MISSION 4 : REDONDANCE AU NIVEAU DES ÉLÉMENTS D'INTERCONNEXIONS RÉSEAUX

I-) Contexte

a) Presentation de stadium company

Stadium Company est une société qui s'occupe de la gestion des stades , qui souhaite moderniser l'infrastructure réseau de son stade , la rendre scalable au fur et à mesure que ses ambitions augmentent . Elle emploie 170 personnes à plein temps et 80 à temps partiels . Elle projette ajouter des fonctions haute technologie afin de pouvoir prendre en charge l'organisation des concerts . La direction de Stadium Company n'étant pas compétente en matière d'Infrastructure réseau décide de faire appel à une entreprise de consultants réseaux qui s'en occupera de la conception à la mise en oeuvre en passant par la gestion du projet . Il sera mis en oeuvre en trois phases à savoir :

- La planification du projet et la préparation de la conception réseau haut niveau
- Le développement de la conception reseau détaillée
- La mise en oeuvre de la conception

b) Presentation NetworkingCompany

Le prestataire désigné pour l'exécution de ce projet est la société Networking Company, une firme locale spécialisée dans la conception d'infrastructure réseau et le conseil . C'est une société Cisco Premier Partner qui emploie 20 ingénieurs réseaux certifiés et expérimentée dans ce secteur.

Dans le but de concevoir le nouveau plan de l'infrastructure de haut niveau , Networking Company a décrit un profil de l'organisation et des installations sur la base des études menées par ses experts notamment en interrogeant le personnel.

Mission 4 :

Solution permettant la redondance des services, la tolérance de panne et l'équilibrage des charges des éléments d'interconnexions de niveau 2 et 3.

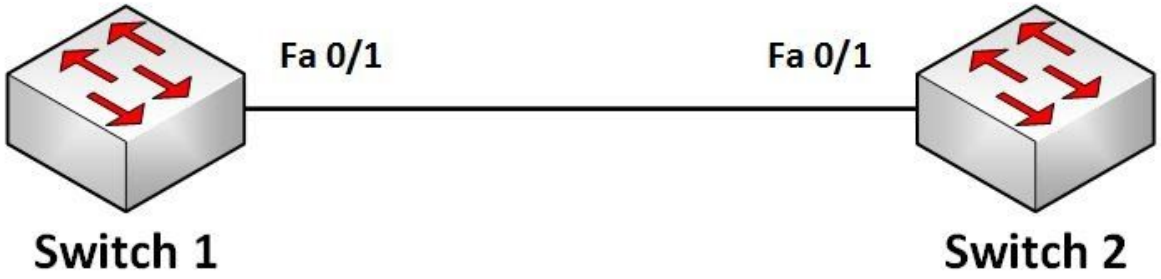
- La durée de l'interruption de service doit être minimale
- Solution permettant d'améliorer la continuité de service des services existants en cas de panne de Commutateurs et liaisons d'accès (FAI)
- Agrégation des liens entre les commutateurs et augmentation de la bande passante.

I- Test et comparaison de solution :

La redondance est un procédé utilisé dans le cas de matériels informatique dédoublés, permettant au deuxième de prendre la place du premier en cas de panne. Le composant de secours identique prend le relais automatiquement assurant ainsi la continuité des services indispensable au fonctionnement de l'entreprise.

Au niveau de la couche 2 : Etherchannel

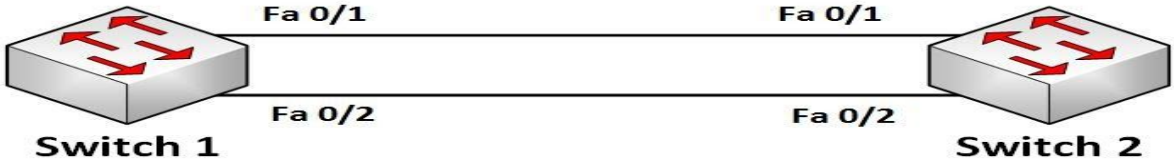
Etherchannel est une technique permettant l'agrégation de lien. Il est souvent utilisé pour augmenter la bande passante entre deux switchs. Nous allons voir comment ce protocole fonctionne, puis comment le mettre en place.



Nous avons ici des switchs avec des ports 100 Mbps. Il y a un lien entre les switch. Ces derniers pourront donc communiquer à une vitesse de 100 Mbps. Pour bénéficier d'une meilleure bande passante, nous pouvons faire une agrégation de lien.

