

DESCRIPTION D'UNE MISSION   BTS SIO			
Prénom – Nom	Ajay Muthu Kumar	N° mission	1
Option	SISR <input checked="" type="checkbox"/>	SLAM	<input type="checkbox"/>
Situation	Formation <input checked="" type="checkbox"/>	Entreprise	<input type="checkbox"/>

Lieu de réalisation	Ecole IRIS Paris 17 <sup>ème</sup>	
Période de réalisation	Du : 07/10/2025	Au : 13/10/2025
Modalité de réalisation	VÉCUE <input checked="" type="checkbox"/>	OBSERVÉE <input type="checkbox"/>

Intitulé de la mission	<b>Restructuration de l'infrastructure de StadiumCompany</b>
Description du contexte de la mission	<p>Description en 2 à 3 lignes maxi</p> <p>Cette mission permet de créer la première étape de l'infrastructure de StadiumCompany.</p> <p>Il se compose de 7 services clés jouant un rôle important dans l'activités de l'entreprise.</p> <p>Elle permet d'assurer le bon fonctionnement de l'informatique afin de garantir la sécurité et la coordination efficace des opérations au sein de l'entreprise.</p>

Ressources et outils utilisés	<p>Liste des ressources disponibles et outils utilisés (Documentations, Matériels et Logiciels)</p> <p>Cisco Packet Tracer – Draw.io – Windows 11</p>
Résultat attendu	<p>Résultat attendu avec la réalisation de cette mission</p> <p>C'est pour obtenir une infrastructure réseau fonctionnelle, segmentée en VLANS, permettant la communication entre services via le routage inter-VLAN, tout en assurant la stabilité et la sécurité du système.</p> <p>Une maquette réseau complète sous Cisco Packet Tracer doit démontrer la connectivité entre tous les services du site principal et des sites distants.</p>
Contraintes	<p>Contraintes : techniques   budgétaires   temps   O.S. ou outils imposés...</p> <p>Les contraintes techniques liées à la configuration du routage inter-VLAN, respect du plan d'adressage, temps limité pour la mise en œuvre, outils imposés (Cisco Packet Tracer, Draw.io).</p>

Compétences associées	Liste des intitulés du tableau de compétences (avec les références)

**Description simplifiée des différentes étapes de réalisation de la mission  
en mettant en évidence la démarche suivie, les méthodes et les techniques utilisées**

## **Mission 1 : Restructuration de l'Infrastructure de StadiumCompany**

### Contexte :

#### **1 - Adressage VLSM (Voir Tableau)**

- ➔ Service
- ➔ Adresse du réseau
- ➔ Masque de sous réseau
- ➔ Adresse valide (IP départ-fin)
- ➔ Adresse de broadcast

Service	Adresse du réseau	Masque sous réseau	Adresse Validé (Début-Fin)	Adresse de broadcast
Administration VLAN 10	172.20.0.0	/24	172.20.0.1 172.20.0.254	172.20.0.255
Equipes VLAN 20	172.20.1.0	/24	172.20.1.1 172.20.1.254	172.20.1.255
Wifi VLAN 30	172.20.2.0	/25	172.20.2.1 172.20.2.126	172.20.2.127
Caméra IP VLAN 40	172.20.2.128	/25	172.20.129 172.20.2.254	172.20.2.255
VIP-Presses VLAN 50	172.20.3.0	/25	172.20.3.1 172.20.3.126	172.20.3.127
Fournisseurs VLAN 60	172.20.3.128	/26	172.20.3.129 172.20.3.190	172.20.3.191
Restaurant VLAN 70	172.20.3.192	/28	172.20.3.193 172.20.3.206	172.20.3.207

#### **2 - Administration et gestion des vlan**

- 1) Introduction sur les protocoles utiliser

#### Définition :

GARP et GVRP = Ces protocoles permettent aux périphériques d'échanger dynamiquement des informations de configuration de réseau local virtuel (VLAN) pour faciliter la configuration des VLAN.

