

BTS SIO2 LM ECOLE IRIS

**Mise en place d'une solution de redondance,
de tolérance et de panne et d'équilibrage de
charge pour les éléments d'interconnexion
de Niveau 2 et 3**

Contexte.....	2
1 - Minimisation de l'Interruption de Service.....	2
2 - Amélioration de la Continuité de Service en Cas de Panne.....	3
3 - Agrégation des Liens et Augmentation de la Bande Passante.....	3
4 - Équilibrage de Charge.....	3
Réflexion technique sur le projet.....	3
La Méthode manuelle : configuration de plusieurs passerelles.....	3
La Méthode automatique : le “routeur virtuel” FHRP (First Hop Redundancy Protocol).....	5
Avantages d’un routeur virtuel pour Stadium.....	6
Notre infrastructure.....	7
Mise en place de la solution.....	8
Méthode HSRP.....	8
Désigner R1-Stade en tant que routeur Actif.....	8
Désigner le routeur Passif.....	9
Méthode VRRP.....	10
Désignation du R1-Stade en tant que routeur Master.....	10
Désignation de R2-Stade en tant que routeur Backup.....	11
Méthode GLBP.....	11
Paramétrer l'équilibrage de charges (load balancing).....	11
Configuration GLBP sur R1-Stade.....	12
Configuration GLBP sur R2-Stade.....	13
Conclusion.....	15

Contexte

Pour Stadium, l'enjeu est de continuer à renforcer la robustesse et la flexibilité du réseau. En effet, Stadium ne peut pas se permettre de subir des interruptions de services ou des pannes sans solutions rapides et pérennes pour son infrastructure et les éléments d'interconnexion de niveau 2 et 3.

1 - Minimisation de l'Interruption de Service

Il est impératif de réduire au maximum la durée de toute interruption de service. Cela peut être réalisé en mettant en place des mécanismes de basculement rapide (failover) en cas de panne, de manière à ce que les services restent disponibles en permanence, même en cas de défaillance d'un composant.

2 - Amélioration de la Continuité de Service en cas de Panne

La solution devra être conçue de manière à améliorer la continuité des services existants en cas de défaillance, aussi bien au niveau des commutateurs que des liaisons d'accès fournies par les FAI. Cela pourrait impliquer la mise en place de chemins de secours, de configurations de basculement ou de redondance au niveau des équipements réseau.

3 - Agrégation des Liens et Augmentation de la Bande Passante

Une partie essentielle de cette mission consiste à agréger les liens entre les commutateurs pour augmenter la bande passante globale du réseau. Cela permettra de mieux gérer la charge de trafic et d'éviter les goulots d'étranglement. Des technologies telles que le trunking Ethernet (agrégation de liens) et le routage dynamique peuvent être envisagées.

4 - Équilibrage de Charge

Pour garantir une utilisation efficace des ressources réseau, il est nécessaire de mettre en place des mécanismes d'équilibrage de charge. Cela permet de répartir équitablement le trafic sur plusieurs liens, évitant ainsi la surcharge de certains équipements ou liaisons. L'utilisation d'un protocole de redondance de premier saut (routeur virtuel partagé) sera donc appliquée.

Réflexion technique sur le projet

La Méthode manuelle : configuration de plusieurs passerelles

Avec cette méthode, chaque poste ou serveur se voit attribuer plusieurs adresses de passerelles (la passerelle principale et une passerelle de secours).

Fonctionnement Actif/Passif

On définit une passerelle principale (actif) et une secondaire (passif) dans la configuration réseau des postes. Tout le trafic sort par la passerelle active. La passerelle passive prend le relais si la passerelle active devient injoignable. En cas de panne de la première, il faut soit une intervention manuelle, soit un paramétrage pour que la deuxième soit utilisée à son tour.

Exemple

Sur Windows, il est possible de saisir plusieurs “Default Gateways” avec des métriques différentes.

La passerelle dont la métrique est la plus basse est la première utilisée.

Si la passerelle active n’est plus disponible, le système détecte alors qu’elle ne répond plus aux paquets ARP ou ICMP, et le client va essayer la passerelle secondaire.

