Documentation ContexteTiersLieux Activité Professionnelle

```
root@srvftp:~# cat testfile.txt
cat: testfile.txt: Aucun fichier ou dossier de ce type
root@srvftp:~# ftp 172.24.1.24
Connected to 172.24.1.24.
220 (vsFTPd 3.0.3)
Name (172.24.1.24:pod4): mtftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd upload
250 Directory successfully changed.
ftp>
ftp> ls
421 Timeout.
ftp> exit
root@srvftp:~# cd /home/mtftp/ftp/upload/
root@srvftp:/home/mtftp/ftp/upload# ls
testfile.txt
root@srvftp:/home/mtftp/ftp/upload# cat testfile.txt
"TEST FTP"
root@srvftp:/home/mtftp/ftp/upload#
```

```
220 (vsFTPd 3.0.3)
200 Always in UTF8 mode.
Utilisateur (172.24.1.24:(none)) : mtftp
331 Please specify the password.
Mot de passe :
230 Login successful.
ftp> cd upload
250 Directory successfully changed.
ftp> binary
200 Switching to Binary mode.
ftp> put testfile.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp : 13 octets envoyés en 0.00 secondes à 13000.00 Ko/s.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
testfile.txt
226 Directory send OK.
ftp : 17 octets reçus en 0.00 secondes à 17000.00 Ko/s.
226 Directory send OK.
```

Documentation : Présentation HSRP et LACP

Introduction Générale

Lors de cette présentation, nous allons aborder trois aspects essentiels de la redondance et de la résilience réseau :

Le protocole HSRP (Hot Standby Router Protocol), qui garantit la disponibilité de la passerelle par défaut. Autrement dit est un protocole de redondance de passerelle, utilisé pour garantir que le trafic réseau puisse passer même si un routeur tombe en panne.

Le protocole LACP (Link Aggregation Control Protocol), qui offre une augmentation de la bande passante et une redondance au niveau des commutateurs.

Le protocole RSTP (Rapid Spanning Tree Protocol) est une amélioration du STP qui prévient les boucles dans les réseaux Ethernet et offre une convergence rapide en quelques secondes.

L'objectif est de démontrer comment ces protocoles assurent la continuité de service même en cas de panne d'un équipement ou d'un lien.

Présentation du réseau

Nous disposons :

Deux routeurs (R1 et R2) configurés en HSRP.

Trois commutateurs (SW1, SW2, SW3) connectés avec des liaisons redondantes et configurés en mode trunk.

Et Jai mis en place RSTP sur mes trois commutateurs

PC1 pour effectuer des tests de connectivité et de basculement.

Plans d'adressages :

Équipement	Interface	Adresse IP	Masque de sous-réseau	VLANs
SW1_SRV_POD	VLAN 40	10.40.41.21	255.255.0.0 /16	VLANS

4				40,401,402
SW2_BUR_POD4	VLAN 40	10.40.41.22	255.255.0.0 /16	VLANS 40,401,402,408
SW3_L3_POD4	VLAN 40	10.40.41.23	255.255.0.0 /16	VLANS 40,110,401,402,408,409
SW3_L3_POD4	VLAN 401	172.24.1.254	255.255.255.0 /24	
SW3_L3_POD4	VLAN 402	172.24.2.254	255.255.255.0 /24	
SW3_L3_POD4	VLAN 110	192.168.24.254	255.255.255.0 /24	
SW3_L3_POD4	VLAN 409	172.24.9.254	255.255.255.0 /24	

Cette ligne indique que le commutateur SW1 est configuré avec l'adresse IP 10.40.41.21 sur le VLAN 40 (sous un masque /16), tout en gérant les VLANs 40, 401, et 402.

Équipement	Interface	Adresse IP	Masque de sous-réseau
R1_POD4	GE0/0/0	10.40.41.1	255.255.255.0 /24
R2_POD4	GE0/0/0	10.40.41.2	255.255.255.0 /24

R1_POD4 GE0/0/0 10.40.41.1 255.255.255.0 /24 : Cette ligne montre que le routeur R1 utilise l'interface GE0/0/0 avec l'adresse IP 10.40.41.1 et un masque /24 pour fournir la passerelle principale pour le réseau.

SSH

Équipement	Adresse IP	Masque de sous-réseau
PC1	10.40.41.3	255.255.255.0 /24

@ IP AD	172.24.1.2	255.255.255.0
@ IP AD DS	172.24.1.3	255.255.255.0
@ IP Serveur GLPI	172.24.1.21	255.255.255.0
@ IP SRVWeb41	172.24.1.20	255.255.255.0

@IP SRV FTP	172.24.1.24	255.255.255.0

Configurer les ports sur le switch de niveau 3 (par exemple, GigabitEthernet1/0/11 et 12) :

- Port **GE1/0/11 → GE0/0/0 R1**
- Port **GE1/0/12 → GE0/0/0 R2**

Architecture

- Les routeurs **R1** et **R2** utilisent une adresse IP virtuelle HSRP (VIP) : **10.40.41.254**.
- Les commutateurs sont connectés via des liens redondants, agrégés avec **LACP**.
- Le SSH fonctionne correctement sur tous les commutateurs (SW1, SW2, SW3).

