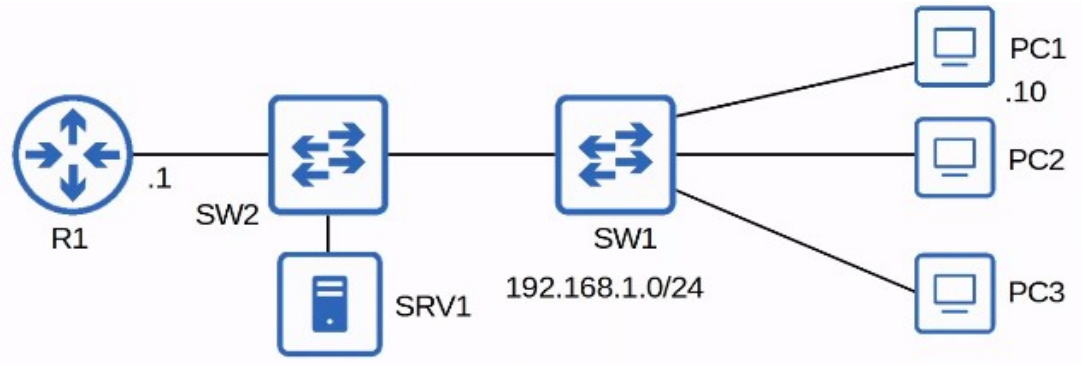
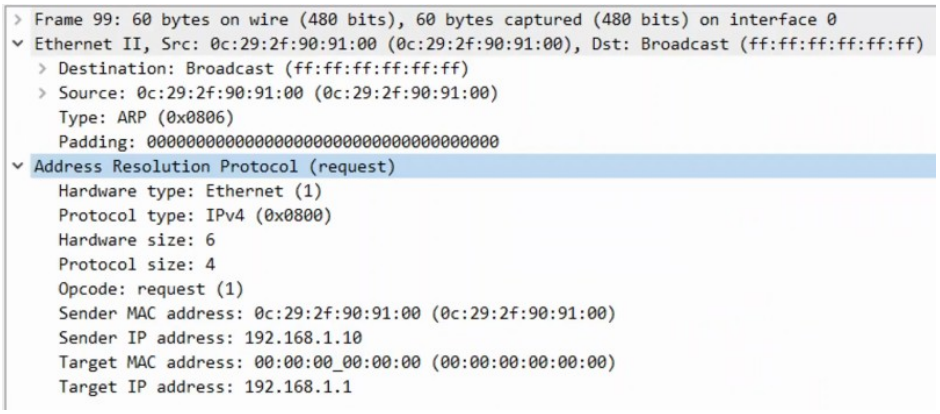
Cours 51 : ARP Inspection

Dans ce cours nous verrons comment ce qu'est le ARP Inspection, il s'agit d'une fonctionnalité de sécurité des Switch, qui inspecte les messages ARP de la même manière que DHCP Snooping inspecte les messages DHCP.
Nous verrons tout d'abord ce qu'est Dynamic ARP Inspection et comment il fonctionne, nous verrons quelles attaques il permet de bloquer et comment le configurer sur un Switch.

Commençons par revoir le fonctionnement du protocole ARP sur le réseau suivant :



ARP est utilisé pour apprendre l'adresse MAC d'un autre appareil avec une adresse IP connu.
Par exemple un PC utilise ARP pour apprendre l'adresse MAC de sa passerelle par défaut pour communiquer avec le réseau externe.
Cela consiste en l'échange de deux messages : la requête et la réponse.
Par exemple PC1 envoie une requête DNS avec pour adresse IP source 192.168.1.10 et adresse IP de destination : 8.8.8.8 mais l'adresse MAC de destination lui est inconnu.
Le PC va envoyer la trame à sa passerelle par défaut car l'adresse 8.8.8.8 est en dehors de son réseau local. Il va donc envoyer en Broadcast la requête ARP suivante avec les informations suivantes :
Adresse IP source : 192.168.1.10, Adresse IP destination : 192.168.1.1, Adresse MAC source : son adresse MAC, Adresse MAC de destination : F.F.F
Tous les appareils vont recevoir ce message puisque l'adresse de destination est l'adresse de Broadcast F.F.F
On peut voir le message suivant sur Wireshark :

