

## CISCO INFRASTRUCTURE M2L





## Sommaire

### **1. Introduction et Topologie Générale**

- a. Architecture à trois niveaux
- b. Rôle des équipements

### **2. Plan d'adressage IP**

- a. Détail des sous-réseaux et VLANs

### **3. Protocoles et Configurations Détaillées**

- a. VLAN (Virtual Local Area Network)
- b. Trunking (802.1Q)
- c. Spanning Tree Protocol (STP) - Rapid PVST+
- d. SSH (Secure Shell)
- e. OSPF (Open Shortest Path First)
- f. HSRP (Hot Standby Router Protocol)
- g. DHCP Helper (ip helper-address)

### **4. Sécurité et Accès**

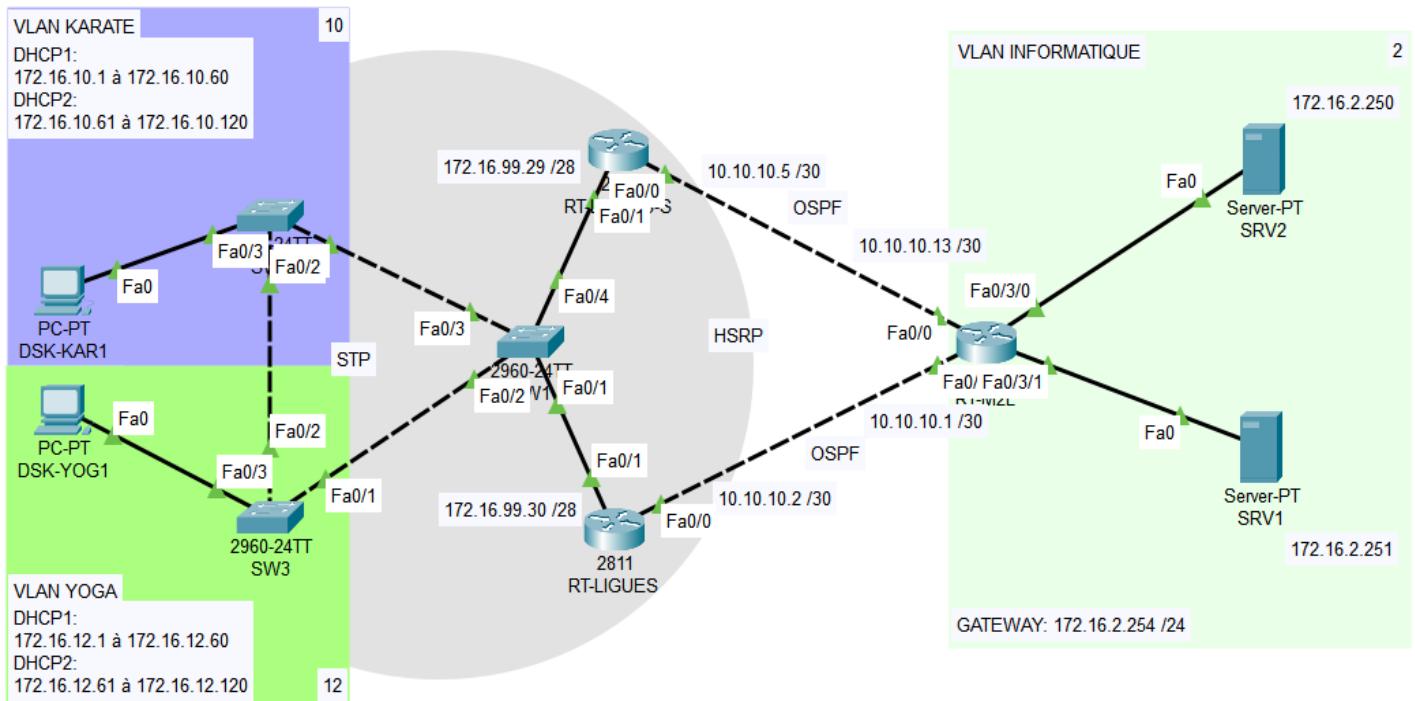
- a. Mesures de sécurité mises en place
- b. Justification des mesures de sécurité.

