Réseaux informatiques

TD2 : Réseau LAN et protocole ARP (Utilisation de Packet Tracer)

Examiner les trames Ethernet / Observation de table ARP

Objectifs

Partie 1 : Examiner les champs d'en-tête dans une trame Ethernet

Partie 2 : Exemple avec Wireshark (capture et analyse de trames Ethernet)

Partie 3 : Adresses MAC

Partie 4 : Observation du protocole ARP

Partie 5 : Mac flooding et mise en œuvre de la sécurité des ports sur un switch

Scénario

Dès lors que des protocoles de couche supérieure communiquent entre eux, les données circulent dans les couches du modèle OSI (Open System Interconnexion) et sont encapsulées dans une trame de couche 2.
La composition des trames dépend du type d'accès aux supports. En effet, si les protocoles de couche supérieure sont TCP (couche 4 du modèle OSI) et IP (couche 3 du modèle OSI) et que l'accès aux supports est Ethernet, l'encapsulation des trames de couche 2 est Ethernet. Cela est habituellement le cas pour un environnement de réseau local (LAN).
Lorsque vous étudiez les concepts de couche 2, il est utile d'analyser les informations d'en-tête des trames.
Dans la première partie de ce TP, vous allez examiner les champs figurant dans une trame Ethernet. Ensuite, vous aurez un exemple d'utilisation de Wireshark (capture et analyse des champs d'en-tête de trame Ethernet pour le trafic local et distant. Ensuite, vous observerez la table d'adresses MAC du switch et enfin, vous observerez le processus ARP. Bon courage !

Instructions

Partie 1 : Examiner les champs d'en-tête dans une trame Ethernet

Durant cette première partie, quelques petits rappels de cours ainsi qu'un petit exemple vous seront fournis.
Après cela, vous examinerez les champs d'en-tête ainsi que le contenu d'une trame Ethernet. Pour cela, vous aurez un exemple d'utilisation de « Wireshark » afin d'examiner le contenu de ces champs.

Petit rappel de la structure d'une trame Ethernet :

Préambule	Adresse MAC destination	Adresse Source destination	Type de trame	Données	FCS
8 octets	6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

PS : Wireshark est un analyseur de réseau ou de protocole. Il est utilisé pour analyser la structure de différents protocoles réseau et possède la capacité de démontrer l'encapsulation en permettant à l'utilisateur de voir tout le trafic transmis sur le réseau. Cet outil d'analyse fonctionne sur les systèmes d'exploitation Unix, Linux et Microsoft Windows.

