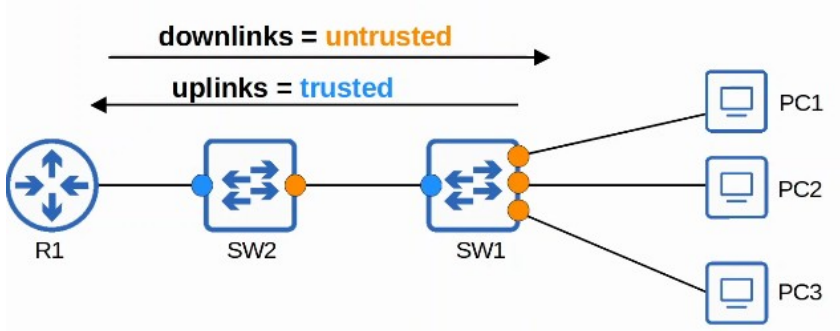
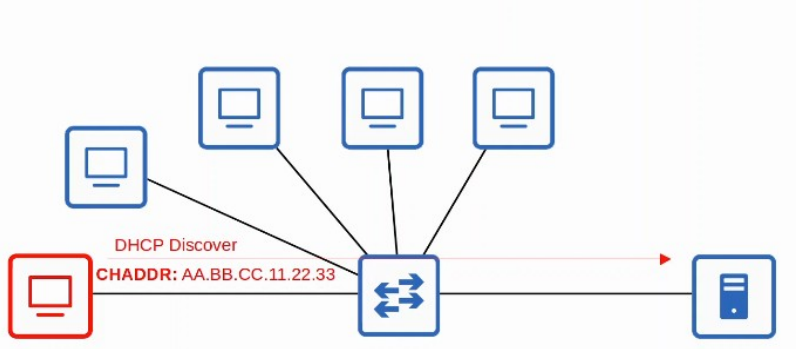
DHCP Snooping

Dans ce cours nous verrons ce qu'est DHCP Snooping qui est une fonctionnalité disponible sur les Switch Cisco qui aide à protéger des attaques qui prennent avantages du DHCP.

Nous ferons d'abord une introduction de ce qu'est le DHCP Snooping et comment il fonctionne, quelle attaque il permet de contrer et comment le configurer sur un Switch Cisco.
DHCP Snooping est une fonctionnalité de sécurité d'un switch qui est utilisé pour filtrer des messages DHCP sur des ports qui ne sont pas de confiance.
Le Snooping DHCP filtre uniquement des messages DHCP. Les messages qui ne sont pas DHCP ne sont pas affectés. Tous les ports ne sont pas de confiance par défaut, il faut ensuite configurer quelles ports faire confiance. Les ports « uplink » sont configurés comme port de confiance et les ports « downlink » ne sont pas de confiance. « downlink » fait référence aux ports d'une interface qui vont dans la direction de l'hôte. « uplink » fait référence aux ports ports qui partent à partir de l'hôte. Par exemple sur le réseau suivant, en bleu les ports uplink et en orange les ports downlink :

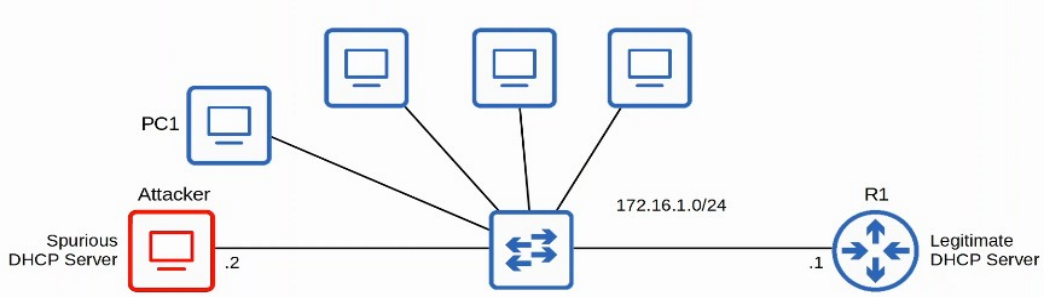


Par exemple dans le cas ou le PC1 envoie un message DHCP, le port étant de confiance est bien réceptionné sur le SW1, le SW2 réceptionne ensuite le message sans le vérifier car il est réceptionné par un port de confiance.
A présent si dans le cas ou le port du PC2 n'est pas de confiance, si le PC2 envoie un message DHCP celui ci ne sera pas repartagé par le Switch.
Un exemple d'une attaque par DHCP est appelé « DHCP starvation » ou aussi appelé « DHCP exhaustion » dans ces attaques un attaquant utilise une fausse adresse MAC pour inonder le Switch de messages DHCP discover. Le serveur DHCP pool ciblé devient rempli ce qui résulte en un denial of service sur d'autres appareils.
Comme dans l'exemple du réseau suivant :



