4.0/30 is directly connected, Serial0/1/0

L 20.4.4.2/32 is directly connected, Serial0/1/0

C 20.5.5.0/30 is directly connected, Serial0/0/1

L 20.5.5.2/32 is directly connected, Serial0/0/1

C 20.6.6.0/30 is directly connected, Serial0/0/0

L 20.6.6.1/32 is directly connected, Serial0/0/0

172.11.0.0/16 is variably subnetted, 2 subnets, 2 masks

--More--

00:49:03: %OSPF-5-ADJCHG: Process 1, Nbr 20.4.4.1 on Serial0/1/0 from LOADING to FULL, Loading Done

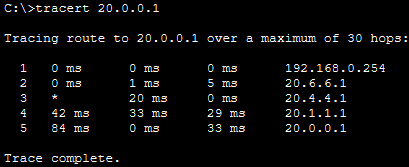
C 172.11.0.0/24 is directly connected, GigabitEthernet0/1

L 172.11.0.254/32 is directly connected, GigabitEthernet0/1

172.12.0.0/24 is subnetted, 1 subnets

O 172.12.0.0/24 [110/65] via 20.2.2.1, 00:48:37, Serial0/1/1

O 192.168.0.0/24 [110/129] via 20.2.2.1, 00:18:02, Serial0/1/1

La principale différence entre les deux tables de routage c’est que le réseau 20.4.4.0/30 n’est plus la donc le routeur choisisse de prendre un autre chemin ce qui montre que le routage OSPF s'est ajusté en fonction de l'état des liens.

Une image contenant texte, capture d’écran, Police

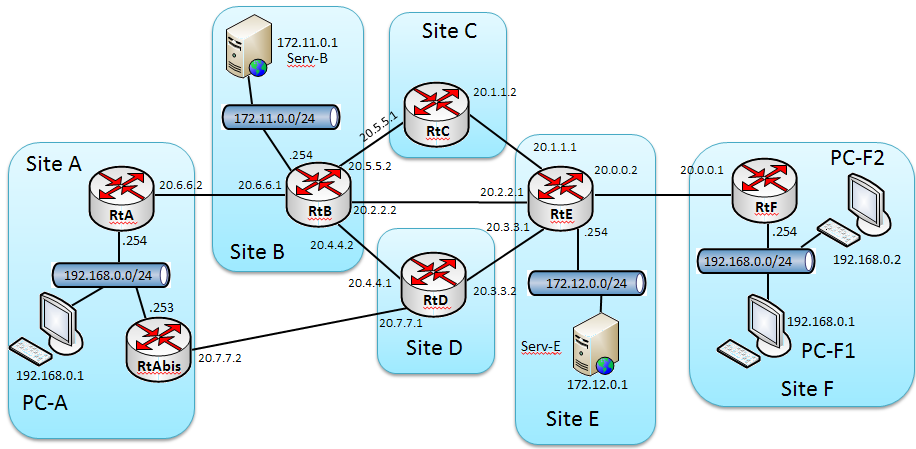
Description générée automatiquementDémontrer le fonctionnement du type « état de liens » du protocole, c’est-à-dire la prise en compte de l’état des liens pour le choix des « meilleures routes » : différencier les débits entre les routes et vérifier le changement de la « meilleure route([[1]](#footnote-1)) ».

#### Protocole HSRP

Note : Cette activité n’est pas forcément la suite de la première. Il s’agit d’assurer une sécurité d’accès au réseau depuis les postes du site A. On reprend ce qui a été fait précédemment pour bénéficier d’une infrastructure ou le routage fonctionne déjà.

Ressource : fiche technique HSRP en annexe 2.

Le site A désire sécuriser ses accès au réseau de liaison en mettant en place deux routeurs pilotés par le protocole HSRP. Ce second routeur RtA-bis sera doté de l’adresse IP 192.168.0.253 en interne et de l’adresse 20.7.7.2 en externe. Il sera relié au routeur RtD sur le réseau 20.7.7.0/30.



Quatrième étape : mise en place du routeur redondant

On utilisera le fichier : <Bloc2_sem3-4_activite-12-Decouverte-OSPF-HSRP-1-Depart-partie-2.pkt>

Mettre en place un second routeur « RtA-bis » sur le site A.

Une image contenant diagramme, ligne, texte, carte

Description générée automatiquement

Compléter le paramétrage OSPF du routeur RtD.

Routeur-D(config)#router ospf 1

Routeur-D(config-router)#network 20.4.4.0 0.0.0.3 area 0

Routeur-D(config-router)#network 20.2.2.0 0.0.0.3 area 0

Routeur-D(config-router)#network 20.7.7.0 0.0.0.3 area 0

Routeur-D(config-router)#exit

Routeur-D(config)#write memory

Tester le nouveau chemin en changeant la passerelle de PC-A.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

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

Description générée automatiquement

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

Description générée automatiquement

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

Description générée automatiquement

Pour tester la modification de la passerelle par défaut en passant par le routeur RtA-bis, j'ai dû installer un switch et modifier l'adresse de l'interface FastEthernet0/1 de RtA-bis afin qu'il puisse également servir de passerelle. De plus, j'ai configuré une adresse IP entre RtA-bis et RtD pour assurer la connectivité. J'ai désactivé l'interface s0/0/0 de RtA pour m'assurer que le trafic ne passe pas par ce chemin. Ensuite, j'ai effectué un test de ping depuis PC-A vers le routeur RtF, car c'est le routeur le plus éloigné, ce qui garantit que le trafic traverse un grand nombre de routeurs.

Cinquième étape : mise en place du protocole HSRP

Mettre en place le protocole HSRP sur les routeurs RtA et RtA-bis. Définir RtA en tant que routeur prioritaire.