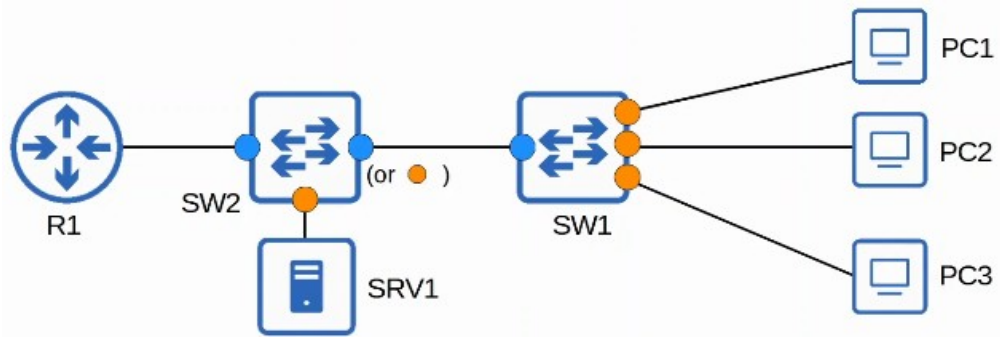


Puisque le routeur R1 est bien l'adresse de Destination de la requête du PC1, R1 va envoyer une réponse ARP afin d'informer le PC1 qu'il s'agit bien de son adresse MAC et qu'il puisse l'enregistrer dans sa table ARP. Le routeur R1 ajoute lui aussi une entrée dans sa table ARP pour le PC1 lorsqu'il reçoit la requête ARP.
Voici la réponse ARP envoyé par le routeur R1 :

```
> Frame 224: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
v Ethernet II, Src: 0c:29:2f:43:b5:00 (0c:29:2f:43:b5:00), Dst: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00)
  > Destination: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00)
  > Source: 0c:29:2f:43:b5:00 (0c:29:2f:43:b5:00)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 0c:29:2f:43:b5:00 (0c:29:2f:43:b5:00)
    Sender IP address: 192.168.1.1
    Target MAC address: 0c:29:2f:90:91:00 (0c:29:2f:90:91:00)
    Target IP address: 192.168.1.10
```

Le PC1 peut à présent ajouter l'adresse MAC du routeur R1 lorsqu'il envoie des requêtes DNS, le routeur R1 recevra la requête puis la retransmettra au réseau externe.
Il existe un autre type de message ARP qui sont appelés les messages« Gratuitous ARP » qui sont des réponses ARP envoyés sans réception de requête ARP.
Ces messages sont envoyés à l'adresse MAC de Broadcast (F.F.F), ces messages permettent aux appareils du réseau d'apprendre les appareils enregistrés sans avoir à envoyer de requêtes ARP.
Certains appareils envoient automatiquement des messages « GARP » lorsque l'interface est activé, que l'adresse IP change, que l'adresse MAC change, etc...
Dans le réseau précédent par exemple la réponse ARP est envoyé vers tous les appareils du réseau local, les PC vont enregistrer le PC2 dans leur table ARP ansi que les Switchs.

DAI est une fonctionnalité de sécurité des switchs qui est utilisé pour filtrer les messages ARP reçus sur des ports qui ne sont pas de confiance. DAI filtre uniquement les messages ARP. Les messages non ARP ne sont pas affectés. Tous les ports ne sont pas de confiance par défaut.
Tous les ports connectés à d'autres appareils du réseau (Switch, routeur) doivent être configurés comme de confiance, les interfaces connectés à des hôtes finaux ne sont pas confiance.
Sur le réseau précédent par exemple les interfaces de confiance sont en bleus celle qui ne le sont pas sont en orange :



Le fonctionnement de Dynamic ARP Inspection est similaire à DHCP, par exemple sur le réseau, le PC1 envoie une requête ARP au SW1, puisque le message arrive sur un port qui n'est pas de confiance le Switch va utiliser DAI pour vérifier que le message est normal, si c'est le cas il va le distribuer au Switch 2, le SW2 ne va pas le vérifier car il reçoit la requête sur une interface de confiance. Le SW2 redistribue le paquet au routeur R1 qui envoie ensuite une réponse ARP.
Si à présent le PC2 envoie le message et que le SW2 décide de bloquer le message car il contredit les règle de DAI (nous verrons comment est ce possible de contredire les règle de DAI), le message ne sera pas redistribué.
Voyons le fonctionnement de ARP poisoning (Man in the Middle)
De manière similaire à DHCP Poisoning, ARP Poisoning implique que attaquant manipule la table de la cible ARP donc le trafique est envoyé à l'attaquant.
Pour faire cela l'attaquant envoie des messages ARP Gratuitous en utilisant l'adresse IP d'un autre appareil. Les autres appareils du réseau reçoivent le GARP et mettent à jour leurs table ARP ce qui cause que le trafique est envoyé à l'attaquant au lieu de l'envoyer à la destination légitime.
A présent lorsque par exemple le PC1 veut envoyer un paquet au réseau externe, il envoie le message au PC2 en premier qui l'enregistre peut le sauvegarder ou même modifier le paquet puis le redistribuer à la destination légitime, dans le réseau précédent le routeur R1.

