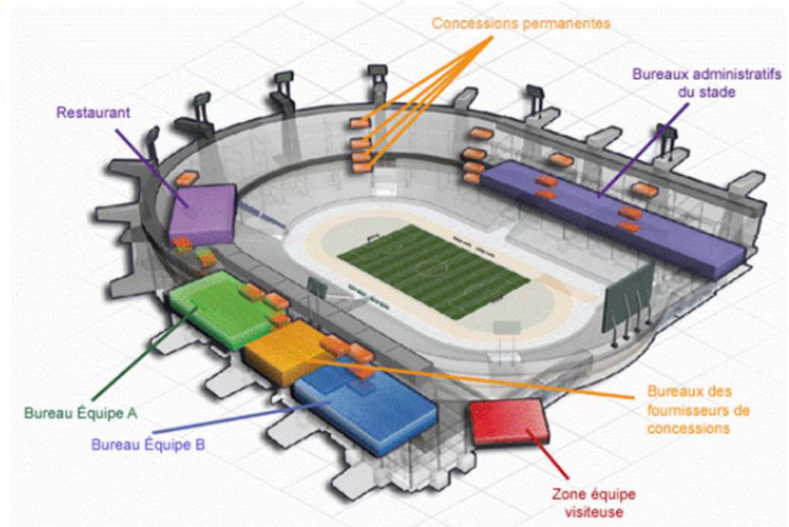


**BTS SIO2 LM  
ECOLE IRIS**

**Restructuration de l'infrastructure de  
Stadium  
(VLSM, VLAN, configuration Switches et  
Routeurs NAT/PAT)**

## Table des matières

|   |           |
|---|-----------|
| <b>I ) Contexte.....</b>  | <b>2</b>  |
| Présentation de Stadium.....  | 2         |
| Présentation du prestataire – Networking Company.....               | 2         |
| <b>II ) Cahier des charges Stadium.....</b>                         | <b>3</b>  |
| <b>III ) Solutions.....</b>   | <b>4</b>  |
| Segmentation VLSM.....  | 4         |
| VTP / GVRP .....  | 4         |
| VLAN.....   | 5         |
| <b>IV ) Mise en œuvre des solutions.....</b>                        | <b>5</b>  |
| Mise en place de la configuration.....                              | 5         |
| Configuration du switch 1 (serveur).....                            | 9         |
| Réinitialisation des commutateurs.....                              | 9         |
| Renommage du switch.....  | 9         |
| Configuration des commutateurs avec VTP.....                        | 10        |
| Administration et Gestion des VLANs.....                            | 10        |
| Attribution des Ports aux VLANs.....                                | 10        |
| Création des Ports Trunk.....                                       | 12        |
| Configuration du switch 2 (client).....                             | 13        |
| Réinitialisation des commutateurs.....                              | 13        |
| Renommage du deuxième switch.....                                   | 14        |
| Configuration des commutateurs.....                                 | 14        |
| Attribution des Ports aux VLANs.....                                | 15        |
| Création des Ports Trunk.....                                       | 15        |
| Configuration du routeur.....                                       | 17        |
| Réinitialisation du routeur et redémarrage.....                     | 17        |
| Renommage du routeur.....   | 17        |
| Configuration de l'interface fastEthernet 0/1 en DHCP.....          | 18        |
| Configuration du NAT/PAT.....                                       | 19        |
| Configuration de l'interface fastEthernet 0/0 en NAT intérieur..... | 19        |
| Configuration des listes d'accès pour le NAT.....                   | 21        |
| Activation du NAT pour chaque VLAN avec la commande ip nat.....     | 22        |
| Configuration IP du Routeur 2.....                                  | 22        |
| Test de la configuration.....                                       | 22        |
| Vérification des traductions NAT.....                               | 22        |
| Ajout de la route par défaut.....                                   | 24        |
| <b>V) Conclusion.....</b>   | <b>24</b> |



## I) Contexte

### Présentation de Stadium

Stadium gère un grand stade doté d'un réseau de communication avancé mis en place lors de sa construction initiale. Cependant, au fil des années, des équipements supplémentaires ont été ajoutés de manière désorganisée, sans planification à long terme ni prise en compte de la conception de l'infrastructure réseau.

Cela a entraîné des problèmes de bande passante et une mauvaise gestion du trafic, limitant la capacité de l'entreprise à offrir des services de qualité.

Actuellement, le réseau ne permet pas de répondre aux exigences nécessaires pour introduire de nouvelles technologies ou organiser des événements comme des concerts, ce qui compromet la satisfaction des clients et l'évolution de l'entreprise.

### Présentation du prestataire – Networking Company

Pour moderniser son infrastructure et répondre à ses nouveaux besoins, Stadium a fait appel à NetworkingCompany, une entreprise spécialisée dans la conception de réseaux. La direction de Stadium souhaite qu'elle guide l'entreprise à travers un projet en trois phases, avec pour première étape la planification et la création d'une conception réseau de haut niveau.

NetworkingCompany a donc interviewé le personnel de Stadium pour comprendre l'organisation et les installations. Le stade emploie 170 personnes, dont 35 dirigeants et responsables, et environ 80 intérimaires lors des événements spéciaux. Le réseau actuel connecte des PC, des téléphones, des bureaux, des locaux techniques sur deux

niveaux, ainsi que deux sites distants via DSL, et doit être modernisé pour répondre aux exigences futures.

## II ) Cahier des charges Stadium

Le Cahier des Charges de Stadium révèle mon intégration au sein de la division Systèmes d'Information (SI) de l'entreprise pour cette année. Ma mission centrale consistera à assumer la responsabilité de l'administration des systèmes et des réseaux informatiques.

Stadium se compose de plusieurs sites distincts, chacun ayant un rôle spécifique :

**Site 1 : Stade** - Ce site est le cœur de l'entreprise, abritant l'hébergement informatique, le siège social et le centre administratif. Il est le pivot autour duquel s'articulent toutes les opérations et activités de l'entreprise.

**Site 2 : Billetterie** - Ce site est dédié à la gestion des ventes de billets, un élément essentiel pour les événements sportifs et les spectacles organisés au stade.

**Site 3 : Magasin** - Ce site est spécialement conçu pour la vente d'articles souvenirs, offrant aux fans et aux visiteurs la possibilité d'acheter des produits liés à l'équipe ou aux événements.

Le centre administratif de Stadium, situé au stade, occupe une position centrale dans l'entreprise, car il gère l'ensemble des opérations liées à la gestion du personnel et à l'administration du stade. Il se compose de trois services clés, chacun ayant un rôle vital dans les activités de l'entreprise :

**1) Service Administration (170 collaborateurs)** : chargé de la gestion administrative de l'entreprise.

**2) Service Équipes (164 collaborateurs)** : chargé de la coordination des équipes opérationnelles.

**3) Service WiFi (100 collaborateurs)** : responsable des réseaux sans fil.

Concernant le réseau de Stadium, plusieurs exigences en matière de sécurité doivent être respectées pour garantir la solidité et la stabilité de l'infrastructure informatique. Ces exigences comprennent :

- L'utilisation d'une plage d'adresses IP spécifique (172.20.0.0/22) : Cette plage d'adresses simplifiera la gestion des noms et des ressources au sein du réseau.
- La mise en place d'un système de segmentation du réseau : Cette solution permettra de séparer différentes parties du réseau pour des raisons de sécurité et d'efficacité. Des commutateurs faciles à administrer seront utilisés pour permettre une configuration rapide et fluide de ces segments.
- La création d'une solution d'interconnexion efficace entre les différents sites : Cette

solution garantira une communication optimale entre le stade, la billetterie et le magasin, favorisant ainsi une coordination sans faille des activités.

