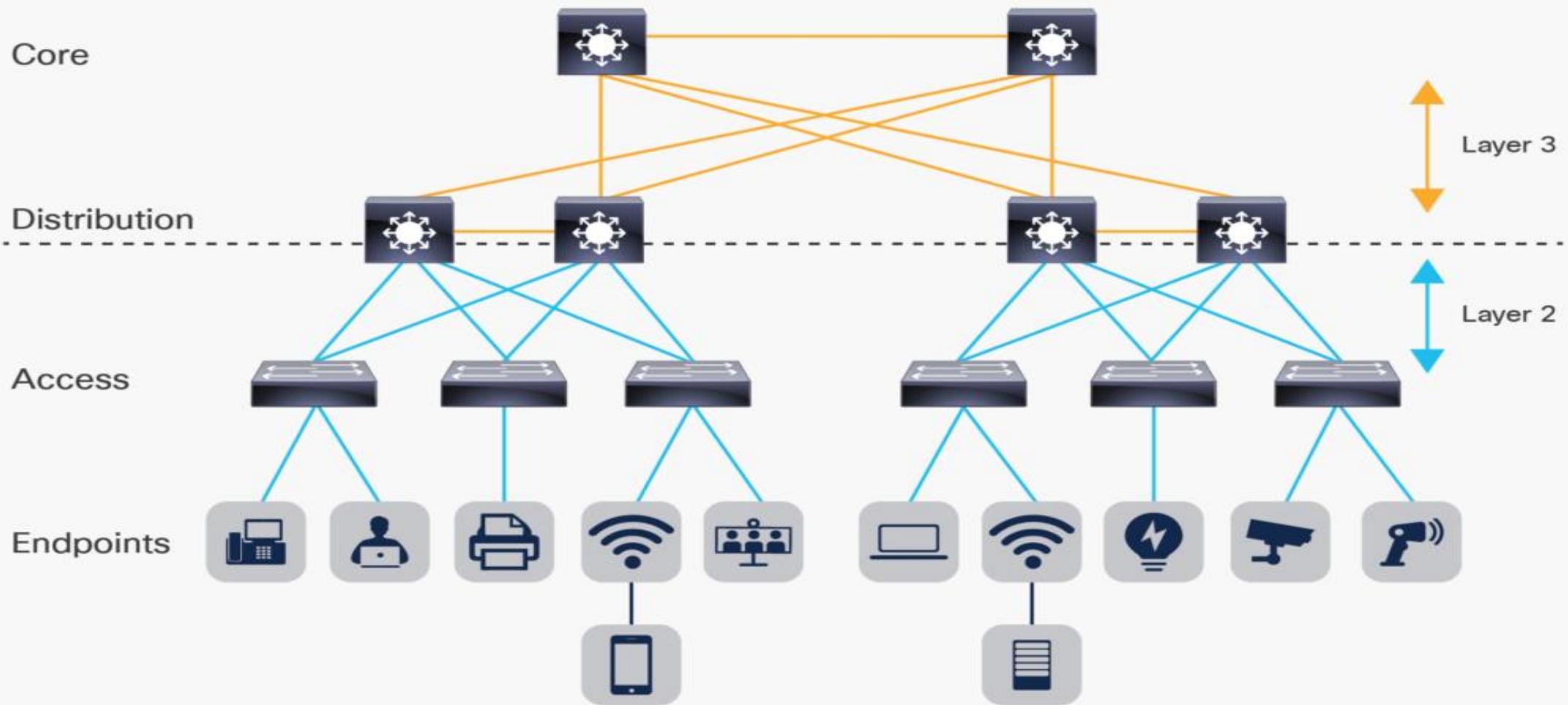


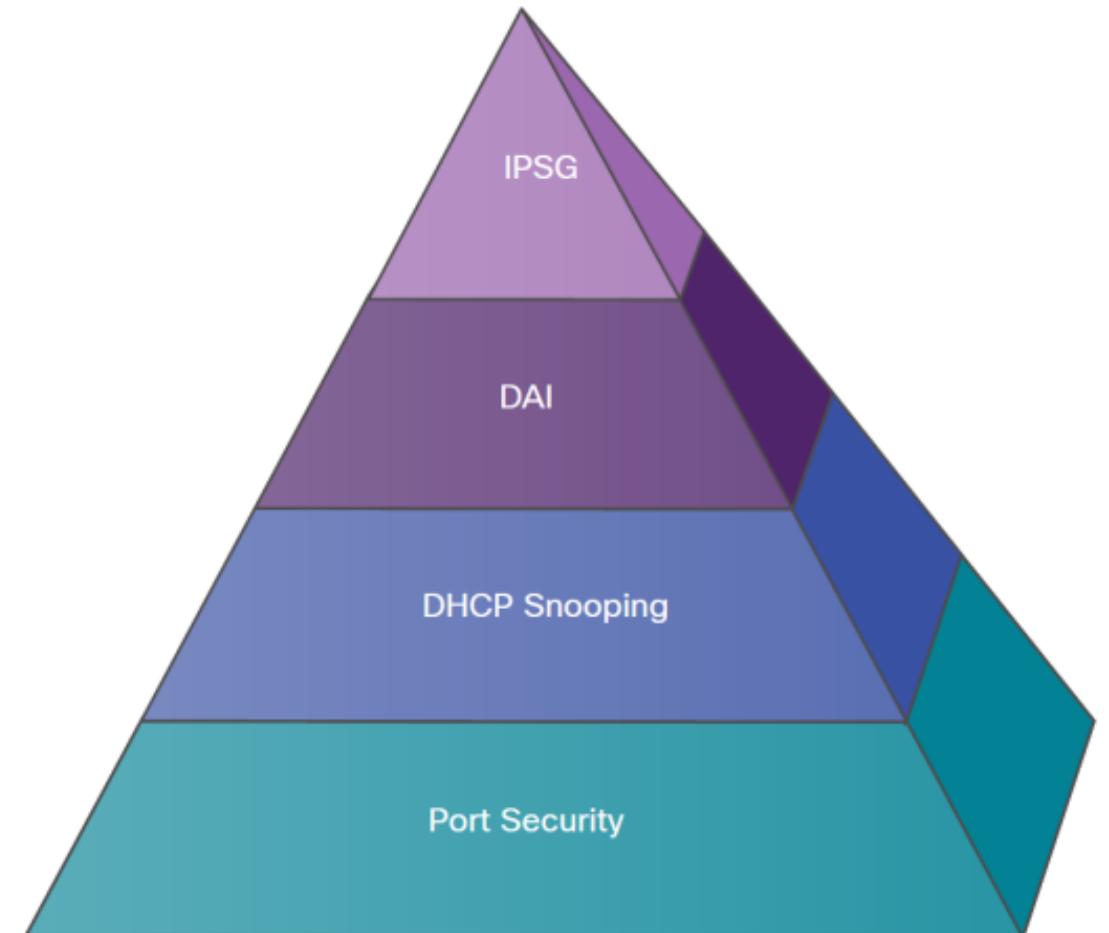
Sécurité de la couche 2 Les attaques

Introduction



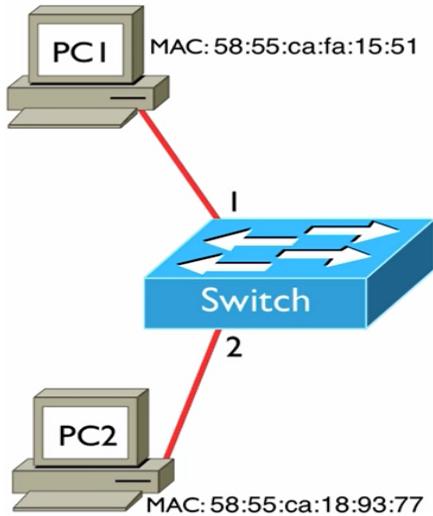
PLAN / Attaques et Contre-mesures

- Attaques MAC**
- Attaques DHCP**
- Attaques ARP**
- Attaques Généraux**



