UNIVERSITÉ DE TECHNOLOGIE D'HAÏTI

PROGRAMME TIC-HAÏTI-BRH

Session-I

DESS

EQUIPE 11

Sujet : HSRP pour un routage IP avec tolérance aux pannes

- Guytompous J. DESMOULIN
- Willy EXANTUS
- Marc-Sene HORNE
- Lamare JOSEPH
- Stanley LOUIS

Architecture Des Reseaux

Professeur: **Judith Soulamite Nouho Noutat**

Table des matieres

1. Introduction et objectifs du projet 3

a) Présentation générale de la haute disponibilité réseau (HSRP). 3

❖ Fonctionnement de HSRP. - 3

❖ Comment les routeurs communiquent entre eux? 4

❖ Avantages d'utiliser HSRP 4

b) Problématique des pannes de routeur et de la continuité de service. 5

c) Présentation des concepts de base : priorité, IP virtuelle et basculement (failover). 5

2. Architecture réseau : VLAN, OSPF et HSRP 6

a) Présentation des VLAN : Segmentation logique, isolation du trafic. 6

b) Présentation de OSPF: Protocole de routage dynamique, convergence rapide. 6

c) Présentation de HSRP : protocole de redondance, fonctionnement maître/esclave. 7

d) Architecture de réseau (Topologie) et Tableau d'adressage IP. 7

3. Configuration générale PCs, VLAN et du routage OSPF 9

a) Création et configuration des VLAN (switchs), attribution des interfaces aux VLAN, inter-VLAN et OSPF (sur les routeurs). 9

b) Compatibilité avec des environnements spécifiques : AppleTalk, Banyan VINES et Novell IPX. 9

c) Configuration des routeurs HSRP (Active, Standby, priorité), mise en place des timers et de la préemption. 10

4. Simulation d'une panne (désactivation du routeur actif). 10

a) **Procédure:** Pendant la présentation, on fait la déconnexion d'un câble dans la couche de distribution reliant la couche d'accès. 10

b) Observation du basculement (failover) vers le routeur standby. 10

5. Évaluation, bonnes pratiques et conclusion 10

a) Bonnes pratiques pour déployer HSRP en production (optimisation, sécurité). 10

b) Limites et améliorations possibles (par exemple : comparaison avec VRRP ou GLBP). 11

c) Comparaison avec d'autres protocoles comme VRRP ou GLBP, et perspectives d'amélioration. 11

Conclusion générale et perspectives. 12

Références et bibliographie : 13

1. Introduction et objectifs du projet

a) Présentation générale de la haute disponibilité réseau (HSRP).

La haute disponibilité **(High Availability, HA)** est un principe fondamental en ingénierie réseau visant à minimiser les temps d'indisponibilité en cas de panne matérielle ou logicielle. HSRP pour Hot Standby Router Protocol est un protocole de redondance de routeurs développé par Cisco. Son but principal est de garantir la continuité de service en cas de défaillance d'un routeur sur un réseau. Lorsque vous configurez plusieurs routeurs dans un réseau, HSRP permet à ces routeurs de collaborer pour assurer que le trafic réseau continue de circuler même si l'un des routeurs devient inopérant.

❖ Fonctionnement de HSRP. -

HSRP permet à un groupe de routeurs de se partager une seule adresse IP virtuelle. Un routeur au sein du groupe est désigné comme « actif » et est responsable de la gestion du trafic. Le routeur de secours est en mode « standby », prêt à prendre la relève si le routeur actif tombe en panne.

Cela se fait par la mise en commun du fonctionnement de plusieurs routeurs physiques (au minimum deux) qui, de manière automatique, assureront la relève entre eux d'un routeur à un autre. Le protocole HSRP présente aussi son semblable normalisé qui se nomme VRRP. Celui-ci étant normalisé, il est disponible sur les routeurs d'autres marques que Cisco. Plus précisément, la technologie HSRP permettra aux routeurs situés dans un même groupe (que l'on nomme « standby group ») de former un routeur virtuel qui sera l'unique passerelle des hôtes du réseau local. En se « cachant » derrière ce routeur virtuel aux yeux des hôtes. Les routeurs garantissent en fait qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe. Un routeur dans ce groupe est donc désigné comme « actif » et ce sera lui qui fera passer les requêtes d'un réseau à un autre. Pendant que le routeur actif travaille, il envoie également des messages aux autres routeurs indiquant qu'il est toujours « vivant » et opérationnel. Si le routeur principal élu actif vient à tomber. Il sera automatiquement remplacé par un routeur qui était jusque-là « passif » et lui aussi membre du groupe HSRP. Aux yeux des utilisateurs toutefois, cette réélection et ce changement de passerelle sera totalement invisible car ils auront toujours pour unique passerelle le routeur virtuel que forment les routeurs membres du groupe HSRP. Le routeur virtuel aura donc toujours la même IP et adresse MAC aux yeux des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets.