Routeur-A(config)#interface FastEthernet0/1

Routeur-A(config-if)#ip address 192.168.0.200 255.255.255.0

Routeur-A(config-if)#standby 1 ip 192.168.0.254

Routeur-A(config-if)#standby 1 priority 110

Routeur-A(config-if)#standby 1 preempt

RtA-bis(config)#interface FastEthernet0/1

RtA-bis(config-if)#ip address 192.168.0.253 255.255.255.0

RtA-bis(config-if)#standby 1 ip 192.168.0.254

RtA-bis(config-if)#standby 1 priority 90

RtA-bis(config-if)#standby 1 preempt

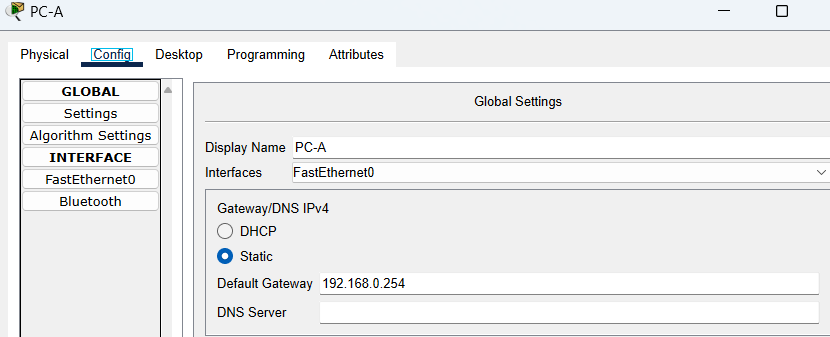
Paramétrer le PC PC-A avec l’adresse de passerelle virtuelle et tester son accès à un serveur Web externe. Vérifier la route empruntée.

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

Description générée automatiquementUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquementUne image contenant texte, logiciel, ligne, Police

Description générée automatiquement



Avec tous les capture d’écran on peut voir que la passerelle virtuelle a fonctionné et que PCA arrive a communique avec le serveur.

Déconnecter la liaison entre RtA et le commutateur du site A : vérifier le basculement vers le routeur de secours.



Une image contenant texte, capture d’écran, Police

Description générée automatiquement

On peut constater que le basculement a bien fonctionné, donc les routeurs sont redondants et que toutes les routes OSPF fonctionnent correctement.

Annexe 1 - Fiche technique OSPF

Principes généraux

OSPF (Open Shortest Path First) est un protocole de routage intérieur à état de liens.

Quelle est la différence fondamentale avec un protocole à « Vecteur de Distance » comme RIP ? Prenons un exemple.

Soit deux routeurs A et B dialoguant pour établir la meilleure route depuis A vers un autre réseau, par exemple 20.9.9.0.

Avec un protocole à vecteur de distance, B communique seulement la métrique vers ce réseau, 4 sauts par exemple (métrique = 4), indépendamment de la bande passante des liens entre les routeurs.

Avec un protocole de routage à état de liens, qui tient donc compte de l’état des liaisons de ses voisins, B va communiquer à A l’état global du réseau. Il faut donc qu’OSPF calcule les coûts vers tous les réseaux pour connaître cet état global.

B va communiquer par exemple à A que pour joindre le réseau 20.9.9.0 :

- cela coûtera « 200 » en passant par le routeur C

- cela coûtera « 300 » en passant par le routeur D.

C’est la route via le routeur C qui est donc retenue. En permanence, il faudra recalculer et communiquer à nouveau sur les coûts pour que les tables de routage contiennent toujours les meilleures routes.

Le processus utilisé par OSPF est le suivant :

Chaque routeur découvre son voisinage et conserve une liste de tous ses voisins ;

Il stocke les informations topologiques apprises dans sa base de données ;

Il exécute l’algorithme « SPF » pour calculer les meilleures routes (le coût total d’une route est la somme des coûts de chaque lien de la route. Pour calculer le coût d’un lien, SPF utilise la formule « 108/bande passante du lien » ;

Il place ensuite la meilleure route vers chaque sous-réseau dans sa table de routage.

Chaque routeur possède, en plus de la table de routage :

Une table de ses voisins, appelée « NeighborTable » ;

Une base de données de la topologie du réseau, appelé « Topology database ».

Les messages OSPF circulent encapsulés dans des paquets IP.

Il y a d’autres différences entre OSPF et RIP comme une convergence plus rapide et une bande passante moins encombrée.

Commandes IOS

Exemple de configuration d’un routeur « R »

R(config)#router ospf 1

R(config-router)#router-id 1.1.1.1

R(config-router)#network 172.16.1.1 0.0.255.255 area 0

R(config-router)#network 172.16.2.1 0.0.255.255 area 0

La commande « router OSPF » met en route le processus OSPF au sein du routeur. Le chiffre 1 qui est placé à la fin de la commande correspond au numéro de processus. Il pourrait y en avoir plusieurs au sein du routeur. Nous nous restreindrons à un processus.

La commande « router-ID » nomme le routeur. Ici on le nomme avec une adresse IP. Si on ne déclare pas cette commande, OSPF choisit lui-même le nom du routeur avec une de ses adresses IP.

Les commandes « network » permettent de déclarer les réseaux connectés au routeur. La clause « AREA 0 » indique le n° de zone (un ensemble de routeurs choisis communiquant entre eux). A noter l’utilisation du masque inversé obtenu de la manière suivante.

Soit le réseau 192.168.1.0/30

Le masque de ce réseau est donc : 255.255.255.252

Le masque inverse s’obtient par soustraction octet par octet à 255.255.255.255

255.255.255.255

- 255 255 255 252

= 000.000.000.003 soit 0.0.0.3

Une autre commande utile de configuration est la commande « passive-interface [interface] » : elle dispense l’interface indiquée de participer au dialogue OSPF.

Exemple :

R(config)#router ospf 1

R(config)#passive-interface fa0/1

Vérification du voisinage d’un routeur

R(config)#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface

20.1.1.1 1 FULL/DR 00:00:38 20.1.1.1 FastEthernet0/0

20.5.5.2 1 FULL/DR 00:00:39 20.5.5.2 FastEthernet0/1

Observation des messages OSPF

R#Debug ip ospf events

Table de routage OSPF

C’est l’indicateur « O » en début de ligne qui indique, dans le résultat de la commande « show ip route » les routes apprises par OSPF.

Exemple

O 20.3.3.0 [110/11] via 20.2.2.1, 00:11:16, FastEthernet0/1

Annexe 2 - 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.