Utilité de l'Etherchannel

Comme dit plus haut l'Etherchannel consiste en une agrégation de lien.Le principe est simple. Il s'agit de combiner plusieurs liens pour obtenir un lien virtuel de meilleure capacité. Pour bénéficier d'une meilleure bande passante, nous pouvons faire une agrégation de lien qui donnera alors une topologie de ce type :



Sans aucune configuration, Spanning Tree se chargerait de désactiver l'un des liens.En configurant l'Etherchannel, les deux switchs ne verront plus qu'un seul lien virtuel.Ce lien virtuel aura une capacité de 200 Mbps.Il peut regrouper jusqu'a 8 liens . Il facilite la redondance , ainsi si l'un des liens tombe , les autres seront toujours là pour assurer la connectivité. La bande passante sera simplement réduite.

Spanning tree

La redondance de niveau 2 (Ethernet) appelé SPANNING TREE (STP) permettant de mettre en oeuvre des réseaux LAN sécurisés. Le constructeur active le protocole Spanning Tree par défaut car s'il existe une boucle dans le réseau et que Spanning Tree n'est pas activé il y a un risque de tempête de broadcast. Le protocole Spanning Tree fait en sorte de supprimer les boucles pour éviter cela.

Link aggregation avec Etherchannel :

Un EtherChannel permet d'agréger de 1 à 8 ports physiques, il y a la possibilité de modifier la méthode de load-balancing sur ces ports. Un EtherChannel peut être de niveau 2 ou niveau 3, de protocole standard LACP (Link Aggregation ControlProtocol) IEEE 802.3ad, propriétaire Cisco PAgP (Port Aggregation Protocol) ou forcé. Les ports doivent avoir le même duplex, speed et VLAN information .Attention, en fonction des modèles de switchs/IOS/protocole, un etherchannel sur des ports des switchs différent.

Link Aggregation Control Protocol (LACP)

LACP est un protocole standardisé par l'IEEE dans sa norme 802.3ad et est implémenté par différents constructeurs. Il fournit un mécanisme permettant de contrôler le groupement de plusieurs ports physiques en un canal logique de communication.

Le principe de fonctionnement consiste à émettre des paquets LACP vers l'équipement partenaire, directement connecté et configuré pour utiliser LACP. Le mécanisme LACP va permettre d'identifier si l'équipement en face prend LACP en charge, et groupera les ports configurés de manière similaire (vitesse, mode duplex, VLAN, trunk de vlan, etc.)

Un équipement configuré pour utiliser LACP peut fonctionner en deux modes :

- *passif* : l'équipement n'initiera pas de négociation LACP. Il répondra uniquement aux sollicitations des équipements « partenaires »,correspond au mode Auto de PAGP : création d'une agrégation si le port en face est en Active.
- *actif* : l'équipement initiera les négociations LACP , correspond au mode Desirable de PAGP : création d'une agrégation si le port d'en face est en Passive ou Active.

Port Aggregation Protocol (PAgP)

PAgP est un protocole propriétaire Cisco, de ce fait disponible sur les commutateurs Cisco ainsi que sur les équipements disposant de la licence adéquate. Son utilisation permet de faciliter et d'automatiser la configuration des agrégats de liens (EtherChannel chez Cisco) en échangeant les informations nécessaires entre les ports Ethernet, à la manière de LACP.

Un équipement configuré pour utiliser PAgP peut fonctionner en deux modes :

- *auto* : négociation passive avec le second équipement , si nous ne voulons pas utiliser de protocole de négociation, le port devra être mis en mode ON, pour forcer l'agrégation de lien.
- *desirable* : négociation active avec le second équipement ,demande avec le switch d'en face pour créer l'agrégation
- **On** : sert à déclarer une agrégation active

Avec PAGP, si le port est en mode Auto, une agrégation de lien sera créée si le port d'en face est en mode Desirable. Si le port d'en face est en mode Auto, aucune agrégation n'est créée.

Si le port est configuré en mode Desirable, une agrégation sera créée à condition que le port d'en face soit en mode Auto ou Desirable.

Attention, il n'est pas possible d'avoir un port en mode ON d'un côté, et d'utiliser un protocole de négociation (PAGP ou LACP) de l'autre côté d'une agrégation.

A partir du moment où nous utilisons le mode ON pour créer une agrégation de lien, aucun protocole de négociation ne sera utilisé. Les ports en face devront donc être en mode ON eux aussi.