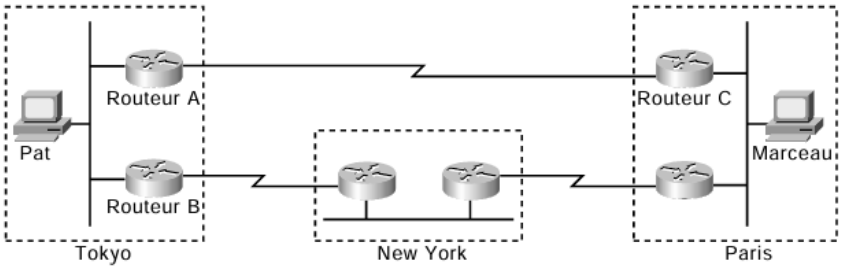


Figure 23.1
Un réseau WAN typique.

Figure prise à partir du document de référence.

❖ Comment les routeurs communiquent entre eux?

Les routeurs configurés pour HSRP échangent trois types de messages multicast :

- **Hello**. Le message Hello communique aux autres routeurs HSRP le niveau de priorité et les informations d'état du routeur.
- **Coup**. Lorsqu'un routeur de secours assure les fonctions du routeur actif, il envoie un message Coup.
- **Resign**. Un routeur actif envoie ce message lorsqu'il est sur le point de s'arrêter, ou quand un routeur Doté d'une priorité plus haute envoie un message Hello.

A n'importe quel moment, les routeurs HSRP peuvent se trouver dans l'un des états suivants :

- **Actif**. Le routeur assure des fonctions de transmission de paquets.
- **Secours**. Le routeur est prêt à assurer les fonctions de transmission de paquets en cas de défaillance du routeur actif.
- **Emission et écoute**. Le routeur envoie et reçoit des messages Hello.
- **Ecoute**. Le routeur reçoit des messages Hello.

❖ Avantages d'utiliser HSRP

L'implémentation du protocole HSRP dans un réseau garantit plusieurs avantages:

1. Haute disponibilité : Assure que le trafic réseau ne soit jamais interrompu en cas de défaillance d'un routeur.
2. Facilité de mise en œuvre : Comparé à d'autres protocoles de redondance, HSRP est relativement simple à configurer et à gérer.

3. Flexibilité : Compatible avec divers types de réseaux, le HSRP peut être utilisé dans une variété de configurations.
4. Tolérance aux pannes : Avec HSRP, le réseau peut continuer de fonctionner même en cas de défaillance matérielle ou logicielle d'un routeur.

b) Problématique des pannes de routeur et de la continuité de service.

Quand on implémente le protocole HSRP dans un réseau cela ne garantit pas que si le routeur par défaut tombe en panne tous les hôtes du LAN perdent leur accès externe du service internet ainsi que les serveurs distants. Aucun basculement n'est prévu sans le mécanisme de redondance.

Et les impacts des pannes de routeur peuvent être de type :

- Défaillance matérielle, quand un routeur est hors service, problème d'alimentation et carte réseau.
- Bug logiciel, lorsque le système d'exploitation plante à répétition.
- Câble déconnecté, la connectivité involontaire du câble peut causer la mise hors réseau.

c) Présentation des concepts de base : priorité, IP virtuelle et basculement (failover).

