

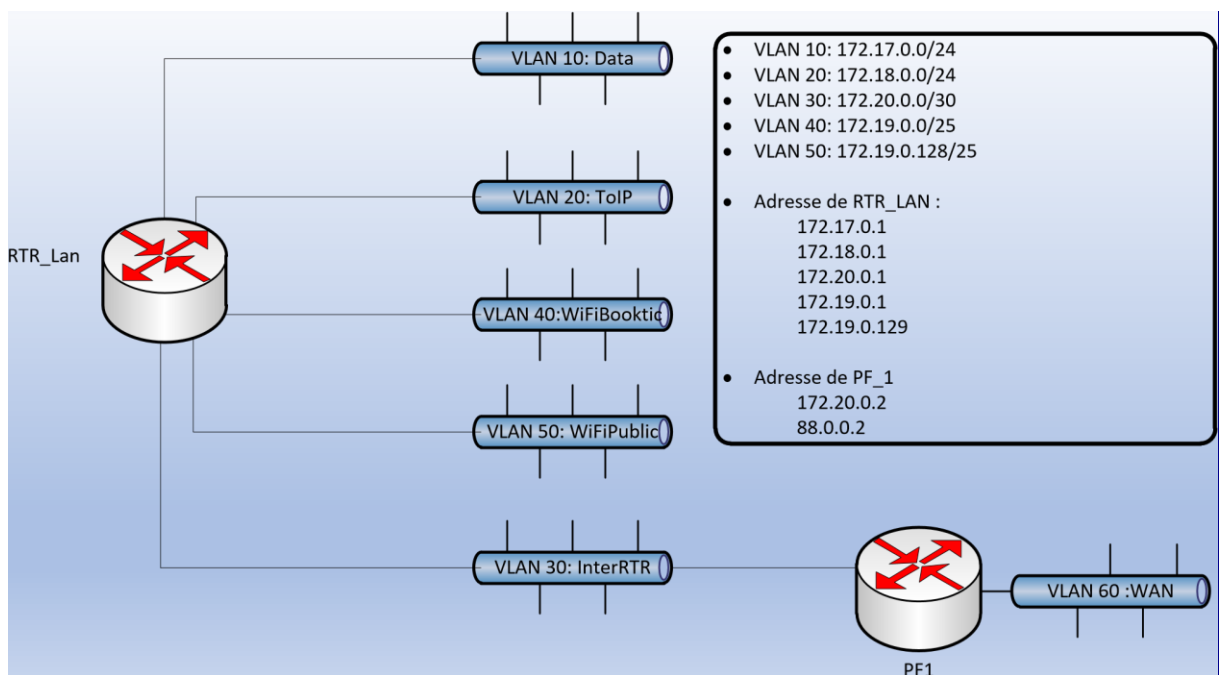
TP3 Maquettage de VLANs et Routage INTER VLAN

Un VLAN (Virtual Local Area Network) est un réseau local virtuel qui permet de segmenter un réseau physique en plusieurs sous-réseaux. Les ordinateurs rattachés à un même VLAN peuvent communiquer entre eux comme s'ils étaient sur le même réseau physique, même s'ils sont physiquement éloignés. Cette technique permet de gérer plus facilement le réseau et de limiter les accès à certaines ressources.

