Sommaire :

Introduction

Objectif : L'objectif de ce TP est de réaliser le plan d'adressage IP d'une entreprise, et de mettre en place les services dont ils ont besoin : Serveur DHCP, une borne Wifi et un AD Windows.

Pré-requis : Des connaissances en adresses IP, en VLAN et VTP, en DHCP, en Wifi et en administration Windows Serveur 2008 sont requis.

Norme : Toutes les commandes issues d'une machine avec un système d'exploitation Debian ou Windows sont écrites ***en gras et en italique***.

Mise en situation:

Matériel nécessaire pour le bâtiment A :

RDC :
1er étage : 1 switch de 26 ports (24 ports 10/100 et 2 ports Gigabits/s)
2ème étage : 1 switch de 26 ports (24 ports 10/100 et 2 ports Gigabits/s)
3ème étage : 1 switch de 26 ports (24 ports 10/100 et 2 ports Gigabits/s)
4ème étage : 1 switch de 26 ports (24 ports 10/100 et 2 ports Gigabits/s)

Matériel nécessaire pour le bâtiment B :

Matériel nécessaire pour le bâtiment C :

RDC :
1er étage :
2ème étage : 4 switchs de 48 ports (en Gigabits/s).
3ème étage :
4ème étage :

Adressage IP :

Masque de sous-réseau : 255.255.0.0
Adresse du réseau : 172.16.0.0
Adresse de diffusion : 172.16.255.255
Passerelle par défaut : 172.16.255.254

Bâtiment A :
RDC : Serveur - 172.16.0.0
1er étage: Clients - 172.16.10.0
2ème étage : Clients - 172.16.20.0
3ème étage : Clients - 172.16.30.0
4ème étage : Clients - 172.16.40.0

Bâtiment C :
1er étage : Clients - 172.16.110.0
2ème étage : Clients - 172.16.120.0
3ème étage : 172.16.130.0
4ème étage : 172.16.140.0

Elaboration d'un plan d'adresse IP en DHCP :

10 ligues de sports à héberger :

- Ligue de Quidditch
- Ligue des Justiciers
- Ligue d'Aqua-Poney
- Ligue de Natation
- Ligue de Pong
- Ligue de Joutes
- Ligue des Fléchettes
- Ligue de Pentathlon moderne
- Ligue des Explorateurs
- Ligue Pokémon

On a choisi de mettre en place du sous-réseau et des VLAN. Pour cela, on utilise un masque de sous-réseau de classe C sur notre adresse de classe B. Ainsi, on peut avoir 253 utilisateurs par sous-réseau. Soit : 172.16.0.0 /24

Ensuite, on créer des VLAN pour chaque sous-réseau (cf. tableau).

Mise en place de VLAN et VTP :

En fonction des besoins de l'organisme, le réseau a donc été découpé en sous-réseaux. Chaque Ligue de sport a le droit à un sous-réseau, et à un VLAN.

N° VLAN	Nom du VLAN	Adresse de réseau
10	Ligue de Quidditch	172.16.10.0
11	Ligue Pokémon	172.16.11.0
12	Ligue Joutes	172.16.12.0
13	Ligue de Natation	172.16.13.0
14	Ligue d'Aqua-Poney	172.16.14.0
15	Ligue Pentathlon	172.16.15.0
16	Ligue Fléchette	172.16.16.0
17	Ligue Pong	172.16.17.0
18	Ligue des Justiciers	172.16.18.0
19	Ligue des Explorateurs	172.16.19.0
40	Wifi public	172.16.40.0
50	Filaire salle ressources	172.16.50.0
60	Admin, repro et multi	172.16.60.0
70	Ecrans d'affichages	172.16.70.0
80	DMZ	172.16.80.0
90	Téléphonie IP	172.16.90.0
100	Salle Serveurs	172.16.100.0
199	Administration des Switchs	172.16.199.0

Une fois que la répartition des différents secteurs de l'organisme dans des VLAN et sous-réseaux a été effectué, on créer les VLAN sur un seul Switch, en ajoutant un VLAN Number (10 par exemple) et un VLAN Name (VLAN-Quidditch par exemple). La commande **show vlan** permet de vérifier l'état de tous les VLAN :

```
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------
1    default                             active    Gig0/1, Gig5/1
10   VLAN-Quidditch                      active
11   VLAN-Pokemon                        active
12   VLAN-Joute                          active
13   VLAN-Natation                       active
14   VLAN-AquaPoney                      active
15   VLAN-Pentathlon                     active
16   VLAN-Flechette                      active
17   VLAN-Pong                           active
18   VLAN-Justiciers                     active
19   VLAN-Explorateurs                   active
40   VLAN-PublicWifi                     active
50   VLAN-PublicFil                      active
60   VLAN-Admin                          active
70   VLAN-Ecran                          active
80   VLAN-DMZ                            active
90   VLAN-Telephone                      active
100  VLAN-Serveur                        active
199  VLAN-Switch                         active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup
```

Ensuite, maintenant qu'un Switch connait tous les VLAN, il faut mettre en place le VTP. Le principe du Vlan Trunking Protocol est d'entrer la liste de tous les VLAN dans un seul Switch, qui fera office de « Serveur », afin qu'il diffuse cette liste vers tous les autres Switchs, qui seront alors des « Clients ». Un Switch dit « Transparent » pourra également être mis en place afin de permettre à un administrateur de créer, de supprimer ou de modifier des VLAN sur un seul Switch sans que l'information ne se propage via tous les autres Switchs. Pour mettre en place un VTP, on choisit donc un Switch qui fera office de Serveur, et tous les autres seront des clients (sauf un qui sera transparent). Il faut également penser à mettre tous les Switchs en client avant de configurer le Switch serveur, pour éviter de synchroniser des erreurs. On utilise ensuite les commandes suivantes pour configurer le VTP :

> enable
 # vlan database
(vlan)# vtp serveur
(vlan)# vtp domain ligue
(vlan)# vtp password ligue
(vlan)# exit