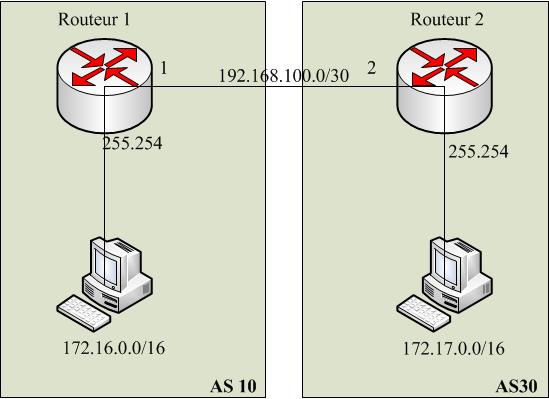
La commande « show standby brief » permet de connaître l’état HSRP du routeur.

### Énoncé 12 : Introduction au protocole BGP

[Bloc2\_sem3-4\_activite-13-configure\_and\_Verify\_eBGP.pka](Bloc2_sem3-4_activite-13-introduction_au_protocole_BGP.pkt)

BGP (Border Gateway Protocol) est un protocole particulier qui permet le routage sur les réseaux de grande taille. Il est principalement utilisé sur Internet. Cet atelier vous propose de le mettre en place.

Le schéma de l’atelier à constituer est le suivant :



Après avoir mis en place l’atelier, assurez-vous que chaque périphérique communique avec son ou ses voisins proches. Mettez en place le protocole de routage BGP pour chaque système autonome, spécifiez les routes à annoncer via BGP, établissez une relation entre chaque routeur voisin, puis montrez que l’ordinateur 1 communique avec l’ordinateur 2.

Pour ce faire, après avoir mis en place la topologie, entrez les commandes suivantes sur le routeur Routeur1 :

Router(config)#router bgp 10

Router(config-router)#net 172.16.0.0

Router(config-router)#neighbor 192.168.100.2 remote-as 30

Router(config-router)#exit

La configuration du protocole de routage BGP nécessite la configuration d’un numéro de système autonome (ici 10), il faut également déclarer tous les routeurs voisins (directement connectés).

Saisissez les instructions suivantes sur le routeur Routeur2 :

Router(config)#router bgp 30

Router(config-router)#net 172.17.0.0

Router(config-router)#neighbor 192.168.100.1 remote-as 10

Router(config-router)#%BGP-5-ADJCHANGE : neighbor 192.168.100.1 Up

Router(config-router)#exit

Router(config)#exit

Router#

Reliez un ordinateur sur chaque réseau 172.16.0.0/16 et 172.17.0.0/16, puis testez la connectivité entre ces deux clients avec les commandes ping et traceroute (tracert sous Windows).

Un système autonome ou AS (Autonomous System) correspond à un ensemble de réseaux IP géré par la même entité administrative. Les systèmes autonomes de 1 à 64511 sont réservés pour une utilisation publique (Internet). Ils sont délivrés par l’ICANN.

Les systèmes autonomes de 64512 à 65535 sont réservés à un usage privé.

Une image contenant texte, capture d’écran, conception

Description générée automatiquement

Maintenant que tout le réseau est en place, pour vérifier que tout fonctionne bien, je vais effectuer des tests de ping et de tracert.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

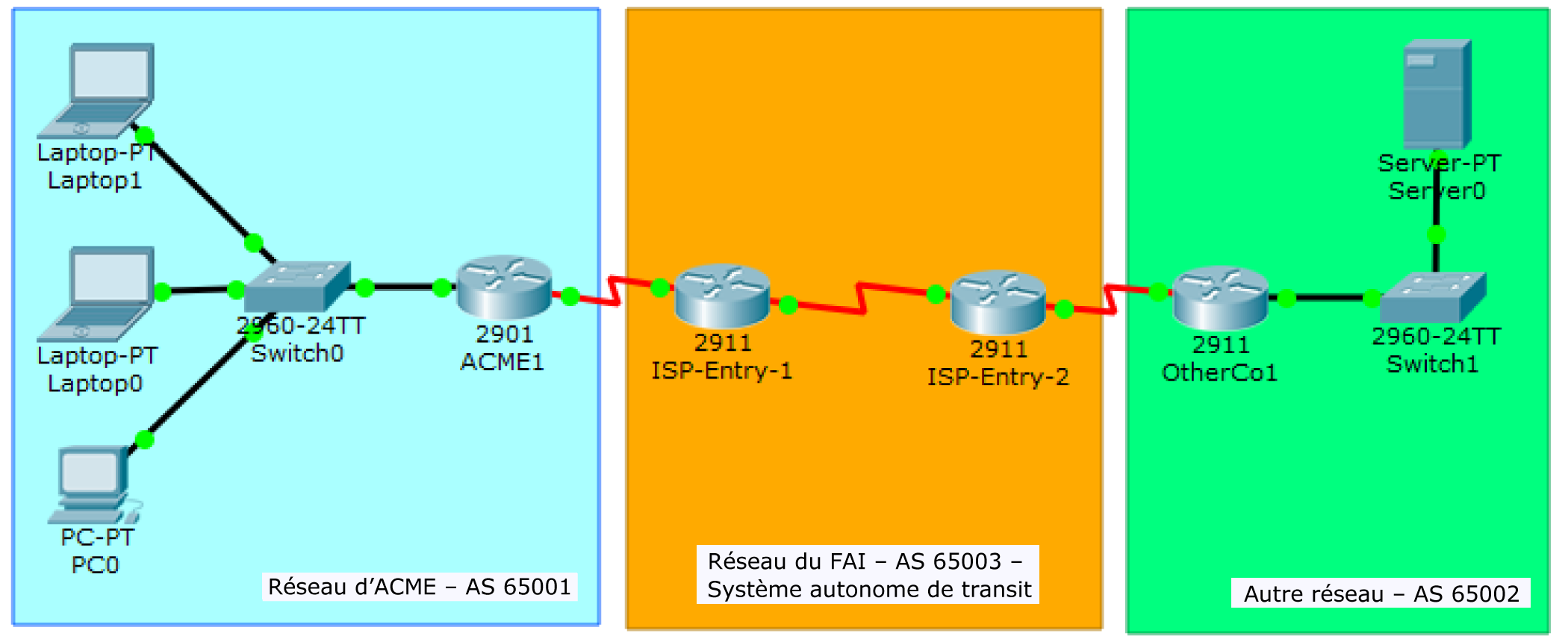
Une image contenant capture d’écran, texte, Icône d’ordinateur, logiciel

Description générée automatiquement

Nous pouvons voir que l’intégralité du réseau fonctionne.

