

---

# RAPPORT SAE 21- Construire un réseau

---

Morgan Bois, Julien Losser, Olivier Lamontagne, Valentin Long

## Introduction

Dans ce projet, nous devons mettre en place un réseau d'entreprise de petite taille. Ce réseau local est constitué de pc, de commutateurs et de routeurs. Il y aura également des règles de sécurité simples, comme une mise en place de mots de passe la gestion des switches et routeurs. Nous avons également fait de nombreuses recherches sur les différents sujets pour approfondir nos connaissances.

Nous avons segmenté la plage d'adresse IP donnée en accord avec les autres groupes. Ainsi chaque groupe dispose de son réseau local qui devra être interconnecté avec le réseau des voisins. Chaque pc dispose de son propre vlan. Plusieurs services devront être déployés dans ce réseau local comme un serveur DHCP ou encore un proxy.

## Configuration

On souhaite créer 3 VLANs :

- Vlan 12 administrateurs
- Vlan 22 utilisateurs
- Vlan 32 test

Tout ces vlan auront chacun 2 ports assignés sur les switches.

Découpage du réseau 172.16.192.0/18

Nous avons 12 groupes qui doivent recevoir une plage d'adresse IP :

$2^3 = 8$

$2^4 = 16 > 12$

Le masque de sous-réseau de chaque groupe pour la plage attribuée sera 255.255.252.0 (/22)

- Réseau : 172.16.216.0/21
- Hôte min : 172.16.216.1
- Hôte max : 172.16.223.254
- Broadcast : 172.16.223.255

---

*Découpage du sous-réseau 172.16.216.0/21 en 6 sous-réseaux pour les VLANs :*

---

### Switch A (Valentin, Olivier)

	Réseau	Hôte min	Hôte max
<b>VLAN 12</b>	172.16.216.0/24	172.16.216.1	172.16.216.254
<b>VLAN 22</b>	172.16.217.0/24	172.16.217.1	172.16.217.254
<b>VLAN 32</b>	172.16.218.0/24	172.16.218.1	172.16.218.254

	VLAN 12	VLAN 22	VLAN 32
<b>Routeur @IP</b>	172.16.216.254	172.16.217.254	172.16.218.254

### Switch B (Morgan, Julien)

	Réseau	Hôte min	Hôte max
<b>VLAN 12</b>	172.16.219.0/24	172.16.219.1	172.16.219.254
<b>VLAN 22</b>	172.16.220.0/24	172.16.220.1	172.16.220.254
<b>VLAN 32</b>	172.16.221.0/24	172.16.221.1	172.16.221.254

### Routeur

	VLAN 12	VLAN 22	VLAN 32
<b>@IP</b>	172.16.219.254	172.16.220.254	172.16.221.254

Nous avons choisi ici de diviser équitablement notre réseau. Ainsi, chaque vlan aura le même nombre d'adresses disponible. La contrainte étant qu'il fallait au moins 2 adresses dans chaque vlan.

⚠ Les 2 switches ont la même configuration sauf les adresses IP d'interface du VLAN admin, qui permet de gérer le switch directement (ex : TFTP, SSH et test de pings.)

---

### *Réseau du Routeur*

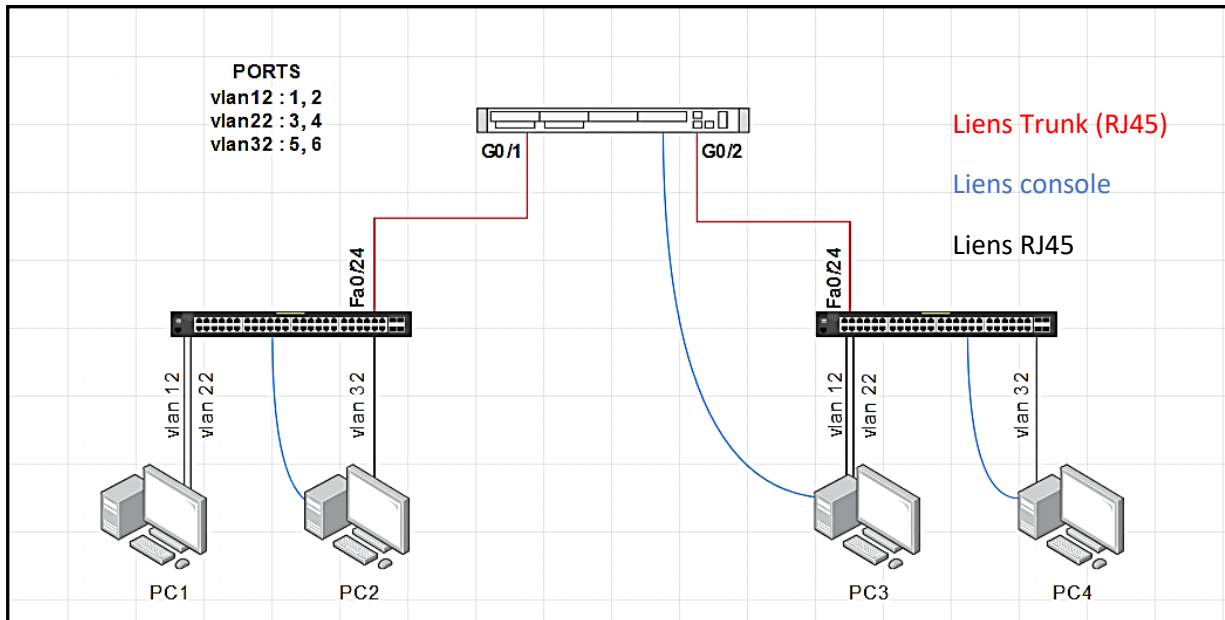
---

	Network	Broadcast	HostMax	HostMin
<b>@IP</b>	172.16.222.0/30 (Class B)	172.16.222.3	172.16.222.2	172.16.222.1

Seulement 2 hôtes sont disponibles car c'est une interconnexion de routeurs.