VTP (VLAN Trunking Protocol) = Ce protocole permet de simplifier l'administration d'un réseau commuté. En effet, avec ce protocole, un commutateur en mode serveur peut créer, modifier ou supprimer des VLAN. De plus, ces informations seront automatiquement communiquées à tous les autres commutateurs du domaine VTP.

Choix du VTP = Etant donné que le protocole VTP est présent par défaut sur le matériel Cisco. Nous allons donc utiliser celui-ci pour notre installation car il est réputé pour être plus simple d'utilisation dans un environnement Cisco contrairement aux autres protocoles comme GVRP.

## 2) Configuration du VTP

Par défaut un switch sera en mode serveur, il est donc important que les switches secondaires soient configurés en mode client car c'est le switch serveur qui véhiculera la configuration aux switches clients.

Ainsi, toutes les VLAN devront être configurés depuis le switch serveur car c'est celui-ci qui partagera la configuration des VLAN aux switches clients.

Pour la configuration du VTP, on a le choix entre la commande « vtp mode server » et « vtp mode client ». Cela permet de configurer un switch en mode serveur ou client en fonction de nos besoins.

Par la suite, il faudra choisir le même domaine sur chaque switch avec la commande « vtp domain » afin de synchroniser les switches entre eux. Pour notre cas, nous utiliserons le nom de domaine suivant : « stadiumcompany.local ».

Enfin, il est important d'utiliser la même version du VTP, que l'on choisira via la commande « vtp version 2 » car sinon la synchronisation ne fonctionnera pas correctement.

```
SW1-Srv#
SW1-Srv#enable
SW1-Srv#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1-Srv(config)#vtp mode server
Device mode already VTP SERVER.
SW1-Srv(config)#vtp domain stadiumcompany.local
Domain name already set to stadiumcompany.local.
SW1-Srv(config)#vtp version 2
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/23 changed state to up
```

```
SW2-Client(config)#
SW2-Client(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2-Client(config)#vtp domain stadiumcompany.local
Changing VTP domain name from NULL to stadiumcompany.local
SW2-Client(config)#vtp version 2
```

Afin de constater que la configuration du VTP aient bien été prise en compte sur les switches, la commande « show vtp status » permet de le vérifier. En effet, on peut alors visualiser les informations qu'on a pu configurer comme la version du VTP, le nom de domaine utilisé et enfin le mode du switch.

```
SW1-Srv#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : stadiumcompany.local
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 000C.CFD2.1D00
Configuration last modified by 0.0.0.0 at 3-1-93 03:29:38
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
Configuration Revision    : 1
MD5 digest                : 0xC4 0xD3 0x19 0xE7 0x78 0x13 0xF4 0x86
                          : 0x3F 0x95 0x95 0x69 0x82 0x96 0x31 0xF3
SW1-Srv#
```

```
SW2-Client#enable
SW2-Client#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : stadiumcompany.local
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 00D0.D320.9B00
Configuration last modified by 0.0.0.0 at 3-1-93 03:29:38

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
Configuration Revision    : 1
MD5 digest                : 0xC4 0xD3 0x19 0xE7 0x78 0x13 0xF4 0x86
                          : 0x3F 0x95 0x95 0x69 0x82 0x96 0x31 0xF3
SW2-Client#
```

« Trunk » est un lien réseau configuré de sorte à faire circuler des trames Ethernet modifiées comportant des informations liées aux différents VLANs d'un réseau.

Pour configurer le trunk, il faut en amont avoir en tête le lien dans lequel passera les trames VLANs. Dans notre cas, nous avons configuré le trunk sur le port gigabitEthernet 0/2 de nos deux switches.

```

SW1-Srv#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1-Srv(config)#interface gigabitEthernet 0/2
SW1-Srv(config-if)#switchport mode trunk
SW1-Srv(config-if)#no shut

SW2-Client#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2-Client(config)#interface gigabitEthernet 0/2
SW2-Client(config-if)#switchport mode trunk
SW2-Client(config-if)#no shut

```

Ainsi, il faut commencer par entrer dans l'interface du port qu'on veut configurer en tapant la commande « interface gigabitEthernet 0/2 ».