Sur les Switchs Clients :

> enable
 # vlan database
(vlan)# vtp client
(vlan)# vtp domain ligue
(vlan)# vtp password ligue
(vlan)# exit

Et sur le Switch Transparent :

> enable
 # vlan database
(vlan)# vtp transparent
(vlan)# vtp domain ligue
(vlan)# vtp password ligue
(vlan)# exit

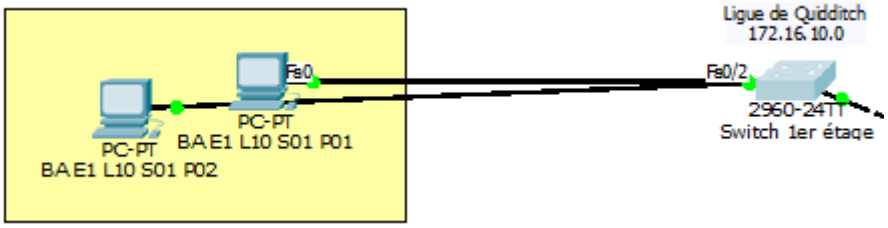
Et pour vérifier leur configuration, on utilise la commande : **show vtp status**

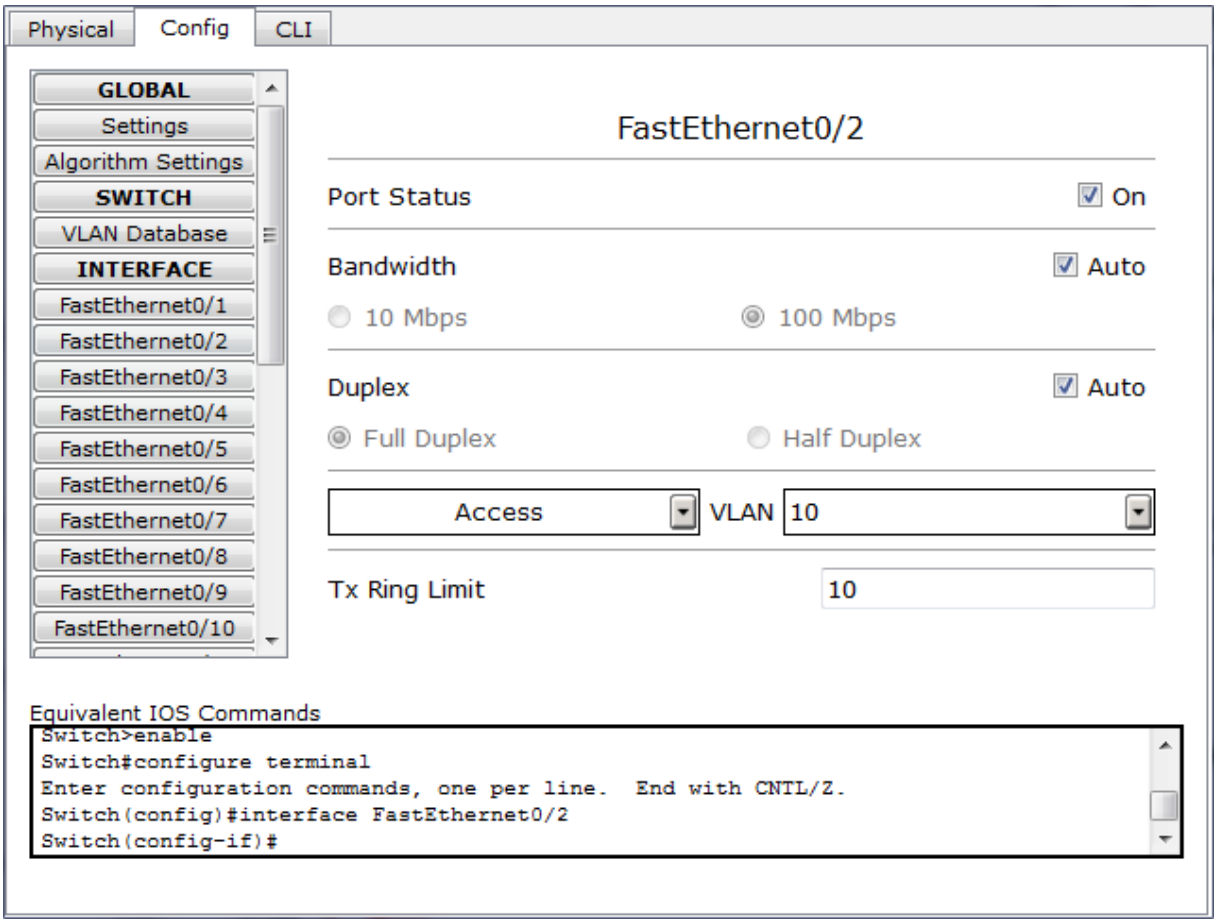
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4/1, changed stat
e to up


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no vlan 25
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 6
Maximum VLANs supported locally : 255
Number of existing VLANs        : 23
VTP Operating Mode              : Server
VTP Domain Name                 : ligue
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x70 0x27 0x52 0x03 0x47 0xDF 0x52 0x1C
Configuration last modified by 0.0.0.0 at 3-1-93 00:03:55
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

On passe ensuite à la mise en place des hôtes dans les différents VLAN, en fonction du plan d'adressage. Une fois la liste des VLAN créée au niveau des Switchs, il faut associer le numéro de port des Switchs auxquelles sont connectés les clients dans le VLAN adéquate :





Nous allons maintenant mettre en place un service de distribution automatique de configuration TCP/IP : le DHCP.