## Schéma de l'installation

Ci-dessous le schéma qui est composé de 4 pc (PC1, PC2, PC3, PC4), 2 switchs et 1 routeur. Les liens rouges sont des liens trunk (RJ45) sur les interfaces Gigabit du routeur et les liens bleus des liens consoles sur les ports console (RS232). Les pcs sont connectés au switch avec des câbles RJ45 ce qui permet de mettre en place les différents VLAN.



1 - Schéma de l'installation

Nous avons dû mettre en place un port mirroring sur le port 23 du switch. Cela permet de dupliquer le trafic d'une ou de plusieurs interfaces vers le dit port. Puisque le switch n'agit pas comme un hub qui redistribue toutes les trames sur toutes les interfaces, le port mirroring est essentiel dans un switch si l'on veut observer les trames du réseau. Ainsi, on peut utiliser Wireshark par exemple pour scruter le trafic réseau.

Pour créer un VLAN :

```
vlan 12
```

```
name administrateur
```

On crée le VLAN 12, et on le nomme administrateur.

Explication sur le TFTP :

TFTP (pour Trivial File Transfer Protocol), est un protocole de transfert de fichiers. C'est en quelque sorte un « cousin » au protocole FTP. Il est moins fiable que ce dernier, mais très utile pour transférer de petits fichiers tels que des configurations entre deux machines. Il est facile à mettre en œuvre, car les routeurs et les switchs l'intègrent par défaut. Il suffit d'ouvrir un serveur TFTP sur un PC dans le même réseau que le switch ou le routeur et taper la commande :

```
copy running-config tftp:
```

```
Address or name of remote host []? <ADRESSE DU PC>
```

## Routage Inter-Vlan

Pour que chaque pc dans notre réseau puisse communiquer entre eux (sauf le vlan test car il est isolé), nous devons mettre en place un routage inter-vlan. Ceci permettra par exemple au PC du vlan 12 de communiquer avec un PC du vlan 22.

Pour mettre cela en exécution, nous devons insérer plusieurs commandes dans le switch et dans le routeur.

---

### Partie Switch

---

Tout d'abord il nous faut assigner un port qui servira de « tunnel universel » pour tout les vlan. Il se chargera de faire passer toutes les trames de chaque vlan vers le routeur. C'est un lien trunk. Nous avons choisi le port 24 comme lien trunk.

On entre dans la configuration de l'interface :

```
interface FastEthernet0/24
```

On lui indique qu'il faut utiliser le mode trunk :

```
switchport mode trunk
```

Pour pouvoir autoriser les vlan à passer à travers le lien trunk (sauf le vlan test), on doit insérer la commande suivante :

```
switchport trunk allowed vlan 12,22
```

---

### Partie Routeur

---

Pour le routeur, l'opération est plus délicate, puisqu'il faut crée des sous interfaces sur chaque port possédant un vlan. Chacune de ces sous interfaces seront assignées à un vlan.

On entre dans la configuration de l'interface :

```
interface GigabitEthernet0/0.1
```

On indique le type de trafic de la sous interface. Le standard utilisé pour les liens trunk est 802.1q d'où la commande suivante :

```
encapsulation dot1Q 12
```

⚠ Le 12 est le numéro de vlan que l'on souhaite encapsuler.

Enfin, il faut lui assigner une adresse IP qui sera l'adresse de passerelle de ce vlan dans ce domaine de collision. Ducoup le vlan 12 aura 2 passerelles, car il y a 2 sous interfaces dans 2 interfaces physique du routeur et de même pour le vlan 22.

```
ip address 172.16.216.254 255.255.255.0
```

## Accès SSH sur le commutateur et le routeur

Le protocole SSH peut s'avérer bien utile sur ce type d'équipement car cela évite de devoir placer un câble console à chaque fois qu'un administrateur veut modifier quelque chose. Cela permet également de se connecter à distance, d'un réseau extérieur par exemple.

Un des grands avantages de SSH est qu'il offre une connexion chiffrée entre l'administrateur et l'équipement. Ainsi, les données sensibles tel que les mots de passes sont illisible par un potentiel intru.

Pour commencer à configurer SSH, il faut déjà vérifier que le switch et le routeur disposent du SSH.

Pour vérifier le SSH du routeur :


`show version`

Cette commande renverra pléthore d'information mais ce qui nous intéresse est le nom de l'image Cisco IOS, ici `C2900-UNIVERSALK9-M`. Si celle-ci contient k9, l'image prend en charge les fonctionnalités de chiffrement et donc, dispose de SSH.

Pour vérifier le SSH du switch :

`show ?`

Si la liste des commandes fournie contient <crypto>, alors le switch dispose du SSH. Cette vérification est aussi possible sur le routeur.

 Un point d'honneur a été mis là-dessus puisque le routeur physique ne disposait pas de SSH. Nous avons donc utilisé le logiciel Cisco packet tracer sur ce point-là.

---

### Mise en place du SSH

---

Pour mettre en place le SSH, il faut tout d'abord créer les identifiants de connexion. Ainsi, l'administrateur souhaitant se connecter au SSH devra utiliser l'adresse IP de l'interface du vlan sur le switch ou l'adresse de passerelle du routeur et, rentrer les identifiants. La commande ci-dessous définit un ID de connexion et un mot de passe :

```
username toto password 123456
```

⚠ Ne pas utiliser ce genre de mot de passe ou d'ID. C'est ici un exemple.