### Énoncé 13 : Packet Tracer – Configuration et vérification du routage eBGP

On utilisera la topologie préparée dans le fichier : <Bloc2_sem3-4_activite-14-configure_and_Verify_eBGP.pka>



#### Objectifs

Configurer et vérifier le routage eBGP entre deux systèmes autonomes.

#### Contexte/scénario

Au cours de cet exercice, vous allez configurer et vérifier le fonctionnement du protocole eBGP entre les systèmes autonomes 65001 et 65002. ACME Inc. est une entreprise qui a conclu, avec Other Company, un partenariat portant sur l’échange de routes. Les deux entreprises possèdent leurs propres systèmes autonomes (AS) et utiliseront le FAI comme système autonome de transit pour communiquer entre elles.

Remarque : seules les entreprises qui possèdent de très vastes réseaux peuvent se permettre de disposer de leur propre système autonome.

Table d’adresses

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appareil | Interface | Adresse IPv4 | Masque de sous-réseau | Passerelle par défaut |
| ACME1 | G0/0 | 192.168.0.1 | 255.255.255.0 | N/A |
| S0/0/0 | 1.1.1.2 | 255.255.255.252 | N/A |
| OtherCo1 | G/0/0 | 172.16.10.1 | 255.255.255.0 | N/A |
| S0/0/0 | 1.1.1.10 | 255.255.255.252 | N/A |
| FAI1 | S0/0/0 | 1.1.1.1 | 255.255.255.252 |  |
| S0/0/1 | 1.1.1.5 | 255.255.255.252 |  |
| FAI2 | S0/0/0 | 1.1.1.9 | 255.255.255.252 |  |
| S0/0/1 | 1.1.1.6 | 255.255.255.252 |  |
| PC0 | Carte réseau | DHCP | | 192.168.0.1 |
| Laptop0 | Carte réseau | DHCP | | 192.168.0.1 |
| Laptop1 | Carte réseau | DHCP | | 192.168.0.1 |
| Serveur | Carte réseau | 172.16.10.2 | 255.255.255.0 | 172.16.10.1 |

Configurez eBGP pour la société ACME Inc.

ACME Inc. a conclu un contrat avec un FAI pour se connecter à une entreprise partenaire appelée Other Company. Le FAI a établi l’accessibilité du réseau au sein de son propre réseau et avec Other Company. Vous devez connecter ACME au FAI de sorte que ACME et Other Company puissent communiquer. Étant donné que le FAI utilise BGP comme protocole de routage, vous devez configurer ACME1, le routeur de frontière de la société ACME, pour établir une connexion de voisinage BGP avec ISP1, le routeur de frontière du FAI qui fait face à ACME.

Montrez que le FAI a fourni l’accessibilité IP via son réseau en envoyant une requête ping à 1.1.1.9, l’adresse IP attribuée à l’interface série 0/0/0 du routeur ISP2.

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

Description générée automatiquementOn peut voir dans le réseau que la FAI a bien donner des adresse IP a tous les routeur mais quelle les protocole de routage ne sont pas encore opérationnel

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

À partir d’un périphérique du réseau de la société ACME, envoyez une requête ping au serveur de la société Other Company à l’adresse 172.16.10.2. Les requêtes ping vont normalement échouer, car aucun routage BGP n’est configuré pour le moment.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquementComme prévu les requêtes ping on échouer, car aucun routage BGP n’est configuré pour le moment.

Configurez ACME1 pour qu’il devienne un homologue eBGP d’ISP1. Le numéro du système autonome d’ACME est 65001, tandis que le FAI utilise le numéro 65003. Utilisez 1.1.1.1 comme adresse IP de voisinage et veillez à ajouter le réseau interne 192.168.0.0/24 d’ACME au protocole BGP.

ACME1(config)#router bgp 65001

ACME1(config-router)#neighbor 1.1.1.1 remote-as 65003

ACME1(config-router)#network 192.168.0.0 mask 255.255.255.0

ACME1(config-router)#end

ACME1#write memory

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

Description générée automatiquement

On peut voir sur cette capture d’écran que le bgp fonctionne correctement.

À partir d’un périphérique du réseau de la société ACME, envoyez une nouvelle requête ping au serveur interne de la société Other Company. Cela fonctionne-t-il ?

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Comme nous le voyons sur la capture d’écran le ping a échouer ce qui est normal car pour le moment le réseau vert avec le serveur n’a pas encore de configuration bgp sur leur routeur.

Configurez eBGP pour la société Other Company Inc.

L’administrateur réseau de la société Other Company ne maîtrise pas bien le protocole BGP et n’est pas parvenu à configurer son côté de la liaison. Vous devez donc vous charger également de cette configuration.

Configurez OtherCo1 pour établir une contiguïté eBGP avec ISP2, le routeur de frontière du FAI qui fait face à OtherCo1. Other Company utilise le système autonome 65002, tandis que le FAI utilise le système 65003. Utilisez 1.1.1.9 comme adresse IP de voisinage du routeur ISP2 et veillez à ajouter le réseau interne 172.16.10.0/24 d’Other Company au protocole BGP.