Ensuite, il faut choisir le mode trunk du port de notre switch avec la commande « switchport mode trunk ».

Enfin, pour que le port reste continuellement ouvert, on peut rajouter la commande « no shutdown ».

La commande « show interface trunk » nous servira à voir sur quel port nos trunk ont été configurés, ainsi que la plage de VLAN autorisée. Il nous indiquera aussi le nombre de VLAN actif sur le réseau ainsi que le nombre de VLAN qui passe par ce switch.

#### Switch serveur :

```

SW1-Srv#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Gig0/2    on        802.1q         trunking      1

Port      Vlans allowed on trunk
Gig0/2    1-1005

Port      Vlans allowed and active in management domain
Gig0/2    1

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/2    1

```

#### Switch client :

```

SW2-Client#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Gig0/2    on        802.1q         trunking      1

Port      Vlans allowed on trunk
Gig0/2    1-1005

Port      Vlans allowed and active in management domain
Gig0/2    1

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/2    none

```

On y voit ci-dessus les mêmes informations que ce soit sur le switch serveur que sur le switch client sauf pour la dernière ligne qui correspond au nombre de VLAN actif sur le switch, on constate que 1005 VLANs sont autorisés et que seulement 1 est actif sur le SW1-SRV actuellement.

Ici en l'occurrence, on peut aller jusqu'à 1005 VLANs car dans nos VLANs par défaut, on a le VLAN 1 mais aussi les VLANs 1002-1005.

```

1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active

```

#### 4) Création des VLANs (SW1-SRV)

Un VLAN (Virtual Local Area Network) est un réseau local virtuel qui permet de segmenter un réseau physique en plusieurs sous-réseaux logiques. Cela permet de renforcer la sécurité, améliorer la gestion du trafic et la flexibilité du réseau.

Pour créer nos VLANs, nous devons passer par le switch configuré en mode serveur VTP afin qu'il partage ensuite les VLANs à tous les switches en mode client.

Voici notre plan pour l'attribution des VLANs de notre réseau

- VLAN 10 : ADMINISTRATION.
- VLAN 20 : EQUIPES.
- VLAN 30 : WIFI.
- VLAN 40 : CAMERA-IP.
- VLAN 50 : VIP-PRESSE.
- VLAN 60 : FOURNISSEUR.
- VLAN 70 : RESTAURANT.

Pour ajouter un VLAN sur notre switch serveur, il faut être en mode configuration « conf t », puis sélectionner le VLAN que nous voulons créer ou modifier. Par exemple « vlan 10 » et on indiquera le nom que l'on souhaite pour ce VLAN avec la commande « name ».

#### Exemple de cette configuration :

```

SW1-Srv>enable
SW1-Srv#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1-Srv(config)#vlan 10
SW1-Srv(config-vlan)#name ADMINISTRATION

```

Nous pouvons donc répliquer cette commande sur chaque VLANs que nous voulons créer :

```

SW1-Srv>enable
SW1-Srv#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1-Srv(config)#vlan 10
SW1-Srv(config-vlan)#name ADMINISTRATION
SW1-Srv(config-vlan)#vlan 20
SW1-Srv(config-vlan)#name EQUIPES
SW1-Srv(config-vlan)#vlan 30
SW1-Srv(config-vlan)#name WIFI
SW1-Srv(config-vlan)#vlan 40
SW1-Srv(config-vlan)#name CAMERAS-IP
SW1-Srv(config-vlan)#vlan 50
SW1-Srv(config-vlan)#name VIP-PRESSE
SW1-Srv(config-vlan)#vlan 60
SW1-Srv(config-vlan)#name FOURNISSEUR
SW1-Srv(config-vlan)#vlan 70
SW1-Srv(config-vlan)#name RESTAURANT