Inconvénients

La bascule reste peu fiable puisqu’il peut s’écouler un délai non négligeable avant que le poste ne détecte la panne et bascule réellement vers la passerelle secondaire, et même si certains outils tels que “Dead Gateway Detection” (sur Windows) existent, ils sont également plus ou moins lent et pas entièrement fiables.

Parfois, il arrive que même après le rétablissement de la passerelle primaire, le poste continue d’utiliser la passerelle secondaire.

Afin d’effectuer ce retour en arrière, aussi appelé “failback”, un redémarrage est nécessaire.

Pour forcer le basculement, il faut repasser sur chaque poste individuellement, ce qui devient rapidement complexe et chronophage dans des environnements plus développés comme ceux de Stadium.

Fonctionnement Actif/Actif :

Ici, on définit plusieurs adresses de passerelle sur chaque poste, mais on souhaite que les deux passerelles soient utilisées simultanément, ou en répartition de charge (load balancing). Ainsi, les flux sont partagés entre deux routeurs différents.

Exemple

Toujours via la table de routage du poste, on peut soit donner la même métrique à deux passerelles par défaut, soit configurer deux routes avec des règles de routage avancées.

Le système d’exploitation tente ensuite de répartir le trafic, parfois en alternant les paquets ou les sessions, selon ses algorithmes internes et le paramétrage indiqué.

Inconvénients

Les mécanismes de répartition de charge au niveau du poste (basés sur la table de routage) sont limités et peu prévisibles.

Le système peut décider d’envoyer tout le trafic par l’une des deux passerelles si elle répond plus rapidement, ou bien il peut le diviser de façon aléatoire. Il n’y a ni de contrôle précis ni d’affectation optimisée.

Si l'on sort par deux routeurs différents vers Internet, la source NAT des paquets peut changer selon le routeur utilisé.

Le risque ? Certains serveurs distants peuvent refuser la session si l'IP publique source change en cours de route. Contrairement à un protocole de redondance, il n'y a pas d'adresse IP "virtuelle" unique qui masquerait la complexité du routage en place.

Pour éviter ces désagréments, des protocoles plus sophistiqués sont mis en place (exemple : load balancing sur un routeur central).

Dans certains cas, si une passerelle tombe en panne, le basculement n'est pas toujours immédiat et crée des pertes de sessions en cours d'utilisation.

Les limites de l'utilisation de la méthode manuelle sont donc multiples

Intervention sur chaque poste : pour changer l'ordre de priorité ou basculer de la passerelle principale à la passerelle secondaire, il faut soit configurer manuellement chaque client, soit prévoir des scripts de bascule.

Risque d'incohérences : si tous les postes ne basculent pas de la même manière ou au même moment, on risque des problèmes de routage ou des pertes de connexion partielles.

Moins de réactivité : le failover n'est pas toujours automatique, ou s'il l'est, il dépend fortement de la configuration des systèmes d'exploitation clients (métriques de route). Cette approche est considérée comme lourde et peu robuste pour un réseau d'entreprise qui exige une haute disponibilité et une fiabilité réelle, sans intervention manuelle.

La Méthode automatique : le "routeur virtuel" FHRP (First Hop Redundancy Protocol)

FHRP répond à la problématique principale suivante : la passerelle par défaut est l'adresse IP du routeur que les postes utilisent pour communiquer avec l'extérieur de leur sous-réseau. Si cette passerelle devient inaccessible (panne du routeur, coupure réseau, etc...), tous les postes du réseau perdront leur accès au reste du LAN/WAN et à Internet.

En instaurant une solution de redondance fiable comme FHRP, nous évitons les interruptions de service réseau lorsque le routeur principal n'est plus disponible, permettant d'assurer la continuité de la connexion et une haute disponibilité pour les utilisateurs et les applications critiques de Stadium.

Au lieu de forcer chaque machine à gérer plusieurs passerelles selon la méthode manuelle, nous déployons ici le protocole FHRP. C'est une catégorie de protocoles qui

assurent la redondance de la passerelle par défaut pour les hôtes d'un réseau (permet d'avoir une « passerelle virtuelle » qui bascule automatiquement d'un routeur à un autre) en un laps de temps réduit.