. HSRP : Redondance de Passerelle

Configuration

- **Sur R1 (Routeur Principal)** :

R1# configure terminal

R1(config)# interface GigabitEthernet0/0/0

R1(config-if)# standby 1 ip 10.40.41.254

R1(config-if)# standby 1 priority 110

R1(config-if)# standby 1 preempt

Sur R2 (Routeur Secondaire) :

R2# configure terminal

R2(config)# interface GigabitEthernet0/0/0

R2(config-if)# standby 1 ip 10.40.41.254

R2(config-if)# standby 1 priority 90

R2(config-if)# standby 1 preempt

Scénario : Basculement des routeurs HSRP

Introduction :

Objectif : Illustrer comment le protocole HSRP facilite le basculement automatique entre deux routeurs afin d'assurer la disponibilité de la passerelle par défaut.

Configuration initiale :

R1 est paramétré avec une priorité HSRP supérieure (110), donc il fonctionne en tant que routeur principal.

R2 possède une priorité inférieure (90), ce qui le désigne comme le routeur de secours.

Test avant la coupure :

Depuis un PC sur le réseau, je vais envoyer un ping à l'adresse 10.40.41.254 (VIP).

Le ping reçoit une réponse, puisque R1 est opérationnel et garantit la communication.

Simuler une coupure de R1 :

Pour tester le basculement, je vais désactiver l'interface sur R1 (par exemple, shutdown sur GigabitEthernet0/0/0).

Test après la coupure :

Je vais relancer un ping vers 10.40.41.254 depuis le PC.

Le ping continue de recevoir des réponses, car R2 prend automatiquement le relais en tant que routeur principal grâce à HSRP, et le trafic se maintient sans interruption.

Rétablissement de la connexion :

Enfin, je vais réactiver l'interface sur R1 (no shutdown) et vérifier que R1 retrouve son rôle principal, R2 devenant ainsi le routeur de secours.

Scénario de présentation de LACP :

Contexte : Nous disposons de deux commutateurs, Switch1 et Switch2, et nous souhaitons établir une agrégation de liens à l'aide du LACP (Link Aggregation Control Protocol) afin d'optimiser la bande passante et garantir une redondance des connexions réseau.

Phases de configuration :

Sur Switch1, nous avons paramétré les interfaces FastEthernet 0/19 et 0/20 en mode trunk et les avons regroupées dans un groupe LACP actif (mode actif) grâce à la commande channel-group 1 mode active. Sur Switch2, une configuration identique a été appliquée aux interfaces FastEthernet 0/19 et 0/20, également en mode trunk et rassemblées dans le même groupe LACP.

Vérification : Pour garantir que tout fonctionne correctement, j'utilise la commande **show etherchannel summary** sur les deux commutateurs. Cela nous révèle que les interfaces 0/19 et 0/20 sont intégrées sous le Port-Channel 1, permettant ainsi une répartition de la charge du trafic réseau entre elles.

```
SW1_SRV_POD4#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/19(P)   Fa0/20(P)
```

Test de basculement : Afin de vérifier le basculement, je simule une défaillance sur Switch1 en désactivant l'interface FastEthernet 0/19 grâce à la commande shutdown. Grâce à l'agrégation LACP, le trafic sera automatiquement redirigé vers l'interface FastEthernet 0/20, garantissant ainsi une continuité de service sans interruption.

Conclusion : L'agrégation de liens LACP permet d'accroître la bande passante et d'assurer une haute disponibilité en cas de panne d'une interface, ce qui est essentiel pour maintenir la résilience et la performance du réseau.

Mettre en place le Serveur Rsyslog

1. Prérequis :

su - « Pour passer en mode administrateur »

Vérifier la connectivité réseau :
ping IP_CLIENT (172,24,1,20)
ping IP_SERVEUR (172,24,1,21)

2. Configuration du serveur Rsyslog :

Vérifier l'installation de Rsyslog sur le serveur :

sudo systemctl status rsyslog

Si Rsyslog n'est pas installé :

apt update

apt install rsyslog

Modifier la configuration pour recevoir les logs : Ouvrir le fichier de configuration :

nano /etc/rsyslog.conf

Moi j'avais choisi d'activer le protocole UDP
Dé-commenter pour activer UDP ou TCP :

Pour UDP (port 514) :

```
module(load="imudp")
input(type="imudp" port="514")
```