### **5. Conclusion**

- a. Résumé des avantages de l'infrastructure

## 1. Introduction et Topologie Générale :

L'infrastructure réseau de M2L est conçue pour assurer une haute disponibilité, une segmentation efficace du trafic et une gestion simplifiée. Elle repose sur une architecture à trois niveaux :



- **Niveau d'accès :**

*Composé des switchs SW2 et SW3, fournissant la connectivité aux utilisateurs .*

- **Niveau de distribution :**

*Représenté par le switch SW1, agrégant les connexions du niveau d'accès et fournissant des liaisons trunk vers les routeurs et les switches.*

- *Niveau cœur :*

*Constitué des routeurs RT\_2800-M2L ,RT\_LIGUES-M2L et RT\_LIGUES-M2L-S, assurant le routage inter-VLAN et la redondance de la passerelle par défaut.*

## 2. Plan d'adressage IP :

### 2.1 Adressage des Routeurs :

| Composant                    | Rôle                                 | Adresse IP/Passerelle   | Masque de sous-réseau   | Sécurité                                   | Redondance  |
|------------------------------|--------------------------------------|---|---|--|---|
| RT_2800-M2L<br>(Serveurs)    | Interconnexion des serveurs, routage | Fa0/0: 10.10.10.13/30<br>Fa0/1: 10.10.10.1/30<br>VLAN 2: 172.16.2.254/24  | 255.255.255.252 (/30)<br>255.255.255.0 (/24)                          | SSH, mots de passe chiffrés, bannière MOTD | Liaisons redondantes vers les routeurs principaux |
| RT_LIGUES-M2L<br>(Principal) | Routage inter-VLAN, HSRP actif       | Fa0/0: 10.10.10.2/30<br>Fa0/1.10: 172.16.10.254/24<br>Fa0/1.11: 172.16.11.254/24<br>Fa0/1.12: 172.16.12.254/24<br>Fa0/1: 172.16.99.30/28<br>HSRP: 172.16.99.1 | 255.255.255.252 (/30)<br>255.255.255.0 (/24)<br>255.255.255.240 (/28) | SSH, mots de passe chiffrés, bannière MOTD | HSRP (priorité 110)                               |
| RT_LIGUES-M2L-S<br>(Secours) | Passerelle de secours (HSRP standby) | Fa0/0: 10.10.10.6/30<br>Fa0/1.10: 172.16.10.254/24<br>Fa0/1.11: 172.16.11.254/24<br>Fa0/1.12: 172.16.12.254/24<br>Fa0/1: 172.16.99.29/28<br>HSRP: 172.16.99.1 | 255.255.255.252 (/30)<br>255.255.255.0 (/24)<br>255.255.255.240 (/28) | SSH, mots de passe chiffrés, bannière MOTD | HSRP (priorité 90)                                |

### Explications :

#### RT\_2800-M2L :

- Les interfaces Fa0/0 et Fa0/1 utilisent des adresses /30 pour des liaisons point à point avec les routeurs principaux.
- L'interface VLAN 2 sert de passerelle pour les serveurs.
- Les helper dhcp sont configurés sur les interfaces fa0/0, et fa0/1, et sur l'interface vlan 2.

### ***RT\_LIGUES-M2L et RT\_LIGUES-M2L-S :***

- Les sous-interfaces Fa0/1.10, Fa0/1.11 et Fa0/1.12 servent de passerelles pour les VLANs respectifs.
- L'interface Fa0/1 et l'adressage en /28 sert à l'adressage du hrsp.
- L'adresse HSRP 172.16.99.1 est l'adresse IP virtuelle partagée.
- Les helper dhcp sont configurés sur les sous interfaces fa0/1.10,fa0/1.11,fa0/1.12.
- Les interfaces fa0/0 sont des liaisons point à point vers le routeur RT\_2800-M2L.