Ce protocole contient 3 solutions principales :

1. **HSRP (Hot Standby Router Protocol)** → Protocole propriétaire Cisco (actif/passif).
2. **VRRP (Virtual Router Redundancy Protocol)** – Standard ouvert (similaire à HSRP, actif/passif).
3. **GLBP (Gateway Load Balancing Protocol)** – Protocole propriétaire Cisco, permet du load balancing (actif/actif).

Quel que soit le protocole utilisé, l'idée reste la même :

- Les deux routeurs physiques se partagent une adresse IP et MAC virtuelle.
- Du point de vue des postes, la passerelle par défaut est cette IP virtuelle unique.
- Les routeurs échangent entre eux des messages de supervision pour déterminer qui est le « routeur actif », c'est-à-dire celui qui transfère réellement le trafic, et qui est le « routeur de secours », qui prend la relève automatiquement en cas de panne de l'actif.
- En cas de panne du routeur actif, le routeur de secours « devient » la passerelle par défaut (en récupérant l'adresse IP virtuelle), et cela sans aucun impact sur la configuration client.

Le fonctionnement Actif/Passif (ex. HSRP ou VRRP) :

Un routeur est actif, l'autre attend. En cas de coupure, le passif prend la main.

Simple à configurer et très fiable.

Le fonctionnement Actif/Actif (ex. GLBP) :

Tous les routeurs participent au routage, avec partage de charge possible ! On profite de la bande passante de plusieurs routeurs mais la mise en place est plus complexe.

Avantages d'un routeur virtuel pour Stadium

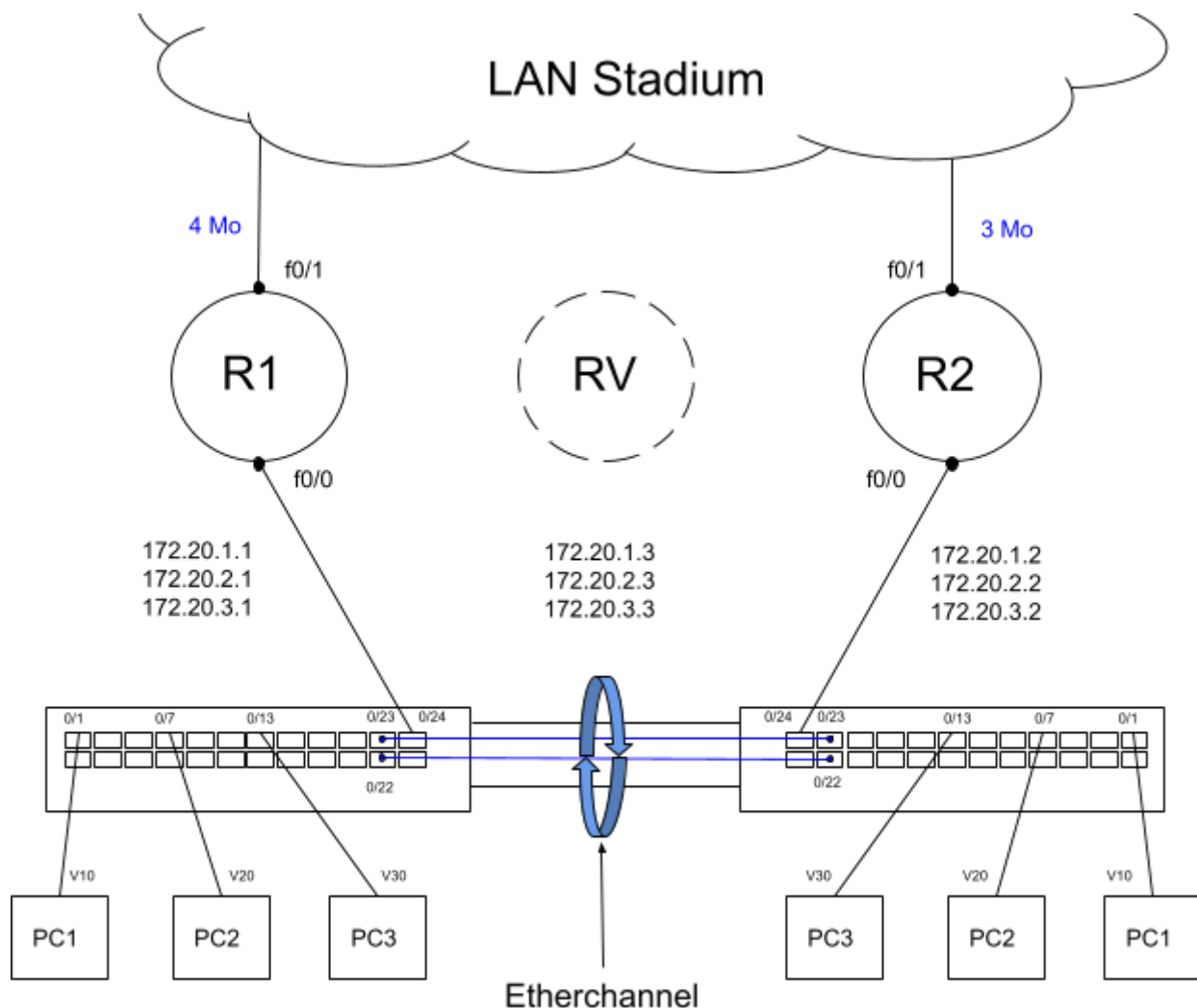
La pertinence d'utiliser un routeur virtuel dans un environnement comme Stadium est multiple. La disponibilité du réseau est critique (événements, billetterie, caméras IP, WiFi, etc...), le nombre d'utilisateurs et de services est conséquent, et la gestion des configurations doit être rapide, flexible et évolutive.