- La configuration uniforme des équipements réseau avec des équipements CISCO : Tous les commutateurs et le routeur seront configurés de manière cohérente à l'aide d'équipements réseau de la marque CISCO pour garantir une compatibilité et une gestion homogène.

- Votre rôle au sein de cette mission est essentiel pour assurer le bon fonctionnement de l'infrastructure informatique de Stadium, ainsi que pour garantir la sécurité et la coordination efficace des opérations au sein de l'entreprise.

Le Cahier des Charges insiste sur la nécessité de documenter les différentes solutions retenues pour le projet en fonction de leur niveau de complexité. Cette approche méthodique garantira que chaque aspect de l'infrastructure informatique soit clairement spécifié et que les procédures soient consignées de manière exhaustive.

Cela s'inscrit dans la vision globale adoptée par Stadium pour assurer une gestion efficace et cohérente de ses ressources informatiques.

Mon rôle au sein de cette mission sera d'une importance cruciale, car je devais contribuer à façonner et à maintenir l'infrastructure technologique qui soutient les opérations de l'entreprise et qui permet de répondre aux défis uniques posés par chaque site.

## III ) Solutions

### Segmentation VLSM

La segmentation VLSM (Variable Length Subnet Mask) permet de diviser un réseau en sous-réseaux de tailles différentes, en fonction des besoins spécifiques de chaque sous-réseau.

Contrairement au découpage classique où tous les sous-réseaux ont la même taille, le VLSM optimise l'utilisation des adresses IP en attribuant une taille de sous-réseau adaptée à chaque segment du réseau.

C'est ce que nous allons appliquer pour mettre en place notre réseau.

### VTP / GVRP

**VTP (VLAN Trunking Protocol)** et **GVRP (GARP VLAN Registration Protocol)** sont deux protocoles utilisés pour la gestion des VLANs sur un réseau, mais ils fonctionnent différemment :

- **VTP** (protocole propriétaire de Cisco) permet de distribuer automatiquement les informations VLAN (création, modification, suppression) entre les switches d'un même domaine VTP. Cela simplifie la gestion des VLANs dans un grand réseau,

car les modifications faites sur un switch en mode serveur se propagent automatiquement aux autres switches, puisque la gestion est centralisée.

- **GVRP** (protocole ouvert standardisé) permet aux switches de s'enregistrer et de se joindre dynamiquement à des VLANs lorsqu'ils reçoivent des requêtes. Contrairement à VTP, il n'y a pas de distribution centralisée des VLANs car les switches rejoignent les VLANs en fonction des besoins du trafic.

Dans notre cas, nous utilisons le protocole VTP car nous utilisons Cisco.

## VLAN

Un VLAN (Virtual Local Area Network) est un réseau virtuel qui permet de segmenter un réseau physique en plusieurs réseaux logiques indépendants. Même si tous les appareils sont connectés à un même switch ou à la même infrastructure physique, les VLANs permettent de les séparer en groupes distincts. Cela sert principalement à isoler les réseaux pour en avoir une meilleure gestion.

Il existe 3 types de VLAN :

**Statique** : Un VLAN statique axé sur un port consiste à assigner manuellement des ports spécifiques d'un switch à un VLAN. Cela signifie que tout appareil branché à un certain port sera automatiquement placé dans le VLAN auquel le port appartient.

**Dynamique MAC** : Un VLAN dynamique basé sur l'adresse MAC attribue automatiquement les appareils à un VLAN en fonction de leur adresse MAC (peu importe à quel port du switch ils sont connectés). Contrairement aux VLANs statiques, où c'est le port qui détermine le VLAN, ici chaque appareil est reconnu par son adresse MAC, et le switch place automatiquement cet appareil dans le VLAN approprié. Cela offre plus de flexibilité, car les appareils peuvent se déplacer sans avoir besoin de reconfigurer les ports, contrairement aux VLANs statiques.

**Dynamique IP** : Les adresses IP dynamiques sont des adresses IP attribuées automatiquement à des appareils par un serveur DHCP (Dynamic Host Configuration Protocol). Cela signifie que l'appareil n'a pas une adresse IP fixe, mais en reçoit une temporaire chaque fois qu'il se connecte au réseau.

Dans notre situation, nous allons utiliser un VLAN statique.