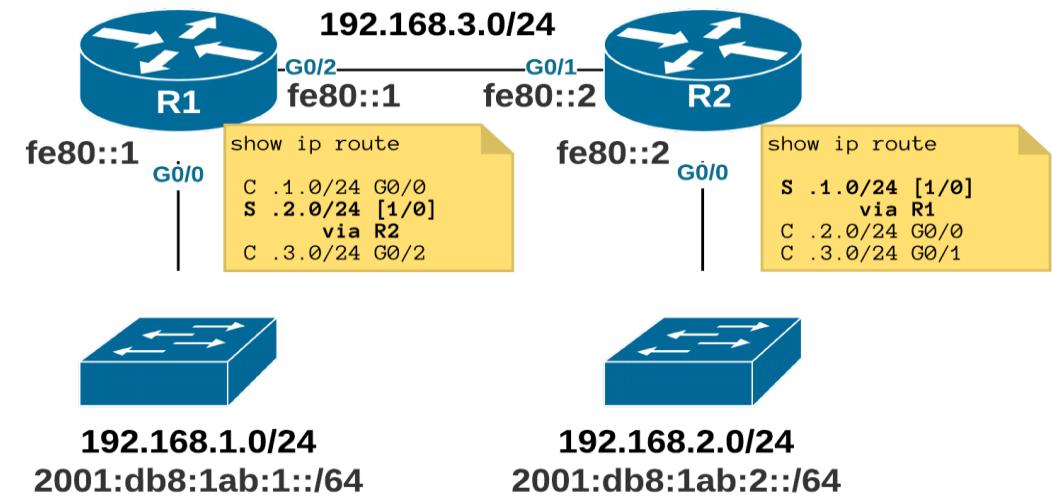
La table CAM (Content-Addressable-Memory)

La Table CAM est la référence de base pour un switch en termes de communication de trames.



Content Addressable Memory (CAM) Table	
Port	MAC Address
1	58:55:ca:fa:15:51
2	58:55:ca:18:93:77

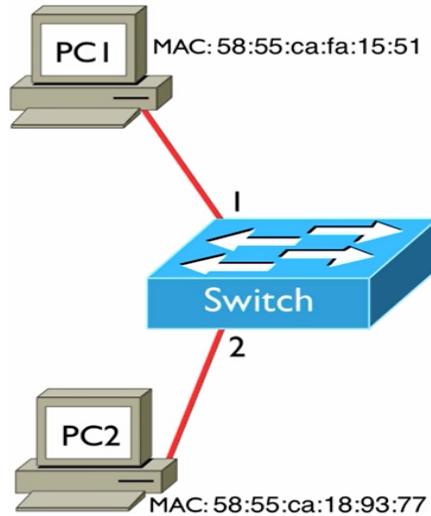
Communication d'une trame :
Switch (Niveau 2)
Table Cam via @MAC



Routage d'un paquet :
Routeur (Niveau 3)
Table de routage via @IP

La table CAM (Content-Addressable-Memory)

Il ne faut pas confondre !



Content Addressable Memory (CAM) Table	
Port	MAC Address
I	58:55:ca:fa:15:51
2	58:55:ca:18:93:77