On met en place un nom de domaine :

```
ip domain-name iut.fr
```

Ceci permet de se connecter à l'aide de iut.fr au lieu d'une adresse IP (optionnel)

On active le SSH :

```
ip ssh version 2
```

On génère une paire de clés de chiffrement :

```
crypto key generate rsa general-keys modulus 1024
```

Le nombre 1024 correspond au nombre de bits. Plus ce chiffre est élevé, plus le chiffrement est fort.

On met en place une ligne virtuelle pour le ssh, on utilise l'ip de l'interface du vlan 12 du switch pour s'y connecter ou le nom de domaine :

```
line vty 0 4
```

```
login local
```

```
transport input ssh
```

Les lignes vty sont des ports de connexion virtuels (virtual teletype). Les chiffres 0 et 4 précisent qu'il peut y avoir 5 connexions (en comptant le 0) simultanées. Les identifiants locaux spécifiés en amont sont utilisés, puis on indique le type de protocole que ces lignes doivent utiliser. Ici SSH.

On souhaite également que l'on puisse se connecter avec le SSH uniquement du vlan administrateur. Pour cela on utilise des ACL (Access control list). Ce sont des règles que l'on définit pour autoriser ou bloquer du trafic en fonction de plusieurs critères comme les adresses IP.

Pour cela on commence par créer notre ACL :

```
access-list 1 permit 172.16.216.0 0.0.0.255
```

Cette règle crée l'ACL 1 et autorise seulement le réseau 172.16.216.0. Pas besoin d'interdire le reste, les ACL le font par défaut.

Et maintenant on l'assigne aux lignes VTY :

```
access-class 1 in
```

Et hop ! Tout ce qui n'est pas du réseau du vlan 12, se voit automatiquement bloqué par l'ACL. On a spécifié ici l'ACL 1 en trafic d'entrée avec « in » (puisque c'est le client qui veut entrer en contact en SSH)

## Service DHCP

Le service DHCP est essentiel dans un réseau bien configuré car il permet d'attribuer des adresses IP dynamiques. Cela évite de rentrer manuellement chaque adresse IP sur chaque équipement surtout s'il y'en a plusieurs dizaines. De plus, on risquerait de se tromper dans l'écriture des adresses et ainsi créer des conflits.

Le service DHCP est appelé ici pool DHCP. Pour configurer le pool dans un routeur Cisco, il est nécessaire de connaître l'adresse réseau ou l'on veut qu'il y ait des IP distribuées. L'adresse du routeur est optionnelle sauf s'il ont voulu que les hôtes puissent accéder aux réseaux externes (de nos voisins par exemple). De même pour l'adresse DNS.

Création du pool dans le routeur :

```
ip dhcp pool VLAN12_A
```

Insertion du réseau ou l'on veut qu'il y ait du DHCP :

```
network 172.16.216.0 255.255.255.0
```

On lui indique la passerelle :

```
default-router 172.16.216.254
```

Ainsi qu'un serveur DNS (celui de google par exemple) :

```
dns-server 8.8.8.8
```

Et voilà ! Notre serveur DHCP interne au routeur distribue un @IP, la passerelle et le serveur DNS à chaque hôte présent dans le réseau entré avec la commande network.

⚠ Ces commandes ont été rentrées 4 fois (vlan\_12a, vlan\_22a, vlan\_12b, vlan\_22b). Ainsi 4 vlan intègrent le DHCP (admin et utilisateur des 2 switches).

Il faut également exclure l'adresse de la passerelle dans le pool DHCP de chaque vlan afin de ne pas déborder de la plage d'adresse :

```
ip dhcp excluded-address 172.16.216.254
```

⚠ Ici c'est un exemple avec le vlan12 du switch 1. Il faut bien entendu le faire avec chaque pool DHCP.

## Interconnexion des routeurs avec OSPF

Le protocole OSPF, Open Shortest Path First est un protocole de routage. C'est un protocole à état de liens, c'est-à-dire qu'il est au courant de chaque changement sur la topologie du réseau (ex : un lien est débranché). Il est plus avantageux que le protocole RIP (Routing Information Protocol), car RIP ne peut pas avoir plus de 15 sauts dans sa topologie. RIP transmet l'intégralité de la table de routage à ses voisins, tandis qu'OSPF transfère uniquement les données de liens utiles de ses voisins tel que la métrique ou encore la vitesse de connexion. C'est pour cela qu'OSPF nécessite moins de bande passante de RIP.

### OSPF VS RIP

OSPF	RIP
<b>Etat de liens</b>	<b>Vecteur de distance</b>
<b>Utilise l'algorithme de Dijkstra</b>	<b>Utilise l'algorithme de Bellman-Ford</b>
<b>Partage des liens</b>	<b>Partage des tables de routage</b>
<b>Convergence rapide</b>	<b>Convergence lente</b>
<b>Utile dans les grands réseaux</b>	<b>Utile dans les petits réseaux</b>

OSPF est plus complexe à mettre en œuvre que RIP mais reste une solution à privilégier pour un routage interne optimal sur les grands réseaux. RIP reste néanmoins une référence car il a une plus grande compatibilité avec les routeurs, puisqu'il est simple à utiliser.

Vecteur de distance :

Utilise la distance ou le nombre de sauts pour déterminer le chemin de transmission.

Etats de liens :

Analyse différentes sources comme la vitesse, le coût et la congestion du chemin tout en identifiant le chemin le plus court.

Sources OSPF :

[https://www.cisco.com/c/fr\\_ca/support/docs/ip/open-shortest-path-first-ospf/7039-1.html](https://www.cisco.com/c/fr_ca/support/docs/ip/open-shortest-path-first-ospf/7039-1.html)

<https://community.fs.com/fr/blog/rip-vs-ospf-what-is-the-difference.html>



---

### Mise en place d'OSPF sur le routeur

---

Pour intégrer OSPF à notre routeur, nous devons commencer par activer OSPF avec la commande ci-dessous :


```
router ospf 1
```

On crée une instance du protocole OSPF nommée avec le numéro 1

On lui indique le réseau dans lequel est le routeur voisin :

```
network 172.16.222.0 0.0.0.3 area 0
```

On utilise ici un masque inversé, et on spécifie la zone 0.