- **Priorité**, concept utilisé en HSRP pour déterminer quel routeur devient **actif** défini par une valeur numérique (0 à 255). La valeur par défaut est 100, le routeur avec la valeur la plus élevée devient routeur actif, en cas d'égalité le routeur avec l'adresse IP la plus élevée est considéré comme routeur actif.
- **IP Virtuelle** autrement dit Passerelle Partagée par le groupe de routeurs HSRP, utilisée par les hôtes du réseau comme passerelle par défaut et n'est assignée à une interface physique d'un routeur, mais est attribuée dynamiquement au routeur actif. Alors les hôtes peuvent communiquer uniquement avec celle-ci, sans tenir compte du routeur actif en arrière-plan, en cas de panne du routeur actif, l'IP virtuelle est automatiquement transférée au routeur de secours(standby).
- **Basculement (Failover)**, le routeur de secours(standby) prend le relai automatiquement que le routeur actif devient indisponible (panne matérielle, interface down, mis en tension, etc.)

2. Architecture réseau : VLAN, OSPF et HSRP

Dans les réseaux de Campus comme les Entreprises modernes, la redondance et la tolérance aux pannes sont essentielles pour assurer une connectivité ininterrompue, on peut combiner :

a) Présentation des VLAN : Segmentation logique, isolation du trafic.

VLAN (Virtual Local Area Network) - Technique de segmentation logique au sein du réseau (LAN) permettant de diviser un réseau physique en plusieurs réseaux logiques, indépendants les uns des autres. Chaque VLAN se comporte comme un réseau distinct, même s'il partage la même infrastructure physique (commutateurs, câble, pc, etc.) par département et services en isolant les domaines de diffusion et mieux organiser les flux.

Les VLANs partagent le trafic du réseau en isolant les postes de services, par exemple un poste de travail se trouvant dans le VLAN 20 ne peut pas communiquer directement avec les autres se trouvant dans le VLAN 30 sans passer par un routeur ou commutateur de niveau 3.

- La sécurité du réseau par isolation et les flux sont mieux gérés (chaque VLAN peut avoir ses propres QoS, ACL).
- Rendre le réseau plus performant en réduisant les domaines de broadcast et assurer la gestion des adresse IP dans les différentes(services/département).

b) Présentation de OSPF: Protocole de routage dynamique, convergence rapide.

OSPF (Open Shortest Path First) - Protocole de routage dynamique standard ie peut être utilisé par tous les constructeurs (Alcatel, Cisco, Huawei, …) ou IGP(Interior Gateway Protocol) pour la redondance des chemins permettant d'atteindre la meilleure destination. C'est un protocole à état de lien qui est ouvert, qui a été créé par le groupe IETF en 1988, utilisant l'algorithme de Dijkstra (algorithme du plus court chemin).

OSPF permet de:

- Prendre en compte la proximité physique lors de la définition des zones.
- Réduire la taille maximale des zones si les liaisons sont instables.

c) Présentation de HSRP : protocole de redondance, fonctionnement maître/esclave.