1. Cette solution garantit une continuité de service, car en cas de panne d'un routeur le service n'est pas interrompu et la bascule est automatique. En effet, le failover et le failback sont entièrement gérés par le protocole de redondance.

2. Les utilisateurs bénéficient d'une transparence totale et l'administration pour les équipes informatiques est facilitée, car l'adresse de passerelle par défaut ne change jamais et aucune intervention n'est requise côté client. Cette souplesse d'administration facilite le suivi des routeurs, qui est automatisé, avec une configuration centralisée.
3. Cette approche est standardisée et évolutive : HSRP/VRRP/GLBP sont des protocoles éprouvés et documentés, faciles à intégrer dans une infrastructure Cisco ou multi-constructeurs.

C'est pourquoi la mise en place d'un « routeur virtuel » entre deux routeurs physiques doit être priorisée pour répondre efficacement aux contraintes de haute disponibilité et de sécurité demandées par Stadium.

Notre infrastructure



Les adresses réseau des VLANs et les interfaces routeurs

V1 : 172.20.1.0 /24 R1 → 1.1 R3 → 1.3 R2 → 1.2
V2 : 172.20.2.0 /24 R1 → 2.1 R3 → 2.3 R2 → 2.2
V3 : 172.20.3.0 :24 R1 → 3.1 R3 → 3.3 R2 → 3.2

Mise en place de la solution

Avec notre configuration actuelle, nous devons choisir une seule des trois solutions envisagées : HSRP, VRRP ou GLBP. Chacune répond aux enjeux de redondance et de continuité de service, mais leur fonctionnement diffère en termes de gestion des basculements et d'optimisation du trafic.

L'enjeu est délectionner la solution la plus adaptée aux besoins techniques de Stadium, où la disponibilité du réseau est primordiale. Une infrastructure de cette envergure doit assurer une transition fluide en cas de panne, tout en évitant les goulots d'étranglement qui pourraient impacter la billetterie, la vidéosurveillance et l'accès WiFi... L'utilisation d'un protocole de redondance est indispensable pour garantir une stabilité et une évolutivité optimales.

Nous avons donc mis en place et testé les trois solutions afin d'évaluer leur efficacité dans notre environnement.

HSRP et VRRP offrent un basculement efficace en mode actif/passif, assurant une prise en charge immédiate des pannes. Néanmoins, dans une infrastructure nécessitant une gestion intelligente des flux et une optimisation des ressources, GLBP s'est imposé comme le choix le plus pertinent. Grâce à son réel équilibrage de charge et sa capacité à exploiter simultanément plusieurs routeurs, il permet une meilleure répartition du trafic et une continuité de service optimisée.

En adoptant GLBP, nous garantissons non seulement une résilience accrue, mais aussi une réduction des points de saturation, tout en facilitant la maintenance et l'administration du réseau.