```

Ils seront configurés automatiquement sur le SW2-Client grâce au VTP. Il est par ailleurs impossible de créer, modifier ou supprimer un VLAN depuis un switch client, ce qui permet de renforcer la sécurité du réseau.

```
SW2-Client#show vlan

VLAN Name                Status
-----
1    default                active

10   ADMINISTRATION          active
20   EQUIPES                 active
30   WIFI                   active
40   CAMERAS-IP             active
50   VIP-PRESSE             active
60   FOURNISSEUR            active
70   RESTAURANT             active
```

Pour vérifier l'ensemble des créations de nos VLANs, nous écrirons « show vlan » comme ci-dessous.

```
SW1-Srv>enable
SW1-Srv#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1
10 ADMINISTRATION	active	
20 EQUIPES	active	
30 WIFI	active	
40 CAMERAS-IP	active	
50 VIP-PRESSE	active	
60 FOURNISSEUR	active	
70 RESTAURANT	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
SW2-Client>enable
SW2-Client#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1
10 ADMINISTRATION	active	
20 EQUIPES	active	
30 WIFI	active	
40 CAMERAS-IP	active	
50 VIP-PRESSE	active	
60 FOURNISSEUR	active	
70 RESTAURANT	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Le fait d'attribuer des ports à des VLANs revient à organiser les prises réseau d'un switch en groupes logiques. Chaque groupe (VLAN) correspond à un réseau distinct, même si physiquement tout passe par le même switch. Chaque port du switch peut être configuré en mode accès (access) ou en mode trunk :

- Pour le mode accès (access), il associe un seul VLAN à un port. C'est le mode utilisé pour connecter à un PC ou tout autre périphérique.
- Pour le mode trunk, quant à lui, il permet à un port de transporter plusieurs VLANs. Il est aussi utilisé entre plusieurs switches ou entre un seul switch et un seul routeur.

Cette configuration doit être effectuée sur le switch client étant donné que l'on peut adapter chaque port en fonction de nos besoins.

Pour le SW2-Client, on fait le choix d'attribuer 3 ports pour chaque VLANs.

Pour attribuer une plage de port à un VLAN, nous avons besoin dans un premier temps de rentrer en mode configuration du terminal avec la commande « conf t ».

Ensuite, on sélectionne la plage de port que l'on souhaite attribuer avec la commande « interface range fastEthernet 0/1-3 ».

Afin de détailler la commande, « interface range » permet de choisir un groupe de port, fastEthernet correspond à un des types de port du switch. De plus, le 1-3 signifie que l'on choisira les ports du numéro 1 au 3.

Ainsi, avec la commande « switchport access vlan \*\* », on sélectionne le VLAN que l'on souhaite attribuer sur la plage de ports.