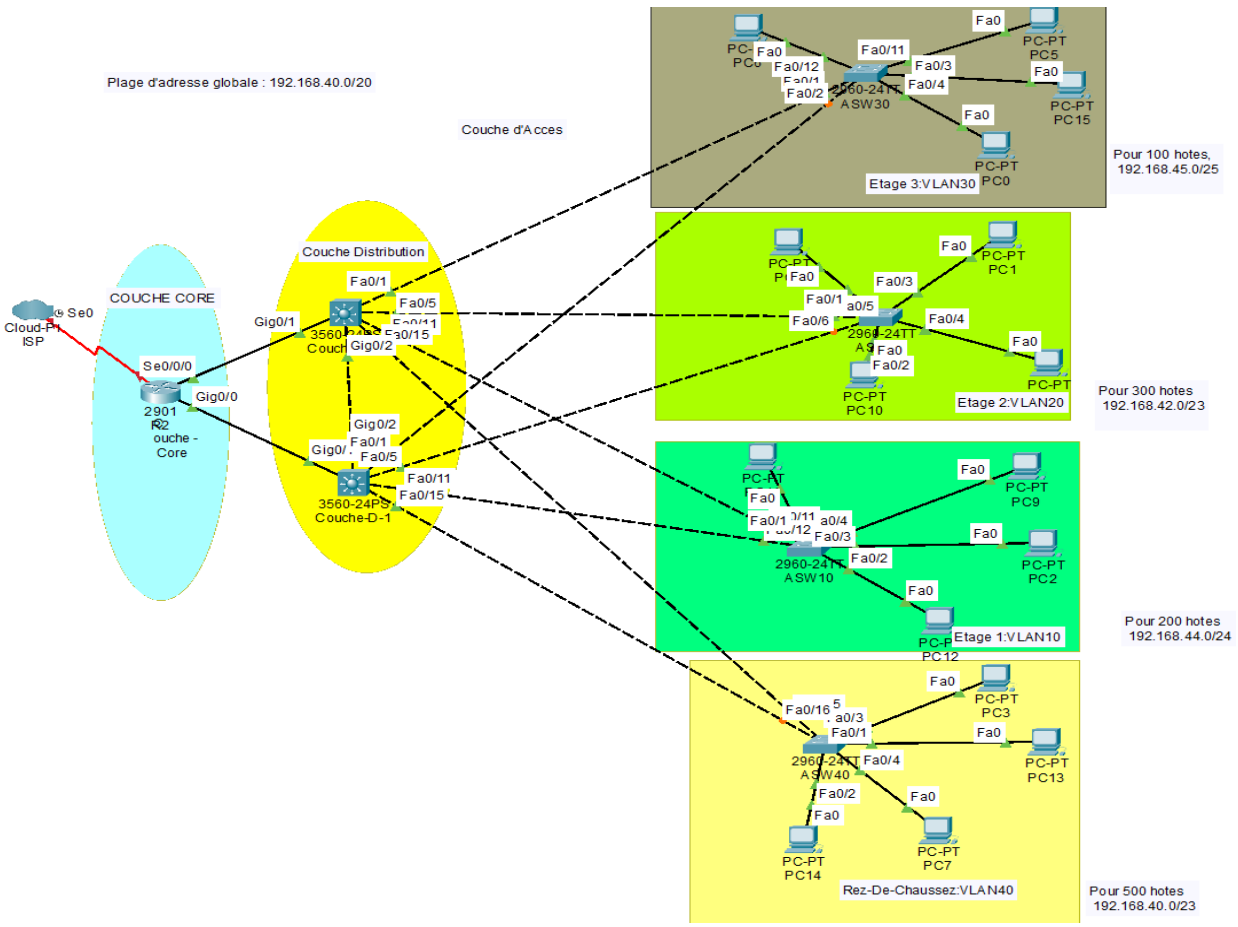
HSRP - protocole de redondance de passerelle par défaut, l'architecture du réseau hautement disponible, plus de détails dans la partie présentation.

d) Architecture de réseau (Topologie) et Tableau d'adressage IP.

Voici les adresses IP que nous avons choisies pour implémenter notre topologie avec 192.168.40.0/20

- VLAN 40: Rez-De-Chaussée pour 500 hôtes
- VLAN 10: Étage 1 pour 200 hôtes
- VLAN 20: Étage 2 pour 300 hôtes
- VLAN 30: Étage 3 : 100 hôtes
- Et enfin l'adresse de l'ISP :10.1.1.0/29
- Connexion LAN

Architecture du réseau



- **Plage d'adresses globale** : 192.168.40.0/20

Sachant que 500 + 300 + 200 + 100 = 1100 soit 2^{11} = 2048 adresses, alors elles seront réparties ainsi :

- Rez-De-Chaussez, Pour 500 hôtes, on a $2^9 – 2 = 512 – 2$, et pour 50 hôtes on a un masque de 32 – 9 = 23 ou 255.255.254.0, alors on aura 192.168.40.0/23.
- Étage 2, Pour 300 hôtes, on a $2^9 – 2 = 512 – 2$, et pour 300 hôtes on a un masque de 32 – 9 = 23 ou 255.255.254.0, alors on aura 192.168.42.0/23.
- Étage 1, Pour 200 hôtes, on a $2^8 – 2 = 256 – 2$, et pour 200 hôtes on a un masque de 32 – 8 = 24 ou 255.255.255.0, alors on aura 192.168.44.0/24.
- Étage 3, Pour 100 hôtes, on a $2^7 – 2 = 128 – 2$, et pour 100 hôtes on a un masque de 32 – 7 = 25 ou 255.255.255.128, alors on aura 192.168.45.0/25.
- Adresse pour les interfaces gigabit et fast Ethernet pour chaque routeur, Switches Layer-3, Switches et PCs.