 Avec OSPF on peut créer des zones (area). Ces zones permettent d'alléger les ressources CPU du routeur, car un routeur connaît seulement la topologie de sa zone. Cela évite d'avoir des bases de liens gigantesques. L'area 0 est une zone obligatoire qui est chargée de diffuser les informations des autres zones OSPF. Elle est appelée backbone.

Enfin on lui passe le paramètre suivant :

```
redistribute connected
```

Par défaut, le protocole OSPF ne redistribue rien. Il faut lui dire de faire connaître ses liens connectés à ses voisins.

Un fois le protocole actif, nous devons encore spécifier quels réseaux doivent être routés. Pour cela on doit aller dans la sous- interface gigabit du routeur (pour les vlan), afin de lui assigner l'instance OSPF ainsi que sa zone.

```
ip ospf 1 area 0
```

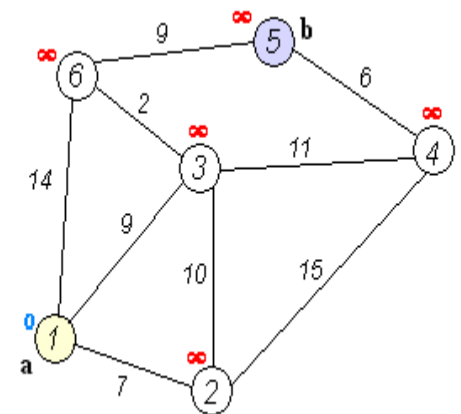
 Le protocole OSPF a été activé dans tous les vlan sauf celui nommé test.

## L'algorithme de Dijkstra

L'algorithme de Dijkstra a pour but de trouver le chemin le plus court.

Sur le schéma ci-contre, le chemin le plus court à trouver est entre « a » et « b ». L'algorithme choisit le sommet non visité avec la distance la plus faible, il calcule la distance à travers lui à chaque voisin non visité, et met à jour la distance du voisin si elle est plus petite. Il marque le sommet visité lorsqu'il a terminé avec les voisins. Ce qui permet un routage très efficace grâce au parcours trouver par l'algorithmes.

L'algorithme de Dijkstra apparaît dans les protocoles de routage interne « à état de liens », tels que Open Shortest Path First (OSPF). Mais l'algorithme de Dijkstra peut-être aussi utilisé pour d'autre domaine que l'informatique. L'algorithme de Dijkstra trouve une utilité dans le calcul des itinéraires routiers. Pour calculer pour le trajet le plus court, le plus rapide et ou le plus économique. Comme vous l'avez compris l'algorithme de Dijkstra permet de trouver la route la plus optimiser pour le trajet.



2 - Schéma de l'algorithme de Dijkstra

## Empoisonnement du cache ARP

L'ARP (pour Address Resolution Protocol) est un protocole de couche 2 du modèle OSI et TCP/IP, lors qu'il y a des échanges sur un réseau, il y a des trames Ethernet et ces trames ont besoin des adresses MAC pour pouvoir être transporter. Le rôle de l'ARP est donc de fournir, à partir d'une adresse IP, l'adresse MAC correspondante. Par défaut, une carte réseau refuse les paquets reçus n'ayant pas son adresse MAC comme adresse MAC de destination. C'est comme si on recevait une lettre dans notre boîte aux lettres avec un nom que n'est pas le nôtre, les cartes réseaux refusent donc d'ouvrir ces lettres. Une trame Ethernet complète doit donc forcément avoir une adresse MAC et une adresse IP correcte dans les champs destination pour transiter sans encombre d'un hôte A à un hôte B.

Cependant, le fonctionnement d'ARP sur les ordinateurs est le suivant :

À chaque réception d'un paquet, la carte réseau va vérifier le couple IP-MAC qu'il contient et mettre à jour sa table ARP, si le couple trouvé n'est pas enregistré. Ceci dans le but de ne pas faire de requête ARP à chaque échange et de remplir son cache ARP de façon dynamique. Le principe de l'ARP ou du MAC spoofing (spoofing voulant dire "parodier", "usurper") est d'envoyer des informations à un système afin de lui faire enregistrer des informations qui ne sont pas les bonnes et qui usurpent l'identité d'un autre système.

## Attaque

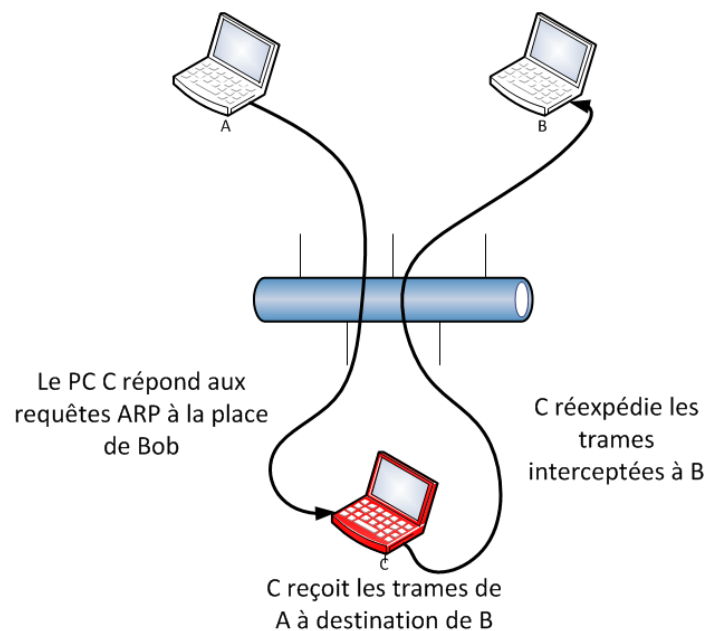
Une méthode très utilisée sur un réseau local afin de réaliser une attaque de type Man In The Middle est de faire de l'ARP Poisonning (ARP Spoofing). Cette attaque consiste à se placer entre 2 machines et de pouvoir voir et contrôler tous les échanges de trames entre les postes. Pour cela la machine malveillante (le pc 'C') doit se faire passer pour le pc B quand le PC A envoie une trame et inversement, pour le PC B il doit se faire passer le pc A. Lors de communications entre le PC A et PC B toutes les requêtes ARP sont faites envoyer au PC C qui les redistribue sans que personne le remarque. Une autre méthode d'attaque courante est d'usurper l'adresse du routeur local, détournant ainsi toutes les trames sortantes du réseau local.