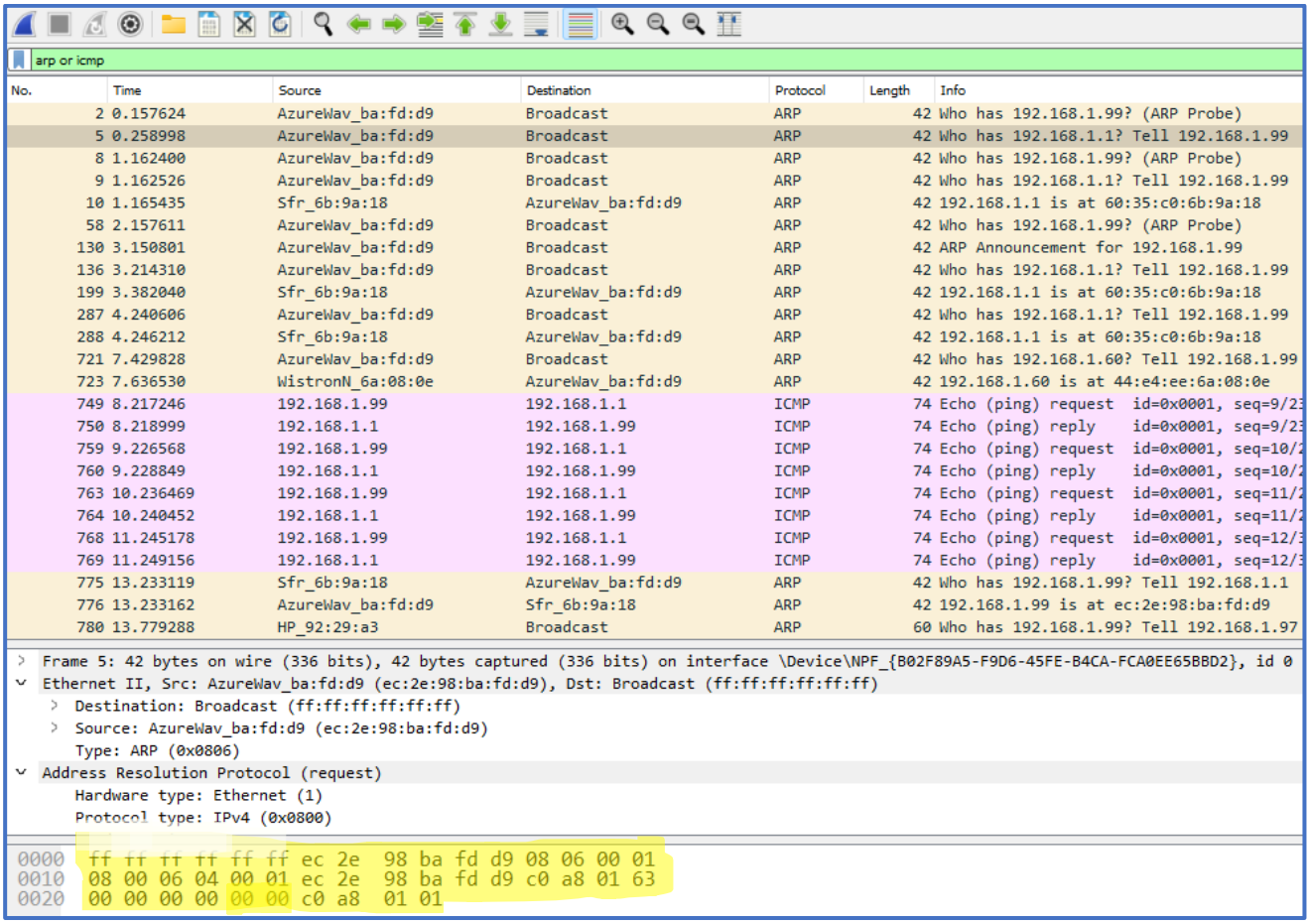
Partie 2 : Rappels de cours et exemple avec Wireshark

Ceci est à présent un exemple que j'ai réalisé afin de vous fournir une meilleure compréhension:

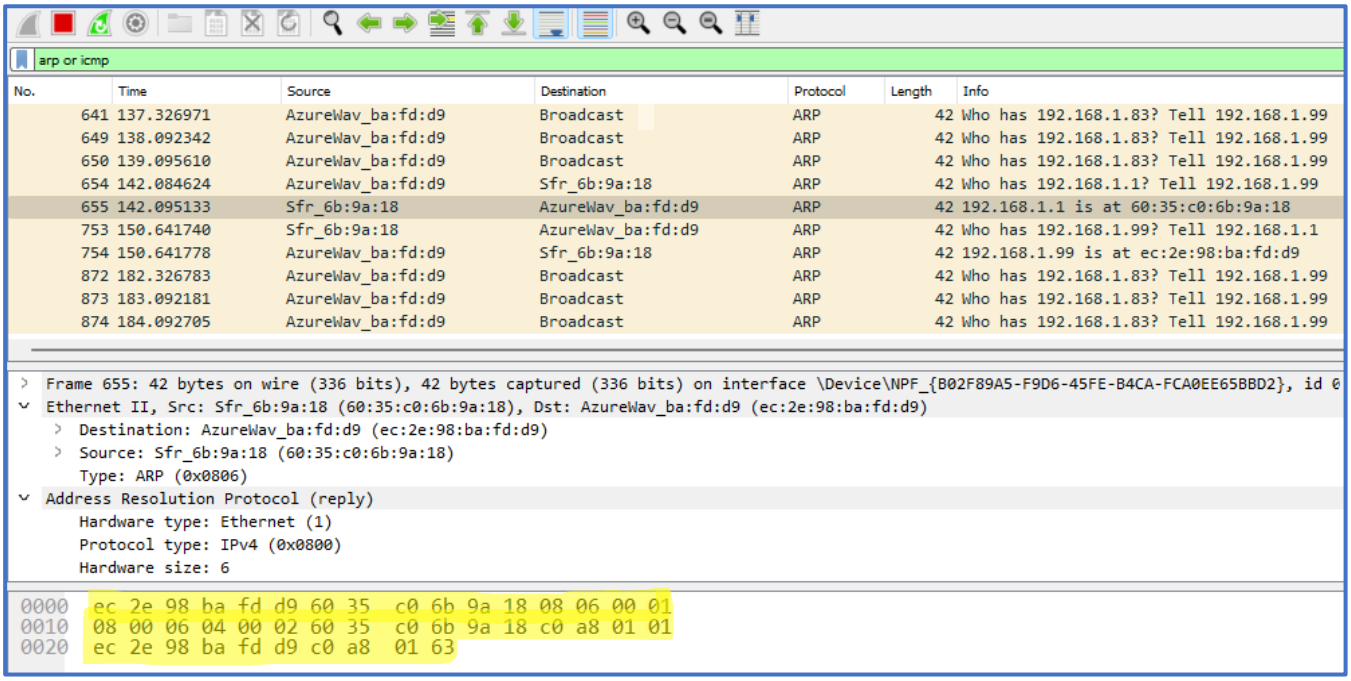
```
C:\Users\Haman>ipconfig /all

Suffixe DNS propre à la connexion. . . :
Description. . . . . . . . . . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
Adresse physique . . . . . . . . . . . : EC-2E-98-BA-FD-D9
DHCP activé. . . . . . . . . . . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.99(préféré)
Masque de sous-réseau. . . . . . . . . : 255.255.255.0
Bail obtenu. . . . . . . . . . . . . . : mardi 11 octobre 2022 03:06:15
Bail expirant. . . . . . . . . . . . . : vendredi 14 octobre 2022 13:31:30
Passerelle par défaut. . . . . . . . . : 192.168.1.1
Serveur DHCP . . . . . . . . . . . . . : 192.168.1.1
Serveurs DNS. . .  . . . . . . . . . . : 192.168.1.1
NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Les captures d'écran de la capture Wireshark ci-dessous montrent les paquets générés par un ping émis depuis un PC hôte vers sa passerelle par défaut. Un filtre a été appliqué à Wireshark pour afficher les protocoles ARP et ICMP uniquement. ARP signifie protocole de résolution d'adresse. ARP est un protocole de communication utilisé pour déterminer l'adresse MAC associée à l'adresse IP. La session commence par une requête ARP pour l'adresse MAC du routeur de passerelle, suivie de quatre requêtes ping et réponses.
La capture d'écran ci-dessous met en évidence les détails du trame pour une requête ARP :



La capture d'écran ci-dessous met en évidence les détails du trame pour une réponse ARP :



Champ	Valeur	Description
Préambule	Non présent dans la capture	Ce champ contient des bits de synchronisation traités par la carte réseau.
Adresse (destination et source)	- Adresse destination: Broadcast (FF:FF:FF:FF:FF:FF) -Adresse source: EC-2E-98-BA-FD-D9	Concernant les adresses de couche 2 trame (Ethernet). La longueur de chaque adresse est de 48 bits, ou 6 octets, exprimés en 12 chiffres hexadécimaux, de 0 à 9 et de A à F. Le format suivant est courant : 12:34:56:78:9A:BC. Les six premiers chiffres hexadécimaux indiquent le fabricant de la carte réseau, les six derniers chiffres hexadécimaux correspondent au numéro de série de la carte réseau. L'adresse de destination peut être une adresse de diffusion (ff:ff:ff:ff:ff:ff), ou une adresse de monodiffusion. L'adresse source est toujours une adresse de monodiffusion.
Type de trame	0x0806	Ce champ possède une valeur hexadécimale qui permet d'indiquer le type de protocole de couche supérieure dans le champ de données. De nombreux protocoles de couche supérieure sont pris en charge par Ethernet. Deux types de trame standard sont : **Valeur Description** 0x0800 IPv4 Protocol 0x0806 Protocol ARP
Données	ARP	Contient le protocole encapsulé de niveau supérieur. Le champ de données comprend entre 46 et 1 500 octets.
FCS	Non présent dans la capture	Séquence de contrôle de trame, que la carte réseau utilise pour identifier les erreurs au cours de la transmission. La valeur est calculée par le dispositif d'envoi, englobant les adresses de trame, le type et le champ de données. Elle est vérifiée par le récepteur.

Questions :

Voici quelques questions sur lesquelles vous vous baserez sur l'exemple précèdent.

1- Pouvez-vous indiquer pourquoi le PC envoie-t-il une diffusion ARP avant d'envoyer la première requête ping ?
2- Veuillez indiquer l'adresse MAC source dans la requête ARP.
3- Veuillez indiquer l'adresse MAC destination dans la requête ARP. A quoi correspond cette adresse ?

Vos réponses :

-
-
-
-
-
-
-

Partie 3 : Adresses MAC

Les commutateurs maintiennent des tableaux qui sont référencés lors de l'acheminement du trafic.