Mise en place d'un Serveur DHCP :

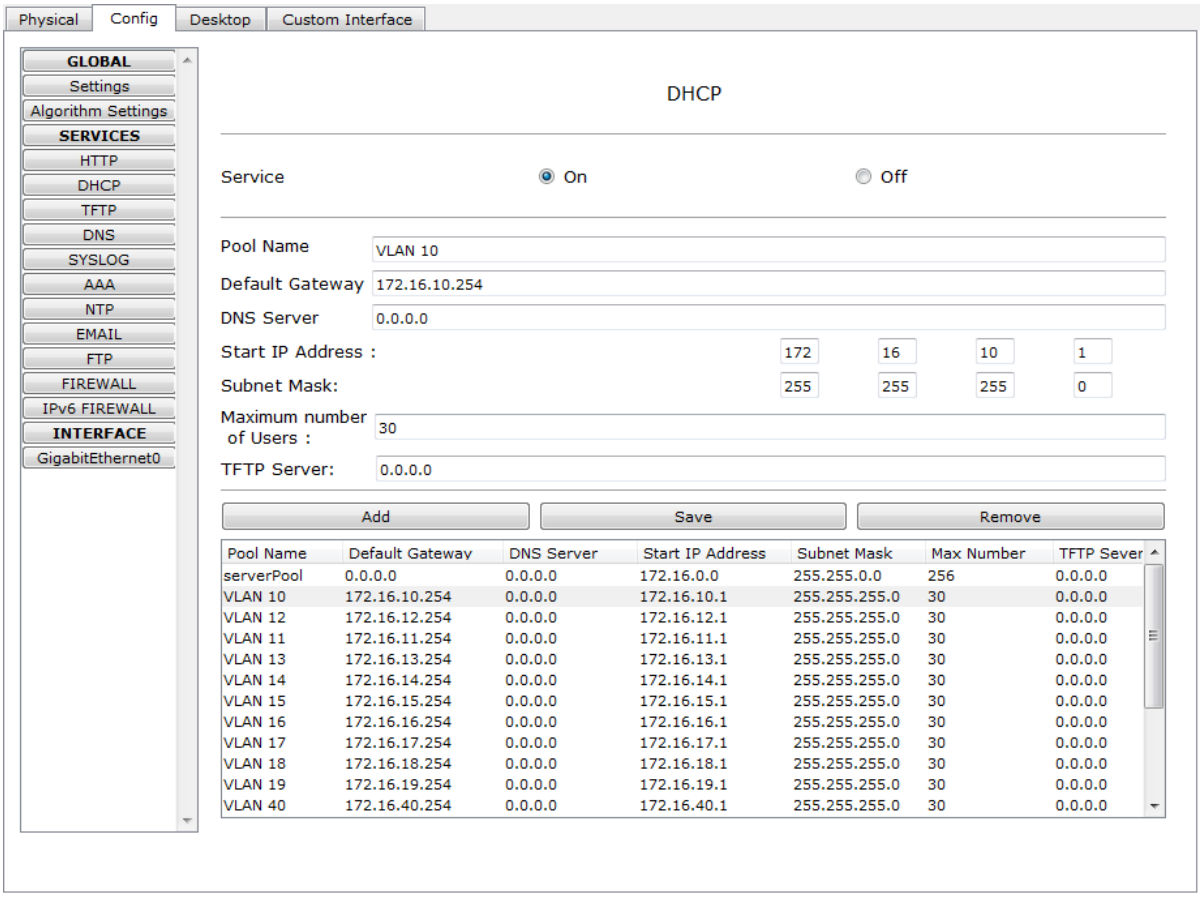
Tout d'abord, il faut tenir compte des besoins de l'organisme. Il y en aura un Serveur DHCP :

VLAN : n°100
Adresse IP : 172.16.100.1
Passerelle par défaut : 172.16.100.254
Masque de sous-réseau : 255.255.255.0

Pour chaque sous-réseau, en fonction du plan d'adressage, on peut constituer nos pools d'adresses à distribuer, avec l'adresse de début, l'adresse de fin et la durée du bail (cf. le tableau) :

N° VLAN	Nom du VLAN	Adresse de début	Adresse de fin	Adresse de passerelle par défaut	Durée du bail	DNS
10	Ligue de Quidditch	172.16.10.1	172.16.10.30	172.16.10.254	24h	Non
11	Ligue Pokémon	172.16.11.1	172.16.11.30	172.16.11.254	24h	Non
12	Ligue Joutes	172.16.12.1	172.16.12.30	172.16.12.254	24h	Non
13	Ligue de Natation	172.16.13.1	172.16.13.30	172.16.13.254	24h	Non
14	Ligue d'Aqua-Poney	172.16.14.1	172.16.14.30	172.16.14.254	24h	Non
15	Ligue Pentathlon	172.16.15.1	172.16.15.30	172.16.15.254	24h	Non
16	Ligue Fléchette	172.16.16.1	172.16.16.30	172.16.16.254	24h	Non
17	Ligue Pong	172.16.17.1	172.16.17.30	172.16.17.254	24h	Non
18	Ligue des Justiciers	172.16.18.1	172.16.18.30	172.16.18.254	24h	Non
19	Ligue des Explorateurs	172.16.19.1	172.16.19.30	172.16.19.254	24h	Non
40	Wifi public	172.16.40.1	172.16.40.30	172.16.40.254	24h	Non
50	Filaire salle ressources	172.16.50.1	172.16.50.30	172.16.50.254	24h	Non
60	Admin, repro et multi	172.16.60.1	172.16.60.30	172.16.60.254	24h	Non
70	Ecrans d'affichages	172.16.70.1	172.16.70.30	172.16.70.254	24h	Non
80	DMZ	172.16.80.1	172.16.80.30	172.16.80.254	24h	Non
90	Téléphonie IP	172.16.90.1	172.16.90.30	172.16.90.254	24h	Non
100	Salle Serveurs	172.16.100.1	172.16.100.30	172.16.100.254	24h	Non
199	Administration des Switchs	172.16.199.1	172.16.199.30	172.16.199.254	24h	Non