Voyons comment DAI peut protéger de ce type d'attaque. DAI inspecte l'adresse MAC de l'envoyeur ainsi que son adresse IP de la partie des messages ARP reçu sur des ports qui ne sont pas de confiance et vérifie s'il y a une entrée qui correspond dans la table DHCP snooping binding.

```
SW1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
0C:29:2F:18:79:00   192.168.100.10   86294       dhcp-snooping   1     GigabitEthernet0/3
0C:29:2F:90:91:00   192.168.100.11   86302       dhcp-snooping   1     GigabitEthernet0/1
0C:29:2F:67:E9:00   192.168.100.12   86314       dhcp-snooping   1     GigabitEthernet0/2
Total number of bindings: 3
```

S'il y a une entrée qui correspond le message ARP est redistribué normalement.
S'il n'y a pas d'entrée qui correspond le message ARP est bloqué.
DAI n'inspecte pas les messages reçus sur des ports de confiance et sont redistribués normalement.
Les ACLs ARP peuvent être configurés manulement pour cartographier des adresses MAC/IP pour vérifier le DAI. Cela peut être utile pour les hôtes qui n'utilisent pas DHCP.
DAI peut être utilisé pour faire des vérifications de paquet plus approfondie mais cela est optionnel.
Tout comme DHCP Snooping, DAI supporte aussi la limité des taux (rate limiting) pour empêcher l'attaquant de surcharger le switch de messages ARP.
DHCP Snooping et DAI requière des ressources du CPU depuis le Switch, donc si même si les messages de l'attaquant sont bloqués cela peut surcharger le CPU avec des messages ARP, si l'attaquant tente de faire cela, la limite des taux va désactiver l'interface.

Voici les commandes à utiliser pour configurer DAI, on commence par configurer le SW2 du réseau précédent :

```
SW2(config)#ip arp inspection vlan 1
SW2(config)#interface range g0/0 - 1
SW2(config-if-range)#ip arp inspection trust
```

`SW2(config)#ip arp inspection vlan 1`
Permet d'activer DAI sur un vlan (ici le vlan 1) il faut ajouter tous les vlan du réseau sinon seulement les vlan spécifiés seront inspectés

```
SW2(config)#interface g0/0 - 1
SW2(config-if-range)#ip arp inspection trust
```

On lance ensuite ces commandes afin d'activer les interface G0/0 et G0/1 comme interfaces de confiance.

On lance les même commandes sur le SW1 sauf que l'on fais cette fois confiance seulement à l'interface G0/0

```
SW1(config)#ip arp inspection vlan 1
SW1(config)#interface g0/0
SW1(config-if)#ip arp inspection trust
```

On peut noter une différence entre la configuration DHCP Snooping et la configuration de DAI :
DHCP snooping requière deux commande pour être activé :

```
ip dhcp snooping
ip dhcp snooping vlan numéro de vlan
```

DAI requière uniquement une seule commande :

```
ip arp inspection vlan numéro de vlan
```

Il est possible d'afficher les interfaces avec l'inspection arp avec la commande :

```
show ip arp inspection interfaces
```

```
SW1#show ip arp inspection interfaces

Interface        Trust State     Rate (pps)     Burst Interval
---------------  -----------     ----------     --------------
Gi0/0            Trusted               None                N/A
Gi0/1            Untrusted               15                  1
Gi0/2            Untrusted               15                  1
Gi0/3            Untrusted               15                  1
Gi1/0            Untrusted               15                  1
Gi1/1            Untrusted               15                  1
Gi1/2            Untrusted               15                  1
Gi1/3            Untrusted               15                  1
Gi2/0            Untrusted               15                  1
Gi2/1            Untrusted               15                  1
Gi2/2            Untrusted               15                  1
Gi2/3            Untrusted               15                  1
Gi3/0            Untrusted               15                  1
Gi3/1            Untrusted               15                  1
Gi3/2            Untrusted               15                  1
Gi3/3            Untrusted               15                  1
```

On peut voir différentes informations comme l'interface, si l'interface est de confiance ou non, le taux de limiting (rate). Il y a une différence entre DAI rate limiting et DHCP snooping rate limiting, DAI rate limiting est activé sur les ports qui ne sont pas de confiance par défaut avec un taux de 15 paquets par secondes. Cela est désactivé sur des ports de confiance par défaut.
Le DHCP snooping est configuré en terme de X paquet par seconde, tandis que DAI interval par rafal (Burst interval) permet de configurer la limite des taux en terme X paquets par Y secondes.