- **Plan d'adressage IP par VLAN**

VLAN	Hôtes requis	Sous-réseau attribué	Masque
40	PC6	192.168.40.10	255.255.254.0
	PC4	192.168.40.11	255.255.254.0
	PC9	192.168.40.12	255.255.254.0
	PC	192.168.40.13	255.255.254.0
30	PC5	192.168.45.10	192.168.45.128
	PC1	192.168.45.11	192.168.45.128
	PC2	192.168.45.12	192.168.45.128
	PC3	192.168.45.13	192.168.45.128
20	PC0	192.168.42.10	255.255.254.0
	PC10	192.168.42.11	255.255.254.0
	PC2	192.168.42.12	255.255.254.0
	PC14	192.168.42.13	255.255.254.0
10	PC15	192.168.44.10	255.255.255.0
	PC8	192.168.44.11	255.255.255.0
	PC11	192.168.44.12	255.255.255.0
	PC13	192.168.44.12	255.255.255.0
WAN	Gig0/0	192.168.45.129	255.255.255.252
	Gig0/1	192.168.45.133	
Layer 3-1	Gig0/1	192.168.45.130	255.255.255.252
Layer 3-2	Gig0/1	192.168.45.134	255.255.255.252

3. Configuration générale PCs, VLAN et du routage OSPF

a) Création et configuration des VLAN (switchs), attribution des interfaces aux VLAN, inter-VLAN et OSPF (sur les routeurs).

- VLAN

```
Couche-D-1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/2
10   Etage1                           active
20   Etage2                           active
30   Etage3                           active
40   RC                               active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Couche-D-1#
```

- Exemple d'un cas de routage avec le protocole OSPF, on effectue un **show run** sous le suitche Layer-3(Couche-D- 1).

```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.45.128 0.0.0.3 area 0
 network 192.168.40.0 0.0.1.255 area 0
 network 192.168.42.0 0.0.1.255 area 0
 network 192.168.44.0 0.0.0.255 area 0
 network 192.168.45.0 0.0.0.127 area 0
!
```

b) Compatibilité avec des environnements spécifiques : AppleTalk, Banyan VINES et Novell IPX.

- Certains environnements anciens peuvent utiliser des protocoles comme AppleTalk, Banyan VINES ou Novell IPX. Étant désormais obsolètes, c'est-à-dire utilisés dans les années 1990 à 2000, ces protocoles la continuent de fonctionner même lorsque le routeur de secours devient le routeur actif, mais ils mettent un certain temps à s'adapter au changement de topologie. Lorsque le routeur actif devient indisponible, ou si sa connexion au réseau devient impraticable, toutes les sessions Banyan VINES qui reposent sur ce routeur sont arrêtées et doivent être réinitialisées.
- AppleTalk : Protocole Apple utilise dans les réseaux locaux (LAN)
- Novell IPX/SPX, était une alternative au TCP/IP utilisé par NetWare.

- Banyan VINES, protocole que les systèmes d'entreprises utilisaient autrefois.

c) Configuration des routeurs HSRP (Active, Standby, priorité), mise en place des timers et de la préemption.

```
Switche#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 10
Switch(config-if)#standby 10 ip 192.168.44.254
Switch(config-if)#standby 10 priority 110
Switch(config-if)#standby 10 preempt
Switch(config-if)#do wr
Building configuration...
[OK]
Switch(config-if)#
Switch#
```

4. Simulation d'une panne (désactivation du routeur actif).

a) **Procédure:** Pendant la présentation, on fait la déconnexion d'un câble dans la couche de distribution reliant la couche d'accès.

b) Observation du basculement (failover) vers le routeur standby.

Avec la commande péremption **preempt**, avec sous le suitche permet d'un routeur passif de prendre la relève après un certain temps.

5. Évaluation, bonnes pratiques et conclusion

a) Bonnes pratiques pour déployer HSRP en production (optimisation, sécurité).

- HSRP (Hot Standby Router Protocol), protocole de redondance propriété de Cisco garantissant la haute disponibilité au niveau de la passerelle par défaut (default gateway), la sécurité et la fiabilité d'un réseau. Ayant un routeur actif(master) et un autre routeur de secours(standby) avec une adresse IP virtuelle partagée.