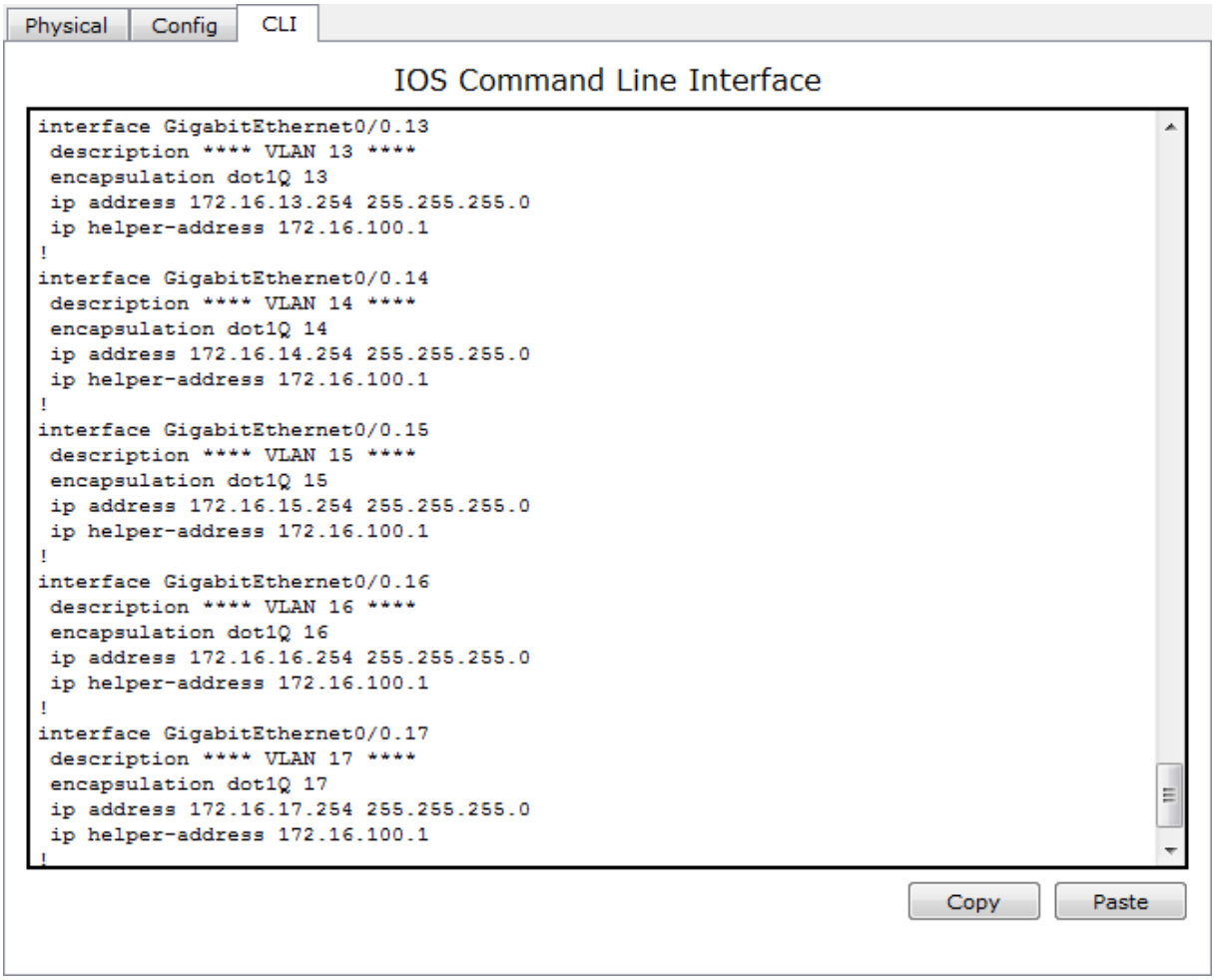
On ajoute ensuite tous ces pools d'adresses dans le Serveur DHCP :



Chaque VLAN à sa propre passerelle par défaut, qui est défini par l'adresse de réseau suivie du dernier octet à 254. Étant donné que le Serveur DHCP se trouve dans un VLAN, pour pouvoir autoriser la communication entre le Serveur DHCP et ses clients, il faut mettre en place un relais DHCP, grâce à un router. Il faut donc entrer les commandes suivantes dans le router pour tous les VLAN :

> enable
 # conf t
(config)# interface GigabitEthernet0/0.10
(config-subif)# description ** VLAN 10 ******
(config-subif)# encapsulation dot1Q 10
(config-subif)# ip address 172.16.10.254 255.255.255.0
(config-subif)# ip helper-address 172.16.100.1

Pour accélérer le processus, on peut utiliser les commandes suivantes :
interface range FastEthernet0/1-5 → Pour sélectionner plusieurs interfaces.



Procédure de validation : cf. le tableau.

Mise en place d'un « DHCP statique » :

Tout en distribuant la configuration IP via un Serveur DHCP, on veut pouvoir toujours assigner la même configuration IP à un poste donné.

Pour cela, on a besoin de l'adresse MAC du poste en question, qui est unique et surtout statique. Par exemple, pour le Poste-01 : on cherche son adresse MAC, grâce à la commande ipconfig /all : 00D0.BACC.ABD0.

Sur le Serveur DHCP, il suffit alors de « lier » l'adresse MAC du Poste-01 avec l'adresse IP de notre choix, selon notre plan d'adressage. Le Serveur DHCP lui attribuera ensuite cette adresse IP, par exemple : 172.16.10.1. Ainsi, ce poste récupérera toujours la même adresse IP.

La distribution des adresses est donc dynamique et fixe en même temps. C'est ce que l'on appelle une réservation DHCP.

Réseau WIFI protégé :

On doit mettre en place deux réseaux Wifi séparés :

- Un public pour les visiteurs, qui sera donc sans sécurité, et qui se trouvera dans le VLAN 40 « Wifi public ».
- Un privé pour les ligues, qui sera sécurisé par une authentification WPA, et qui se trouvera dans le nouveau VLAN 30 « Wifi privé ».