De ce fait, toutes les connexions devant traverser la cible passent d'abord au travers du PC malveillant (PC C). Celui-ci peut alors extraire toutes les informations diffusées sans chiffrement comme les mots de passes par exemple, et les stocker afin d'essayer de casser le chiffrement après coup.

## Défense

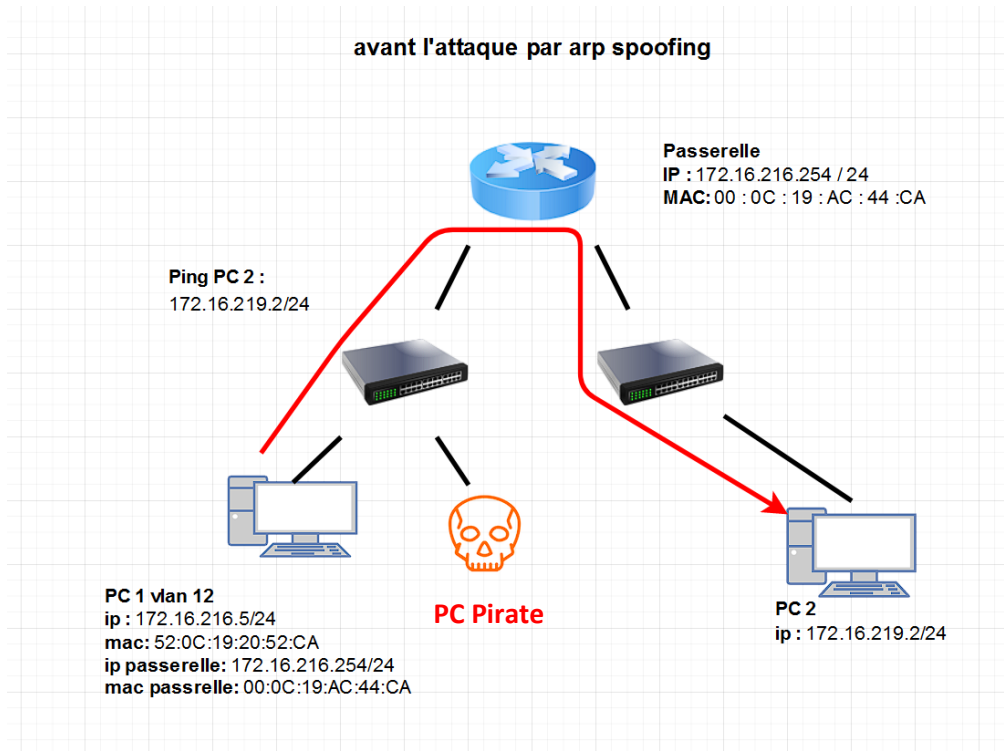
Pour se protéger contre cette attaque, une solution est de consister à fixer les adresses MAC des équipements (routeurs, serveurs, ...) dans les tables ARP des clients. De cette manière, la cible de l'attaque (ex PC A) n'aurait pas besoin d'effectuer une requête ARP pour résoudre l'IP d'une de ces machines et enverrait systématiquement ses trames Ethernet à celles-ci, sans détour par le PC C.

Pour des réseaux plus importants, une solution assez efficace pour se prémunir de ce genre d'attaque est d'activer l'inspection protocolaire de l'ARP sur les switches. Ainsi, il sera possible aux switches de voir qu'une réponse ARP est légitime en fonction d'une base de données DHCP. En cas d'attaque, les switches observeront donc une réponse ARP avec une IP qui ne correspond pas à l'adresse MAC fournie. Dans ce cas, le switch pourra, bloquer le port et prévenir un administrateur ou simplement rejeter le paquet.