Ce choix s'inscrit dans une démarche d'optimisation à long terme, répondant aux exigences de performance et de fiabilité imposées par l'infrastructure de Stadium.

Méthode HSRP

Nous allons maintenant tester la mise en place de la méthode HSRP en tant que protocole propriétaire Cisco, pour activer la redondance de passerelle par défaut sur le réseau

Désigner R1-Stade en tant que routeur Actif

#interface fastEthernet 0/0.10 → Sélectionner l'interface

#encapsulation dot1Q 10 → Indique le taggage

#ip address 172.20.1.1 255.255.255.0 → indique la passerelle vlan de R1 + le masque

#standby 10 ip 172.20.1.3 → Affecte un VLAN sur l'interface virtuelle du routeur

#standby 10 priority 150 → Indique une priorité plus élevée

#standby 10 preempt → Autorise R1 à reprendre le rôle s'il redevient disponible

#exit

```
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.20.1.1 255.255.255.0
R1(config-subif)#standby 10 ip 172.20.1.3
R1(config-subif)#standby 10 priority 150
R1(config-subif)#standby 10 preempt
```

#interface fastEthernet 0/0.20

#encapsulation dot1Q 20

#ip address 172.20.2.1 255.255.255.0

#standby 20 ip 172.20.2.3

#standby 20 priority 150

#standby 20 preempt

#exit

```
R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 172.20.2.1 255.255.255.0
R1(config-subif)#standby 20 ip 172.20.2.3
R1(config-subif)#standby 20 priority 150
R1(config-subif)#standby 20 preempt
```

#interface fastEthernet 0/0.30

#encapsulation dot1Q 30

#ip address 172.20.3.1 255.255.255.128

#standby 30 ip 172.20.3.3

#standby 30 priority 150

#standby 30 preempt

#exit

```
R1(config)#interface fastEthernet 0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.20.3.1 255.255.255.128
R1(config-subif)#standby 30 ip 172.20.3.3
R1(config-subif)#standby 30 priority 150
R1(config-subif)#standby 30 preempt
```

Désigner le routeur Passif

On ne précise pas de priorité qui reste celle par défaut (100)

#interface fastEthernet 0/1.10

#encapsulation dot1Q 10

#ip address 172.20.1.2 255.255.255.0

#standby 10 ip 172.20.1.3

```
R2(config)#interface fastEthernet 0/0.10
R2(config-subif)#encapsulation dot1Q 10
R2(config-subif)#ip address 172.20.1.2 255.255.255.0
R2(config-subif)#standby 10 ip 172.20.1.3
```

#interface fastEthernet 0/1.20

#encapsulation dot1Q 20

#ip address 172.20.2.2 255.255.255.0

#standby 20 ip 172.20.2.3

#interface fastEthernet 0/0.30

#encapsulation dot1Q 30

#ip address 172.20.3.2 255.255.255.128

#standby 30 ip 172.20.3.3

#exit

Méthode VRRP

Il est également possible de mettre en place la méthode VRRP en tant que protocole standard qui assure de la même manière la redondance de passerelle.

Il suffit de remplacer la commande standby (HSRP) par la commande VRRP :

Désignation du R1-Stade en tant que routeur Master

```
#interface fastEthernet 0/0.10
#encapsulation dot1Q 10
#ip address 172.20.1.1 255.255.255.0
#vrrp 10 ip 172.20.1.3
#vrrp 10 priority 150
#vrrp 10 preempt
#exit
#interface fastEthernet 0/0.20
#encapsulation dot1Q 20
#ip address 172.20.2.1 255.255.255.0
#vrrp 20 ip 172.20.2.3
#vrrp 20 priority 150
#vrrp 20 preempt
#exit
#interface fastEthernet 0/0.30
#encapsulation dot1Q 30
#ip address 172.20.3.1 255.255.255.128
#vrrp 30 ip 172.20.3.3
#vrrp 30 priority 150
#vrrp 30 preempt
#exit
```