Pour configurer DAI rate limiting on lance les commandes suivantes :

```
SW1(config)#interface range g0/1 - 2
SW1(config-if-range)#ip arp inspection limit rate 25 burst interval 2
```

`ip arp inspection limit rate 25 burst interval 2`

Ici les interface G0/1 et G0/2 ont été configurés pour avoir un taux de limite de 25 paquet, le burst interval a été changé pour passer de 1 à 2 par secondes. La configuration du Burst Interval est optionnel si elle n'est pas configuré, par défaut ce sera 1 par seconde.

On configure ensuite l'interface G0/3 avec les commandes :

```
SW1(config-if-range)#interface range g0/3
SW1(config-if)#ip arp inspection limit rate 10
```

Ici le Burst interval n'est pas configuré.
On peut ensuite afficher la configuration :

```
SW1(config-if)#do show ip arp inspection interfaces

 Interface        Trust State     Rate (pps)     Burst Interval
 --------------   -----------     ----------     --------------
 Gi0/0            Trusted              None               N/A
 Gi0/1            Untrusted              25                 2
 Gi0/2            Untrusted              25                 2
 Gi0/3            Untrusted              10                 1
![output omitted]
```

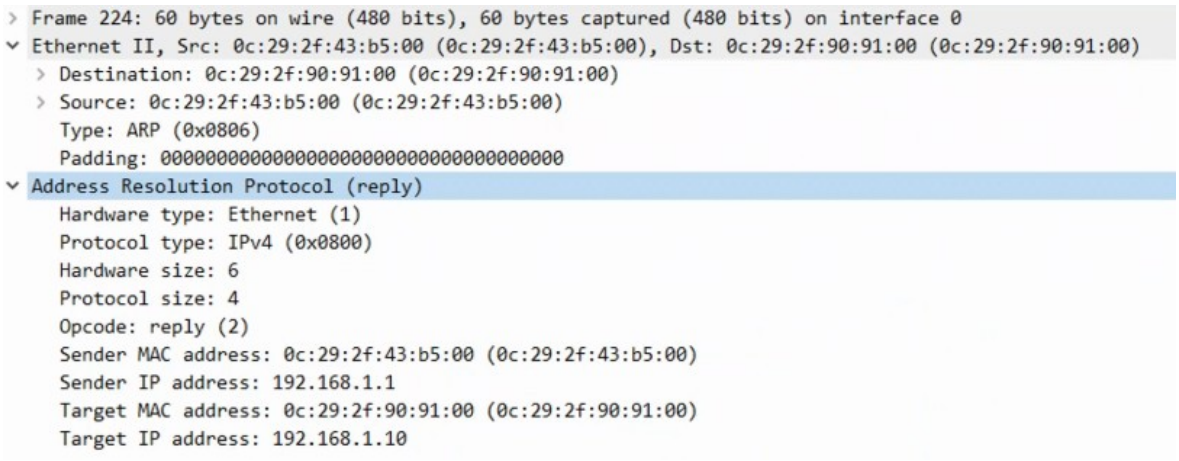
Si les messages ARP sont reçus plus vite que le taux spécifié, l'interface passera en err-disabled. Pour la réactiver il faudra soit :
- éteindre (`shutdown`) et ralumer l'interface (`no shutdown`)
- utiliser `errdisable recovery cause arp-inspection`

Par défaut DAI vérifie l'adresse MAC de l'envoyeur et son adresse IP, il est cependant possible de modifier cela avec la commande :
`SW1(config)#ip arp inspection validate src-mac`

```
SW1(config)#ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
```

Voici la définition donnée par Cisco pour les options de la commande :
dst-mac :Compare l'adresse MAC de destination dans l'en-tête Ethernet avec l'adresse MAC cible dans le corps ARP. Cette vérification est effectuée pour les réponses ARP. Lorsqu'ils sont activés, les paquets avec différentes adresses MAC sont classés comme non valides et sont supprimés.
Ip : Compare le corps ARP pour les adresses IP non valides et inattendues. Les adresses comprennent 0.0.0.0, 255.255.255.255, et toutes les adresses de multidiffusion IP. Les adresses IP de l'expéditeur sont comparées dans toutes les demandes et réponses ARP. Les adresses IP cibles sont comparées uniquement dans les réponses ARP.
Src-mac : Compare l'adresse MAC source dans l'en-tête Ethernet avec l'adresse MAC de l'expéditeur dans le corps ARP. Cette vérification est effectuée sur les demandes et les réponses ARP. Lorsqu'ils sont activés, les paquets avec différentes adresses MAC sont classés comme non valides et sont supprimés.