Il conviendra donc de choisir un protocole de négociation (de préférence LACP car il est standard) puis de choisir le mode des ports.

Par sécurité, le mieux est d'utiliser le mode Desirable (ou Active) des deux côtés.

Il est aussi tout à fait possible de se passer de protocole de négociation, en utilisant le mode ON.

Attention, en cas de mauvaise configuration, cela peut parfois mener à des boucles réseau, que même Spanning Tree ne pourra empêcher.

Le mode ON est donc à utiliser avec précaution.

STP vs RSTP :

- **Le Spanning Tree Protocol (STP)**

L'algorithme original de Spanning Tree a été écrit par Radia Perlman alors employée par Digital Equipment Corporation, il est nommé DEC STP. En 1990, l'IEEE publié le premier standard 802.1D basé sur le travail de Perlman. Les ports des commutateurs où STP est actif sont dans l'un des états suivants :

Listening : le commutateur « écoute » les BPDU et détermine la topologie réseau.

Learning : le commutateur construit une table faisant correspondre les adresses

MAC aux numéros des ports.

Forwarding : un port reçoit et envoie des données, opération normale.

Blocking : un port provoquant une boucle, aucune donnée n'est envoyée ou reçue

mais le port peut passer en mode forwarding si un autre lien tombe.

Disabled : désactivé, un administrateur peut manuellement désactiver un port s'il le

souhaite.

Le délai de transition entre les modes Listening vers Learning et Learning vers Forwarding est nommé forward delay, il est fixé par le root bridge et vaut 15 secondes par défaut.

Quand un client tel qu'un ordinateur, une imprimante ou un serveur est connecté au réseau, son port se mettra automatiquement d'abord en mode listening puis en mode learning, avant de se mettre en mode forwarding.

- **Le Rapide Spanning Tree Protocol (RSTP)**

Le Rapid Spanning Tree Protocol (RSTP) :

En 1998, l'IEEE publie le document 802.1w qui accélère la convergence du protocole STP après un changement de topologie. Il est inclus dans standard IEEE 802.1D-2004. Tandis que le STP classique peut prendre de 30 à 50 secondes pour converger après un changement de topologie,RSTP est capable de converger en 3 fois la valeur du délai Hello (6 secondes par défaut)

États des ports RSTP :

Root : le port vers le root bridge.

Designated : le port qui transmet les trames sur un segment.

Alternate : un port distinct du root port vers le root bridge.

Backup : un autre port vers un segment connecté au pont.

Le fonctionnement général de RSTP est semblable à celui du STP classique. Les

différences sont les suivantes :

-une défaillance du root bridge est détectée en 3 délais hello, c'est-à-dire 6 secondes avec les valeurs par défaut,
-les portes qui ne sont pas connectées à d'autres commutateurs (edge ports) peuvent basculer immédiatement dans l'état forwarding.
-RSTP continue à observer l'arrivée de BPDU sur ces portes pour s'assurer qu'aucune boucle n'est possible.
-Si un BPDU est observé, la porte bascule dans le statut non edge.
-Contrairement au STP classique, RSTP réagit aux annonces BPDU qui proviennent du root bridge.
-Un bridge RSTP diffuse son information RSTP sur ses designated ports.
-Si un bridge reçoit un BPDU indiquant un meilleur root bridge, il place tous les autres ports dans l'état Discarding et informe ce bridge de ce qu'il est le meilleur chemin vers le root.
-En recevant cette information, celui-ci peut faire transiter le port vers ce bridge immédiatement dans l'état Forwarding sans passer par les états Listening et Learning, puisqu'aucune boucle n'est possible. Ceci constitue une amélioration majeure en termes de vitesse de convergence.
-RSTP conserve des informations au sujet d'un chemin alternatif vers le root bridge, ainsi qu'un chemin de Backup vers les segments, ceci permet une transition rapide en cas de problème sur une liaison.
-le RSTP est plus ou moins rétro compatible avec le STP, mais une hétérogénéité de cette configuration sur un parc de switch entraînera inévitablement la propagation du fonctionnement en STP classique de l’ensemble de ces switchs, les switchs STP n’interprétant pas les BPDUs générées par les switchs opérant le RSTP.