```
SW2-Client#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2-Client(config)#interface range fastEthernet 0/1-3
SW2-Client(config-if-range)#switchport access vlan 10
SW2-Client(config-if-range)#exit
SW2-Client(config)#interface range fastEthernet 0/4-6
SW2-Client(config-if-range)#switchport access vlan 20
SW2-Client(config-if-range)#interface range fastEthernet 0/7-9
SW2-Client(config-if-range)#switchport access vlan 30
SW2-Client(config-if-range)#interface range fastEthernet 0/10-12
SW2-Client(config-if-range)#switchport access vlan 40
SW2-Client(config-if-range)#interface range fastEthernet 0/13-15
SW2-Client(config-if-range)#switchport access vlan 50
SW2-Client(config-if-range)#interface range fastEthernet 0/16-18
SW2-Client(config-if-range)#switchport access vlan 60
SW2-Client(config-if-range)#interface range fastEthernet 0/19-21
SW2-Client(config-if-range)#switchport access vlan 70
SW2-Client(config-if-range)#exit
SW2-Client(config)#
```

Il faut ensuite utiliser la commande « show vlan », afin de vérifier que l'ensemble des ports pour chaque VLANs ont bien été attribués.

### SRV

SW1-Srv#show vlan

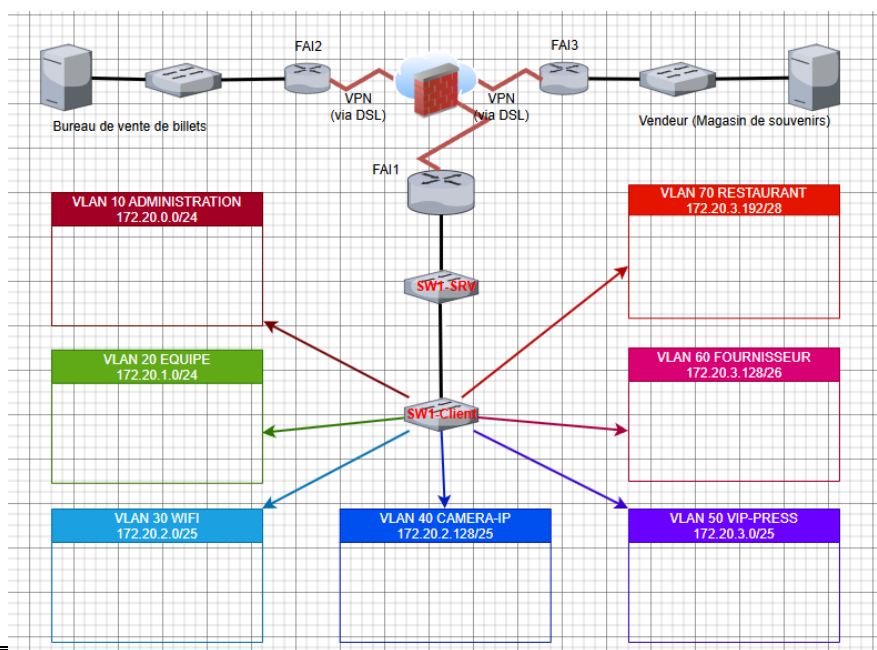
VLAN Name	Status	Ports
1 default	active	Fa0/22, Fa0/23, Fa0/24, Gig0/1
2 VLAN0002	active	
10 ADMINISTRATION	active	Fa0/1, Fa0/2, Fa0/3
20 EQUIPES	active	Fa0/4, Fa0/5, Fa0/6
30 WIFI	active	Fa0/7, Fa0/8, Fa0/9
40 CAMERAS-IP	active	Fa0/10, Fa0/11, Fa0/12
50 VIP-PRESSE	active	Fa0/13, Fa0/14, Fa0/15
60 FOURNISSEUR	active	Fa0/16, Fa0/17, Fa0/18
70 RESTAURANT	active	Fa0/19, Fa0/20, Fa0/21
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

### Client

SW2-Client#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/22, Fa0/23, Fa0/24, Gig0/1
2 VLAN0002	active	
10 ADMINISTRATION	active	Fa0/1, Fa0/2, Fa0/3
20 EQUIPES	active	Fa0/4, Fa0/5, Fa0/6
30 WIFI	active	Fa0/7, Fa0/8, Fa0/9
40 CAMERAS-IP	active	Fa0/10, Fa0/11, Fa0/12
50 VIP-PRESSE	active	Fa0/13, Fa0/14, Fa0/15
60 FOURNISSEUR	active	Fa0/16, Fa0/17, Fa0/18
70 RESTAURANT	active	Fa0/19, Fa0/20, Fa0/21
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

## 6) Schéma du réseau





### 3- Routage

#### 1) Routage inter-vlan

Il faut mettre en place un routage inter-vlan lorsqu'il y a un besoin de communication entre deux groupes de travail. De ce fait, il est possible de faire communiquer deux VLANs sans compromettre leur sécurité.

Ainsi, il faut utiliser un routeur qui soit relié à un des switches, dans notre cas il sera relié au switch serveur.

Le routeur va alors par intermédiaire d'un seul lien physique router et faire transiter un ensemble de VLAN.

Ensuite il faudra créer les sous interfaces virtuels et en attribuer la plage IP de chaque réseau en suivant le tableau suivant :

Service	Adresse de l'interface	Masque sous réseau
Administration VLAN 10	172.20.0.1	255.255.255.0
Equipes VLAN 20	172.20.1.1	255.255.255.0
Wifi VLAN 30	172.20.2.1	255.255.255.128
Caméra IP VLAN 40	172.20.2.129	255.255.255.128
VIP-Presses VLAN 50	172.20.3.1	255.255.255.128
Fournisseurs VLAN 60	172.20.3.129	255.255.255.192
Restaurant VLAN 70	172.20.3.193	255.255.255.240

Pour mettre en place le routage inter-vlan. Dans un premier temps, à partir du switch, il faut activer le mode trunk sur le port du switch qui sera relié vers le routeur, afin de faire transiter les informations des VLANs.