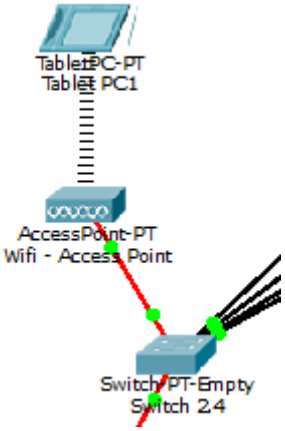
Chaque étage doit avoir un point d'accès Wifi. Il y aura donc 2 points d'accès par switch, un public et un privé.

Il faut commencer par créer le pool d'adresse réservé aux réseaux Wifi dans le DHCP. Le réseau public est déjà créé, il ne reste donc plus qu'à rentrer le VLAN 30.

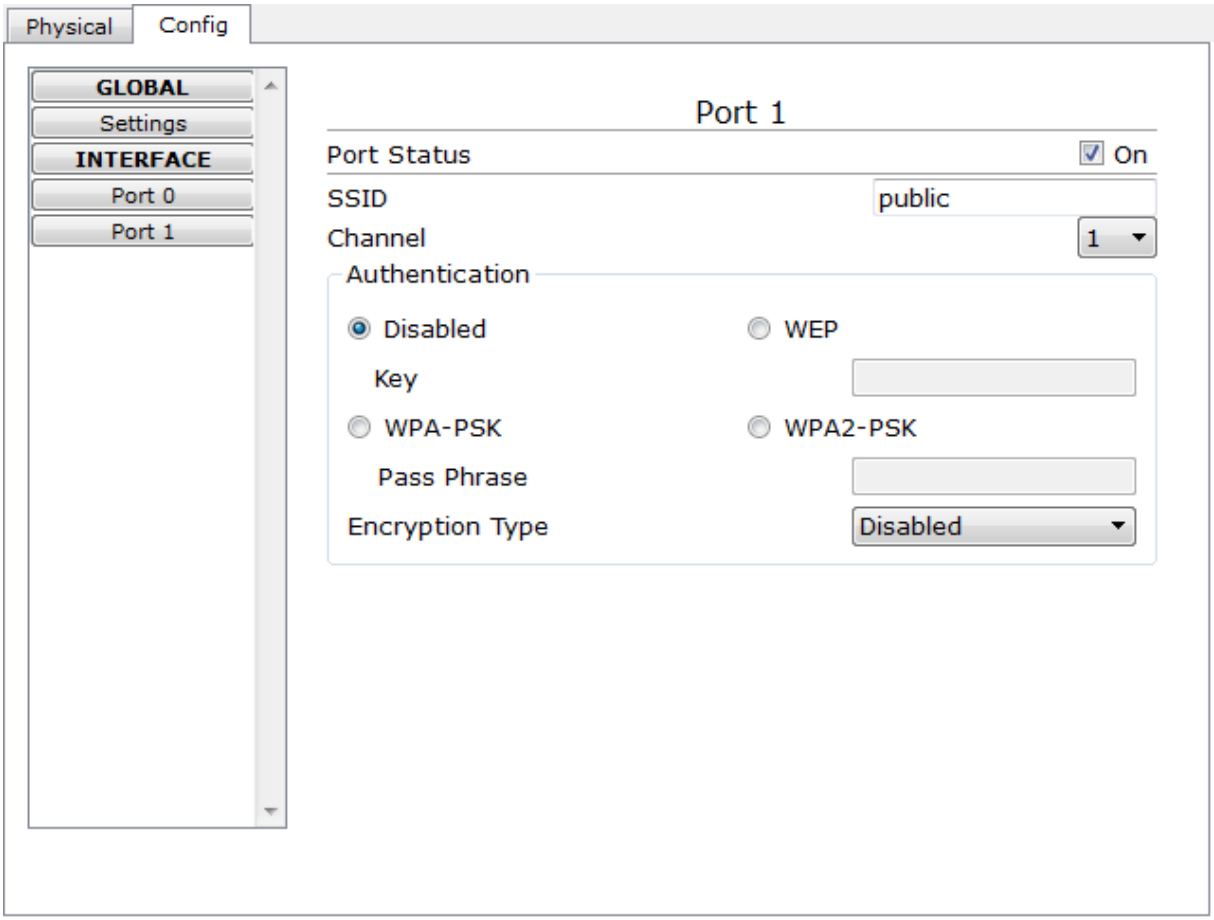
Ensuite, il faut créer le VLAN 30 dans le Switch Serveur VTP, et faire son encapsulation dans le Router.
Ensuite, on va configurer le réseau Wifi public. Pour cela, on a besoin d'attribuer un SSID : acronyme de Service Set Identifier, est le nom d'un réseau sans fil (Wi-Fi) selon la norme IEEE 802.11. Ce nom comporte au plus 32 caractères. Il n'y a pas de sécurité à affecter à ce réseau. On place ensuite le

port du switch auquel est connecté le point d'accès dans le VLAN 30. Et on test la connexion en réclamant une configuration IP avec le nouvel hôte.