Au niveau de la couche 3 :

Protocole HSRP

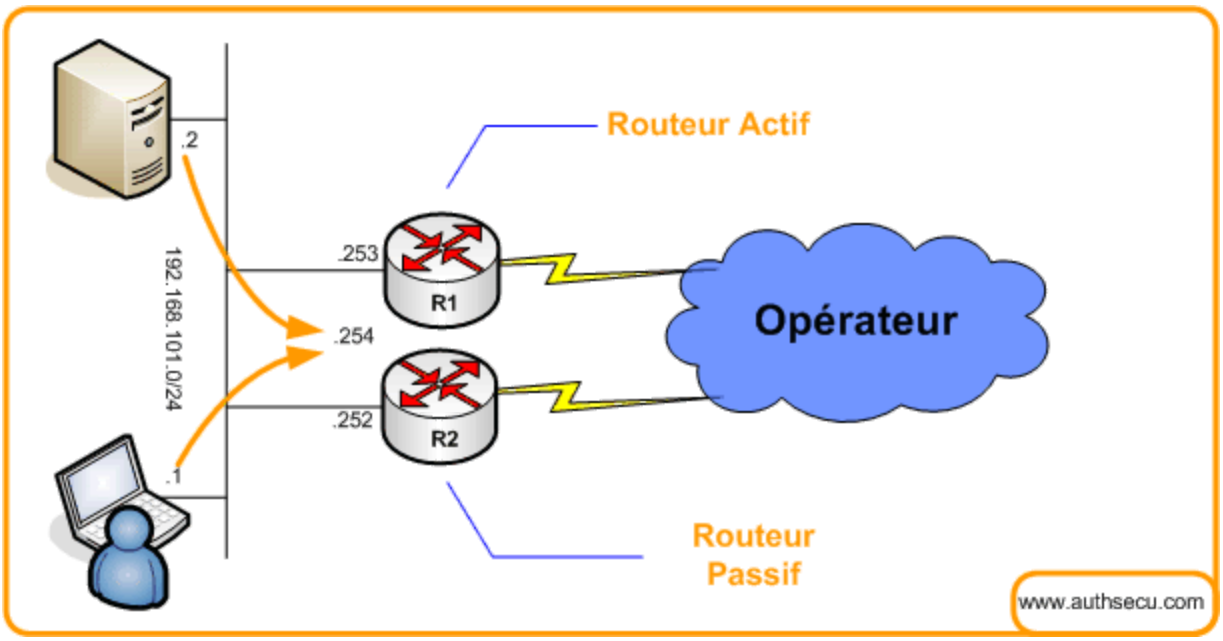
Le protocole HSRP (Hot Standby Routing Protocol) est un protocole propriétaire de continuité de service implémenté dans les routeurs Cisco pour la gestion des liens de secours. Le protocole HSRP présente aussi son semblable normalisé qui se nomme VRRP. Celui-ci étant normalisé, il est disponible sur les routeurs d'autres marques que Cisco. Il permet à partir de deux routeur physique (un en actif et l'autre en standby) de mettre en place un routeur virtuel afin d'augmenter la tolérance aux pannes.

Fonctionnement du protocole HSRP

Le principe de fonctionnement de HSRP est que tous les routeurs émulent une adresse IP virtuelle qui sera utilisée comme passerelle par défaut par les équipements du réseau. Chacun des routeurs configurera son protocole HSRP avec un niveau de priorité. Celui qui disposera du plus grand se verra élu et sera actif. Les autres seront passifs en attendant la perte du premier routeur.
La communication liée au protocole HSRP entre les routeurs se fait par l'envoi de paquets Multicast à l'adresse IP 224.0.0.2 vers le port UDP 1985. Cela permet principalement d'élire le routeur actif et de vérifier sa présence.
Tout ceci se fait par la mise en commun de plusieurs routeurs physiques qui, par un système d'élection basé sur des priorités attribuées à chacun assurerons la relève entre eux d'un routeur à un autre. Plus précisément, la technologie HSRP permettra aux routeurs situés dans un même groupe qu'on appelle ''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 assurent qu'il y est toujours un routeur qui garantisse le trafic pour l'ensemble du groupe. Un routeur dans ce groupe est élu comme « actif » et ce sera lui qui fera transiter les requêtes du réseau local.
Pendant que le routeur actif travail, il envoie également des messages aux autres routeurs indiquant qu'il est toujours « vivant » et opérationnel. L'élection se fait un peu comme pour le spanning-tree, en prenant en compte une priorité.
Cette priorité est réalisé grâce à la configuration du paramètre "priority" sur le routeur compris entre 1 et 255 (255 étant le plus prioritaire) et de l'adresse IP de l'interface (par défaut la priorité est à 100).
À priorités égales, la plus haute adresse IP sera élue. Plusieurs groupes HSRP peuvent exister au sein d'un même routeur sans que cela ne pose problème (depuis l'IOS 10.3). Seuls les routeurs du même numéro de groupe s'échangeront les messages HSRP. Si le routeur principal tombe, il sera automatiquement après un temps de décalage de 9 secondes, remplacé par un routeur qui était alors jusque-là en mode « passif » et lui aussi membre du groupe HSRP. Aux yeux des utilisateurs 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 adresse 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. En réalité, le routeur que voient les utilisateurs est un routeur virtuel composé de plusieurs routeurs qui travaillent via le protocole HSRP. Formant un groupe dans lequel un routeur sera désigné comme étant en mode actif et qui travaillera réellement et les autres se tiendront prêt à prendre la relève si besoin. Ce qui permet une continuité de service si un routeur venait à tomber.