### **2 . 2 Adressage des Switchs :**

| Composant                          | Rôle  | Adresse IP/Passerelle | Masque | Sécurité                                   | Redondance                 | Protocoles   |
|------------------------------------|---|-----------------------|--------|--|----------------------------|--|
| SW1-C2960-LIGUES<br>(Distribution) | Agrégation, trunking, root bridge STP           | Gestion par VLAN 1    | N/A    | SSH, mots de passe chiffrés, bannière MOTD | Liaisons trunk redondantes | 802.1Q, STP (Rapid PVST+), PortFast, BPDU Guard, SSH |
| SW2-C2960-LIGUES<br>(Accès)        | Connexion utilisateurs, ports d'accès, PortFast | Gestion par VLAN 1    | N/A    | SSH, mots de passe chiffrés, bannière MOTD | Liaisons trunk redondantes | 802.1Q, STP (Rapid PVST+), PortFast, BPDU Guard, SSH |
| SW3-C2960-LIGUES<br>(Accès)        | Connexion utilisateurs, ports d'accès, PortFast | Gestion par VLAN 1    | N/A    | SSH, mots de passe chiffrés, bannière MOTD | Liaisons trunk redondantes | 802.1Q, STP (Rapid PVST+), PortFast, BPDU Guard, SSH |

### **Explications :**

#### ***SW1-C2960-LIGUES (Distribution)***

Rôle :

- Ce switch sert de point de distribution central, interconnectant les switches d'accès et les routeurs.

- Il est configuré comme root bridge STP pour éviter les boucles de commutation.

**Protocoles :**

- 802.1Q : Permet le trunking pour transporter plusieurs VLANs.
- STP (Rapid PVST+) : Assure une topologie sans boucle et une convergence rapide.
- BPDU Guard : Protège contre les BPDU errantes.
- SSH : Assure un accès sécurisé à distance.

### ***SW2-C2960-LIGUES et SW3-C2960-LIGUES (Accès)***

**Rôle :**

- Ces switches fournissent la connectivité aux utilisateurs finaux.
- Ils sont configurés avec PortFast et BPDU Guard pour optimiser la convergence et la sécurité.

**Protocoles :**

- 802.1Q : Permet le trunking vers le switch de distribution.
- STP (Rapid PVST+) : Assure une topologie sans boucle.
- PortFast : Accélère la convergence sur les ports d'accès.
- BPDU Guard : Protège contre les BPDU errantes.
- SSH : Assure un accès sécurisé à distance.

### **2.3 Adressage des VLANs :**

| VLAN | Nom           | Rôle                      | Adresse Réseau | Masque de sous-réseau | Sécurité                  | Redondance                              | Protocoles   |
|------|---------------|---------------------------|----------------|-----------------------|---------------------------|---|--------------|
| 2    | Informatique  | Serveurs                  | 172.16.2.0     | 255.255.255.0 (/24)   | Contrôle d'accès par VLAN | Redondance au niveau des liaisons trunk | VLAN, 802.1Q |
| 3    | Administratif | Département Administratif | 172.16.3.0     | 255.255.255.0 (/24)   | Contrôle d'accès par VLAN | Redondance au niveau des liaisons trunk | VLAN, 802.1Q |

|    |                |                        |                   |                 |  |   |              |
|----|----------------|------------------------|-------------------|-----------------|--|---|--------------|
| 10 | Karate         | Département Karate     | 172.16.10.0 (/24) | 255.255.255.0   | Contrôle d'accès par VLAN                  | Redondance au niveau des liaisons trunk | VLAN, 802.1Q |
| 11 | Athlétisme     | Département Athlétisme | 172.16.11.0 (/24) | 255.255.255.0   | Contrôle d'accès par VLAN                  | Redondance au niveau des liaisons trunk | VLAN, 802.1Q |
| 12 | Yoga           | Département Yoga       | 172.16.12.0 (/24) | 255.255.255.0   | Contrôle d'accès par VLAN                  | Redondance au niveau des liaisons trunk | VLAN, 802.1Q |
| 99 | Gestion Ligues | HSRP                   | 172.16.99.0 (/28) | 255.255.255.240 | Aucune (sécurité assurée par les routeurs) | Routeurs redondants                     | VLAN, HSRP   |

### Explications :

#### Rôle :

- Ces VLANs segmentent le réseau en domaines de diffusion logiques, améliorant la sécurité et les performances.
- Chaque VLAN est associé à un département ou une fonction spécifique.

#### Adresses IP :

- Chaque VLAN a une adresse réseau et une étendue d'adresses IP dédiées.

#### Protocoles :

- VLAN : Assure la segmentation du réseau.
- 802.1Q : Permet le transport des VLANs sur les liaisons trunk.
- HSRP : (VLAN 99) Fournit une redondance de la passerelle par défaut.