Plus exactement, les commutateurs utilisent les adresses MAC de destination. Ils dirigent ainsi les communications du réseau à travers le commutateur. Les communications se font vers la destination, à l'exception du port approprié.
Pour qu'un commutateur sache vers quel port transférer une trame, il doit tout d'abord apprendre quels périphériques existent sur chaque port.
À mesure que le commutateur apprend la relation entre les ports et les dispositifs, il construit une table appelée table d'adresses MAC. Ce tableau est stocké dans la mémoire de contenu (CAM – Content Adressable Memory). C'est un type particulier de mémoire utilisé dans les applications de recherche à haute vitesse. Pour cette raison, la table d'adresses MAC est parfois aussi appelée table CAM.

Topologie :

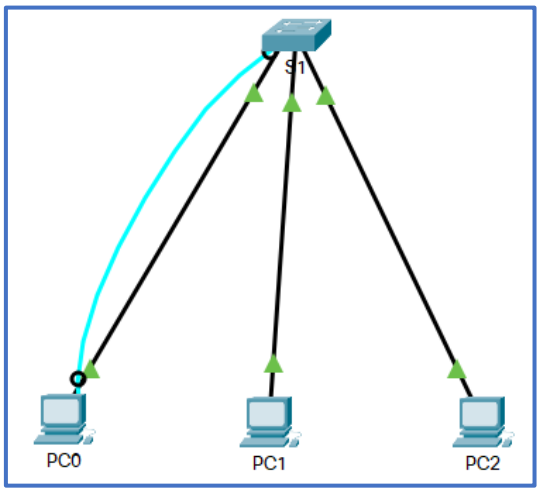


Table d'adressage :

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Default Gateway
S1	VLAN 1	192.168.10.1	255.255.255.0	N/A
PC0	Carte réseau	192.168.10.2	255.255.255.0	N/A
PC1	Carte réseau	192.168.10.3	255.255.255.0	N/A
PC2	Carte réseau	192.168.10.4	255.255.255.0	N/A

PS :Chaque liaison à Internet requiert un type de support réseau spécifique, ainsi qu'une technologie réseau particulière. Par exemple, l'Ethernet est la technologie de réseau local (LAN) la plus répandue aujourd'hui. Les ports Ethernet sont présents sur les périphériques des utilisateurs finaux, les commutateurs et d'autres périphériques réseau pouvant se connecter physiquement au réseau à l'aide d'un câble.
Les commutateurs Cisco IOS de couche 2 sont équipés de ports physiques pour permettre à des périphériques de s'y connecter. Ces ports ne prennent pas en charge les adresses IP de couche 3. Par conséquent, les commutateurs ont une ou plusieurs interfaces de commutateur virtuelles (SVI). Ces interfaces sont virtuelles car il n'existe aucun matériel sur le périphérique associé. Une interface SVI est créée au niveau logiciel.
L'interface virtuelle est un moyen de gérer à distance un commutateur sur un réseau grâce à l'IPv4 et l'IPv6 Chaque commutateur dispose d'une interface SVI apparaissant dans la configuration par défaut prête à l'emploi. L'interface SVI par défaut est l'interface VLAN1.

***Remarque**: un commutateur de couche 2 ne nécessite pas d'adresse IP. L'adresse IP attribuée à l'interface SVI sert à accéder à distance au commutateur. Une adresse IP n'est pas nécessaire pour permettre au commutateur d'accomplir ses tâches.*

Instructions

Au sein de cette partie, vous configurerez la topologie du réseau et les paramètres de base, tels que les adresses IP de l'interface et les nom des périphériques (voir la table d'adressage).

Connectez les périphériques conformément à la topologie et effectuez le câblage nécessaire.

1-a : Configurez l'adresse IPv4, le masque de sous-réseau pour les PC.

1-b : À partir de l'invite de commandes de PC0, envoyez une requête ping à l'adresse du commutateur.

Question : Les requêtes ping ont-elles abouti ? Expliquez votre réponse.

-

-

1-c : Veuillez fermer la fenêtre d'invite de commandes, configurez les paramètres de base du commutateur. Au cours de cette étape, vous configurerez le nom et l'adresse IP du périphérique. Accédez au commutateur par la console et passez en mode de configuration globale.

Pour cela, voici les commandes à appliquer (plus de détails concernant l'IOS vous seront donnés lors des prochains TDs):

A : Accédez au commutateur par la console et passez en mode de configuration globale :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

B. Attribuez un nom d'hôte au commutateur selon la table d'adressage (S1) :