```
Sw1-SRV>enable
Sw1-SRV#config t
Sw1-SRV(config)#interface fastEthernet 0/23
Sw1-SRV(config-if)#switchport mode trunk
Sw1-SRV(config-if)#
```

Ensuite, nous devons créer les sous interfaces sur le routeur avec la commande « interface 0/0.10 ». Par exemple pour l'interface du VLAN10, il faut ensuite faire la commande « encapsulation dot1Q 10 ». A partir de là, il faut indiquer l'IP du routeur pour cette sous-interface avec la commande « address 172.20.0.1 255.255.255.0 » = «ip address *ip du routeur masque de sous réseau* ».

```
R1-Stade>enable
R1-Stade#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-Stade(config)#interface gigabitEthernet 0/0/0.10
R1-Stade(config-subif)#encapsulation dot1Q 10
R1-Stade(config-subif)#ip address 172.20.0.1 255.255.255.0
R1-Stade(config-subif)#exit
R1-Stade(config)#
```

Par la suite, il faut reproduire cela pour tous les autres VLANs.



```

R1-Stade>enable
R1-Stade#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-Stade(config)#interface gig
R1-Stade(config)#interface gigabitEthernet 0/0/0.10
R1-Stade(config-subif)#encapsulation dot1Q 10
R1-Stade(config-subif)#ip address 172.20.0.1 255.255.255.0
R1-Stade(config-subif)#exit
R1-Stade(config)#interface gigabitEthernet 0/0/0.20
R1-Stade(config-subif)#encapsulation dot1Q 20
R1-Stade(config-subif)#ip address 172.20.1.1 255.255.255.0
R1-Stade(config-subif)#exit
R1-Stade(config)#interface gigabitEthernet 0/0/0.30
R1-Stade(config-subif)#encapsulation dot1Q 30
R1-Stade(config-subif)#ip address 172.20.2.1 255.255.255.128
R1-Stade(config-subif)#exit
R1-Stade(config)#interface gigabitEthernet 0/0/0.40
R1-Stade(config-subif)#
R1-Stade(config-subif)#encapsulation dot1Q 40
R1-Stade(config-subif)#ip address 172.20.2.129 255.255.255.128
R1-Stade(config-subif)#exit
R1-Stade(config)#interface gigabitEthernet 0/0/0.50
R1-Stade(config-subif)#
R1-Stade(config-subif)#encapsulation dot1Q 50
R1-Stade(config-subif)#ip address 172.20.3.1 255.255.255.128
R1-Stade(config-subif)#exit
R1-Stade(config)#interface gigabitEthernet 0/0/0.60
R1-Stade(config-subif)#
R1-Stade(config-subif)#encapsulation dot1Q 60
R1-Stade(config-subif)#ip address 172.20.3.129 255.255.255.192
R1-Stade(config-subif)#exit
R1-Stade(config)#interface gigabitEthernet 0/0/0.70
R1-Stade(config-subif)#
R1-Stade(config-subif)#encapsulation dot1Q 70
R1-Stade(config-subif)#ip address 172.20.3.193 255.255.255.240
R1-Stade(config-subif)#exit
R1-Stade(config)#

```

Afin de vérifier la bonne configuration des sous-interfaces, on peut utiliser la commande « show ip interface brief ».

On peut y voir les différentes sous-interfaces rattachées au VLAN qui leur correspond ainsi que l'adresse IP.