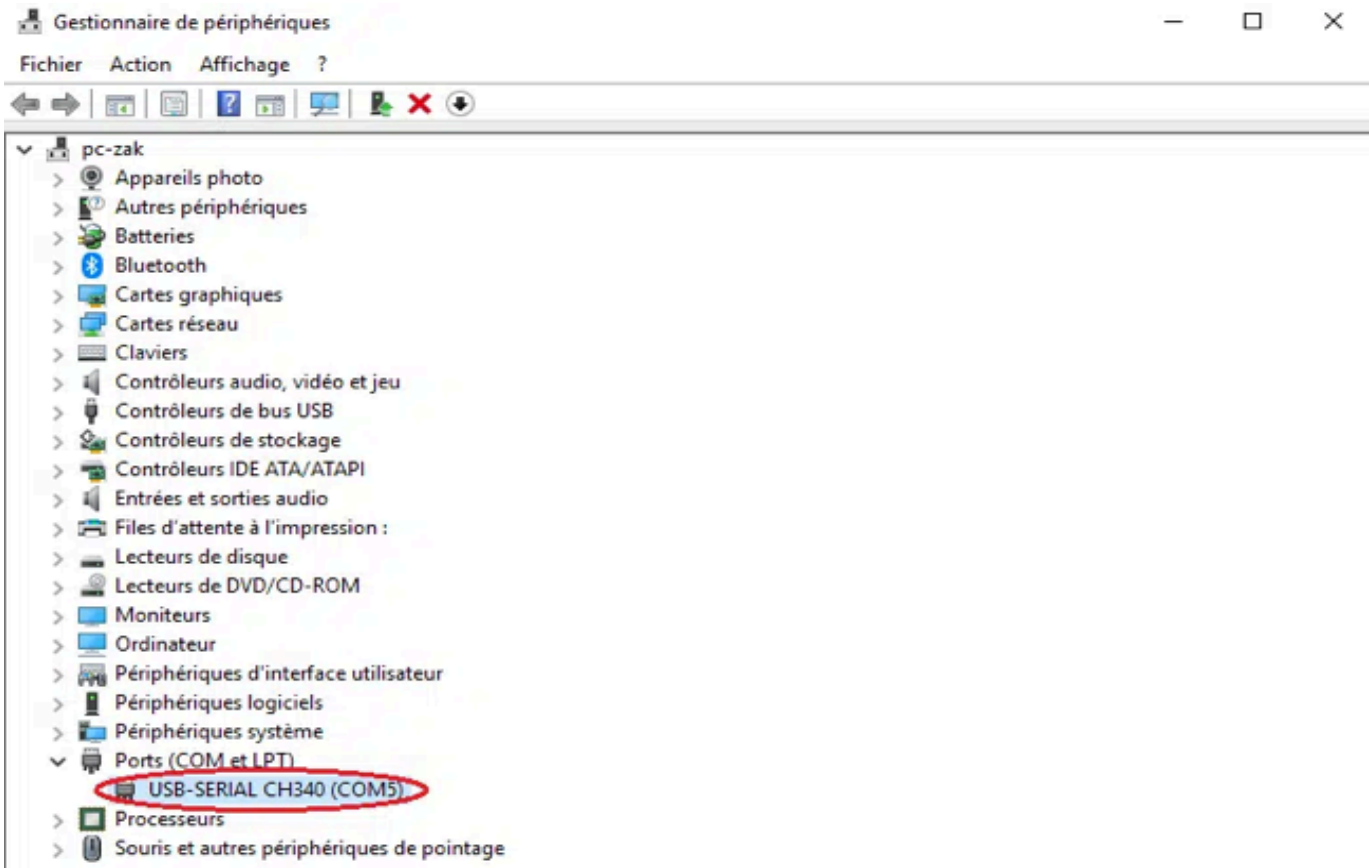
## IV ) Mise en œuvre des solutions

### Mise en place de la configuration

Nous avons les équipements suivants :

- 2 switches
- 1 routeur
- 1 câble croisé qui relie les ports 24 des 2 switches
- 1 câble RJ45 du boîtier internet jusqu'au routeur
- 1 câble console depuis l'équipement jusqu'à notre ordinateur

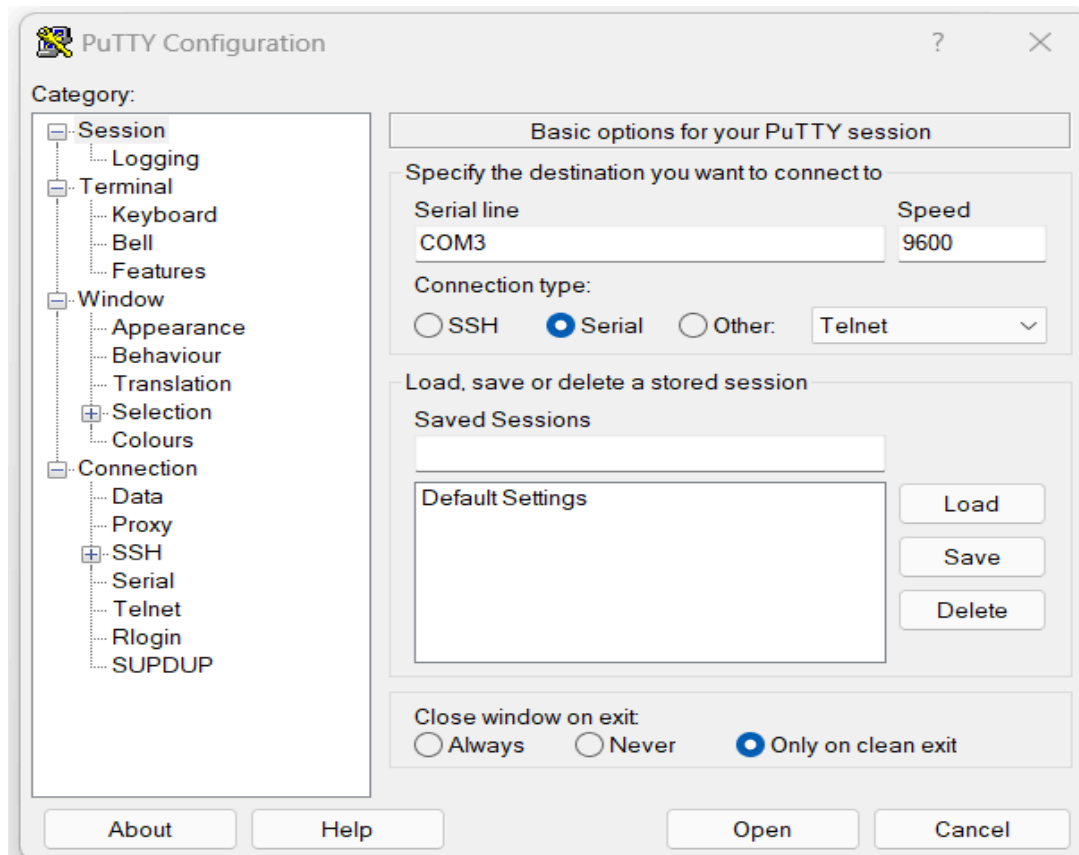
Ensuite, il faut aller dans le **gestionnaire de périphérique** pour savoir où est connecté l'équipement, puis regarder le **Port Com** affiché (le Port Com5 comme dans l'exemple ci-dessous) :



Il faut ensuite chercher l'application **PuTTY** via la barre de recherche Windows.

- Dans **Connection Type** → sélectionner **Serial**
- Configurer le **Serial line** sur le **Port COM** affiché sur le gestionnaire de périphérique, ici le « **COM3** »
- Une fois le "**Serial Line**" en **COM3**, il faut vérifier la configuration de la vitesse (**baud rate**) à **9600** (la vitesse par défaut pour les connexions série avec les équipements Cisco).





Puis, on clique sur **Open** pour accéder au **Terminal de configuration du switch**.  
Il se peut que le port ne soit pas reconnu, il faut donc effectuer les dernières mises à jour Windows pour que le pilote soit installé.

Nous allons mettre en place notre configuration à partir de ce tableau :

| Équipement | VLAN | Adresse réseau | Masque             | Première adresse | Dernière adresse | Adresse broadcast | Nombre d'adresses utilisables |
|------------|------|----------------|--------------------|------------------|------------------|-------------------|-------------------------------|
| SW-SRV     | 10   | 172.20.0.0     | 255.255.255.0/24   | 172.20.0.1       | 172.20.0.254     | 172.20.0.255      | 254                           |
| SW-Client  | 20   | 172.20.1.0     | 255.255.255.0/24   | 172.20.1.1       | 172.20.1.254     | 172.20.1.255      | 254                           |
| Routeur    | 30   | 172.20.2.0     | 255.255.255.128/25 | 172.20.2.1       | 172.20.2.126     | 172.20.2.127      | 126                           |

Comme expliqué précédemment, nous utilisons la segmentation **VLSM** afin de segmenter les **VLANs** et ainsi avoir différentes tailles de sous-réseaux.  
Ici, ce seront des **VLANs statique** axé sur une range de ports spécifique.

### VLAN 10 (SW-SRV)

C'est un VLAN dédié aux serveurs avec un sous-réseau plus large pour accueillir plus de machines. Le masque /24 permet d'avoir **254 adresses utilisables**, suffisant pour un réseau de taille moyenne. Un VLAN spécifique aux serveurs permet d'isoler les machines critiques pour plus de sécurité et une gestion simplifiée.