```
Switch(config)#hostname S1
```

C : Configurez et activez l'interface SVI pour VLAN 1 :

```
S1(config)#interface vlan 1
S1 (config-if)# ip address 192.168.10.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
```

A présent, vérifions la connectivité réseau, pour ce faire, envoyez une requête ping au commutateur à partir de PC0.

Les requêtes ping ont-elles abouti ?

-

-

D : Veuillez noter l'adresse MAC de chaque périphérique :

Adresse MAC S1	
Adresse MAC PC0	
Adresse MAC PC1	
Adresse MAC PC2	

PS : pour voir l'adresse MAC du commutateur, il est possible d'utiliser diverses commandes. Récupérez l'adresse MAC en vous appuyant sur l'exemple sur la capture ci-dessous. Pour les PC, utilisez la commande ipconfig /all.

Accédez à S1 via la console et utilisez la commande show interfaces vlan 1 pour trouver les informations d'adresse MAC.

```
S1>show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 000a.4125.9a18 (bia
000a.4125.9a18)
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Exécutez la commande show mac-address-table sur S1, Voyez l'exemple ci-dessous. Utilisez le résultat généré par le commutateur pour répondre aux questions.

```
S1>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0030.f257.e33e    DYNAMIC     Fa0/1
   1    00d0.bc12.7b00    DYNAMIC     Fa0/3
```

PS : Pour afficher les interfaces (Fa0/1…)sur les différents périphériques, vous pouvez cliquer sur Options, Préférences, et cocher « Always Show Port Labels in Logical Workspace ».

Questions :

1- Le commutateur a-t-il affiché l'adresse MAC de PC0 ? Si vous répondez oui, précisez sur quel port.
2- Envoyez différents pings entre les différents périphériques, et observez la table d'adresses MAC de S1. La table est-elle modifiée au fur et à mesure des différents ping ?
3- Les diffusions sont-elles possibles au niveau de la couche 2 ? Si oui, quelle serait l'adresse MAC ?
4- Pourquoi faut-il connaître l'adresse MAC d'un appareil ?