Désignation de R2-Stade en tant que routeur Backup

On ne précise pas de priorité qui reste celle par défaut (100)

```
#interface fastEthernet 0/0.10
#encapsulation dot1Q 10
#ip address 172.20.1.2 255.255.255.0
#vrrp 10 ip 172.20.1.3
#exit
#interface fastEthernet 0/0.20
#encapsulation dot1Q 20
#ip address 172.20.2.2 255.255.255.0
#vrrp 20 ip 172.20.2.3
#exit
#interface fastEthernet 0/0.30
#encapsulation dot1Q 30
#ip address 172.20.3.2 255.255.255.128
#vrrp 30 ip 172.20.3.3
#exit
```

Méthode GLBP

Contrairement à HSRP et VRRP qui ont un routeur actif et un routeur en attente, GLBP a l'avantage de permettre la répartition de charge (*load balancing*) sur plusieurs routeurs en partageant la passerelle par défaut.

Pour mettre en place **GLBP** à la place de HSRP ou VRRP, il suffit de changer les commandes **standby** ou **vrrp** par les commandes **glbp**.

Le principe est similaire : on définit un **groupe** et on attribue **une IP virtuelle** sur chaque sous-interface.

Paramétrer l'équilibrage de charges (load balancing)

Il existe 3 modes d'équilibrage de charge : round-robin, host-based et weighted.

Par défaut, c'est le mode round-robin qui est activé, mais il est possible d'imposer un mode, en utilisant la commande suivante :

```
#glbp <num_groupe> load-balancing [round-robin / host-based / weighted]
```

Le mode round-robin

Par défaut, GLBP est paramétré pour faire un round-robin entre les routeurs, pour distribuer la passerelle ARP aux clients afin d'assurer un certain équilibrage de charge. Cet algorithme de répartition induit qu'à chaque nouvelle requête ARP (d'un nouveau PC qui cherche l'adresse MAC du routeur virtuel), GLBP va donner la MAC virtuelle du Routeur1, puis la prochaine fois du Routeur2, puis R1, en alternance. L'adresse MAC virtuelle indiquée au PC est changeante afin d'adapter le trafic en temps réel, toujours selon la configuration de répartition de charge définie en amont.

Ce mode est utile dans un environnement où chaque machine client peut envoyer son trafic par n'importe quel routeur, garantissant une répartition automatique de la charge.

Si la table ARP expire (après un certain temps défini par l'OS ou si forcé par un administrateur), si le PC est redémarré et refait une requête ARP, si le routeur actuellement utilisé tombe en panne, alors ce mode réattribuera une nouvelle MAC qui sera soit celle de R1, soit celle de R2.

Le mode host-based

Dans ce mode, chaque host se voit systématiquement attribuer la même adresse MAC virtuelle. Ainsi, un PC qui reçoit l'adresse MAC de R1 utilisera toujours cette adresse pour le routage, même après redémarrage, expiration de la table ARP. Le seul cas où

l'adresse MAC change, c'est lors d'une panne du routeur de référence. On peut paramétrer des VLANs spécifiquement sur une passerelle, pour les rediriger sur un seul routeur. Ce fonctionnement reste pertinent dans un contexte où la gestion efficace des ressources réseau est primordiale, en répartissant le trafic entre les routeurs, avec un fort besoin de prévisibilité du réseau.

Le mode weighted : Indication poid de distribution

Le mode weighted dans GLBP permet d'attribuer un poids spécifique à chaque routeur afin d'ajuster la répartition du trafic en fonction de leur capacité ou de leur priorité. Contrairement aux modes round-robin et host-based, qui distribuent les requêtes de manière égale ou fixe, ce mode offre une approche plus granulaire et optimisée en fonction des besoins du réseau.

Chaque routeur se voit attribuer un poids (weighting) qui influence la quantité de trafic qu'il prendra en charge. Plus un routeur a un poids élevé, plus il recevra de requêtes ARP et donc plus de charge réseau. GLBP calcule ensuite la répartition du trafic selon une proportion basée sur ces poids, et ajuste sa répartition au prorata de la capacité restante de chaque routeur, en temps réel.

Configuration GLBP sur R1-Stade

Il est par exemple possible d'attribuer le poids de **150 à R1** et le poids **100 à R2**.