Pour TCP (port 10514) :

```
module(load="imtcp")
input(type="imtcp" port="10514")
```

Autoriser les clients à envoyer des logs : Ajouter ces lignes dans /etc/rsyslog.conf :

$AllowedSender UDP, 172.16.1.21, 172.16.1.20/24

OU
$AllowedSender TCP, 172.16.1.21, 172.16.1.20/24

Configurer les logs par client : Ajouter la ligne suivante pour enregistrer les logs de chaque client dans des fichiers distincts :

$template DynamicFile,"/var/log/syslogclients/%fromhost%-syslog.log"
***.* ?DynamicFile**

Redémarrer le service Rsyslog en utilisant la commande :

sudo systemctl restart rsyslog
sudo systemctl status rsyslog

Vérifier que le service écoute sur les bons ports :

ss -tnulp

3. Configuration du client Rsyslog (Linux) :

Vérifier l'installation de Rsyslog sur le client :

systemctl status rsyslog

Si Rsyslog n'est pas installé :

apt install rsyslog

Configurer l'envoi des logs au serveur Rsyslog : Ouvrir le fichier de configuration :

nano /etc/rsyslog.conf

Ajouter ces lignes pour envoyer les logs au serveur :

Pour TCP (port 10514) :

***.* @@IP_SERVEUR:10514**
Pour UDP (port 514) :

***.* @IP_SERVEUR:514**

sudo systemctl restart rsyslog
sudo systemctl status rsyslog

4. Vérification des logs sur le serveur :

Vérifier les fichiers de logs des clients :

Dans un premier temps il faut se placer dans le répertoire **« var/log/syslogclients/ »**

Voici la commande :

cd /var/log/syslogclients/

une fois qu'on est dans le répertoire, on va utiliser la commande **ls** pour lister tout les fichiers de ce répertoire :

puis il faut entrer la commande suivante pour vérifier les logs :

cat 172,24,1,20-syslog,log ou more 172,24,1,20-syslog,log

172,24,1,20 (@IP de Client Rsyslog)

5. Configuration du client Windows :

Télécharger et installer l'agent Rsyslog Windows : Télécharge depuis https://www.rsyslog.com/windows-agent/windows-agent-download/

Configurer l'agent Windows :

Ouvrir l'outil de configuration Rsyslog Windows Agent.
Choisir le protocole UDP (514) ou TCP (10514) et spécifier l'IP du serveur Rsyslog.
Sauvegarder et démarrer l'agent.
Vérifier les logs Windows sur le serveur : Vérifier que les logs de Windows sont bien remontés :

ls /var/log/syslogclients/

Mettre en place un Serveur FTP

Pour commencer il faut installer l'outil « vsftpd » et « FTP »

Installation de vsftpd

Connecte-toi en SSH à ton serveur Debian et exécute :

```
sudo apt update & apt install vsftpd & apt install ftp
```

➤Configuration de vsftpd

Édite le fichier de configuration de vsftpd :

```
sudo nano /etc/vsftpd.conf
```

Modifie ou ajoute ces lignes pour sécuriser le FTP :

```
ini
```

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=50000
user_sub_token=$USER
local_root=/home/$USER/ftp
```

Ensuite, redémarre vsftpd :

```
sudo systemctl restart vsftpd
```

Ensuite, il faut créer un utilisateur FTP

Non d'utilisateur : mtftp

Mot de passe : P@ssw0rd

1 Créer le dossier FTP de l'utilisateur

```
sudo mkdir -p /home/mtftp/ftp
```

2 Changer les permissions

On interdit l'accès au répertoire personnel et on autorise uniquement l'accès au dossier `ftp` :

```
sudo chown nobody:nogroup /home/mtftp/ftp
sudo chmod a-w /home/mtftp/ftp
```

3 Créer un dossier où stocker les fichiers

```
sudo mkdir /home/mtftp/ftp/upload
sudo chown mtftp:mtftp /home/mtftp/ftp/upload
```

4 Redémarrer le serveur FTP

```
sudo systemctl restart vsftpd
```

Pour effectuer le teste de la connexion FTP depuis mon serveur FTP, il faut entrer cette commande : **« ftp 172,24,1,24 »**

puis « ls » : cette commande permet de lister tout les fichiers et dossiers par exemple dans ce cas la on peut voir **le dossier upload (Un dossier ou stocker les fichiers)**

Pour tester si l'utilisateur peut envoyer des fichiers :

Connexion FTP depuis Windows (DEPUIS MON POSTE CMD) :

- Utilisation de la commande ftp 172.24.1.24 pour se connecter au serveur FTP.
- Authentification réussie avec l'utilisateur **mtftp** et son mot de passe.
- Passage en mode binaire avec la commande **binary** pour éviter la corruptions des fichiers
- Accès au répertoire **upload** avec la commande cd **upload**.

Sur mon serveur FTP :