OtherCo1(config)#router bgp 65002

OtherCo1(config-router)#neighbor 1.1.1.9 remote-as 65003

OtherCo1(config-router)#%BGP-5-ADJCHANGE: neighbor 1.1.1.9 Up

OtherCo1(config-router)#network 172.16.10.0 mask 255.255.255.0

OtherCo1(config-router)#end

OtherCo1#write memory

**Vérification eBGP**

OtherCo1#show ip bgp summary

BGP router identifier 172.16.10.1, local AS number 65002

BGP table version is 6, main routing table version 6

5 network entries using 660 bytes of memory

5 path entries using 260 bytes of memory

4/3 BGP path/bestpath attribute entries using 644 bytes of memory

2 BGP AS-PATH entries using 48 bytes of memory

0 BGP route-map cache entries using 0 bytes of memory

0 BGP filter-list cache entries using 0 bytes of memory

Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory

BGP using 1644 total bytes of memory

BGP activity 5/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

1.1.1.9 4 65003 6 2 6 0 0 00:00:31 4

OtherCo1#show ip bgp

BGP table version is 6, local router ID is 172.16.10.1

Status codes: s suppressed, d damped, h history, \* valid, > best, i - internal,

r RIB-failure, S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path

\*> 1.1.1.0/30 1.1.1.9 0 0 0 65003 i

\*> 1.1.1.4/30 1.1.1.9 0 0 0 65003 i

\* 1.1.1.8/30 1.1.1.9 0 0 0 65003 i

\*> 172.16.10.0/24 0.0.0.0 0 0 32768 i

\*> 192.168.0.0/24 1.1.1.9 0 0 0 65003 ?

Le routeur OtherCo1 a établi la session eBGP avec ISP2. Les routes sont échangées correctement. OtherCo1 a appris la route vers le réseau 192.168.0.0/24 d'ACME. Cette route est bien présente dans la table de routage. La communication entre les réseaux d'ACME et d'Other Company est désormais possible via le FAI.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquementMontrez que le routeur ACME1 a établi une contiguïté eBGP correcte avec ISP1. La commande show ip bgp summary se révèle très utile ici.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

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

Description générée automatiquement

Grâce à tous ces tests ping et aux commandes tracert, je peux confirmer que le protocole BGP a bien été configuré sur les différents routeurs et que tout fonctionne correctement. La connectivité entre les réseaux est établie correctement.

Utilisez la commande show ip bgp neighbors pour vérifier toutes les routes acquises par ACME1 via eBGP, ainsi que leur état.

ACME1#show ip bgp neighbors

BGP neighbor is 1.1.1.1, remote AS 65003, external link

BGP version 4, remote router ID 1.1.1.5

BGP state = Established, up for 00:19:22

Last read 00:19:22, last write 00:19:22, hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:

Route refresh: advertised and received(new)

Address family IPv4 Unicast: advertised and received

Message statistics:

InQ depth is 0

OutQ depth is 0

Sent Rcvd

Opens: 1 1

Notifications: 0 0

Updates: 1 5

Keepalives: 20 20

Route Refresh: 0 1

Total: 22 27

Default minimum time between advertisements runs is 30 seconds

For address family: IPv4 Unicast

BGP table version 6, neighbor version 6/0

Output queue size : 0

Index 1, Offset 0, Mask 0x2

1 update-group member

Sent Rcvd

Prefix activity: ---- ----

Prefixes Current: 1 4 (Consumes 115 bytes)

Prefixes total: 1 4

Implicit Withdraw: 0 0

Explicit Withdraw: 0 0

Used as bestpath: n/a 1

Used as multipath: n/a 0

Outbound Inbound

Local Policy Denied Prefixes: -------- -------

Total: 0 0

Number of NLRIs in the update sent: max 3, min 1

Address tracking is enabled, the RIB does have a route to 1.1.1.1

Connections established 1; dropped 0

Last reset never

Transport(tcp) path-mtu-discovery is enabled

Connection state is ESTAB, I/O status: 1, unread input bytes: 0

Connection is ECN Disabled, Minimum incoming TTL 0, Outgoing TTL 1

Local host: 1.1.1.2, Local port: 1025

Foreign host: 1.1.1.1, Foreign port: 179

Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xC69F4):

Timer Starts Wakeups Next

Retrans 0 0 0x0

TimeWait 0 0 0x0

AckHold 25 0 0x0

SendWnd 0 0 0x0

KeepAlive 20 0 0x0

GiveUp 0 0 0x0

PmtuAger 0 0 0x0

DeadWait 0 0 0x0

Linger 0 0 0x0

ProcessQ 0 0 0x0

iss: 2057115318 snduna: 2057115748 sndnxt: 2057115748 sndwnd: 15955

irs: 3480424370 rcvnxt: 3480424751 rcvwnd: 16004 delrcvwnd: 380

SRTT: 259 ms, RTTO: 579 ms, RTV: 320 ms, KRTT: 0 ms

minRTT: 16 ms, maxRTT: 300 ms, ACK hold: 200 ms

Status Flags: passive open, gen tcbs

Option Flags: nagle, path mtu capable

IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):

Rcvd: 26 (out of order: 0), with data: 1, total data bytes: 24

Sent: 21 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 1, total data bytes: 24

Packets received in fast path: 0, fast processed: 0, slow path: 0

fast lock acquisition failures: 0, slow path: 0

La session BGP entre ACME1 et ISP1 est bien établie et stable. ACME1 a reçu 4 routes via eBGP et en a annoncé 1. La communication entre les routeurs fonctionne correctement, avec un échange actif de messages BGP. Les routes apprises sont valides et sont utilisées pour le routage.

Examinez les tables de routage sur ACME1 et OtherCo1. ACME1 devrait normalement avoir découvert la route 172.16.10.0/24 de la société Other Company. De même, OtherCo1 devrait maintenant connaître la route 192.168.0.0/24 d’ACME.