Ainsi, par équivalence, R1 va recevoir 60% du trafic, et R2 recevra 40% du :

```
#interface fastEthernet 0/0.10
#encapsulation dot1Q 10
#ip address 172.20.1.1 255.255.255.0
#glbp 10 ip 172.20.1.3 → Indique l'IP virtuelle GLBP du routeur virtuel
#glbp 10 priority 150 → Indique la priorité plus élevée (Active Virtual Gateway Router)
#glbp 10 preempt → Autorise R1 à reprendre le rôle s'il revient en ligne
#glbp 10 weighting 150 → Indique la pondération du routeur
#glbp 10 load-balancing weighted → Active le mode d'équilibrage de charge
#exit
#interface fastEthernet 0/0.20
#encapsulation dot1Q 20
#ip address 172.20.2.1 255.255.255.0
#glbp 20 ip 172.20.2.3
#glbp 20 priority 150
#glbp 20 preempt
```

```
#glbp 20 weighting 150
#glbp 20 load-balancing weighted
#exit
#interface fastEthernet 0/0.30
#encapsulation dot1Q 30
#ip address 172.20.3.1 255.255.255.128
#glbp 30 ip 172.20.3.3
#glbp 30 priority 150
#glbp 30 preempt
#glbp 30 weighting 150
#glbp 30 load-balancing weighted
#exit
```

Configuration GLBP sur R2-Stade

Sur le R2, il faut mettre la même configuration GLBP, avec les mêmes numéros de groupe et la même IP virtuelle, mais l'IP "physique" du routeur R2 est différente. La pondération est moindre, pour 40% de charge de trafic maximale sur R2 :

```
#interface fastEthernet 0/0.10
#encapsulation dot1Q 10
#ip address 172.20.1.2 255.255.255.0
#glbp 10 ip 172.20.1.3
#glbp 10 priority 100
#glbp 10 preempt
#glbp 10 weighting 100
#glbp 10 load-balancing weighted
#exit
#interface fastEthernet 0/0.20
#encapsulation dot1Q 20
#ip address 172.20.2.2 255.255.255.0
#glbp 20 ip 172.20.2.3
#glbp 20 priority 100
#glbp 20 preempt
#glbp 20 weighting 100
#glbp 20 load-balancing weighted
#exit
#interface fastEthernet 0/0.30
#encapsulation dot1Q 30
#ip address 172.20.3.2 255.255.255.128
```

```
#glbp 30 ip 172.20.3.3
#glbp 30 priority 100
#glbp 30 preempt
#glbp 30 weighting 100
#glbp 30 load-balancing weighted
#exit
```

Il n'est pas techniquement nécessaire de préciser la **priority 100** et le **weighting 100**, puisqu'il utilise déjà les valeurs par défaut ou s'aligne sur le mode de load-balancing choisi, mais nous choisissons de le spécifier pour des raisons de documentation.

Précisions : Dans notre architecture, GLBP attribue une seule adresse IP virtuelle partagée entre plusieurs routeurs. Cette IP virtuelle est associée à plusieurs adresses MAC, chacune attribuée dynamiquement à un routeur en fonction du mode d'équilibrage de charge choisi (round-robin, host-based ou weighted).

→ Contrairement à HSRP et VRRP, où un seul routeur actif possède l'adresse IP virtuelle et la MAC associée, GLBP permet à plusieurs routeurs d'avoir des adresses MAC différentes pour la même IP virtuelle, ce qui optimise la distribution du trafic.

→ Sur R2, la même configuration GLBP doit être appliquée avec les mêmes numéros de groupe et la même IP virtuelle, mais avec une adresse IP physique différente pour R2 (ex. 172.20.1.2). Cela permet à GLBP de gérer intelligemment la répartition de charge sans conflit d'adresses.

Différence entre le suivi HSRP et la supervision GLBP/VRRP

HSRP utilise le "tracking" (suivi des interfaces et routes) et peut surveiller l'état d'une interface spécifique ou d'une route (via object tracking) pour modifier les priorités et forcer une bascule en cas de problème.

Si un lien critique tombe en panne, le routeur HSRP ajuste sa priorité, permettant à un autre routeur de devenir actif. Par exemple, si un lien vers l'Internet principal tombe, HSRP détecte cette panne et bascule automatiquement vers un routeur de secours.