### 3. Protocoles et Configurations Détaillées :

## 1. VLAN (Virtual Local Area Network)



Rôle :

- Segmentation du réseau pour limiter la diffusion des trames et renforcer la sécurité.
- Permet d'isoler les départements pour éviter le trafic inutile.
- Facilite l'application de règles de sécurité .



Sur un switch, on crée les VLANs et on leur attribue un nom :

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch(config)# vlan 10
```

```
Switch(config-vlan)# name Karate
```

```
Switch(config-vlan)# vlan 11
```

```
Switch(config-vlan)# name Athletisme
```

```
Switch(config-vlan)# vlan 12
```

```
Switch(config-vlan)# name Yoga
```

```
Switch(config-vlan)# vlan 99
```

```
Switch(config-vlan)# name Gestion_Ligues
```

```
Switch(config-vlan)# vlan 2
```

```
Switch(config-vlan)# name Informatique
```

```
Switch(config-vlan)# vlan 3
```

```
Switch(config-vlan)# name Administratif
```

```
Switch(config)# exit
```



Pourquoi ?

- La segmentation VLAN permet de séparer les différents départements, évite le broadcast excessif et renforce la sécurité en empêchant les utilisateurs non autorisés d'accéder à d'autres VLANs.
- 

## 2. Trunking (802.1Q)



Rôle :

- Permet à plusieurs VLANs de passer sur une seule liaison physique entre switches ou entre un switch et un routeur.



Sur un switch, activation du mode trunk et spécification des VLANs autorisés :

```
Switch> enable
```

```
Switch# configure terminal
```

```
Switch(config)# interface fa0/1
```

```
Switch(config-if)# switchport mode trunk
```

```
Switch(config-if)# switchport trunk allowed vlan 2,3,10,11,12,99
```

```
Switch(config-if)# exit
```



Pourquoi ?

- Réduit le nombre de câbles nécessaires, simplifie la gestion réseau et permet une meilleure évolutivité.
-

### 3. Spanning Tree Protocol (STP) - Rapid PVST+ :

#### 💡 Rôle :

- Empêche les boucles de commutation, qui peuvent paralyser le réseau.
- Accélère la convergence pour une réaction plus rapide en cas de panne.

#### 🛠 Configuration :

Activation de Rapid PVST+ et définition de la priorité pour contrôler l'élection du root bridge

Switch> enable

Switch# configure terminal

Switch(config)# spanning-tree mode rapid-pvst

Switch(config)# spanning-tree vlan 10,11,12,99 priority 4096

Switch(config)# spanning-tree guard root

Switch(config)# interface range FastEthernet 0/5-24

Switch(config)# spanning-tree bpduguard enable

Switch(config)# spanning-tree portfast default

Switch(config)# exit

#### 🔍 Pourquoi ?

- Rapid PVST+ accélère la reprise après une panne.
- BPDU Guard empêche l'activation d'un switch non autorisé.
- PortFast réduit le délai d'activation des ports d'accès.

## 4. SSH (Secure Shell) :



Rôle :

- Sécurise l'administration des équipements réseau en remplaçant Telnet (non chiffré).



**Switch# configure terminal**

**Switch(config)# ip domain-name monreseau.local**

**Switch(config)# crypto key generate rsa modulus 1024**

**Switch(config)# ip ssh version 2**

**Switch(config)# line vty 0 4**

**Switch(config-line)# transport input ssh**

**Switch(config-line)# login local**

**Switch(config-line)# exit**



Pourquoi ?

- Chiffre les communications pour éviter l'interception des mots de passe.

## 5. OSPF (Open Shortest Path First) :

### Rôle :

- Protocole de routage dynamique pour trouver le meilleur chemin entre routeurs.
- Permet une convergence rapide et une meilleure gestion des routes.

### Configuration :

Sur le routeur :

```
Router# configure terminal
```

```
Router(config)# router ospf 1
```

```
Router(config-router)# network 172.16.10.0 0.0.0.255 area 0
```

```
Router(config-router)# network 172.16.11.0 0.0.0.255 area 0
```

```
Router(config-router)# network 172.16.12.0 0.0.0.255 area 0
```

```
Router(config-router)# exit
```

### Pourquoi ?

- Plus efficace que RIP (distance vector).
- S'adapte dynamiquement aux pannes.

## **6. HSRP (Hot Standby Router Protocol) :**

### Rôle :

- Met en place une passerelle redondante pour assurer la continuité du service en cas de panne d'un routeur.

### Configuration :

Sur RT\_LIGUES-M2L (principal) :