Schema d'un reseau HSRP :



Avantage de HSRP :

Ø Assure la redondance et la continuité de service
Ø Adresse IP virtuel
Ø Compatible sur tous les équipements réseau Cisco

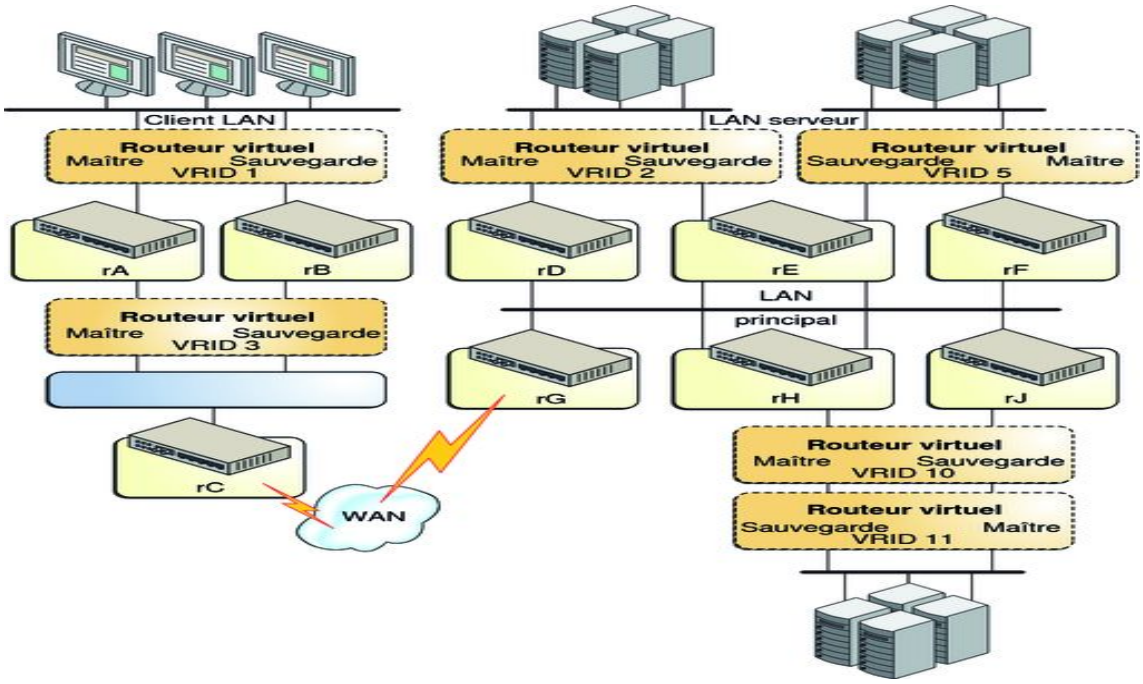
Limite de HSRP :

Ø L'Authentification des requêtes est envoyée en claire sur le réseau
Ø Ne gère pas l'équilibrage des charges
Ø Le trafic des messages hello sont envoyés aux routeurs en multicast (sécurité)
Ø Protocole propriétaire de Cisco qui donc ne fonctionne que sur du matériel Cisco

Protocole VRRP :
Virtual Router Redundancy Protocol est un protocole standard dont le but est d'augmenter la disponibilité de la passerelle par défaut des hôtes d'un même réseau.