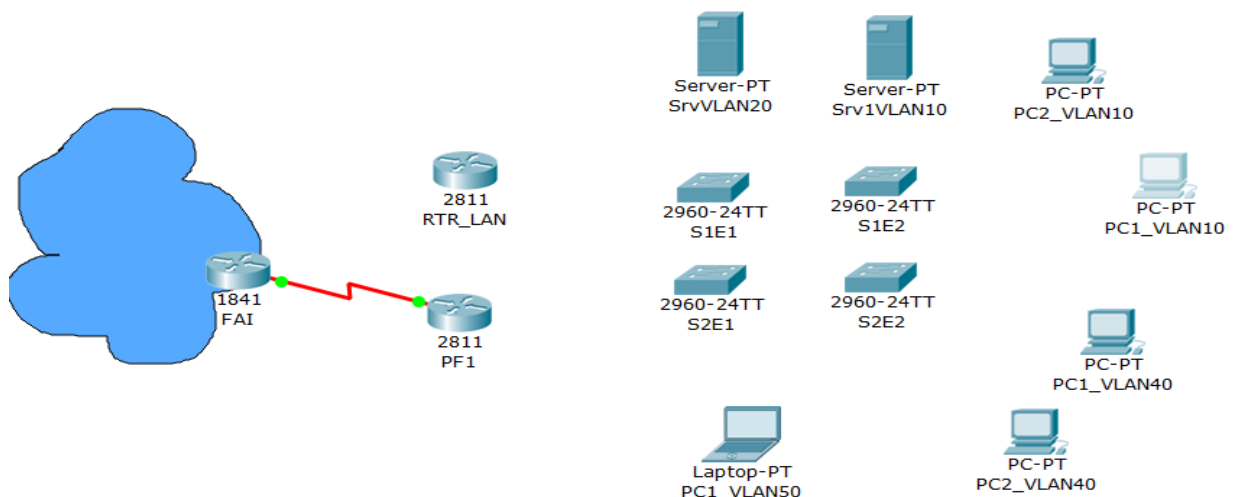
Objectifs de la maquette :


- Celle-ci ne représentera pas tous les ordinateurs du réseau mais quelques exemples dans chaque VLAN pour tester la communication.
- Elle mettra en œuvre des commutateurs et routeurs de tests respectant les noms et les configurations proposés dans le TP.

La segmentation est décrite sur le schéma ci-dessous :



1. Création des réseaux et manipulation



- Après avoir au préalable copiez le fichier B2_TP3_VLAN_routage.pkt. ci-dessus 
- On procèdera à l'adressage des machines et à la création des réseaux selon le tableau fourni en annexe.

Nom de la machine	VLAN	Adresse IP	masque	Passerelle	Commutateur de connexion
PC1_VLAN10	10	172.17.0.2	255.255.255.0	172.17.0.1	S2E1
PC2_VLAN10	10	172.17.0.3	255.255.255.0	172.17.0.1	S2E1
Srv1VLAN10	10	172.17.0.4	255.255.255.0	172.17.0.1	S1E1
PC1_VLAN40	40	172.19.0.2	255.255.255.128	172.19.0.1	S2E2
PC2_VLAN40	40	172.19.0.3	255.255.255.128	172.19.0.1	S2E2
SrvVLAN20	20	172.18.0.2	255.255.255.0	172.18.0.1	S1E2
PC1_VLAN50	50	172.19.0.138	255.255.255.128	172.19.0.129	S1E2

On va câbler nos PC aux commutateurs selon le tableau fourni en annexe

Commutateurs	VLAN	Ports	Tagué
S1E1	10	2-8	Non
	20	9-12	Non
	40	13-18	Non
	30	19-21	Non
	60	22-23	Non
	-	24	Oui
	-	Giga0/1-2	Oui
S1E2	20	2-17	Non
	40	18-20	Non
	50	21-23	Non
	-	Giga0/1-2	Oui
S2E1	10	2-19	Non
	20	20-21	Non
	40	22-24	Non
	-	Giga0/1-2	Oui
S2E2	10	2-18	Non
	20	19-21	Non
	40	22-24	Non
	-	Giga0/1-2	Oui

- On va relier les commutateurs entre eux comme ceci :

Les ports Gigabits 0/1 et 0/2 de tous les commutateurs ainsi que le port FA0/24 de S1E1 sont réservés aux liens tagués.