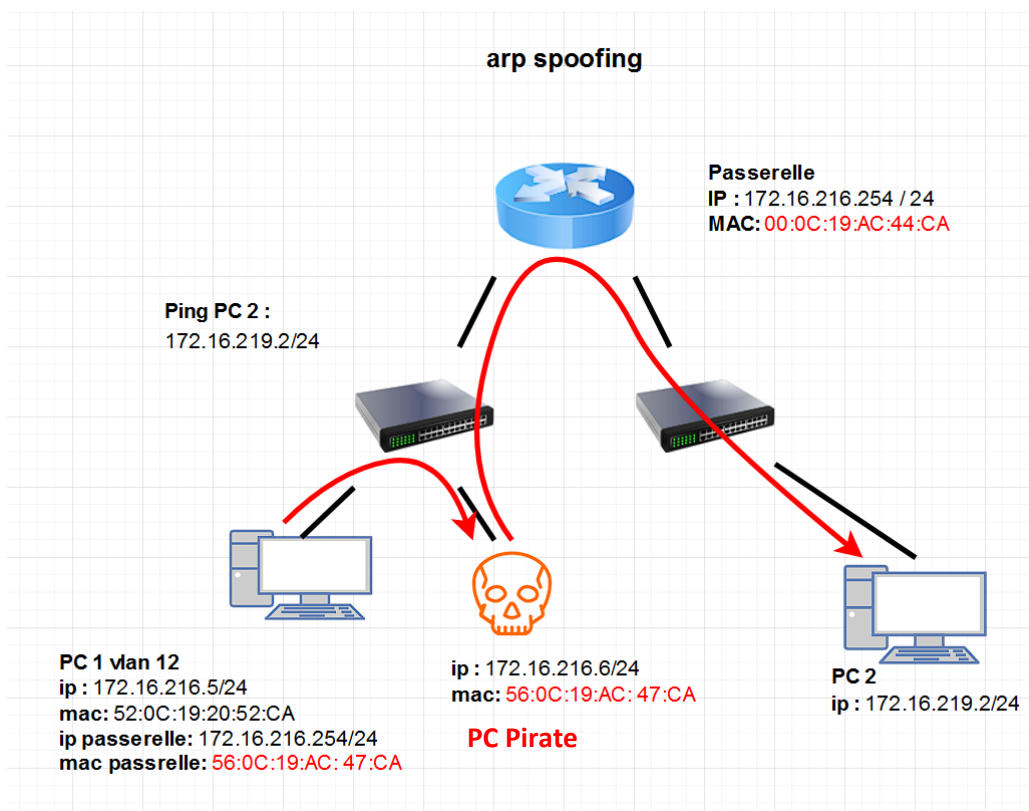


3 - Schéma de la topologie d'attaque ARP

Il est de plus à noter que cette attaque s'effectue au niveau de la couche 2 du réseau. De ce fait, la création de VLANs permet de limiter fortement le nombre de client vulnérable sur chaque domaine Ethernet. Même si les VLANs n'empêchent pas l'attaque, ils permettent dans tous les cas d'en limiter l'impact.



#### 4 – Requêtes ARP sans spoofing



#### 5 – Requêtes ARP avec spoofing

On voit ici, que le PC du pirate intercepte la communication entre le PC1 et le PC2 (tracé en rouge), car PC1 croit fermement qu'il envoie ses trames à la passerelle.

## Sécurité des ports des commutateur

Activer l'inspection protocolaire du protocole ARP :

```
#conf t
#ip arp inspection vlan 1
#interface fastEthernet 1/0/3
#ip arp inspection trust
! -- Définir le port du serveur DHCP (ici le fa1/0/3) comme sûr.
```

Vérifier le fonction de l'inspection protocolaire :

```
#show ip arp inspection vlan 1
```

```
SwitchD(config)#int range fa0/1-fa0/24
SwitchD(config-if-range)#switchport port-security maximum 1
```

On définit le nombre de ports où on veut appliquer la réglé de sécurité

Les ports passent en mode security, cela veut dire l'adresse mac sera pris en compte. Et on définit le maximum d'adresse mac a 1, cela veut dire que seul le premier pc branché à cette interface sera défini par le service DHCP.

## Mise en place de services

### Serveur FTP

Le protocole FTP (File Transfer Protocol) est un protocole de transfert de fichier non sécurisé. FTP est l'ancêtre de FTPS (et FTPES). FTPS utilise une connexion chiffrée qu'FTP ne possède pas. Il est tout de même pratique pour transférer des fichiers en local.

Sur linux, plusieurs logiciels proposent ce service comme vsftpd ou proftpd par exemple. On nous impose ici d'utiliser proftpd. Pour avoir utilisé les 2, proftpd semble plus complet et modulable grâce à ses modules.

Pour installer ce package, on tape la commande :

```
apt install proftpd
```

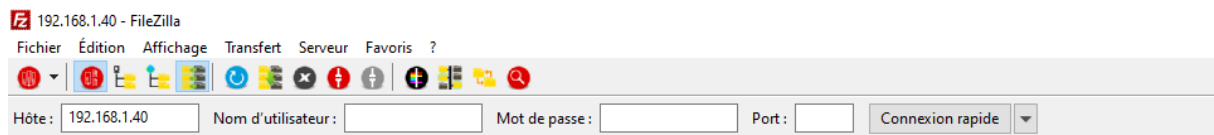
Pour configurer l'accès anonyme, on écrit ces lignes suivantes dans le fichier proftpd.conf :

```
<Anonymous ~ftp>          # On ouvre la balise pour configurer anonymous
User ftp
Group nogroup
UserAlias anonymous ftp
MaxClients 10              # Au maximum 10 clients en même temps
RequireValidShell off      # Pas besoin d'avoir un terminal (shell) valide
AnonRequirePassword off    # Cette ligne permet de se connecter sans mot de passe
<Limit WRITE>
DenyAll                    # On empêche l'écriture (Téléchargement uniquement)
</Limit>
</Anonymous>
```

Puis on redémarre le service :

```
service proftpd restart
```

Puis on s'y connecte à l'aide de Filezilla qui est un client ftp (il gère aussi d'autres protocoles comme le sftp par exemple)



On renseigne juste l'adresse IP, cela suffit car le compte anonyme et le port (21) sont sélectionnés par défaut dans Filezilla.

Site distant : /					
Nom de fichier	Taille de fichier	Type de fic...	Dernière modification	Droits d'accès	Propriétaire...
..					
welcome.msg	170	Élément O...	30/08/2021 20:35:11	adfr (0644)	ftp nogroup

Nous pouvons ainsi voir grâce au « / » que l'utilisateur Anonymous est chrooté (prisonnier de son répertoire). Impossible qu'il crée, supprime ou modifie le contenu de son répertoire. Seul le téléchargement est possible.