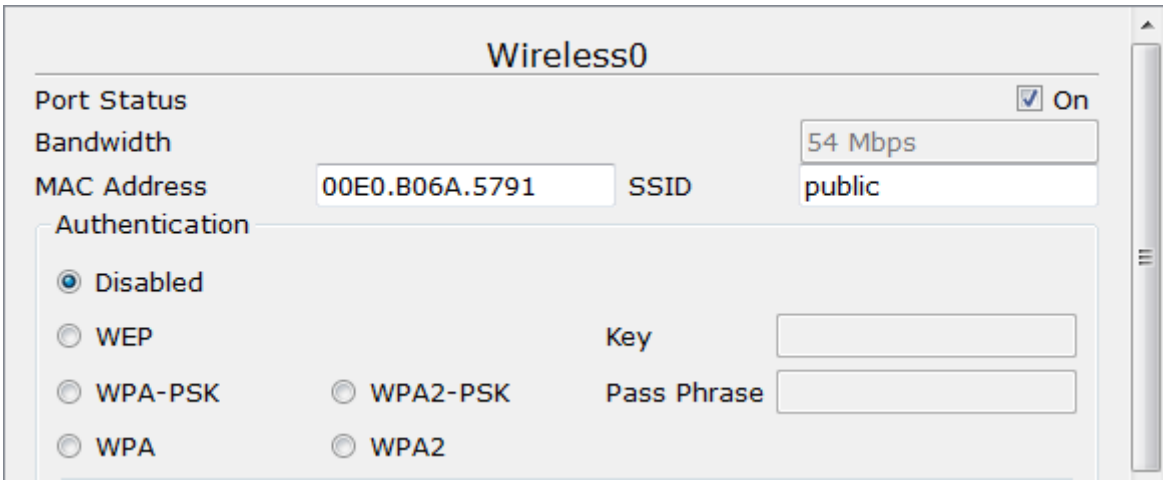
Le câblage :



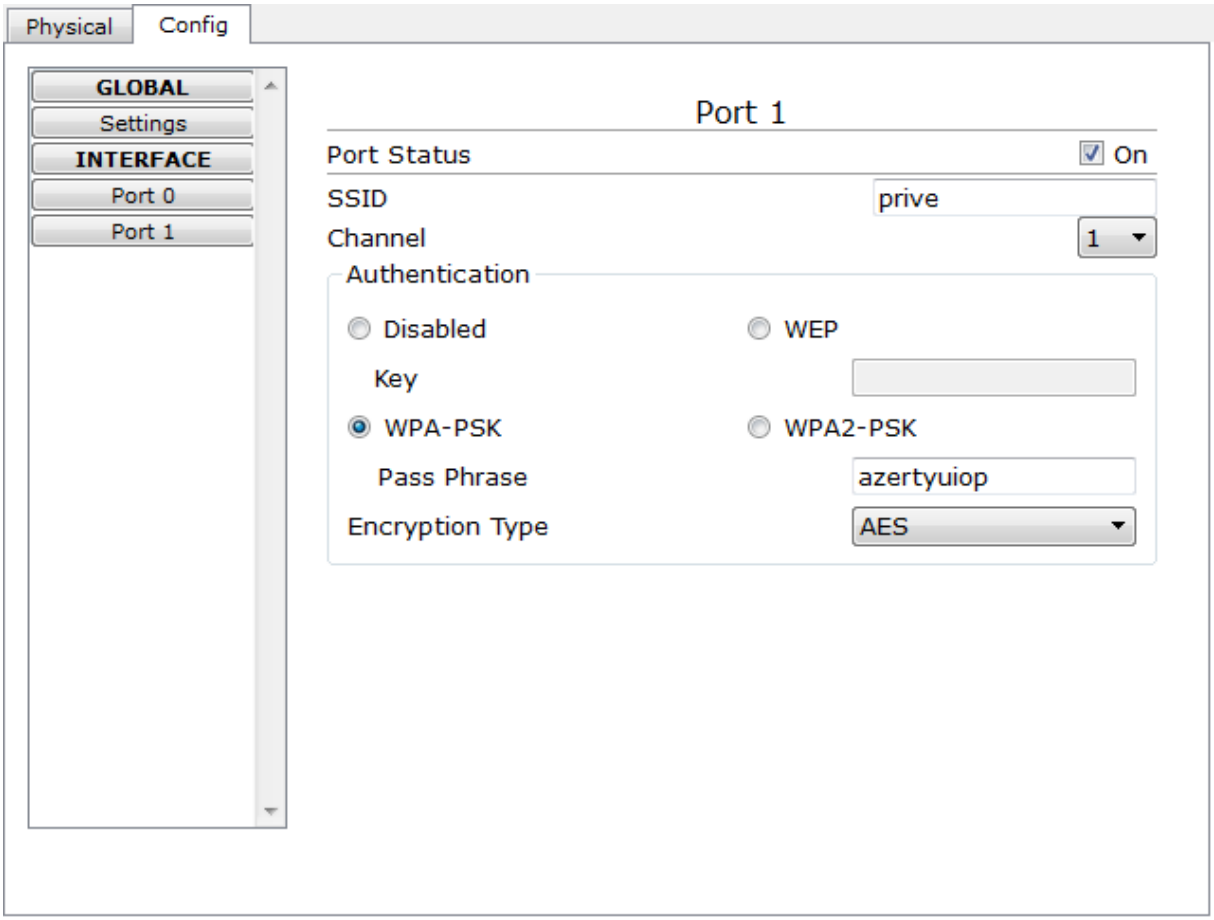
Sur le point d'accès :

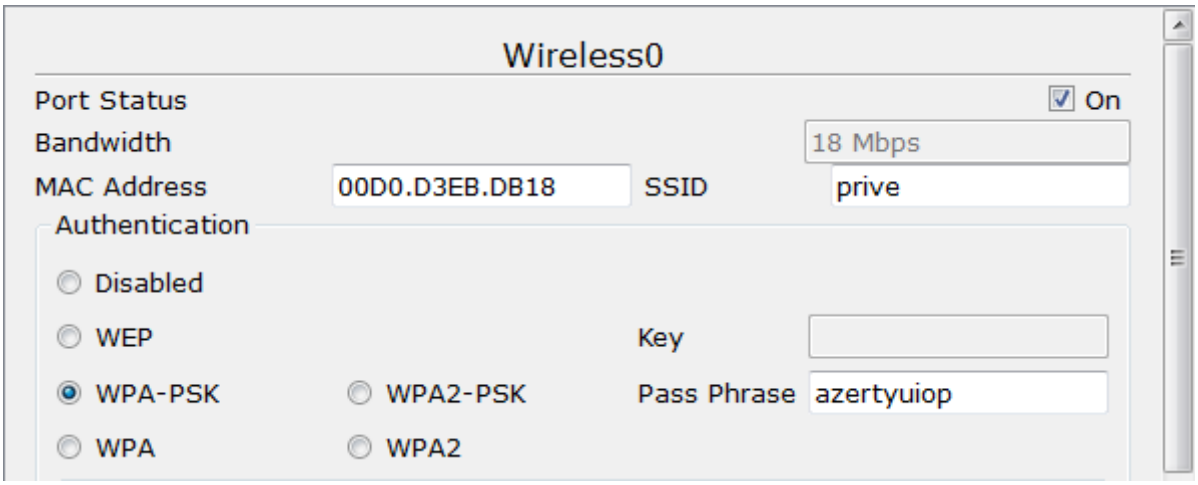


Sur l'hôte :