Les commutateurs sont liés entre eux via des ports Gigabits, le Gigabit 0/1 en priorité :

S1E1 Giga 0/1 ? ? S1E2 Giga 0/1

S1E1 Giga 0/2 ? ? S2E1 Giga 0/1

S2E1 Giga 0/2 ? ? S2E2 Giga 0/1

Le ports FA0/24 de S1E1 permet de relier le routeur RTR_LAN via son port FA 0/0

2. L'environnement CLI (console line interface)

Exemple sur le switch S1E1

On se met en mode **enable** en tapant la commande **enable** (pour être en super utilisateur #)

```
Switch>enable
Switch#
```

Avec la commande **show version** . On repère les informations essentielles fournies :

- la version de l'IOS
- le nom du fichier
- la valeur du registre de configuration

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 0002.166E.50C2
Motherboard assembly number    : 73-9832-06
Power supply part number       : 341-0097-02
Motherboard serial number      : FOC103248MJ
Power supply serial number     : DCA102133JA
Model revision number          : B0
Motherboard revision number    : C0
Model number                   : WS-C2960-24TT
System serial number           : FOC103321EY
```

En mode super-utilisateur, on teste les commandes suivantes :

- ?
- s?
- show ?

```
Switch#? ←
Exec commands:
clear          Reset functions
clock          Manage the system clock
configure      Enter configuration mode
connect        Open a terminal connection
copy           Copy from one file to another
debug          Debugging functions (see also 'undebug')
delete         Delete a file
dir            List files on a filesystem
disable        Turn off privileged commands
disconnect     Disconnect an existing network connection
enable         Turn on privileged commands
erase          Erase a filesystem
exit           Exit from the EXEC
logout         Exit from the EXEC
more           Display the contents of a file
no             Disable debugging informations
ping           Send echo messages
reload         Halt and perform a cold restart
resume         Resume an active network connection
setup          Run the SETUP command facility
show           Show running system information
```

```
Switch#s? ←
setup show ssh
Switch#s
```

```
Switch#show ? ←
access-lists  List access lists
arp            Arp table
boot          show boot attributes
cdp           CDP information
clock         Display the system clock
crypto        Encryption module
dhcp          Dynamic Host Configuration Protocol status
dtp           DTP information
etherchannel  EtherChannel information
flash:        display information about flash: file system
history       Display the session command history
hosts         IP domain-name, lookup style, nameservers, and host table
interfaces    Interface status and configuration
ip            IP information
ipv6          IPv6 information
logging       Show the contents of logging buffers
mac           MAC configuration
mac-address-table MAC forwarding table
mls           Show MultiLayer Switching information
port-security Show secure port information
privilege     Show current privilege level
processes     Active process statistics
```

On vérifie la configuration du **switch** (commutateur) avec un **show startup-config** et **show running-config**

```
Switch#show startup-config
startup-config is not present
Switch#
```

La commande **show startup-config** ne fonctionne pas car aucun fichier n'a été configuré comme l'indique la capture d'écran ci-dessus

```
Switch#show running-config
Building configuration...

Current configuration : 1043 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
--More--
```

On exécute la commande **copy running-config startup-config**

```
Switch#show startup-config ←
Using 1043 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
```

Cette fois ci le **startup-config** contient des éléments

On va ensuite se mettre en mode **enable** puis en mode **conf t** et donner un nom à notre appareil avec la commande **hostname** puis **reload** (faire un copie avant avec la commande « **wr m** » !)

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
(config)#hostname S1E1
```

```
S1E1#wr m
Building configuration...
[OK]
S1E1#reload
Proceed with reload? [confirm]
```

On va protéger le mode enable en mettant un mot de passe grâce à **enable secret ...**

```
S1E1>enable
S1E1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1E1(config)#enable secret Ligfy!
S1E1(config)#end
S1E1#
%SYS-5-CONFIG_I: Configured from console by console

S1E1#wr m
Building configuration...
[OK]
S1E1#
```

Vérifions si le mot de passe apparait bien en mode **crypté** avec la commande **show running-config**

```
S1E1# show running-config
Building configuration...

Current configuration : 1090 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1E1
!
enable secret 5 $1$mERr$OkM/BZP6szHkRTajalQ9C0
!
```

On va configurer notre appareil pour ne plus faire apparaître les logs à l'écran afin d'éviter une recherche DNS extérieure systématique avec les commandes suivantes :

no logging console

no ip domain-lookup

```
no logging console
enable secret 5 $1$mERr$OkM/BZP6szHkRTajalQ9C0
!
!
!
no ip domain-lookup
```

En tapant la commande running on voit que le **no logging console** et le **no ip domain-lookup** apparaissent bien.