```

R1-Stade#show ip interface brief
Interface                IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0/0    unassigned      YES NVRAM   up             up
GigabitEthernet0/0/0.10 172.20.0.1      YES manual  up             up
GigabitEthernet0/0/0.20 172.20.1.1      YES manual  up             up
GigabitEthernet0/0/0.30 172.20.2.1      YES manual  up             up
GigabitEthernet0/0/0.40 172.20.2.129    YES manual  up             up
GigabitEthernet0/0/0.50 172.20.3.1      YES manual  up             up
GigabitEthernet0/0/0.60 172.20.3.129    YES manual  up             up
GigabitEthernet0/0/0.70 172.20.3.193    YES manual  up             up
GigabitEthernet0/0/1    unassigned      YES NVRAM   administrativ down down
GigabitEthernet0/0/2    unassigned      YES NVRAM   administrativ down down
Serial0/2/0              200.200.200.1   YES manual  up             up
Serial0/2/1              200.200.200.5   YES manual  up             up
Vlan1                    unassigned      YES unset   administrativ down down
R1-Stade#

```

## 2) Route statique

Un routage statique est une méthode de routage utilisée en réseau pour définir manuellement les chemins que les paquets doivent emprunter pour atteindre un réseau.

Contrairement au routage dynamique, il ne nécessite pas de protocole d'échange automatique d'information entre les routeurs.

Chaque route indique :

- La passerelle de sortie (Gateway).
- La masque sous-réseau.
- Le réseau de destination.

Ainsi, pour pouvoir configurer une route statique, il faut tout d'abord entrer en mode configuration avec la commande « conf t ».

Après cela, il faut connaître vers quel réseau nous souhaitons aller et par quel routeur nous allons passer.

Grâce à ces informations, on va pouvoir utiliser la commande « ip route <réseau distant> <masque réseau distant> <passerelle d'accès> ».

Exemple : `R1-Stade(config)#ip route 192.168.1.0 255.255.255.0 200.200.200.2`

Nous allons procéder de la même façon sur chacun des routeurs en rajoutant les routes statiques dont nous avons besoin afin que tous les sites puissent communiquer ensemble.

Pour vérifier toutes les informations configurées, on fera la commande : « show ip route », elle nous servira donc à voir quelles routes le routeur a en sa possession et comment les informations seront acheminées vers les réseaux.

<code>S</code>	<code>192.168.1.0/24 [1/0] via 200.200.200.2</code>	Commande « show ip route » effectué sur le R1-Stade (Routeur Principal)
<code>S</code>	<code>192.168.2.0/24 [1/0] via 200.200.200.6</code>	

<code>S</code>	<code>172.20.0.0/22 [1/0] via 200.200.200.5</code>	Commande « show ip route » effectué sur le R-MS (Routeur Boutique)
<code>S</code>	<code>192.168.1.0/24 [1/0] via 200.200.200.5</code>	

<code>S</code>	<code>192.168.2.0/24 [1/0] via 200.200.200.1</code>	Commande « show ip route » effectué sur le R-Bill (Routeur Billetterie)
<code>S</code>	<code>172.20.0.0/22 [1/0] via 200.200.200.1</code>	

Les adresses IP statiques vues via la commande « show ip route » : correspondent aux routes statiques configurées pour connecter les trois sites entre eux (Stade, Boutique, Billetterie). Ils utilisent tous 200.200.200.0/24 comme réseau d'interconnexion entre routeurs et assurent que toutes les communications passent par le routeur principal (R1-Stade), qui fait office de réseau central.

### **3- Conclusion**

Afin de correspondre à la demande du cahier des charges de la mission 1, des configurations ont été réalisées.