Vos réponses :

-

-

-

-

-

-

-

-

-

-

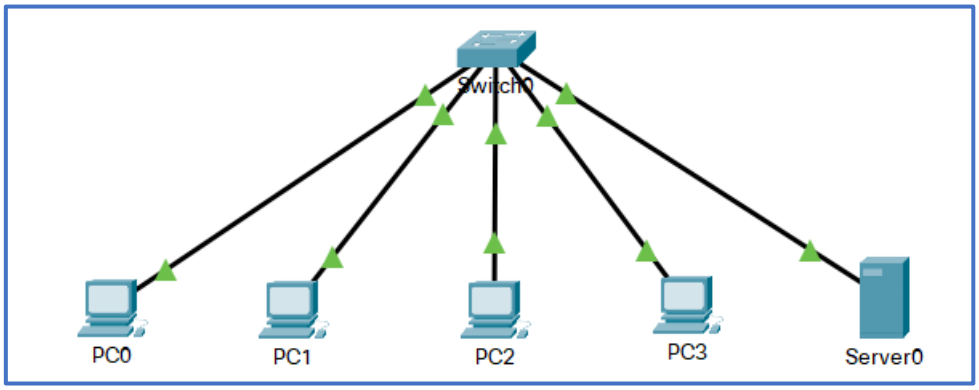
Partie 4 : Observation du protocole ARP

Simulation de cas de communication.

Table d'adressage

Périphérique	Interface Client	Interface Switch	Adresse IP	Masque de sous-réseau	Default Gateway
PC0	**Fa0**	**Fa0/1**	**192.168.10.1**	**255.255.255.0**	**N/A**
PC1	**Fa0**	**Fa0/2**	**192.168.10.2**	**255.255.255.0**	**N/A**
PC2	**Fa0**	**Fa0/3**	**192.168.10.3**	**255.255.255.0**	**N/A**
PC3	**Fa0**	**Fa0/4**	**192.168.10.4**	**255.255.255.0**	**N/A**
Server0	**Fa0**	**Fa0/5**	**192.168.10.5**	**255.255.255.0**	**N/A**

Topologie



Instructions

1-a :Veuillez commencer par créer le réseau sur la topologie et ensuite attribuer les adresses IP et masques de sous-réseau sur les différentes machines.

1-b : A présent, veuillez passer en simulation mode, cliquez sur Edit Filters, et sélectionnez uniquement ARP ainsi que ICMP.

Envoyez un ping du PC0 au Server0, et veuillez laisser la simulation se dérouler jusqu'à ce que la réponse à la commande ping soit obtenue.

Nous allons nous focaliser à présent sur la requête ARP transmise par PC0.

Questions

A- Pouvez vous indiquer à quelle couche du modèle OSI le protocole ARP appartient-il ?
B- Pouvez-vous expliquer pourquoi une requête ARP a été initiée avant que la requête « écho request » n'ai pu être envoyée ?
C- Quelles sont les adresses MAC source et destination concernant cette requête ? Comment se fait-il que la requête ait été transmise en broadcast (diffusion) ?