### VLAN 20 (SW-Client)

Ce VLAN est destiné aux clients ou aux utilisateurs. Le masque est également en /24, ce qui laisse de la place pour **254 adresses utilisables**. Cela correspond à un réseau de taille similaire à celui des serveurs. Un VLAN pour les clients/utilisateurs garantit que leurs activités n'interfèrent pas avec celles du serveur.

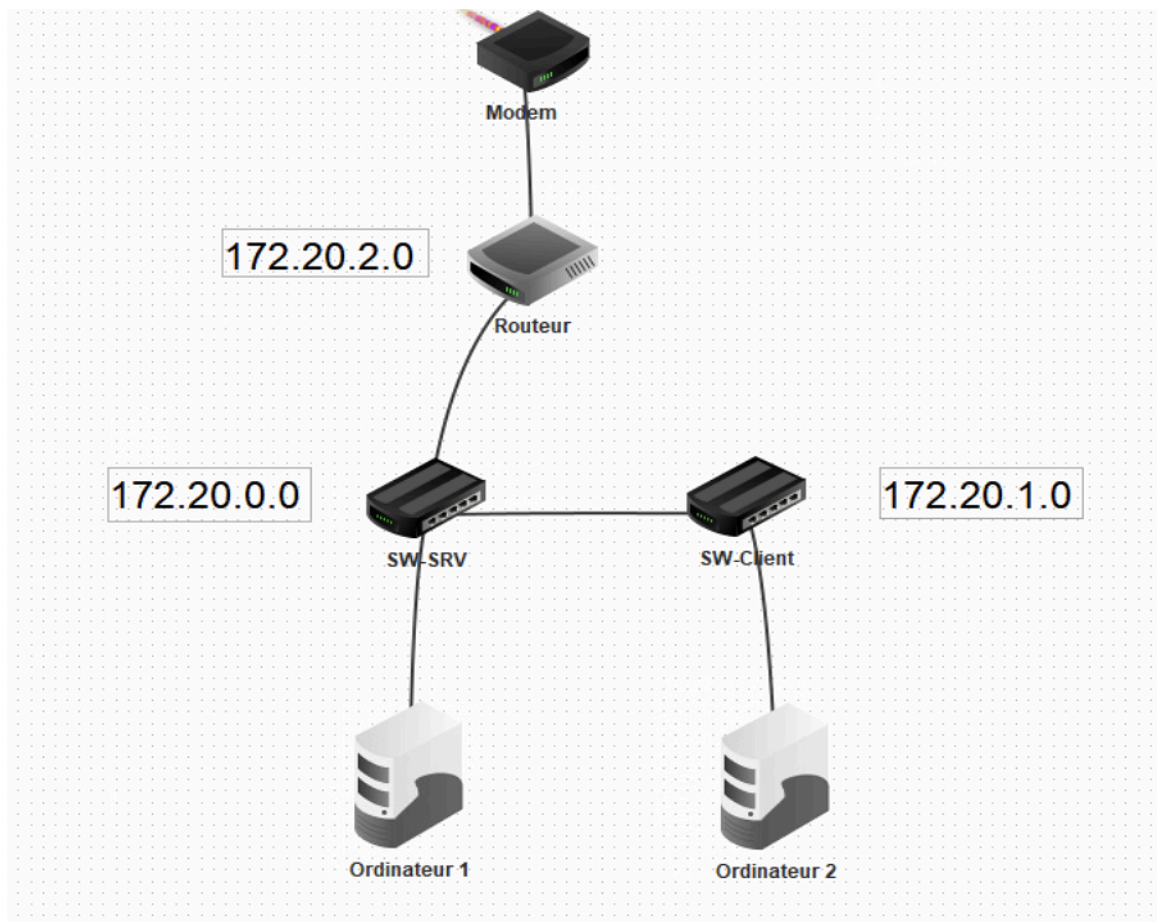
### VLAN 30 (Routeur)

Ici, avec un masque /25, la taille du sous-réseau est réduite, car seulement **126 adresses utilisables** sont nécessaires pour les besoins du routeur et des interconnexions. Cela montre une segmentation fine pour éviter le gaspillage d'adresses. Un VLAN dédié aux interconnexions routeur/switch sert pour les communications internes entre les équipements réseaux.

Précision : les VLAN techniques sont définies pour isoler et organiser le trafic réseau selon les équipements et leur rôle dans l'infrastructure. Ils permettent d'organiser le réseau de manière logique pour répondre aux besoins de sécurité, et cela indépendamment de la structure organisationnelle (Services administration, équipes et Wi-Fi).

Les services fonctionnels regroupent des personnes et de postes, mais ces derniers utilisent souvent différents types d'équipements nécessitant une segmentation technique (serveurs, routeurs, etc...). Un service fonctionnel peut donc être réparti sur plusieurs VLAN, et un VLAN peut contenir plusieurs services fonctionnels.

Voici la maquette de notre réseau réalisé sur **Filius** :



## CONFIGURATION DU SWITCH 1 (SERVEUR)

### Réinitialisation des commutateurs

Tout d'abord, nous devons réinitialiser les commutateurs dans le fichier de démarrage, afin de partir sur une base propre, sans aucune ancienne configuration.

**#erase startup-config** > Efface la configuration de démarrage actuelle, dans le fichier de démarrage. Cela réinitialise donc le commutateur

**#delete flash:vlan.dat** > Supprime le fichier de données VLAN, pour effacer toutes les configurations VLAN précédentes spécifiques à la segmentation VLAN

**#reload** > Redémarre le commutateur pour appliquer les changements

```
Switch>en
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV BLOCK INIT: Initialized the geometry of nvram
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0003.E449.021E
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4670455
flashfs[0]: Bytes available: 59345929
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...
##### [OK]
```

### Renommage du switch

Puis, entrer à nouveau en mode privilégié sur le switch pour le renommer :

**#enable** > entrer en mode privilégié

**#conf t** > accéder à la configuration du switch  
**#hostname SW1-SRV** > pour renommer le switch en "SW1-SRV"

```
Switch>en
Switch#Conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1-SRV
```

### Configuration des commutateurs avec VTP

**#vtp mode server** > configure le commutateur SW1-SRV en mode VTP Server, permettant la gestion des VLANs (le mode serveur est celui par défaut)  
**#vtp domain Stadium.local** > définit le domaine VTP pour synchroniser les informations des VLANs avec les autres commutateurs.

```
SW1-SRV(config)#vtp mode server
Device mode already VTP SERVER.
SW1-SRV(config)#vtp domain Stadium.local
Changing VTP domain name from NULL to Stadium.local
SW1-SRV(config)#
```

---

### Administration et Gestion des VLANs

Nous allons maintenant créer les VLANs et les renommer.