ACME1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

1.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 1.1.1.0/30 is directly connected, Serial0/0/0

L 1.1.1.2/32 is directly connected, Serial0/0/0

B 1.1.1.4/30 [20/0] via 1.1.1.1, 00:00:00

B 1.1.1.8/30 [20/0] via 1.1.1.1, 00:00:00

172.16.0.0/24 is subnetted, 1 subnets

B 172.16.10.0/24 [20/26114560] via 1.1.1.1, 00:00:00

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.0.0/24 is directly connected, GigabitEthernet0/0

L 192.168.0.1/32 is directly connected, GigabitEthernet0/0

OtherCo1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

1.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

B 1.1.1.0/30 [20/0] via 1.1.1.9, 00:00:00

B 1.1.1.4/30 [20/0] via 1.1.1.9, 00:00:00

C 1.1.1.8/30 is directly connected, Serial0/0/0

L 1.1.1.10/32 is directly connected, Serial0/0/0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.10.0/24 is directly connected, GigabitEthernet0/0

L 172.16.10.1/32 is directly connected, GigabitEthernet0/0

B 192.168.0.0/24 [20/26114560] via 1.1.1.9, 00:00:00

Les tables de routage montrent que la configuration eBGP est réussie. ACME1 a appris la route vers le réseau 172.16.10.0/24 d'Other Company, et OtherCo1 a appris la route vers le réseau 192.168.0.0/24 d'ACME. Cela confirme que les deux réseaux sont désormais connectés via BGP et que la communication est possible.

Ouvrez un navigateur Web sur un périphérique final d’ACME Inc. et accédez au serveur de la société Other Company en saisissant son adresse IP 172.16.10.2

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Le serveur arrive à transmettre les données jusqu'à Laptop1, ce qui confirme que la configuration des deux réseaux est correcte. Cela prouve encore que le routage BGP est bien en place et que les réseaux ACME et Other Company peuvent communiquer sans problème.

À partir d’un périphérique de la société ACME Inc., envoyez une requête ping au serveur de la société Other Copán à l’adresse 172.16.10.2

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

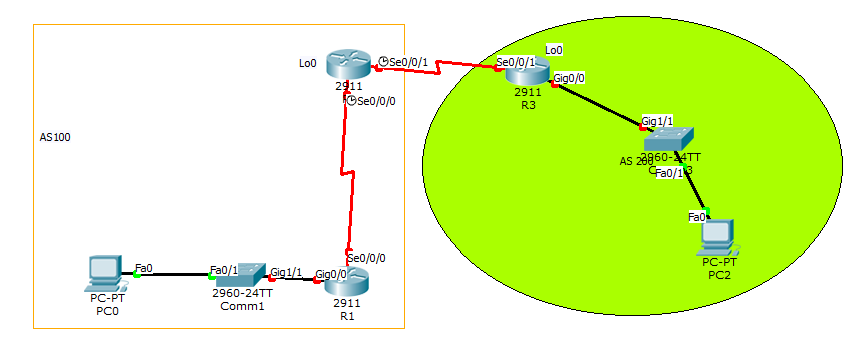
Description générée automatiquementLa requête ping montre que PC0 communique sans problème avec le serveur, confirmant ainsi que tous les appareils du réseau peuvent bien communiquer entre eux. Cela valide la configuration correcte des réseaux et du routage via BGP.

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

### Énoncé 14 : Atelier BGP Configuration du protocole BGP avec un routage par défaut

Voici le schéma final sous Packet Tracer du réseau, il est à faire, on utilisera le fichier : [Bloc2\_sem3-4\_activite-15-bgp-debut.pkt](Bloc2_sem3-4_activite-15-bgp-debut.pkt" \o "Bloc2_sem3-4_activite-15-bgp-debut.pkt)



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Périphérique | Nom de l’hôte | Interface | Adresse IP | Masque de sous-réseau |
| R1 | CR | Serial 0/0/0 (DTE) | 10.10.10.1 | 255.255.255.0 |
|  |  | Giga Ethernet 0/0 | 192.168.1.1 | 255.255.255.0 |
| R2 | FAI1 | Serial 0/0/0 (DCE) | 10.10.10.2 | 255.255.255.0 |
|  |  | Serial 0/0/1 (DCE) | 172.16.1.1 | 255.255.255.0 |
|  |  | Boucle 0 | 192.168.100.1 | 255.255.255.0 |
| R3 | FAI2 | Serial 0/0/1 (DTE) | 172.16.1.2 | 255.255.255.0 |
|  |  | Giga Ethernet 0/0 | 172.31.0.1 | 255.255.255.0 |
|  |  | Boucle 0 | 192.168.200.1 | 255.255.255.0 |

#### Objectifs

Configurer le routeur client avec un réseau interne annoncé par FAI1 via le protocole BGP (Border Gateway Protocol)

Configurer le protocole BGP pour l’échange d’informations de routage entre FAI1 dans AS 100 et FAI2 dans AS 200

#### Contexte/Préparation

Une petite société a besoin d’un accès à Internet. Elle a demandé à son FAI local (FAI1) de lui fournir ses services. FAI1 se connecte à Internet par l’intermédiaire de FAI2 à l’aide d’un protocole de routage externe. Le protocole BGP4 est le protocole de routage le plus courant entre les FAI sur Internet. Au cours de ces travaux pratiques, le routeur client se connecte au FAI à l’aide d’une route par défaut et FAI1 se connecte à FAI2 via le protocole BGP4.

Installez un réseau similaire à celui du schéma.

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

Description générée automatiquement

Établir la liste des ressources nécessaires si vous aviez à installer cette configuration physiquement

Routeurs : 3x Cisco 2911.

Commutateurs : 2x Cisco 2960-24TT.

PC : 2x ordinateurs.

Câblage :

* Câbles série pour les connexions entre les routeurs.
* Câbles Ethernet RJ45 pour les connexions routeurs/switches et PC.

Interfaces série : Cartes d'interface série à installer sur les routeurs.

Racks pour montage : Pour fixer les routeurs et commutateurs.

Alimentation électrique : Câbles d'alimentation pour tous les équipements.

Câbles console : Pour la configuration des équipements.

Configuration réseau : Adresses IP et routage.

Étape 1 : configuration des informations de base sur chaque routeur

Envoyez une requête ping pour tester la connectivité entre les routeurs connectés directement.

Le routeur CR est-il en mesure d’atteindre le routeur FAI2 ?

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

Description générée automatiquement

Oui d’après le ping le routeurs CR est capable d’atteindre le routeur de FAI2

L’hôte client est-il en mesure d’atteindre le routeur FAI1 ?



D’après le ping oui le client est en mesure d’atteindre le routeur de FAI1

Sur les routeurs FAI1 et FAI2, configurez une interface de bouclage en lui donnant une adresse IP, comme indiqué dans le schéma topologique. Une interface de bouclage est une interface virtuelle qui simule un réseau réel à des fins de tests.