Nous souhaitons également ajouter 2 utilisateurs dans le ftp qui peuvent eux, écrire et modifier le contenu de leur dossier. La commande pour ajouter un utilisateur est la suivante :

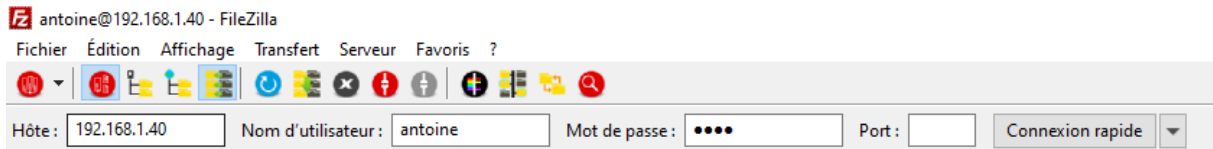
```
useradd -d /home/antoine antoine
```

-d spécifie le chemin de son répertoire home. Il faut bien entendu l'avoir créé avant (mkdir).

```
passwd antoine
```

On lui assigne un mot de passe

On s'y connecte avec Filezilla :



Un problème subsiste néanmoins :

Site distant : /home/antoine						
Nom de fichier	Taille de fichier	Type de fic...	Dernière modification	Droits d'accès	Propriétaire...	
..						
.bash_logout	220	Fichier sou...	05/06/2022 20:37:03	adfrw (0644)	antoine ww...	
.bashrc	3 526	Fichier sou...	05/06/2022 20:37:03	adfrw (0644)	antoine ww...	
.profile	807	Fichier sou...	05/06/2022 20:37:03	adfrw (0644)	antoine ww...	

L'utilisateur peut remonter jusqu'à l'arborescence primaire du serveur comme le montre le chemin /home/antoine. Il n'est pas chrooté.

Site distant : /						
Nom de fichier	Taille de fichier	Type de fic...	Dernière modification	Droits d'accès	Propriétaire...	
..						
.cache		Dossier de ...	17/04/2022 21:55:40	0700	antoine ww...	
bin		Dossier de ...	17/04/2022 21:45:32	adfr (0777)	antoine ww...	
boot		Dossier de ...	13/05/2022 23:27:39	fle (0755)	antoine ww...	
dev		Dossier de ...	05/06/2022 20:18:40	fle (0755)	antoine ww...	
etc		Dossier de ...	05/06/2022 20:37:08	fle (0755)	antoine ww...	
home		Dossier de ...	05/06/2022 20:37:03	fle (0755)	antoine ww...	
initrd.img		Dossier de ...	17/04/2022 21:47:46	adfr (0777)	antoine ww...	
initrd.img.old		Dossier de ...	17/04/2022 21:46:20	adfr (0777)	antoine ww...	
lib		Dossier de ...	17/04/2022 21:45:32	adfr (0777)	antoine ww...	
lib32		Dossier de ...	17/04/2022 21:45:32	adfr (0777)	antoine ww...	
lib64		Dossier de ...	17/04/2022 21:45:32	adfr (0777)	antoine ww...	
libx32		Dossier de ...	17/04/2022 21:45:32	adfr (0777)	antoine ww...	
lost+found		Dossier de ...	17/04/2022 21:45:26	0700	antoine ww...	
media		Dossier de ...	17/04/2022 21:45:26	fle (0755)	antoine ww...	
mnt		Dossier de ...	17/04/2022 21:45:38	fle (0755)	antoine ww...	
opt		Dossier de ...	17/04/2022 21:45:38	fle (0755)	antoine ww...	
proc		Dossier de ...	05/06/2022 20:18:21	fle (0555)	antoine ww...	
root		Dossier de ...	14/05/2022 00:04:38	0700	antoine ww...	
run		Dossier de ...	05/06/2022 20:29:43	fle (0755)	antoine ww...	
sbin		Dossier de ...	17/04/2022 21:45:32	adfr (0777)	antoine ww...	
srv		Dossier de ...	05/06/2022 20:21:14	fle (0755)	antoine ww...	
sys		Dossier de ...	05/06/2022 20:18:21	fle (0555)	antoine ww...	

Ci-dessus, Antoine peut seulement voir l'arborescence du serveur et non écrire. Il pourrait s'il le voulait, jeter un œil dans le répertoire des autres utilisateurs comme montré ci-dessous.

Site distant : /home						
Nom de fichier	Taille de fichier	Type de fic...	Dernière modification	Droits d'accès	Propriétaire...	
..						
antoine		Dossier de ...	05/06/2022 20:37:03	flecdmpe (0755)	antoine ww...	
toto		Dossier de ...	13/05/2022 23:15:25	fle (0755)	antoine ww...	
user		Dossier de ...	12/05/2022 21:30:00	fle (0755)	antoine ww...	

Il faut donc rajouter (ou décommenter) la ligne suivant le fichier proftpd :

DefaultRoot ~

Cette ligne spécifie la racine de chaque utilisateur dans son dossier home représenté par un ~

Site distant : /					
Nom de fichier	Taille de fichier	Type de fic...	Dernière modification	Droits d'accès	Pr
..					
travail		Dossier de ...			
scolaire		Dossier de ...			

Et voilà. Antoine est piégé dans son répertoire. Il peut écrire et modifier son contenu. Sa racine est /

Pour l'utilisateur Cathy, il suffit simplement de recrée un utilisateur et un dossier home.