**#vlan 10** > pour créer un VLAN, il suffit d'entrer la commande suivante avec son numéro  
**#name Administration** > Nomme le VLAN 10 qui s'appelle désormais "Administration"

```
SW1-SRV(config)#vlan 10
SW1-SRV(config-vlan)#name Administration
SW1-SRV(config-vlan)#exit
SW1-SRV(config)#vlan 20
SW1-SRV(config-vlan)#name Equipes
SW1-SRV(config-vlan)#exit
SW1-SRV(config)#vlan 30
SW1-SRV(config-vlan)#name WiFi
SW1-SRV(config-vlan)#
```

### Attribution des Ports aux VLANs

Nous passons en mode interface pour désigner la range des ports de chaque VLAN, après les avoir configuré en tant que port d'accès :

**#interface range fastEthernet 0/1 - 6** > permet de sélectionner plusieurs interfaces pour les configurer en une seule fois

**#switchport mode access** > indique explicitement que ces interfaces doivent fonctionner en mode accès (cad qu'elles n'appartiennent qu'à 1 seul VLAN)  
**#switchport access vlan 10** > Indique que le VLAN auquel les ports seront associés est le VLAN 10  
**#exit** > on sort de la range créée pour revenir en mode de configuration global  
On réitère les lignes de commandes pour chaque range d'interfaces :

**#interface range fastEthernet 0/7 - 12**  
**#switchport mode access**  
**#switchport access vlan 20**  
**#exit**  
**#interface range fastEthernet 0/13 - 14**  
**#switchport mode access**  
**#switchport access vlan 30**  
**#exit**

```
SW1-SRV(config)#interface range fastEthernet0/1-6
SW1-SRV(config-if-range)#switchport mode access
SW1-SRV(config-if-range)#switchport access vlan 10
SW1-SRV(config-if-range)#exit
SW1-SRV(config)#interface range fastEthernet0/7-12
SW1-SRV(config-if-range)#switchport mode access
SW1-SRV(config-if-range)#switchport access vlan 20
SW1-SRV(config-if-range)#exit
SW1-SRV(config)#interface range fastEthernet0/13-14
SW1-SRV(config-if-range)#switchport mode access
SW1-SRV(config-if-range)#switchport access vlan 30
SW1-SRV(config-if-range)#exit
SW1-SRV(config)#
```

**#show vlan** > On sort du mode configuration global pour vérifier que la configuration mise en place est correcte

```
SW1-SRV#show vlan
```

| VLAN | Name               | Status | Ports  |
|------|--------------------|--------|--|
| 1    | default            | active | Fa0/15, Fa0/16, Fa0/17, Fa0/18<br>Fa0/19, Fa0/20, Fa0/21, Fa0/22<br>Fa0/23, Gig0/1, Gig0/2 |
| 10   | Administration     | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4<br>Fa0/5, Fa0/6   |
| 20   | Equipes            | active | Fa0/7, Fa0/8, Fa0/9, Fa0/10<br>Fa0/11, Fa0/12  |
| 30   | WiFi               | active | Fa0/13, Fa0/14   |
| 1002 | fddi-default       | active |  |
| 1003 | token-ring-default | active |  |
| 1004 | fddinet-default    | active |  |
| 1005 | trnet-default      | active |  |

| VLAN | Type  | SAID   | MTU  | Parent | RingNo | BridgeNo | Stp  | BrdgMode | Trans1 | Trans2 |
|------|-------|--------|------|--------|--------|----------|------|----------|--------|--------|
| 1    | enet  | 100001 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 10   | enet  | 100010 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 20   | enet  | 100020 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 30   | enet  | 100030 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 1002 | fddi  | 101002 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 1003 | tr    | 101003 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 1004 | fdnet | 101004 | 1500 | -      | -      | -        | ieee | -        | 0      | 0      |
| 1005 | trnet | 101005 | 1500 | -      | -      | -        | ibm  | -        | 0      | 0      |

| VLAN  | Type  | SAID  | MTU   | Parent | RingNo | BridgeNo | Stp   | BrdgMode | Trans1 | Trans2 |
|-------|-------|-------|-------|--------|--------|----------|-------|----------|--------|--------|
| ----- | ----- | ----- | ----- | -----  | -----  | -----    | ----- | -----    | -----  | -----  |

```
Remote SPAN VLANs
```

| Primary | Secondary | Type  | Ports |
|---------|-----------|-------|-------|
| -----   | -----     | ----- | ----- |

```
SW1-SRV#
```

### Création des Ports Trunk

Ces deux lignes de commandes permettent de configurer le commutateur pour qu'il gère les VLANs et facilite la communication entre les deux switches via les ports trunk.

**#interface range fastEthernet 0/22 - 24** > sélectionne les interfaces FastEthernet 0/22 à 0/24 pour les configurer en mode trunk.

**#switchport mode trunk** > configure ces interfaces pour transporter plusieurs VLANs entre les commutateurs.

**#no shutdown** : active les interfaces

Pour les anciens modèles de switches, il est possible que le mode trunk soit refusé tel quel, car il faut au préalable préciser le **mode de tagage**, qui était à l'époque encore divisé en **2 tags** : le tagage **dot1q** et la norme **ISL** (disparue sur les équipements plus récents)

**#switchport trunk encapsulation dot1Q** > pour spécifier le tagage

**#switchport mode trunk** > on peut entrer cette fois-ci la commande  
**#no shutdown** : active les interfaces  
**#show interfaces trunk** > permet de vérifier que les ports sélectionnés précédemment sont bien en mode trunk

```
SW1-SRV(config)#interface range fastEthernet 0/22-24
SW1-SRV(config-if-range)#switchport mode trunk

SW1-SRV(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SW1-SRV(config-if-range)#
```

Par soucis de vérification :

Le fichier running-config contient tous les paramètres actifs de l'appareil (interface réseau, VLANs, les routes, etc...). Chaque changement de configuration sur le switch est appliqué à ce fichier, mais ne sont pas permanents tant qu'ils ne sont pas sauvegardés dans le fichier startup-config, stocké dans la NVRAM :

**#show run interface fastEthernet 0/22** > affiche la configuration actuelle de l'interface choisie (ici /22) dans le fichier de configuration en cours (running-config)

**#interface fastEthernet 0/22** > permet d'entrer dans une interface spécifique et d'agir dessus si besoin

**#show ip interface brief** > pour vérifier rapidement l'état IP et le statut général des interfaces.

**#show interfaces status** > pour des informations détaillées sur la connectivité physique, la vitesse, le duplex, et les VLANs associés aux ports trunk

**#show vlan brief** > Affiche un résumé des VLANs configurés sur le switch

Il est normal que les ports **0/22** et **0/23** restent "down" pour le moment, car le 2ème switch n'est pas encore configuré

**#copy running-config startup-config** > Copie la configuration du fichier running-config en cours vers le fichier de démarrage startup-config

**Le SW-SRV est désormais configuré !**

## CONFIGURATION DU SWITCH 2 (CLIENT)

### Réinitialisation des commutateurs

De la même manière que pour le switch Serveur, nous devons réinitialiser les commutateurs dans le fichier de démarrage, afin de partir sur une base propre, sans aucune ancienne configuration.