On passe ensuite à la mise en place du point d'accès wifi privé, et donc sécurisé. On va mettre en place une authentification par WPA : Wi-Fi Protected Access (WPA et WPA2) est un mécanisme pour sécuriser les réseaux sans-fil de type Wi-Fi.





SSID : Nom du point d'accès
Canal :
WEP : Chiffrement de données
WPA : Chiffrement + cryptage

http://www.commentcamarche.net/contents/1284-securiser-un-reseau-wifi

https://lafibre.info/wifi/quel-canal-wi-fi-choisir-pour-optimiser-son-debit/

Norme IEEE 802.11 :

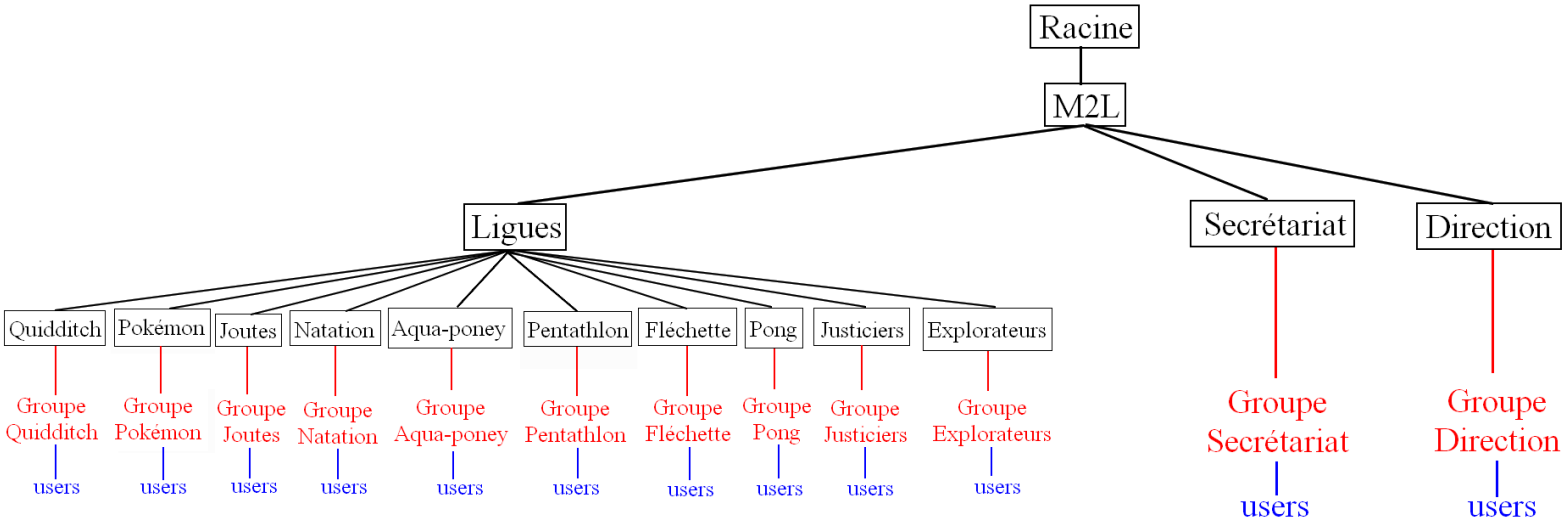
802.11	Bande de fréquence	Débit théorique maximal	Portée	Congestion	Largeur canal	MIMO
a	5 GHz	54 Mbps	Faible	Faible	20 MHz	Non
b	2,4 GHz	11 Mbps	Correcte	Elevée	20 MHz	Non
g	2,4 GHz	54 Mbps	Correcte	Elevée	20 MHz	Non
n	2,4 GHz et 5 GHz	De 72 à 450 Mbps	Bonne	Elevée et faible	20 ou 40 MHz	Oui
ac	5 GHz	De 433 à 1300 Mbps	Bonne	Faible	40 ou 80 MHz	Oui

Il faut maintenant mettre en place des listes d'accès pour empêcher tous les VLAN de communiquer entre eux.

Gestion des utilisateurs via Windows Serveur 2008 :

1- Mise en place d'une arborescence :

Le domaine sera nommé M2L.local. Au sein des bâtiments, il y a : 10 Ligues de sport, un Secrétariat, et un groupe de Direction.



2- Création des groupes et des utilisateurs :

Il y aura donc une unité d'organisation par Ligues, une pour le Secrétariat et une pour la Direction. Chacune de ses unités d'organisations aura un groupe qui définira les droits des utilisateurs.

3- Partages et droits :

Chaque Ligue aura accès à un document en commun, disponible au chemin suivant :

\\172.16.0.??\Commun\NomDuGroupe

Chaque utilisateur des Ligues aura un dossier personnel pour y stocker ses documents, au chemin suivant :

\\172.16.0.??\Perso\%username%

Tous les utilisateurs auront également un profil itinérant si, par exemple, une Ligue se voit affecter un autre bureau, qui sera stocké au chemin suivant :

\\172.16.0.??\Profils\%username%

4- Les restrictions horaires :

Les Ligues pouvant organiser des évènements la semaine comme le week-end, en soirée comme tôt le matin, il n'y aura pas de restrictions horaires.