GLBP et VRRP utilisent plutôt la "supervision de ports" : au lieu de suivre des routes ou des interfaces spécifiques, ces protocoles vérifient l'état général des routeurs en

échangeant des messages réguliers. En cas d'inaccessibilité d'un routeur, la bascule s'effectue sans intervention manuelle.

Différence clé avec HSRP : Ils ne modifient pas la priorité en fonction de l'état d'un lien spécifique, mais détectent directement si un routeur est toujours fonctionnel ou non.

Explication de l'etherchannel :

L'EtherChannel est une technologie d'agrégation de liens qui permet de regrouper plusieurs interfaces physiques en une seule interface logique appelée Port-Channel. Cette approche permet d'augmenter la bande passante, d'assurer une meilleure tolérance aux pannes et d'optimiser la gestion du trafic réseau.

GLBP s'occupe de la redondance de la passerelle, mais au niveau du lien entre les switches, c'est l'EtherChannel qui garantit une connexion plus performante et résiliente.

Comment ?

→ En augmentant la capacité du lien : Plusieurs interfaces sont agrégées pour former un lien unique avec une bande passante cumulée (ex. 2 interfaces de 1 Gb = 2 Gb/s)

→ En réduisant les risques de boucles : L'agrégation est vue comme un seul lien logique, évitant les problèmes avec STP (Spanning Tree Protocol).

→ En améliorant la redondance : Si une interface tombe, le trafic continue de passer par les autres sans interruption.

Sur le 1er switch :

#interface range fa 0/22 - 23 → Sélectionne les interfaces 22 et 23

#channel-group 1 mode auto → indique le mode auto, signifiant que les ports attendent une demande d'agrégation initiée par le mode désirable du switch client

#interface port-channel 1 → entre dans la configuration de l'interface logique port-channel 1

#switchport mode trunk → Indique le mode trunk pour toutes les interfaces physiques membre du port-channel 1

Sur le 2ème switch :

#interface range fa 0/22 - 23 → Sélectionne à nouveau les interfaces

#channel-group 1 mode desirable → Le mode desirable indique que les ports initient la négociation avec le switch serveur configuré en mode auto

#interface port-channel 1 → entre dans la configuration de l'interface logique port-channel 1

#switchport mode trunk → indique le mode trunk pour toutes les interfaces physiques membre du port-channel 1

#show interface port-channel 1 trunk → Afficher l'état des interfaces port-channel

Pour les ports destinés à être agrégés, ils doivent posséder les mêmes caractéristiques. Le même débit (Gb avec Gb et fa avec fa) car deux capacités de débits différents (Gb et fa) ne fonctionnent pas, le même mode duplex et bien sûr le même mode d'accès.

Une fois l'EtherChannel configuré, il est essentiel de vérifier son bon fonctionnement avec les commandes suivantes :

#show interface port-channel 1 trunk → Vérifier que l'interface logique est bien active

#show ip interface brief → Lister les interfaces actives et vérifier leur état

#show ip nat translation → Vérifier les traductions NAT

#show ip route → Vérifier que les routes sont correctement propagées et que l'agrégation ne cause pas de conflits.

Si un lien tombe, l'EtherChannel continue de fonctionner, mais avec une bande passante réduite.

Conclusion

Dans un environnement où la disponibilité réseau est non négociable, le choix du protocole de redondance ne peut pas se faire à la légère. HSRP et VRRP restent des solutions viables pour des besoins plus simples, mais ils se limitent à une logique actif/passif qui ne tire pas pleinement parti des ressources disponibles.

En optant pour GLBP, nous avons privilégié une approche plus moderne, efficace et évolutive, garantissant une continuité de service optimale tout en maximisant l'utilisation des équipements réseau.

L'EtherChannel avec PAgP est une solution efficace pour regrouper plusieurs interfaces réseau et garantir une bande passante plus élevée et une redondance accrue. Il s'intègre parfaitement avec les protocoles de redondance comme GLBP, HSRP ou VRRP, permettant d'optimiser les performances et la résilience du réseau. PAgP en mode Auto/Désirable permet une configuration flexible et sécurisée, pour une agrégation automatique des liens sans intervention manuelle sur chaque interface.

Ces différentes solutions apportent un équilibre parfait entre performance, fiabilité et flexibilité, répondant aux exigences de Stadium company et à ses impératifs de résilience et de fluidité du trafic.