**#erase startup-config** > Efface la configuration actuelle enregistrée dans le fichier de démarrage. Cela réinitialise donc le commutateur

**#delete flash:vlan.dat** > Supprime le fichier VLAN, pour effacer toutes les configurations VLAN précédentes

**#reload** > Redémarre le commutateur pour appliquer les changements

```
Switch>
Switch>en
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0050.0F95.4EA1
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4670455
flashfs[0]: Bytes available: 59345929
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...
##### [OK]
```

### Renommage du deuxième switch

Puis, entrer à nouveau en mode privilégié sur le switch pour le renommer :

**#enable** > entrer en mode privilégié

**#conf t** > accéder à la configuration du switch

**#hostname SW2-Client** > pour renommer le switch en "SW-Client"

```
Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW2-Client
SW2-Client(config)#
```

### Configuration des commutateurs



**#vtp mode client** > configure le commutateur SW2-Client en mode VTP Client, ce qui signifie qu'il recevra les informations de VLAN du serveur VTP sans pouvoir en créer ou modifier

**#vtp domain Stadium.local** > définit (ou vérifie) le domaine VTP pour synchroniser les informations des VLANs avec les autres commutateurs. Cela garantit que le switch appartient au domaine VTP nommé Stadium.local, garantissant que les informations VLAN sont synchronisées entre les switches du même domaine.

```
SW2-Client(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2-Client(config)#vtp domain Stadium.local
Domain name already set to Stadium.local.
SW2-Client(config)#
```

### Attribution des Ports aux VLANs

Sur le SW2-Client, il n'est pas nécessaire de créer les VLANs manuellement, **car ce switch est en mode VTP Client et recevra donc automatiquement toutes les informations des VLANs depuis le SW1-Server.**

Nous passons directement à l'étape de configuration des Ports VLANs.

```
SW2-Client(config)#interface range fastEthernet0/1-6
SW2-Client(config-if-range)#switchport mode access
SW2-Client(config-if-range)#switchport access vlan 10
SW2-Client(config-if-range)#exit
SW2-Client(config)#interface range fastEthernet0/7-12
SW2-Client(config-if-range)#switchport mode access
SW2-Client(config-if-range)#switchport access vlan 20
SW2-Client(config-if-range)#exit
SW2-Client(config)#interface range fastEthernet0/13-14
SW2-Client(config-if-range)#switchport mode access
SW2-Client(config-if-range)#switchport access vlan 30
SW2-Client(config-if-range)#exit
SW2-Client(config)#
```

### Création des Ports Trunk

La commande configure les interfaces FastEthernet 0/22 à 0/24 du switch SW2-Client en mode trunk, permettant à ces ports de transporter du trafic pour plusieurs VLANs simultanément.

**#interface range fastEthernet 0/22 - 24** > sélectionne les interfaces FastEthernet 0/22 à 0/24 pour les configurer en mode trunk.

**#switchport mode trunk** > configure ces interfaces pour transporter plusieurs VLANs entre les commutateurs.

**#no shutdown** > active toutes les interfaces

```
SW2-Client(config)#interface range fastEthernet0/22-24
```

```
SW2-Client(config-if-range)#switchport mode trunk
```

```
SW2-Client(config-if-range)#
```

**#show interfaces trunk** > permet de vérifier que les ports sélectionnées précédemment sont bien en mode trunk

**#show ip interface brief** > pour vérifier rapidement l'état IP et le statut général des interfaces.

**#show interfaces status** > pour des informations détaillées sur la connectivité physique, la vitesse, le duplex, et les VLANs associés (dont les ports trunk)

**#show vlan brief** > Affiche un résumé des VLANs configurés sur le switch

**#copy running-config startup-config** > Copie la configuration en cours vers la configuration de démarrage

```
SW2-Client#sh vlan
```

| VLAN | Name               | Status | Ports  |
|------|--------------------|--------|--|
| 1    | default            | active | Fa0/15, Fa0/16, Fa0/17, Fa0/18<br>Fa0/19, Fa0/20, Fa0/21, Fa0/22<br>Fa0/23, Gig0/1, Gig0/2 |
| 10   | Administration     | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4<br>Fa0/5, Fa0/6   |
| 20   | Equipes            | active | Fa0/7, Fa0/8, Fa0/9, Fa0/10<br>Fa0/11, Fa0/12  |
| 30   | WiFi               | active | Fa0/13, Fa0/14   |
| 1002 | fddi-default       | active |  |
| 1003 | token-ring-default | active |  |
| 1004 | fddinet-default    | active |  |
| 1005 | trnet-default      | active |  |

| VLAN | Type  | SAID   | MTU  | Parent | RingNo | BridgeNo | Stp  | BrdgMode | Trans1 | Trans2 |
|------|-------|--------|------|--------|--------|----------|------|----------|--------|--------|
| 1    | enet  | 100001 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 10   | enet  | 100010 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 20   | enet  | 100020 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 30   | enet  | 100030 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 1002 | fddi  | 101002 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 1003 | tr    | 101003 | 1500 | -      | -      | -        | -    | -        | 0      | 0      |
| 1004 | fdnet | 101004 | 1500 | -      | -      | -        | ieee | -        | 0      | 0      |
| 1005 | trnet | 101005 | 1500 | -      | -      | -        | ibm  | -        | 0      | 0      |

| VLAN | Type | SAID | MTU | Parent | RingNo | BridgeNo | Stp | BrdgMode | Trans1 | Trans2 |
|------|------|------|-----|--------|--------|----------|-----|----------|--------|--------|
|------|------|------|-----|--------|--------|----------|-----|----------|--------|--------|

```
Remote SPAN VLANs
```

```
Primary Secondary Type Ports
```

```
SW2-Client#
```

## CONFIGURATION DU ROUTEUR

### Réinitialisation du routeur et redémarrage

Pour configurer manuellement les interfaces du routeur, nous entrons **no** lors de la proposition de configuration initiale

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Puis on peut entrer les lignes de commande :

**#erase startup-config** > on efface également la configuration de démarrage actuelle  
**#reload** > redémarrage du routeur

```
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by Cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bblc58
Self decompressing the image :
##### [OK]
```

### Renommage du routeur

Toujours en mode config :

**#en**  
**#conf t**  
**#hostname R1-Stade**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1-Stade
R1-Stade(config)#
```

### Configuration de l'interface fastEthernet 0/1 en DHCP

On va maintenant suivre une série d'étapes afin de configurer le NAT/PAT sur les interfaces et le routage inter-VLANs.

#### On commence par activer l'interface fastEthernet 0/1

La commande **no shut** sur l'**interface fastEthernet 0/1** sert à activer l'interface réseau sur le routeur. Par défaut, une interface est souvent désactivée (en état

administrativement down), et cette commande permet de la rendre opérationnelle, autorisant ainsi le passage du trafic réseau.

**#interface fastEthernet 0/1**  
**#no shut**

```
R1-Stade(config)#interface fastEthernet 0/1
R1-Stade(config-if)#no shu
```

```
R1-Stade(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
```

On définit l'interface externe pour le NAT :

Maintenant que l'**interface fastEthernet 0/1** du routeur R1 est activée, on veut obtenir une **adresse IP via DHCP**, puis la définir comme **interface NAT extérieure**, permettant ainsi de traduire les adresses IP internes vers l'extérieur du réseau.

**#ip address dhcp** > configure l'interface pour obtenir dynamiquement une adresse IP via DHCP

**#ip nat outside** > définit l'interface comme étant l'interface NAT extérieure. Cela signifie que tout le trafic sortant de l'interface sera soumis à la traduction d'adresses IP (NAT), permettant ainsi aux adresses IP privées de communiquer avec des réseaux extérieurs