Voici un message Wireshark qui contient une réponse ARP :



Ici on peut voir que l'adresse de destination correspond à celle contenu dans la réponse ARP donc le message est accepté.
Ces vérifiations sont faites en plus de la vérification standard DAI.
Si configuré les messages ARP devront tous passer les vérifications pour être validés.

DAI peut aussi être configuré pour faire d'autres vérifications :
Ici on lance les trois commandes suivante :

```
SW1(config)#ip arp inspection validate dst-mac
SW1(config)#ip arp inspection validate ip
SW1(config)#ip arp inspection validate src-mac
```

On vérifie ensuite laquelle est retenue dans la configuration, on peut voir que seulement la dernière commande est correctement enregistré.

```
SW1(config)#do show running-config | include validate
ip arp inspection validate src-mac
```

Par contre si l'on lance la configuration pour inspecter les 3 en une commande, cette fois les trois paramètres sont enregistrés :

```
SW1(config)#ip arp inspection validate ip src-mac dst-mac

SW1(config)#do show running-config | include validate
ip arp inspection validate src-mac dst-mac ip
```

Il faut donc lancer la vérification de validation en une seule commande.

Voyons rapidement le fonctionnement de ARP ACLs :
On affiche d'abord la table DHCP snooping binding du SW2

```
SW2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
0C:29:2F:18:79:00   192.168.1.12     79226       dhcp-snooping   1     GigabitEthernet0/1
0C:29:2F:90:91:00   192.168.1.10     79188       dhcp-snooping   1     GigabitEthernet0/1
0C:29:2F:67:E9:00   192.168.1.11     79210       dhcp-snooping   1     GigabitEthernet0/1
Total number of bindings: 3
```

Le SRV1 a une adresse IP statique, lorsqu'il essaie d'envoyer une requête ARP, le message sera bloqué avec le message d'erreur suivant :

```
!SRV1 has a static IP address of 192.168.1.100, so it does not have an entry in SW2's DHCP
!snooping binding table.

*Jun 19 05:56:15.538: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi0/2, vlan 1.
([0c29.2f1e.7700/192.168.1.100/0000.0000.0000/192.168.1.1/05:56:14 UTC Sat Jun 19 2021])
```

Cela est dû au fais que le SRV1 n'est pas enregistré dans la table DHCP snooping Binding.
Pour configurer l'interface on lance les commandes suivante :

```
SW2(config)#arp access-list ARP-ACL-1
SW2(config-arp-nacl)#permit ip host 192.168.1.100 mac host 0c29.2f1e.7700

SW2(config)#ip arp inspection filter ARP-ACL-1 vlan 1
```

```
SW2(config)#arp access-list ARP-ACL-1
SW2(config-arp-nacl)#permit ip host 192.168.1.100 mac host 0c29.2f1e.7700
SW2(config)#ip arp inspection filter ARP-ACL-1 vlan 1
```

Ici une ACL appelé ARP-ACL-1 été crée avec la première commande, puis l'hôte avec l'adresse IP et l'adresse MAC spécifié ont été autorisés. On applique ensuite la configuration en lançant la commande arp inspection.
Cela permet à ce que le SRV1 puisse à présent envoyer une requête ARP et que le SW1 le retransmette bien qu'il n'y ait pas d'entrée dans la table DHCP snooping binding.

Une commande utile pour afficher la configuration arp inspection est :

```
SW2#show ip arp inspection
```

```
SW2#show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active      ARP-ACL-1          No

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
    1     Deny             Deny              Off

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    1             56              4              4              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
    1              0              1              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
    1                   0                        0                      0
```

On peut voir que les validation source mac, dest mac et ip son activés, on voit aussi que DAI est activé sur la Vlan 1 et que l'ARP-ACL est fonctionnel. Le statique AC est configuré comme « no » si le static ACL est en « yes » le déni implicite à la fin de l'ARP-ACL prendra effet, cela cause que les messages ARP non permis par l'ARP ACL d'être bloqués. Cela signifie que seulement l'ARP-ACL peut être vérifié, la table DHCP snooping ne sera pas vérifié.