3. Création des VLANs

On va maintenant créer les VLANs sur chaque commutateur **en respectant les contraintes de noms et de numérotation du schéma** (ex avec le switch **S1E1** pour les Vlan 10 et Vlan 20)

```
S1E1>enable
Password:
S1E1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1E1(config)#vlan 10
S1E1(config-vlan)#name data
S1E1(config-vlan)#wr m
% Invalid input detected at '^' marker.
S1E1(config-vlan)#end
S1E1#wr m
Building configuration...
[OK]
S1E1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1E1(config)#vlan 20
S1E1(config-vlan)#name ToIP
S1E1(config-vlan)#exit
S1E1(config)#vlan exit
```

- On va affecter les ports **non tagués** sur chaque commutateur **tel que cela est décrit dans le tableau** (réitérer la même opération pour l'ensemble des vlan de S1E1 puis faire de même avec l'ensemble des autres commutateurs)

```
S1E1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1E1(config)#interface range Fast
S1E1(config)#interface range FastEthernet 0/2-8
S1E1(config-if-range)#switchport mode access
S1E1(config-if-range)#switchport access vlan 10
S1E1(config-if-range)#
```

- Nous allons déterminer une méthode pour tester en utilisant les PC à notre disposition : Si la communication est possible dans un VLAN
Si la communication est possible hors de ce VLAN

Pour vérifier si la communication est possible dans un VLAN entre 2 machines , il suffit de faire un ping. On s'aperçoit que les machines d'un même Vlan peuvent communiquer entre elles, mais que les machines de Vlan différent ne peuvent pas.

4. Routage INTERVLAN

a) Gestion des liens tagués

- Les différents commutateurs doivent être reliés entre eux via un lien tagué afin de permettre la communication entre les VLANs
- Les commandes suivantes permettent de créer un lien tagué :

```
S1E1(config)#interface GigabitEthernet 0/1
```

```
S1E1 (config-if)#switchport mode trunk
```

```
S1E1 (config-if)#switchport trunk allowed vlan 10,20,30,40,50,
```

```
S1E1 (config)#interface GigabitEthernet0/1
S1E1 (config-if) #swit
S1E1 (config-if) #switchport mode trunk
S1E1 (config-if) #switchport trunk
S1E1 (config-if) #switchport trunk allowed vlan 10,20,30,40,50,60
S1E1 (config-if) #interface GigabitEthernet0/2
S1E1 (config-if) #switchport mode trunk
S1E1 (config-if) #switchport trunk allowed vlan 10,20,30,40,50,60
S1E1 (config-if) #
```

b) Création des d'une interface virtuelle

Nous devons faire communiquer entre eux le VLANs mais par l'intermédiaire d'un routeur.

Le lien entre le routeur RTR_LAN et le commutateur S1E1 se fait sur le **port 24** du commutateur. Nous allons devoir créer une sous interface virtuelle par VLAN à router .


```
Router#conf t
Router(config)#hostname RTR_LAN
RTR_LAN (config)#interface fa0/0.1
RTR_LAN (config-subif)#encapsulation dot1Q 10
RTR_LAN (config-subif)#ip address 172.17.0.1 255.255.255.0
RTR_LAN (config-subif)#exit
```

(Réitérer cette action à toutes les interfaces)

Pour finir il faut activer l'interface physique du router RTR_LAN avec la commande **no shutdown** sur l'interface **fa0/0**

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

```
RTR_LAN (config-if)# no shutdown
```