```
R1-Stade(config-if)#ip address dhcp
R1-Stade(config-if)#ip nat outside
R1-Stade(config-if)#
```

---

#### Configuration de l'interface fastEthernet 0/0 en NAT intérieur

Il faut attribuer une adresse IP à l'interface FastEthernet 0/0 du routeur, pour garantir la connectivité réseau et définir correctement les interfaces "inside" et "outside" :

**# interface fastEthernet 0/0** > Sélectionne l'interface FastEthernet 0/0

**# no shutdown** > Active l'interface

**# ip nat inside** > Définit cette interface comme l'interface NAT interne

```

R1-Stade(config)#interface fastEthernet 0/0
R1-Stade(config-if)#no shutdown

R1-Stade(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

R1-Stade(config-if)#ip nat inside

```

On crée et configure les interfaces interne pour le NAT :

Afin de communiquer entre chaque VLANs, nous allons devoir configurer l'adresse passerelle de chaque VLANs sur le routeur, sur le port 0/0 (côté switch) à l'aide des commandes suivantes :

VLAN 10 :

**#interface fastEthernet 0/0.10** → sélectionne la sous-interface 0/0.10 sur l'interface fastEthernet 0/0

**#encapsulation dot1Q 10** → configure l'encapsulation de la sous-interface en utilisant le protocole IEEE 802.1Q

**#ip address 172.20.0.1 255.255.255.0** → attribue l'adresse IP et le masque à la sous-interface. Cette adresse sera utilisée par les dispositifs dans le VLAN 10 comme passerelle par défaut pour communiquer avec d'autres réseaux.

**#ip nat inside** → marque la sous-interface comme étant à l'intérieur du réseau NAT. Ainsi, les adresses IP des dispositifs connectés à ce VLAN seront traduites lorsque le trafic sortira vers l'extérieur du réseau.

**#exit** → on sort de la configuration de la sous-interface

On répète l'opération pour les VLANs 20 et 30 en adaptant les adresses IP et les masques de sous-réseau :

VLAN20 :

**#interface fastEthernet 0/0.20**

**#encapsulation dot1Q 20**

**#ip address 172.20.1.1 255.255.255.0**

**#ip nat inside**

**#exit**

VLAN 30 :

```
#interface fastEthernet 0/0.30
#encapsulation dot1Q 30
#ip address 172.20.2.1 255.255.255.128
#ip nat inside
#exit
```

```
R1-Stade(config)#interface fastEthernet 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)#ip nat inside
R1-Stade(config-subif)#exit
R1-Stade(config)#interface fastEthernet 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)#ip nat inside
R1-Stade(config-subif)#exit
R1-Stade(config)#interface fastEthernet 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)#ip nat inside
R1-Stade(config-subif)#exit
R1-Stade(config)#
```

**Précision :** La passerelle n'est pas un équipement physique distinct, mais une **adresse IP attribuée à une interface ou sous-interface sur le routeur**. Cette adresse logique agit comme le point de sortie pour les appareils dans chaque VLAN, leur permettant de communiquer avec d'autres réseaux ou VLANs.

### Configuration des listes d'accès pour le NAT

Créer une liste d'accès qui permet au réseaux des VLANs d'utiliser le NAT

VLAN 10 :

**#access-list 10 permit 172.20.0.0 0.0.0.255** > Permet aux adresses du réseau 172.20.0.0/24 d'utiliser le NAT

VLAN 20 :

**#access-list 20 permit 172.20.1.0 0.0.0.255** > Permet aux adresses du réseau 172.20.1.0/24 d'utiliser le NAT

VLAN 30 :

**#access-list 30 permit 172.20.2.0 0.0.0.127** > Permet aux adresses du réseau 172.20.2.0/25 d'utiliser le NAT

```
R1-Stade(config)#access-list 10 permit 172.20.0.0 0.0.0.255
R1-Stade(config)#access-list 20 permit 172.20.1.0 0.0.0.255
R1-Stade(config)#access-list 30 permit 172.20.2.0 0.0.0.127
R1-Stade(config)#
```



Précision sur la liste d'accès unique : Plutôt que de créer une liste d'accès par VLAN (10, 20, 30) comme c'est le cas ici, il est plus courant de regrouper toutes les adresses des VLANs dans une seule liste d'accès pour le NAT. Cela simplifie la configuration et l'application de la liste d'accès au NAT. Cependant, nous choisissons de créer plusieurs listes dans un souci de meilleure visibilité.

#### Activation du NAT pour chaque VLAN avec la commande **ip nat**

VLAN 10 :

**#ip nat inside source list 10 interface fastEthernet 0/1 overload** > Active la traduction d'adresses NAT pour les adresses listées dans la liste d'accès 10 via l'interface externe fastEthernet 0/1, avec surcharge (PAT)

VLAN 20 :

**#ip nat inside source list 20 interface fastEthernet 0/1 overload** > Active le NAT pour le VLAN 20, utilisant également l'interface externe fastEthernet 0/1

VLAN 30 :

**#ip nat inside source list 30 interface fastEthernet 0/1 overload** > Active le NAT pour le VLAN 30, utilisant également l'interface externe fastEthernet 0/1

```
R1-Stade(config)#ip nat inside source list 10 interface fastEthernet 0/1 overload
R1-Stade(config)#ip nat inside source list 20 interface fastEthernet 0/1 overload
R1-Stade(config)#ip nat inside source list 30 interface fastEthernet 0/1 overload
```

#### Configuration IP du Routeur 2

**#ip address 10.0.228.1 255.255.254.0** > adresse ip et masque du serveur DNS de l'école (représenté par un "modem" sur l'illustration sur [Filius page 8](#) )

**# no shutdown** > active l'interface

```
(config-if)#ip address 10.0.228.1 255.255.254.0
(config-if)#no shutdown
(config-if)#exit
```

**# exit** → Quitte le mode de configuration de l'interface