Vos réponses

-

-

-

-

-

Partie 5 : Mac flooding et mise en œuvre de la sécurité des ports sur un switch

Topologie

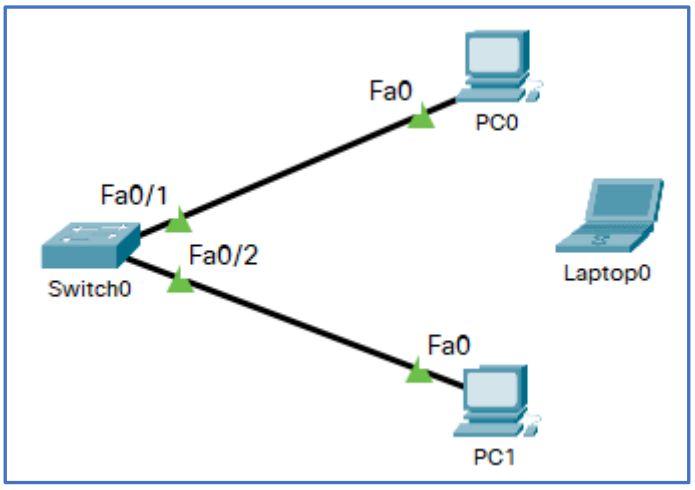


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
Switch0	**Vlan 1**	**192.168.10.2**	**255.255.255.0**
PC0	**Carte réseau**	**192.168.10.10**	**255.255.255.0**
PC1	**Carte réseau**	**192.168.10.11**	**255.255.255.0**
Laptop0 (pirate informatique)	**Carte réseau**	**192.168.10.12**	**255.255.255.0**

Mac flooding

Les commutateurs tiennent à jour une table d'apprentissage qui associe les adresses MAC Ethernet (des équipements connectés) aux différents ports physiques du commutateur. Cela permet au commutateur d'envoyer les trames Ethernet directement aux machines à qui elles sont destinées. Pour cela, le commutateur regarde l'adresse destination de la trame, puis il en déduit le port correspondant qui figure dans la table d'apprentissage.

Cette méthode d'envoi ciblé s'oppose à la diffusion (*broadcast*) aveugle telle qu'elle est pratiquée par les concentrateurs (*hubs*) et qui consiste à envoyer sur tous les ports, que le destinataire y soit connecté ou pas. Dans le processus d'apprentissage, le commutateur apprend les adresses MAC associées à chaque port en regardant les adresses sources des trames qui le traversent.

Dans une attaque par saturation ou « Mac flooding », le pirate envoie de nombreuses trames Ethernet au commutateur, chacune d'entre elles ayant une adresse MAC source différente. Le but est de remplir l'espace nécessairement limité de la mémoire du commutateur consacré à la table d'apprentissage.

L'effet de cette attaque peut varier suivant la marque et le modèle du commutateur. L'effet désiré par l'attaquant est néanmoins que le commutateur se mette à envoyer les trames sur tous les ports, y compris à cet attaquant, qui pourra ainsi écouter des échanges qui ne le concernent pas.

Il se peut en effet que les adresses légitimes soient expulsées de la table d'apprentissage quand celle-ci sature, ou que de nouvelles adresses légitimes ne puissent plus être apprises[1].

Contexte

Les appareils de couche 2 sont considérés la liaison le plus faible de l'infrastructure de sécurité d'une entreprise. Les attaques de couche 2 sont parmi les plus faciles à déployer pour les pirates, mais ces menaces peuvent également être atténuées avec certaines solutions de couche 2 courantes.
Tous les ports (interfaces) du commutateur doivent être sécurisés avant que le commutateur soit déployé pour une utilisation en production. La façon dont un port est sécurisé dépend de sa fonction.
Une méthode simple que nombreux administrateurs utilisent pour aider à sécuriser le réseau contre les accès non autorisé est de désactiver tous les ports qui ne sont pas exploités sur un commutateur. Par exemple, si un commutateur Catalyst 2960 à 24 ports et si trois connexions Fast Ethernet sont utilisées, il est conseillé de désactiver les 21 ports inutilisés.

Dans cette activité, vous allez configurer et vérifier la sécurité des ports sur un commutateur. La sécurité des ports vous permet de restreindre le trafic entrant d'un port en limitant les adresses MAC autorisées à envoyer du trafic vers le port.

PS : La sécurité des ports ne peut être configurée que sur des ports d'accès configurés manuellement ou des ports de trunk de réseau configurés manuellement. Par défaut, les ports de commutateur de couche 2 sont réglés sur l'auto dynamique (trunking activée).
Le trunking dépasse le cadre de TD et ne sera pas abordé.

1-Veuillez réaliser le schéma réseau en vous basant sur la topologie et la table d'adressage.

