

**HSRP**

**DOCUMENTATION**

**BLOC 2**

# 1. Introduction

La haute disponibilité est cruciale dans les environnements d'entreprise pour garantir la continuité de service et la tolérance de panne.

**HSRP (Hot Standby Routing Protocol)**, développé par Cisco, est une solution permettant de créer un routeur virtuel à partir de plusieurs routeurs physiques pour augmenter la tolérance de panne. Il permet à un routeur secondaire de prendre immédiatement la relève si le routeur principal devient inactif.

- **Avantages :**
  - Continuité de service transparente.
  - Sécurité accrue via la redondance.
- **Limite :** HSRP ne gère pas l'équilibrage de charge.

## Comparaison avec VRRP :

HSRP est propriétaire Cisco, tandis que VRRP est un protocole standard et interopérable.

# 2. Fonctionnement de HSRP

- Les routeurs partagent une **adresse IP** et une **adresse MAC virtuelle** pour être vus comme un seul routeur virtuel par les appareils du réseau.
- **Rôles des routeurs :**
  - **Routeur actif :** transmet le trafic réseau.
  - **Routeur standby :** en attente de défaillance du routeur actif pour prendre la relève.
- **Processus d'élection :**
  - Le routeur avec la **priorité la plus élevée** devient actif.
  - En cas d'égalité, l'adresse IP la plus haute détermine le gagnant.
  - La commande preempt permet au routeur actif d'être remplacé si un routeur avec une priorité plus élevée devient disponible.
- **Communication HSRP :**
  - Les messages sont échangés en multicast.
  - Si aucun message n'est reçu par le standby, il devient actif.

### 3. Mise en Œuvre HSRP

#### Exemple de Topologie :

Un réseau avec :

- **R1** (prioritaire, primaire).
- **R2** (standby, secondaire).
- **R3** (routeur tiers avec accès au LAN).
- **PC1** (utilisateur dans le LAN).
- Une adresse IP virtuelle partagée : 192.168.0.100/24.

#### Étapes de Configuration :

##### 1. Configurer les interfaces des routeurs :

Attribuer des adresses IP aux interfaces réseau des routeurs.

##### 2. Renommer les routeurs avec la commande hostname

##### 3. Configurer le routage statique :

##### 4. Configurer HSRP :

R1 (prioritaire) :

```
R1(config)# interface gig0/0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 192.168.0.100
R1(config-if)# standby 1 priority 105
R1(config-if)# standby 1 preempt
```

R2 (standby) :

```
R2(config)# interface gig0/0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 192.168.0.100
R2(config-if)# standby 1 preempt
```

##### 5. Ajouter la passerelle HSRP au PC :

Configurer l'adresse IP virtuelle comme passerelle par défaut pour les appareils du réseau.

## 4. Tests

### 1. Vérifications Initiales :

- Commande pour analyser la configuration :

```
#show standby brief
```

## 5. Fonctionnalité Avancée : Tracking

### Objectif :

Surveiller une interface spécifique et ajuster dynamiquement la priorité HSRP si celle-ci devient inactive.

### Configuration :

- R1 + R2 :

```
R1(config)# interface gig0/0  
R1(config-if)# standby 1 track gig0/1
```

Par défaut, le décrétement est de **10**. Si gig0/1 tombe en panne, la priorité de R1 passe à 95.

R2 devient actif si sa priorité (100) dépasse celle de R1.

## 6. Sécurisation des Échanges

Problème : Les mots de passe HSRP circulent en clair sur le réseau.

Solution : Ajouter une authentification HSRP sécurisée (hachage).

```
R1(config)# interface gig0/0  
R1(config-if)# standby 1 authentication md5 key-string (votre_mot_de_passe)
```

## 7. Améliorations et NAT

### Problème :

Les réponses réseau peuvent être envoyées via un routeur inactif.

### Solution :

Configurer la translation NAT sur chaque routeur HSRP.

- Exemple de configuration NAT sur R1 + R2 :

```
R1(config)# interface gig0/0
R1(config-if)# ip nat inside
R1(config)# interface gig0/1
R1(config-if)# ip nat outside
R1(config)# access-list 1 permit 192.168.0.0 0.0.0.255
R1(config)# ip nat inside source list 1 interface gig0/1 overload
```

## 8. Conclusion

HSRP est une solution efficace pour assurer la haute disponibilité réseau en entreprise. Avec des fonctionnalités comme le tracking, l'authentification et l'intégration avec NAT, il garantit une continuité de service robuste et sécurisée.