FAI1>en

FAI1#conf t

FAI1(config)#interface loopback0

FAI1(config-if)#ip address 192.168.100.1 255.255.255.0

FAI2>en

FAI2#conf t

FAI2(config)#interface loopback0

FAI2(config-if)#ip address 192.168.200.1 255.255.255.0

Étape 2 : configuration des routes par défaut et des routes statiques

Sur le routeur CR, configurez la route par défaut pour permettre aux utilisateurs d’accéder à FAI1.

CR(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2



Sur le routeur FAI1, configurez une route statique de retour au réseau du client.

FAI1(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1



Testez la connectivité en envoyant une requête ping à partir de l’hôte vers FAI1 à l’adresse 10.10.10.2.

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

Description générée automatiquement

Le ping a réussi avec sucer.

Étape 3 : configuration du protocole BGP sur les deux routeurs FAI

Configurez le protocole BGP sur le routeur FAI1.

FAI1(config)#router bgp 100

FAI1(config-router)#neighbor 172.16.1.2 remote-as 200

FAI1(config-router)#network 192.168.1.0

FAI1(config-router)#network 192.168.100.0

FAI1(config-router)#end

FAI1#copy running-config startup-config

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

Description générée automatiquement

Remarque : il est recommandé d’enregistrer fréquemment la configuration, en particulier après avoir terminé plusieurs étapes importantes de configuration.

Configurez le protocole BGP sur le routeur FAI2.

FAI2(config)#router bgp 200

FAI2(config-router)#neighbor 172.16.1.1 remote-as 100

FAI2(config-router)#network 192.168.200.0

FAI2(config-router)#network 172.31.0.0

FAI2(config-router)#end

FAI2#copy running-config startup-config

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

Description générée automatiquement

Étape 4 : affichage des tables de routage

La configuration BGP est terminée. Montrez la table de routage de chaque routeur (selon le modèle de routeur utilisé, la sortie peut être légèrement différente que celle présentée ci-dessous).

FAI2>sh ip route

Codes : L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.1.0/24 is directly connected, Serial0/0/1

L 172.16.1.2/32 is directly connected, Serial0/0/1

172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.31.0.0/24 is directly connected, GigabitEthernet0/0

L 172.31.0.1/32 is directly connected, GigabitEthernet0/0

B 192.168.1.0/24 [20/0] via 172.16.1.1, 00:06:18

B 192.168.100.0/24 [20/0] via 172.16.1.1, 00:06:18

192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.200.0/24 is directly connected, Loopback0

L 192.168.200.1/32 is directly connected, Loopback0

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

Description générée automatiquement

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

Description générée automatiquement

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

Description générée automatiquement

Proposez votre affichage des tables de routage et montrer les différences tout en en donnant une explication avec celle proposée.

Passerelle par défaut :

CR# a une passerelle de dernier recours (10.10.10.2), ce qui en fait probablement un routeur de bordure.

FAI1# et FAI2# n'ont pas de passerelle par défaut.

Routes BGP :

FAI1# et FAI2# échangent des routes via BGP.

CR# n'a pas de route BGP et utilise une route par défaut statique.

Routes statiques :

FAI1# a une route statique vers 192.168.1.0/24.

FAI2# n'a pas de route statique explicite.

Réseaux Loopback :

FAI1# a le réseau 192.168.100.0/24.

FAI2# a le réseau 192.168.200.0/24.

Le réseau 192.168.1.0 est-il dans la table de routage du routeur FAI2 ?



Dans la table de routage de FAI2 on peut voir que le réseau 192.168.1.0 a bien était mis.

Quelle lettre se trouve à gauche de l’entrée du réseau 192.168.1.0 ?



La lettre située à gauche de l’entrée du réseau est B, qui, selon la légende de la table de routage, correspond au protocole BGP.



Que signifie cette lettre ?

Ce que signifie la lettre est le protocole de routage BGP (Border Gateway Protocol)

Le réseau 192.168.100.0 est-il dans la table de routage ?



Oui on peut voir que le réseau 192.168.100.0 est dans la table de routage. Il a également la lettre B de BGP.

Quel routeur a annoncé le réseau 192.168.1.0 ? Voici mes résultats, répondez à la question en dessous pour ces derniers.

FAI1#sh ip route

Codes : L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.10.10.0/24 is directly connected, Serial0/0/0

L 10.10.10.2/32 is directly connected, Serial0/0/0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.1.0/24 is directly connected, Serial0/0/1

L 172.16.1.1/32 is directly connected, Serial0/0/1

S 192.168.1.0/24 [1/0] via 10.10.10.1

192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.100.0/24 is directly connected, Loopback0

L 192.168.100.1/32 is directly connected, Loopback0

B 192.168.200.0/24 [20/0] via 172.16.1.2, 01:27:35

Le réseau 192.168.1.0/24 est indiqué dans la table de routage du routeur FAI1 comme une route statique (code S) via l'adresse 10.10.10.1. Cela signifie que ce réseau a été configuré manuellement sur FAI1 avec une route statique pointant vers un autre routeur.

Et pour vous qu’en est-il ?

Dans ma table de routage de FAI1, le réseau 192.168.1.0/24 est annoncé comme une route statique (indiqué par le code S), via l'adresse 10.10.10.1. Cela signifie que FAI1 utilise une route statique pour atteindre ce réseau en passant par 10.10.10.1.

Quels sont les réseaux signalés par le routeur FAI2 au routeur FAI1 ?



Sur la table de routage de FAI1, on peut observer qu'il reçoit des réseaux via BGP depuis le routeur FAI2.

Comment le réseau 192.168.1.0 a-t-il été signalé au routeur FAI1 ?

Le réseau 192.168.1.0/24 a été signalé au routeur FAI1 par le biais d'une route statique, configurée manuellement pour pointer vers l'adresse 10.10.10.1.

Le routeur FAI1 va-t-il annoncer des réseaux au routeur client ? Qu’en est-il avec mon résultat obtenu ?