Connectez un câble console de PC0 vers le switch, et entrez en mode de configuration globale. Sur les interfaces « FastEthernet0/1 » et « FastEthernet0/2 » du switch réalisez cette configuration :

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#exit

Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#exit
```

Étape 1: configurer la sécurité des ports

PS : Afin d'apporter une meilleure visibilité, vous pouvez afficher les interfaces des différents périphériques raccordés, en vous rendant dans « Options », « Préférences », et en cliquant sur « Always Show Port Labels in Logical Workspace ».

a. Sur les commutateurs Cisco, il est possible de faire un contrôle sur les ports en limitant l'accès à certaines adresses MAC, cela permet de sécuriser l'accès. Pour cela, il faut utiliser l'option « **Port-security** ». L'adresse MAC autorisée est celle de l'hôte qui va se connecter et envoyer une trame en premier au port du Switch.
Pour rappel, l'adresse MAC correspond à l'adresse physique de la machine c'est-à-dire de sa carte réseau.

[1] https://fr.wikipedia.org/wiki/Saturation_de_la_table_d%27apprentissage

Accédez via la ligne de commande sur le Switch0 et activez la sécurité des ports sur les ports Fast Ethernet 0/1 et 0/2.

```
Switch(config)# interface range f0/1 - 2
Switch(config-if-range)# switchport port-security
```

b. Fixez le maximum d'adresses MAC autorisé à 1 pour qu'un seul périphérique puisse accéder aux ports Fast Ethernet 0/1 et 0/2.

```
Switch(config-if-range)# switchport port-security maximum 1
```

c. Sécurisez les ports afin que l'adresse MAC d'un périphérique soit apprise dynamiquement et ajoutée à la configuration en cours (mémoire) :running-config.

```
Switch(config-if-range)# switchport port-security mac-address sticky
```

d. Définissez le mode de violation afin que les ports Fast Ethernet 0/1 et 0/2 ne soient pas désactivés lorsqu'une violation se produit, mais qu'une notification de la violation de sécurité soit générée et les paquets provenant de la source inconnue sont supprimés.

```
Switch(config-if-range)# switchport port-security violation restrict
```

PS: Une "Violation" est une action prise en cas de non-respect d'une règle port-Security. En mode 'restrict' : dès que la "violation" est constatée, le port arrête de transférer le trafic des adresses non autorisées et transmet un message de log.

e. Désactivez tous les ports inutilisés restants. Utilisez le mot clé « range » pour appliquer cette configuration à tous les ports simultanément.

```
Switch(config-if-range)#interface range f0/3 - 24 , g0/1 - 2
Switch(config-if-range)# shutdown
```

Étape 2: vérifier la sécurité des ports

a. De PC0, envoyer un message Ping à PC1.

A partir de la commande Ipconfig /all, veuillez noter les adresses Mac de PC0 et de PC1.

Mac address PC0 :

Mac address PC1 :

b. Vérifiez que la sécurité des ports est activée et que les adresses MAC de PC0 et PC1 ont été ajoutés à la configuration en cours.

```
Switch# show run | begin interface
```

c. Utilisez les commandes show port-Security pour afficher les informations de configuration.

```
Switch# show port-security
Switch# show port-security address
```

d. Connectez l'Ordinateur portable du pirate à tout port de commutateur inutilisé et notez que les voyants de liaison sont rouges.

e. Activez le port et vérifiez que l'Ordinateur portable peut envoyer un message Ping à PC0 et PC1. Après vérification, fermez le port connecté à l'Ordinateur portable du pirate.

f. Déconnectez PC1 et Connectez l'Ordinateur portable à F0/2, qui est le port auquel PC1 était initialement connecté. Vérifiez que l'Ordinateur portable ne soit pas en mesure d'envoyer un message ping à PC0.

g. Affichez les violations de sécurité du port pour le port auquel le Laptop est connecté.

```
Switch# show port-security interface f0/2
```

Combien de violations se sont produites?

-

h. Déconnectez l'Ordinateur portable et reconnectez PC1. Vérifiez que PC1 peut envoyer un message Ping PC0.

Veuillez expliquer pourquoi PC1 peut-il envoyer un message ping à PC0, mais que l'ordinateur portable du pirate n'y parvient pas?

-

-

-