Fonctionnement VRRP :

Le principe est de définir la passerelle par défaut pour les hôtes du réseau comme étant une adresse IP virtuelle référençant un groupe de routeurs. VRRP est comme HSRP un protocole qui fournit une solution de continuité de service pour la redondance de passerelles par défaut.
Pour chaque réseau, les interfaces des routeurs seront associées à un groupe VRRP (le même n° de groupe pour toutes les interfaces qui doivent assurer le même rôle).
A ce groupe on associe une adresse IP virtuelle.
La redondance est mise en place par le biais du protocole ARP. Lorsque l'hôte doit envoyer une trame à sa passerelle, il émet une requête ARP et celle-ci répond en fournissant son adresse MAC.
Dans le cas de VRRP, les routeurs vont associer une adresse MAC particulière à l'adresse IP virtuelle sous la forme 00:00:5E:00:01:XX (où XX est le n° du groupe VRRP). Pour l'hôte, ce sera cette adresse MAC qui identifiera sa passerelle. De leur côté les routeurs dialoguent par multicast à l'adresse (224.0.0.18) afin d'élire quel routeur devra se charger de traiter la trame destinée à l'adresse MAC VRRP. Cette adresse MAC virtuel est associé à un des routeurs du groupe grâce à un système d'élection basé sur la priorité un routeur avec la priorité la plus forte ce voit élire routeur maître et les autres routeurs comme routeur backup.
Schéma d'un réseau VRRP :



Avantage VRRP :
Ø Assure la redondance et la continuité de service
Ø Standardisé donc compatible avec n'importe quel équipement réseau
Ø Rapidité de réactivité du routeur backup inférieur à 4 secondes
Ø Adresse IP et Mac virtuelle

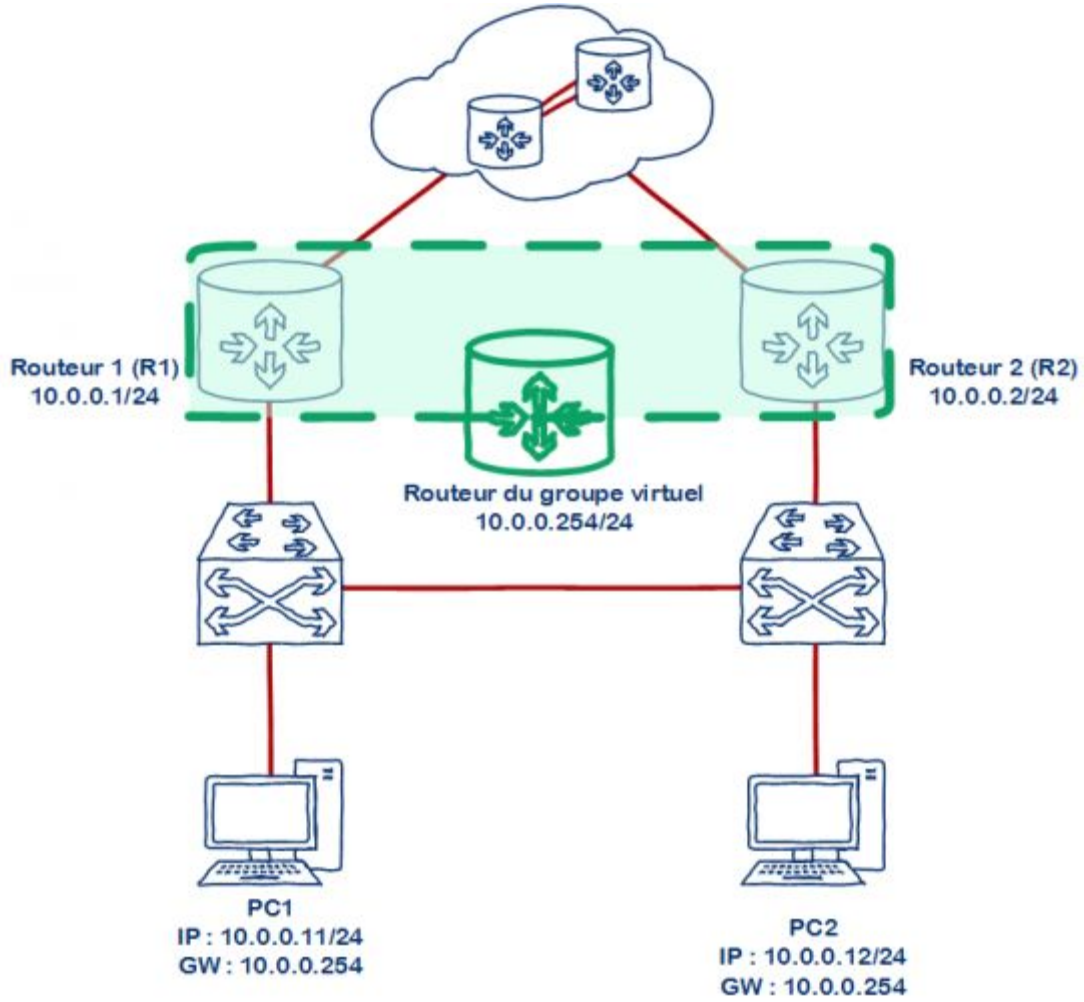
Inconvénient VRRP :
Ø Authentification par mot de passe en claire sur le réseau
Ø Adresse Mac virtuel unique