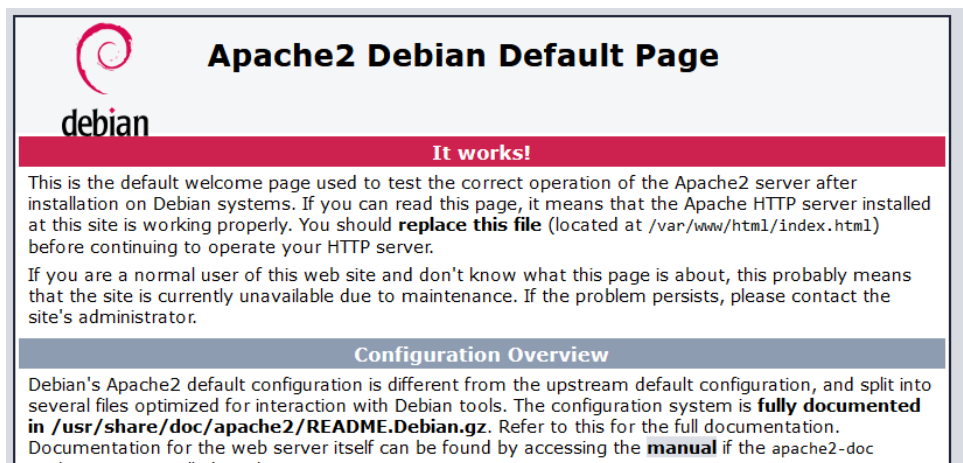
## Serveur Web

Pour le serveur web, nous avons choisi d'utiliser apache. Pour l'installer :

`apt install apache2`

Une fois le serveur installé, il est directement opérationnel. Il suffit d'entrer l'adresse IP de la machine virtuelle (qui est connecté en bridge sinon ça ne fonctionnera pas) dans un navigateur.

Voici la page par défaut :



**Apache2 Debian Default Page**

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

**Configuration Overview**

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented** in `/usr/share/doc/apache2/README.Debian.gz`. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

Si l'on veut modifier le contenu, il suffit d'éditer le fichier index.html dans le chemin `/var/www/html/`

On peut bien évidemment ajouter des images, un autre fichier css, etc...

Par défaut, apache utilise une connexion http non chiffrée sur le port 80.



## Proxy Squid

Un proxy sert à contrôler le trafic entrant et sortant de la couche application. On peut par exemple interdire l'accès à certains sites. On peut s'en servir également pour optimiser le trafic internet en stockant temporairement certains sites souvent visités comme google. On appelle cela le cache.

Pour installer squid :

```
apt install squid3
```

Pour paramétrer squid, on crée une copie du fichier /etc/squid/squid.conf qu'on nomme old.conf. Ainsi on pourra définir la configuration souhaitée dans un fichier squid.conf vide.

```
http_port 3128                                #Le port d'écoute du proxy
visible_hostname squid.local                  #Le nom du proxy
acl localnet src 172.16.217.0/24              #Le réseau sur lequel le proxy écoute
acl all src all                               # Tout les équipement différents du réseau
                                              172.16.217.0
http_access allow localnet                    #On autorise l'AC localnet à utiliser http
http_access deny all                          #On bloque le reste (qui n'est pas du réseau de l'ACL
                                              localnet)
access_log /var/log/squid/access.log          #Le fichier des logs de chaque page internet visitée
```

⚠ On remarquera que ce qui n'est pas du réseau 172.16.217.0 n'est pas autorisé à accéder à http

Le proxy est maintenant configuré et utilisable mais l'utilisateur n'est pas forcé de l'utiliser donc cela n'a presque aucun intérêt. L'opération étant fastidieuse et nécessitant des connaissances approfondies avec iptables, nous avons préféré nous concentrer sur les étapes précédentes, et puis les consignes ne précisent pas qu'il faut obligatoirement utiliser ce proxy.

Si l'utilisateur veut l'utiliser, il faut qu'il renseigne dans son système l'adresse IP du proxy ainsi que le port 3128.

Pour utiliser le cache on rajoute les lignes suivante dans le même fichier de configuration :

```
cache_dir ufs /var/cache 100 8 8              #Précise le répertoire devant accueillir le cache des
                                              pages internet. Le 100 correspond à la taille max du
                                              cache en mégaoctets. Le 1er 8 au nombre de
                                              répertoires racines et le seconde 8 au nombre de
                                              sous-répertoires pour le cache.

cache_access_log /var/log/squid3/access.log    # fichier log des requêtes appelées
cache_log /var/log/squid3/cache.log            # Journal des évènements du cache de squid
```

⚠ Nous n'avons pas bien compris tous les paramètres entrés du proxy. Nous nous sommes surtout concentrés sur les étapes précédentes. Nous n'avons effectué qu'un seul TP sur squid mais ce n'est pas forcément suffisant pour tout bien comprendre. (Sur internet ce n'est pas forcément plus facile)

## Conclusion

Tout au long de la préparation de notre projet, nous avons essayé de mettre en pratique les connaissances acquises durant nos études, et cela, dans le but de mettre en place un réseau d'entreprise de petite taille.

Plusieurs difficultés ont été rencontrées, tout d'abord par la compréhension du sujet et de certains protocoles non étudiés, mais grâce à des recherches et de la documentation le projet a pu commencer.

Les plus grosses difficultés du projet ont été la mise en place d'OSPF et l'empoisonnement ARP, car aucune étude ne nous a été donnée. Elles ont été résolues avec des recherches et beaucoup de tests.

Ce projet nous a apporté de l'expérience en groupe, grâce à la segmentation des adresses IP ainsi qu'à l'interconnexion des routeurs qui ont été fait en commun et en groupe pour que tout fonctionne correctement.

La compréhension du sujet était assez facile (plus claire que les autres) et avec tous les TP qui ont été réalisés en amont, qui nous ont grandement aidé pour la rapidité des différentes parties du projet comme le Routage Inter-Vlan, l'Accès SSH et le Service DHCP.

Merci à vous d'avoir pris le temps de lire notre rapport.

Cordialement

Le groupe

Morgan Bois, Julien Losser, Olivier Lamontagne, Valentin Long