5- Quotas :

Chaque Ligue peut accueillir au maximum 12 personnes, les dossiers personnels seront limités à 500 Mo de données. Sachant qu'il y a 10 Ligues, il y aura donc un stockage maximum de 60 Go.

Les personnels de la direction et du secrétariat auront quant à eux un quota de 1 Go.

Mise en place d'un service DHCP :

N° VLAN	Nom du VLAN	Adresse de début	Adresse de fin	Adresse de passerelle par défaut	Durée du bail	DNS
10	Ligue de Quidditch	172.16.10.1	172.16.10.30	172.16.10.254	24h	Non
11	Ligue Pokémon	172.16.11.1	172.16.11.30	172.16.11.254	24h	Non
12	Ligue Joutes	172.16.12.1	172.16.12.30	172.16.12.254	24h	Non
13	Ligue de Natation	172.16.13.1	172.16.13.30	172.16.13.254	24h	Non
14	Ligue d'Aqua-Poney	172.16.14.1	172.16.14.30	172.16.14.254	24h	Non
15	Ligue Pentathlon	172.16.15.1	172.16.15.30	172.16.15.254	24h	Non
16	Ligue Fléchette	172.16.16.1	172.16.16.30	172.16.16.254	24h	Non
17	Ligue Pong	172.16.17.1	172.16.17.30	172.16.17.254	24h	Non
18	Ligue des Justiciers	172.16.18.1	172.16.18.30	172.16.18.254	24h	Non
19	Ligue des Explorateurs	172.16.19.1	172.16.19.30	172.16.19.254	24h	Non
30	Wifi privé	172.16.30.1	172.16.30.30	172.16.30.254	24h	Non
40	Wifi public	172.16.40.1	172.16.40.30	172.16.40.254	24h	Non
50	Filaire salle ressources	172.16.50.1	172.16.50.30	172.16.50.254	24h	Non
60	Admin, repro et multi	172.16.60.1	172.16.60.30	172.16.60.254	24h	Non
70	Ecrans d'affichages	172.16.70.1	172.16.70.30	172.16.70.254	24h	Non
80	DMZ	172.16.80.1	172.16.80.30	172.16.80.254	24h	Non
90	Téléphonie IP	172.16.90.1	172.16.90.30	172.16.90.254	24h	Non
100	Salle Serveurs	172.16.100.1	172.16.100.30	172.16.100.254	24h	Non
199	Administration des Switchs	172.16.199.1	172.16.199.30	172.16.199.254	24h	Non

1) Lister les différents services que l'on peut retrouver en entreprise.
2) Qu'est-ce qu'une DMZ, et pourquoi certains services sont à l'intérieur et d'autres non ?
3) Lister les solutions de sauvegarde : pour les données applicatives et clientes. Doit-on tout sauvegarder ? On ne sauvegarde par exemple que des fichiers intègres (pas modifiés, et pas supprimés – lien avec le checksum).

Les services en entreprise :

En entreprise, on trouve généralement les services suivant :

- Un service d'annuaire est installé sur un contrôleur de domaine (Domain Controller – sous Windows Server 2008 par exemple ou ldap).

- Un service DNS, pour résoudre les noms de domaines.

Les données d'un serveur DNS n'ont pas besoin d'être sauvegardées. Il suffit de mettre en place un deuxième serveur DNS qui peut répondre à la place du premier s'il est en panne. On peut ainsi mettre en place un serveur DNS secondaire, ou avoir deux serveurs DNS primaires.

- Un service DHCP, qui permet de distribuer des adresses IP aux clients.

Les données applicatives d'un serveur DHCP sont sauvegardées, de différentes manières (synchrone ou asynchrone). Les étendues, les réservations, les baux et les options sont sauvegardées.

- Un service de fichiers pour pouvoir sauvegarder des données. Un serveur NAS est par exemple une solution matérielle pour réaliser du stockage.

Les données clientes, c'est-à-dire les dossiers personnels des utilisateurs par exemple, doivent être sauvegardées, sur un NAS qui servira de périphérie de stockage, ou sur un serveur externe grâce au cloud.

- Un service d'impression : une imprimante est le pilote installé sur les clients, c'est le logiciel. La partie physique est un périphérique d'impression. Le service d'impression permet de centraliser les demandes d'impression : une demande du client va directement sur le serveur, puis est envoyé vers le bon périphérique.

Sont sauvegardés : les queues d'impression, les pilotes, les ports et les processeurs d'impression.

- Un service antiviral : il ne faut pas que tous les postes clients mettent à jour leur base de signatures un par un. Toutes les mises à jour sont effectuées par le serveur antiviral, puis transmises aux clients (Trend Micro par exemple).

- Un service web ou intranet

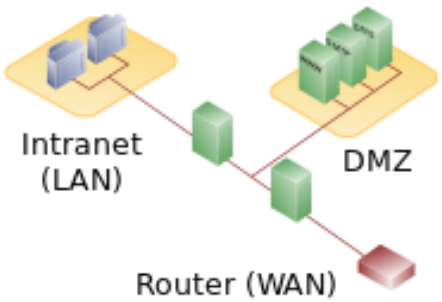
- Un service de base de données

Pour un serveur de base de données, il faut sauvegarder toutes les bases de données.

- Un service de messagerie (par exemple Exchange sous Windows).

La DMZ (Demilitarized Zone) ou Zone démilitarisée :

Une zone démilitarisée est une zone qui regroupe plusieurs services (Web, FTP, Messagerie, VoIP) protégée par un ou plusieurs pare-feu. Elle permet d'isoler des services afin que l'on puisse y accéder de l'extérieur sans pour autant avoir accès au réseau intérieur qui est lié à ses services.



Ainsi, le réseau interne de l'entreprise est protégé des intrusions extérieures, et un client extérieur peut accéder aux services proposés par les serveurs de la DMZ.

Les solutions de sauvegarde :