```
Router# configure terminal
```

```
Router(config)# interface fa0/1
```

```
Router(config-if)# standby 1 ip 172.16.99.1
```

```
Router(config-if)# standby 1 priority 110
```

```
Router(config-if)# standby 1 preempt
```

```
Router(config-if)# exit
```

Sur RT\_LIGUES-M2L-S (secondaire) :

```
Router# configure terminal
```

```
Router(config)# interface fa0/1
```

```
Router(config-if)# standby 1 ip 172.16.99.1
```

```
Router(config-if)# standby 1 priority 90
```

```
Router(config-if)# standby 1 preempt
```

```
Router(config-if)# exit
```

### Pourquoi ?

- En cas de panne du routeur principal, le second routeur prend automatiquement le relais.

## 7. DHCP Helper (*ip helper-address*) :



Rôle :

- Permet aux clients d'un VLAN d'obtenir une adresse IP d'un serveur DHCP situé dans un autre VLAN.



Sur l'interface VLAN des clients :

```
Router# configure terminal
```

```
Router(config)# interface fa0/0
```

```
Router(config-if)# ip helper-address 172.16.2.250
```

```
Router(config-if)# ip helper-address 172.16.2.251
```

```
Router(config-if)# exit
```



Pourquoi ?

- Sans DHCP Helper, les requêtes DHCP ne traversent pas les VLANs.
- Cela permet d'avoir un serveur DHCP centralisé.

## 4. Sécurité et Accès :

Nous avons mis en place plusieurs mesures de sécurité pour garantir la protection du réseau.

### Configuration SSH sécurisée :

```
conf t  
hostname RT-M2L  
ip domain-name m2l4.local  
crypto key generate rsa 2048  
ip ssh version 2  
line vty 0 4  
transport input ssh  
login local  
exit
```

### *Explication des commandes :*

- **hostname RT-M2L** → Définit un nom d'hôte unique pour le routeur.
- **ip domain-name m2l.local** → Définit un domaine pour générer la clé RSA.
- **crypto key generate rsa 2048** → Génère une clé RSA de 2048 bits pour sécuriser SSH.
- **ip ssh version 2** → Active SSH version 2 pour une meilleure sécurité.
- **line vty 0 4** → Configure les lignes d'accès distant (VTY).
- **transport input ssh** → Autorise uniquement SSH et bloque Telnet.
- **login local** → Oblige l'authentification avec des comptes locaux.

### Chiffrement des mots de passe :

```
enable secret M2L@2024          (FAUX MDP POUR  
LA DOC)  
service password-encryption
```

### *Explication des commandes :*

- **enable secret** → Définit un mot de passe chiffré pour le mode privilégié.
  - **service password-encryption** → Chiffre tous les mots de passe en clair dans la configuration.
- 

### 5. Conclusion :

L'infrastructure réseau M2L, dans sa configuration actuelle, démontre une conception axée sur la fourniture d'une connectivité fiable et d'une sécurité de base. Les choix de configuration reflètent une approche pragmatique, privilégiant la stabilité et la disponibilité essentielles.

### **Points forts :**

- **Disponibilité :**
  - **La redondance au niveau des routeurs assure une continuité de service en cas de défaillance d'un équipement.**
  - **La configuration des commutateurs garantit une topologie sans boucle, améliorant la stabilité du réseau.**
- **Sécurité :**
  - **L'accès sécurisé aux équipements, l'authentification locale et la protection des mots de passe protègent contre les accès non autorisés.**
  - **La séparation du trafic par département réduit les risques de propagation d'incidents.**
- **Routage :**
  - **Le routage dynamique permet une adaptation aux changements de topologie et une connectivité continue.**
- **Gestion :**
  - **Le plan d'adressage facilite la gestion et la compréhension du réseau.**
  - **La centralisation de la distribution d'adresses IP simplifie l'administration.**

### **En résumé :**

**L'infrastructure M2L fournit une connectivité fiable et une sécurité de base. Pour répondre aux besoins futurs, des améliorations pourraient être apportées en matière de sécurité, de contrôle du trafic et de visibilité du réseau.**