```
R1-Stade(config)#interface fastEthernet 0/1
R1-Stade(config-if)#ip address 10.0.228.30 255.255.254.0
R1-Stade(config-if)#no shutdown
R1-Stade(config-if)#ip nat outside
R1-Stade(config-if)#exit
R1-Stade(config)#
```

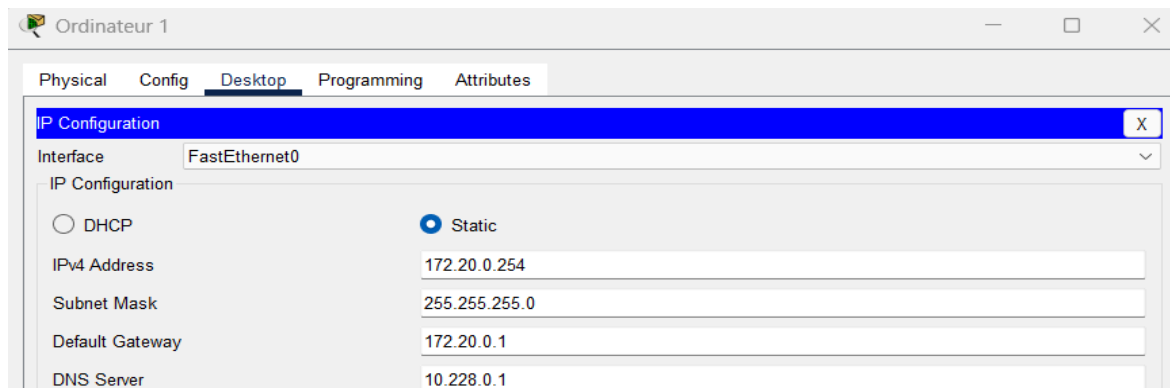
## **Test de la configuration**

#### Vérification des traductions NAT

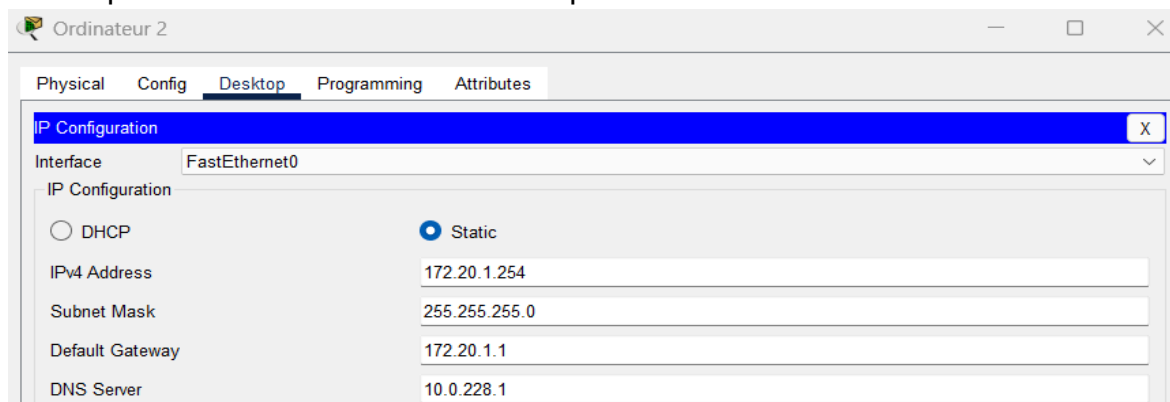
On vérifie d'abord que le NAT fonctionne bien, avant d'ajouter la route par défaut, pour assurer que le trafic peut sortir vers l'extérieur.

On va donc simuler un ping depuis le routeur vers l'Ordinateur 1 qui est sur le VLAN 10. C'est l'occasion de configurer ce PC :

- On clique sur **Ordinateur 1** puis sur **Desktop**, puis sur **IP Configuration**, et on entre les données suivantes :



On fait pareil avec l'Ordinateur 2 en adaptant les informations :



Puis on test la connectivité :

**#ping 172.20.0.1** → Ping la passerelle (de la sous-interface fastEthernet 0/0.10 elle-même posée sur l'interface fastEthernet 0/0 définie sur le routeur) depuis le PC1

```
C:\>ping 172.20.0.1

Pinging 172.20.0.1 with 32 bytes of data:

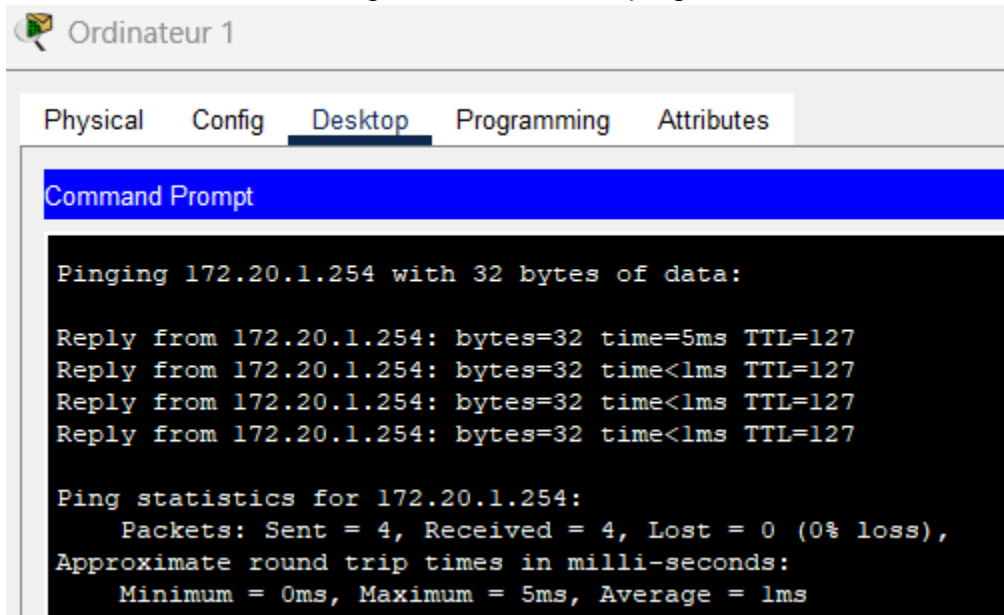
Reply from 172.20.0.1: bytes=32 time=3ms TTL=255
Reply from 172.20.0.1: bytes=32 time<1ms TTL=255
Reply from 172.20.0.1: bytes=32 time<1ms TTL=255
Reply from 172.20.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.20.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

**#ping 10.228.0.1** → Ping le serveur DNS depuis le PC1

```
Ping statistics for 10.0.228.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

L'inter-VLAN fonctionne également : le PC1 ping le PC2 avec succès



**#show ip nat translation** → Affiche les traductions NAT en cours, avec de l'activité (ping continu)

[Ajout de la route par défaut](#)

# ip route 0.0.0.0 0.0.0.0 10.0.228.1 > Définit une route par défaut pour diriger le trafic vers l'extérieur, via l'interface fastEthernet 0/1

## V) Conclusion

Stadium, ayant rencontré des difficultés avec son réseau vieillissant et mal organisé, a entrepris un projet ambitieux de modernisation de son infrastructure pour répondre aux besoins croissants liés à l'organisation d'événements et à l'amélioration des services clients.

La solution technique repose sur la segmentation du réseau en sous-réseaux adaptés via le VLSM, ainsi que la gestion optimisée des VLANs grâce au protocole VTP. Le choix de VLANs statiques permet d'améliorer la sécurité et la gestion du réseau, en garantissant que chaque appareil soit associé au bon sous-réseau, selon ses fonctions et besoins spécifiques. Enfin, la mise en place du routage inter-VLAN et des

mécanismes NAT/PAT sur le routeur assure la fluidité des communications entre les différents sous-réseaux et facilite l'accès à l'extérieur du réseau.

Ce projet de modernisation, fondé sur une approche méthodique et des technologies de pointe, permet à Stadium de relever les défis futurs en matière de connectivité et d'événements, tout en optimisant la gestion des ressources et en améliorant l'expérience client.