Dans les messages DHCP envoyé il y a aussi une entête dans laquelle est contenu le CHADDR (Client Hardware Address) qui permet d'indiquer l'adresse MAC du client.
Cette entête est nécessaire dans le cas ou un message est envoyé vers une destination externe au réseau local, par exemple dans le cas ou le serveur DHCP est dans un réseau externe et que le message DHCP est partagé par un relais DHCP lorsque le serveur reçoit cette trame par le client, l'adresse MAC source de la trame ne sera pas l'adresse MAC du client.

Un autre type d'attaque possible avec DHCP est appelé le DHCP Poisoning (Man in the Middle)
De même type que le ARP poisoning, le DHCP poisoning peut être utilisé pour faire fonctionner une attaque Man in the Middle. Un serveur DHCP parasite répond aux messages clients DHCP Discover et leurs assigne une adresse IP mais fais que les clients utilisent le serveur DHCP parasite comme passerelle par défaut.
Les clients acceptent le premier message client qu'ils reçoivent.
Cela cause que le client envoie le trafique à l'attaquant au lieu de la passerelle par défaut.
L'attaquant peut ensuite examiner/modifier le trafique avant de le partager à la passerelle par défaut.



Dans le réseau précédent par exemple le PC1 envoie un message Discover au Switch qui envoie en Broadcast à tous les appareils du réseau local en incluant l'attaquant. Le serveur DHCP légitime envoie une DHCP OFFER et le serveur DHCP parasite envoie lui aussi un DHCP OFFER.
C'est le message DHCP OFFER du serveur parasite qui est réceptionné en premier par le PC1.
Le PC1 va donc envoyer une réponse DECLINE au routeur R1, le DHCP légitime.
Donc si le PC1 veut envoyer un message il passera par le serveur parasite qui est le PC de l'attaquant qui lui même repartagera le message au serveur DHCP légitime qui est le routeur R1.
Lorsque DHCP snooping filtre les messages il les différencie entre les messages du serveur DHCP et le message du client DHCP.
Les messages envoyés par le serveur DHCP sont :
- OFFER
- ACK
- NAK est l'opposé de ACK est est utilisé pour décliner les messages REQUEST des clients

Les messages DHCP envoyés par les clients sont :
- DISCOVER
- REQUEST
- RELEASE est utilisé pour dire au serveur que le client n'a plus besoin d'adresse IP
- DECLINE est utilisé pour décliner une offre d'adresse IP d'un serveur DHCP

Si un message est reçu sur un port qui est de confiance il sera repartagé sans inspection.
Si un message DHCP est reçu sur un port qui n'est pas de confiance il sera inspecté comme suit :
- Si c'est un serveur DHCP il sera bloqué
- Si c'est un message client DHCP il aura le fonctionnement suivant :
Les requêtes de messages DISCOVER/REQUEST vérifie si la trame de l'adresse MAC source et les messages DHCP CHADDR correspondent si c'est le cas le message est partagé si ça ne l'est pas le message n'est pas partagé.

Les messages RELEASE/DECLINE est vérifié si l'adresse IP du paquet source et de l'interface de réception correspondent avec l'entrée de la table DHCP Snooping. Si elles correspondent le paquet est repartagé si elles ne correspondent pas le paquet est bloqué.
Lorsque le client prend une adresse IP d'un serveur cela crée une nouvelle entrée dans la table DHCP snooping.

Voyons à présent comment faire la configuration basique de DHCP snooping, pour cela on utilise les commandes suivantes :
On commence par configurer le SW2 avec les commandes :

```
SW2(config)#ip dhcp snooping
SW2(config)#ip dhcp snooping vlan 1
SW2(config)#no ip dhcp snooping information option
SW2(config)#interface g0/0
SW2(config-if)#ip dhcp snooping trust
```

On configure ensuite le SW1 avec les commandes suivante :

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 1
SW1(config)#no ip dhcp snooping information option
SW1(config)#interface g0/0
SW1(config-if)#ip dhcp snooping trust

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
```

Une autre fonctionnalité de DHCP Snooping est le Rate-Limiting
Le DHCP Snooping peut limité le taux auquel les messages DHCP sont permis pour entrer une interface. Si le taux de messages DHCP croise la limite configuré l'interface est err-disabled.
Tout comme port security l'interface est manuellement réactivé ou automatiquement réactivé avec errdisable recovery.

Voici comment configurer errdisable recovery :