Protocole GLBP :
Gateway Load Balancing Protocol est un protocole propriétaire Cisco permettant de mettre en place de la redondance et de la répartition de charge sur plusieurs routeurs en utilisant une seule adresse IP virtuelle, associée à plusieurs adresses MAC virtuelles. GLBP utilise l'adresse IP multicast 224.0.0.102 pour l'envoi des paquets Hello et le numéro de port UDP 3222.

Fonctionnement de GLBP :
Le protocole HSRP est très utile mais ne permet pas la mise en place de Load-Balancing entre les routeurs membres du groupe HSRP. Si un routeur est choisi comme routeur "maître" vers lequel tous les paquets vont transiter tant qu'il sera opérationnel, les autres routeurs "passifs" sont eux totalement inutiles tant qu'il n'y a pas de panne sur le routeur maître.
Avec le protocole GLBP qui reprend le principe de continuité de service (Tolérance aux pannes), il y a également une notion de Répartition de charge. Les routeurs membres du groupe virtuel vont se répartir le traitement des paquets et leur routage afin d'alléger la charge de chacun tout en assurant une continuité du service sur la même IP si un des routeurs du groupe vient à tomber sa charge sera répartie sur les autres routeurs disponible. Cela permet d'utiliser la totalité des ressources disponibles plutôt que d'en laisser une partie en mode standby.
Le principe d'élection des routeurs est légèrement différent de HSRP et VRRP dans la mesure ou GLBP n'élu pas un routeur actif mais un AVG (active virtual gateway ou passerelle active virtuelle) et des AVF (Active Virtual Forwarder). Le routeur avec la priorité la plus forte ou l'adresse IP la plus forte du groupe prendra le statut de « AVG ». Ce routeur va intercepter toutes les requêtes ARP effectuées par les clients pour avoir l'adresse MAC de la passerelle par défaut, et grâce à l'algorithme d'équilibrage de charge précédemment configuré (généralement l'algorithme RoundRobin), il va renvoyer l'adresse MAC virtuelle d'un des routeurs du groupe GLBP.
C'est aussi le routeur AVG qui va attribuer les adresses MAC virtuelles aux routeurs du groupe, Ainsi ils ont le statut « AVF ». Un maximum de 4 adresses MAC virtuelle est défini par groupe, les autres routeurs ayant des rôles de backup en cas de défaillance des AVF.

Les routeurs communiquent entre eux par multicast (224.0.0.102) en s'échangeant des messages HELLO. Si l'un d'eux manque à l'appel il disparaît de la rotation au niveau des réponses ARP et si c'est l'AVG qui disparaît, c'est l'AVF avec la plus grande priorité qui prendra sa place.
Avec GLBP les requêtes d'authentification son crypté, il y a trois type d'authentification :
Authentification par **mot de passe**
Authentification par **key-string** (activer le chiffrement mdp sur chaque routeur)
Authentification par **key-chain** (activer le chiffrement mdp sur chaque routeur)

Schema d'un reseau GLBP



Avantage GLBP :

Ø Assure la redondance et la continuité de service
Ø Assure la répartition des charges (load balancing)
Ø Adresse IP virtuelle

Ø Jusqu’à 4 adresses Mac virtuelle possible par groupe GLBP
Ø Requête d’authentification cryptée

Inconvénient GLBP :
Ø Protocole propriétaire Cisco donc compatible que pour les équipements Cisco