R1#sh ip route

Codes : L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 10.10.10.2 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.10.10.0/24 is directly connected, Serial0/0/0

L 10.10.10.1/32 is directly connected, Serial0/0/0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

S\* 0.0.0.0/0 [1/0] via 10.10.10.2

FAI1 annoncera-t-il des réseaux au routeur client (R1) ?

FAI1 pourrait annoncer des réseaux à R1 s'il y avait un protocole de routage dynamique) configuré entre eux. Cependant, aucune présence de protocole de routage dynamique entre FAI1 et R1. R1 reçoit une route par défaut via une configuration statique via 10.10.10.2, ce qui suggère que l'annonce de routes par FAI1 à R1 ne se fait pas automatiquement.

Avec le résultat obtenu :

R1 ne semble pas recevoir de réseaux spécifiques via un protocole de routage dynamique. Il utilise une route statique par défaut. Pour que FAI1 annonce des réseaux à R1, un protocole de routage devrait être configuré entre les deux routeurs. Actuellement, R1 n'apprend que les réseaux directement connectés et utilise la route par défaut pour le reste du trafic.

Qu’en est-il pour vous ?

FAI1 n'annonce pas automatiquement de réseaux au routeur R1, car il n'y a pas de protocole de routage dynamique comme BGP configuré entre eux. R1 utilise une route statique par défaut, ce qui signifie qu'il envoie tout le trafic non spécifié à FAI1 via l'adresse 10.10.10.2.

Pourquoi les réseaux 192.168.100.0 et 192.168.200.0 n’apparaissent-ils pas dans la table de routage du routeur CR ?

Les réseaux 192.168.100.0 et 192.168.200.0 n'apparaissent pas dans la table de routage de CR car ils ne sont pas annoncés par FAI1 et FAI2 via un protocole de routage dynamique, ou aucune route statique n'est configurée. CR ne peut pas apprendre ces réseaux sans protocole de routage ou sans routes statiques explicites.

Étape 5 : vérification de la connectivité

À partir de l’hôte PC0, envoyez une requête ping sur le réseau Ethernet du CR à destination de l’interface de bouclage du routeur FAI2.



Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

On peut voir a l’aide des ping sur PC0 arrive a communique avec FAI2 sur l’interface de bouclage du routeur FAI2.

À partir du routeur FAI2, envoyez une requête ping à l’hôte PC0 sur le réseau Ethernet du CR.

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

Description générée automatiquement

On peut voir que le routeur FAI2 arrive a envoyez une requête ping à l’hôte PC0 sur le réseau Ethernet du CR.

Étape 6 : affichage des informations BGP sur les routeurs FAI

Sur le routeur FAI1, affichez le routage BGP au moyen de la commande appropriée.

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

Description générée automatiquement

Sur le routeur FAI2, affichez le routage BGP.

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

Description générée automatiquement

Étape 7 : remarques générales

Pourquoi le routeur FAI1 n’annonce-t-il pas de réseau au routeur client ?

Le routeur FAI1 n'annonce pas de réseau au routeur client car il n'y a pas de protocole de routage dynamique configuré entre eux. BGP est configuré entre FAI1 et FAI2, mais pas entre FAI1 et le client. Le routeur client utilise une route statique par défaut pour envoyer le trafic via FAI1, ce qui rend inutile l'échange dynamique de routes. Sans protocole dynamique ou annonce explicite, FAI1 ne transmet pas de réseaux au client.

Pour faire une dernière vérification, j'ai effectué une série de tests pour m'assurer que tout le monde parvient à communiquer, ce qui est bien le cas.

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

Description générée automatiquement

# Conclusion :

Cet atelier vise à synthétiser les différents protocoles de routage abordés dans les activités et les fichiers fournis. L'atelier couvre des aspects essentiels de la configuration et de la gestion des protocoles de routage tels que EIGRP, OSPF, et BGP, tout en mettant en évidence la redistribution des routes entre ces protocoles. Chaque activité explore des configurations spécifiques, comme le routage statique flottant, les tunnels GRE, et les concepts avancés comme les Virtual Links dans OSPF ou la redondance avec HSRP.

Cet ensemble de fichiers Packet Tracer et GNS3 permet une compréhension approfondie des techniques de routage avancées et de la convergence des protocoles. En particulier, la redistribution des routes entre EIGRP et OSPF, et la mise en place de BGP, sont des points centraux pour les environnements multi-domaines. Les différentes étapes permettent de tester et de vérifier la robustesse du réseau, notamment avec la configuration de routes statiques flottantes pour assurer la redondance.

Cet atelier est une immersion complète dans la configuration et l'optimisation des réseaux, allant des routes statiques aux protocoles de routage avancés. Il aborder la gestion des réseaux complexes en mettant en œuvre des scénarios de convergence, de redistribution, et de routage entre différentes technologies.

# Webographie :

« Routing algorithms and protocols (RIP, OSPF, BGP) - Computer Networks ». Consulté le

20 septembre 2024. [https://noobtomaster.com/computer-networks/routing-algorithms-and protocols-rip-ospf-bgp/](https://noobtomaster.com/computer-networks/routing-algorithms-and%20protocols-rip-ospf-bgp/).

IPCisco. « IPCisco | Cisco Networking Academy | Network Certification | Learn ».

Consulté le 28 septembre 2024. <https://ipcisco.com/>.

Tiwary, Satish. « Route Redistribution between RIP and OSPF Routing Domain ». *Learn Linux CCNA  CCNP CEH CISSP CISA Penetration-Testing Bug Bounty  IPv6 Cyber-Security Network-Security Online* (blog), 18 janvier 2018. <https://linuxtiwary.com/2018/01/18/route-redistribution-between-rip-and-ospf-routing-domain/>.

Source : <http://www.nolot.eu/Download/Cours/reseaux/m2pro/ASR0708/Cours3-OSPF-EIGRP.pdf>

1. Par défaut, la bande passante des liens série entre les routeurs de liaison est à 1544 kbps. On peut par exemple positionner la bande passante de liens qu’on souhaite moins rapides à 64 ou 256 kbps. Ceci se fait par la commande « Bandwith » appliquée sur une interface. Par exemple : bandwith 64. [↑](#footnote-ref-1)