```
SW1(config)#interface range g0/1 - 3
SW1(config-if-range)#ip dhcp snooping limit rate 1

*Jun  5 13:15:14.180: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 1 DHCP packets on
interface Gi0/1
*Jun  5 13:15:14.181: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Gi0/1 is receiving more
than the threshold set
*Jun  5 13:15:14.182: %PM-4-ERR_DISABLE: dhcp-rate-limit error detected on Gi0/1, putting Gi0/1 in err-disable
state
*Jun  5 13:15:15.185: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
*Jun  5 13:15:16.190: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
```

Voici comment réactiver err-disable recovery :

```
SW1(config)#errdisable recovery cause dhcp-rate-limit
```

On vérifie ensuite la configuration errdisable avec la commande :

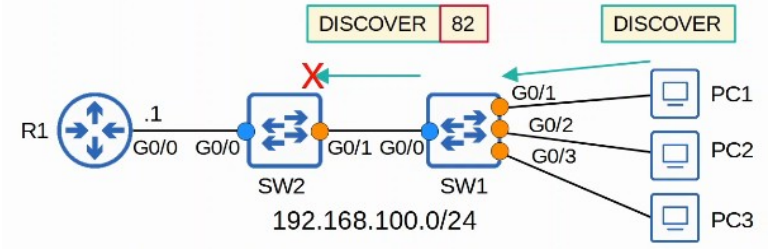
```
SW1#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Enabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
![output omitted due to length]


Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Interface       Errdisable reason       Time left(sec)
---------       -----------------       --------------
Gi0/1            dhcp-rate-limit          293
```

La limite de taux peut être très utile pour protéger contre des attaques DHCP exhaustion.
L'option 82 aussi connu comme DHCP agent de relaie option d'information ou en Anglais « DHCP relay agent information option » est l'une des nombreuses options DHCP.
L'option 82 fournit des informations additionnels à propos des agent de relais DHCP qui reçoivent les messages clients sur quelle interface, quelle VLAN, etc...
L'agent de relais DHCP peut ajouter l'option 82 aux messages qu'ils repartagent vers le serveur DHCP.
Avec le DHCP snooping activé, par défaut les switchs Cisco ajoutent l'option 82 aux messages DHCP qu'ils reçoivent du client, même si le switch ne fonctionne pas comme agent relais DHCP.
Par défaut les switchs Cisco bloquent les messages DHCP avec l'option 82 qui sont reçu sur un port qui n'est pas de confiance.
Par exemple si un message contenant l'option 82 est envoyé par l'agent relais celui ci sera bloqué par le Switch si celui ci n'est pas de confiance :



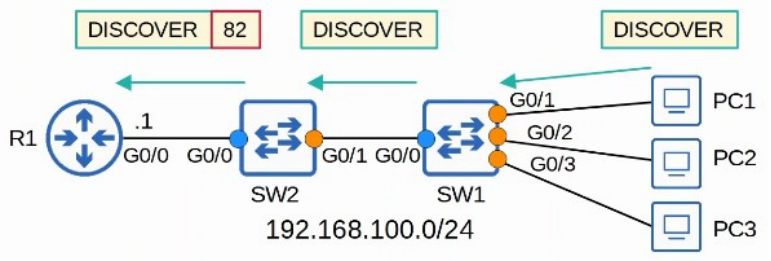
On peut voir ici que le message est bloqué par le Switch

```
SW2#
*Jun  6 01:36:15.298: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message with non-
zero giaddr or option82 value on untrusted port, message type: DHCPDISCOVER, MAC sa: 0c29.2f67.e900
```

C'est pour cela qu'il peut être utilisé la commande suivante :

```
SW1(config)#no ip dhcp snooping information option
```

Ici la commande est lancé sur le Switch 1 ce qui cause que l'option 82 est supprimé, mais qu'ensuite l'option 82 est ajouté par le Switch 2 :



Le Routeur R1 va lui bloquer le message car l'option 82 y est présente dans l'entête.

```
R1#
*Jun  6 01:46:46.763: DHCPD: inconsistent relay information.
*Jun  6 01:46:46.763: DHCPD: relay information option exists, but giaddr is zero
```

On ajoute donc la commande sur le Switch 2 :

```
SW2(config)#no ip dhcp snooping information option
```

Cette fois le Switch va repartager les messages DHCP Discover et répond normalement :