Il y a eu le protocole VTP qui a été mis en place afin d'assurer une distribution automatique des VLANs vers les futurs commutateurs ajoutés au réseau (en mode client).

Les liaisons trunk entre les commutateurs ont été correctement établies, permettant la circulation du trafic de plusieurs VLANs sur les mêmes liens physiques.

Avec bien entendu la création de 7 VLANs afin de séparer chaque services présente dans le stade.

De plus, la mise en œuvre du routage inter-VLAN assure désormais la communication entre les différents services du site principal, tout en maintenant une séparation logique pour des raisons de sécurité.

Enfin, la connectivité avec les sites distants est opérationnelle via la liaison Internet et la mise en place des routes statiques, permettant l'échange d'informations entre tous les réseaux de l'entreprise. Cette première mission valide la restructuration du réseau interne et pose les bases solides pour la poursuite des missions suivantes.

### **4- Annexe**

Pour pouvoir réaliser cette mission, nous avons utilisé plusieurs ressources.

Pour commencer, nous avons utilisé un PC sous le système d'exploitation Windows 11. Ainsi, avec l'application Draw.io nous avons pu schématiser notre réseau pour ainsi avoir une meilleure visibilité du matériel à mettre en place.

Après cela, nous avons utilisé Cisco Packet Tracer afin de créer une simulation du réseau que nous avons schématisé plus tôt grâce à Draw.io.

Deux sites internet nous ont aidé ([www.cisco.com](http://www.cisco.com) et [www.it-connect.fr](http://www.it-connect.fr)) pour expliquer, définir, et vérifier les commandes à utiliser pour faire la configuration des switches, création des VLANs, la mise en place des routes...

De plus, nous avons eu deux documents à notre disposition, un schéma sur Draw.io et une maquette Cisco Packet Tracer, nous permettant d'avoir la vision du chemin à prendre.

Resources: Cisco, windows 11, Draw.io, [www.cisco.com](http://www.cisco.com), <https://www.it-connect.fr/>

Conclusion	Que pouvez-vous dire de cette mission : apport personnel, expérience, etc
	<p>Au cours de cette mission, j'ai pu renforcer mes compétences en administration réseau, en particulier dans la configuration des VLANS, du VTP, du routage inter-VLAN et du routage statique.</p> <p>J'ai appris à organiser une infrastructure globale, à contrôler la connectivité et à manipuler les commandes Cisco de manière autonome.</p> <p>Cette expérience m'a également permis de mieux appréhender la logique de segmentation réseau et d'améliorer ma façon de travailler en équipe.</p>

Evolution possible	Evolution du service concerné par cette mission qui pourrait être envisagée
	<p>Pour améliorer le réseau, on pourrait ajouter de nouveaux VLANS pour d'autres services de l'entreprise. On pourrait également améliorer le routage inter-VLAN pour faciliter la communication entre les différents services.</p> <p>On pourrait automatiser la création des VLANS, qu'il peut utiliser le protocole VTP sur un plus grand nombre de commutateurs. Enfin, si le nombre d'utilisateurs augmente, il serait possible d'étendre le plan d'adressage VLSM.</p>

--	--

Productions associées	Liste des documents produits et description
	<ul style="list-style-type: none"> <li>- Pour le schéma réseau, on a utilisé Draw.io</li> <li>- Pour la maquette fonctionnelle, on a utilisé Cisco Packet Tracer</li> <li>- Tableau d'adressage VLSM</li> </ul>