- Bonne pratique d'optimisation, utilisant un mécanisme de priorité pour déterminer le routeur actif dans un groupe et le routeur actif avec la priorité la plus élevée. On doit configurer les priorités en fonction des capacités matérielles, de la puissance de traitement, de la mémoire et de la topologie réseau.
- Bonne pratique pour la sécurité, l'activation de l'authentification HSRP permet d'empêcher des appareils non autorisés de rejoindre le réseau utilisant le protocole HSRP, cela garantit que seuls les routeurs de confiance participent à HSRP. L'authentification MD5 fournit une méthode sécurisée pour rendre les messages authentiques "Key-string", utiliser des listes de contrôle d'accès (ACL) pour restreindre le trafic via HSRP aux appareils de confiance uniquement.

b) Limites et améliorations possibles (par exemple : comparaison avec VRRP ou GLBP).

- HSRP, bien que fiable pour la redondance de passerelle, présente des limites notables. En tant que protocole propriétaire Cisco, il manque d'interopérabilité dans les environnements multi-vendeurs. De plus, il ne permet qu'un seul routeur actif à la fois, sous-utilisant les ressources disponibles, et son temps de basculement par défaut (jusqu'à 10 secondes) peut être trop long pour les applications critiques. Contrairement à GLBP, HSRP ne prend pas en charge la répartition de charge, limitant son efficacité dans les architectures modernes. Pour y remédier, plusieurs améliorations sont envisageables : l'adoption de HSRPv2 pour un meilleur support IPv6, l'optimisation des timers (par exemple, standby 1 timers 1 3 pour un basculement plus rapide), ou encore l'intégration avec des protocoles de routage dynamique comme OSPF pour une résilience accrue.

c) Comparaison avec d'autres protocoles comme VRRP ou GLBP, et perspectives d'amélioration.

- En comparaison, VRRP se distingue par son statut de protocole ouvert, facilitant les déploiements multi-constructeurs, même s'il fonctionne également sur le principe d'un seul routeur maître. GLBP apporte une vraie valeur ajoutée grâce à sa capacité de répartition dynamique du trafic entre plusieurs routeurs actifs, optimisant ainsi l'utilisation des ressources et renforçant la tolérance aux pannes. Selon les objectifs, il peut donc être pertinent de privilégier VRRP dans des environnements hétérogènes ou de migrer vers GLBP pour bénéficier de la haute disponibilité et du load

balancing, tout en intégrant ces solutions à des infrastructures évolutives comme le SDN ou les environnements cloud.

Conclusion générale et perspectives.

- En synthèse, le choix entre HSRP, VRRP et GLBP dépend avant tout des exigences de redondance, de répartition de charge et d'interopérabilité propres à chaque organisation. Si HSRP demeure une solution fiable et simple à déployer dans des environnements Cisco homogènes, ses limites en matière de flexibilité et d'équilibrage de trafic peuvent constituer des freins dans des architectures plus avancées ou multi-constructeurs. À l'inverse, VRRP s'impose par son ouverture et sa compatibilité multi-vendeurs, tandis que GLBP se distingue par sa capacité à répartir efficacement la charge entre plusieurs passerelles.
- Pour répondre aux besoins critiques des réseaux modernes, l'intégration de protocoles ouverts, de solutions automatisées et de technologies virtualisées (comme SDN ou NFV) devient essentielle afin d'assurer une haute disponibilité, une gestion dynamique des basculements et une meilleure résilience face aux pannes. Les évolutions récentes tendent aussi vers l'adoption de protocoles évolutifs et l'utilisation de l'intelligence artificielle pour anticiper les défaillances et optimiser les performances réseau.
- En résumé, le choix de la solution de redondance doit être guidé par les impératifs techniques et stratégiques de l'entreprise, avec une préférence croissante pour les approches ouvertes, automatisées et évolutives, capables d'accompagner la transformation et la complexification des infrastructures réseau.

Références et bibliographie :

- Architecture de réseaux et études de cas Seconde édition ampus Press
- Cisco.Press.CCNA.Portable.Command.Guide.2nd.Edition.Jul.2007
- Mise en place du protocole HSRP | Cisco | IT-Connect
- Sécurité du protocole HSRP - FRAMEIP.COM
- https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html.