Table CAM :
Relation entre une @IP et une
@MAC

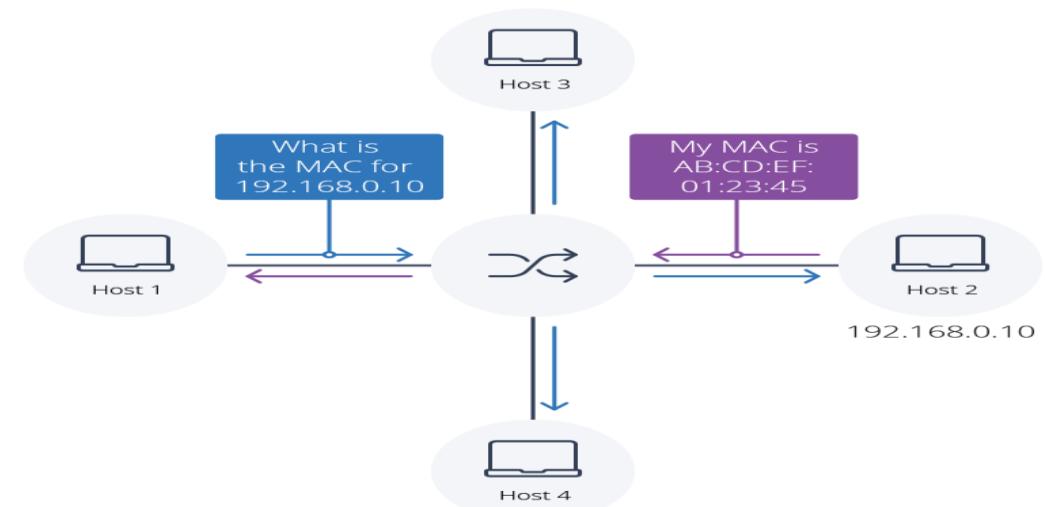
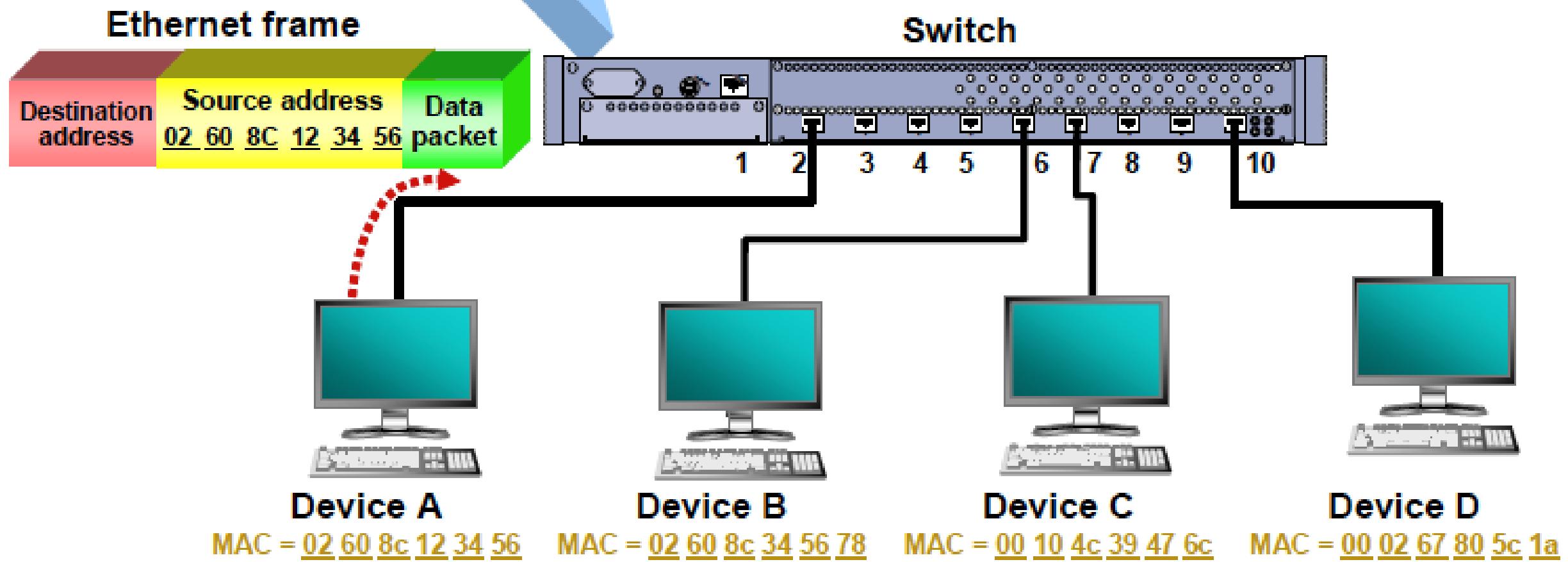


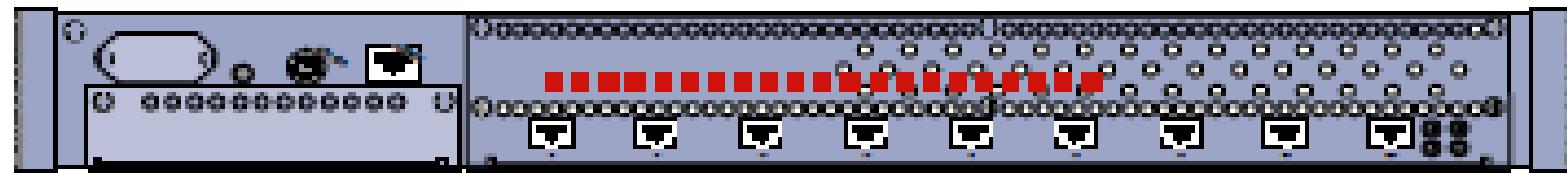
Table ARP :
Relation entre une @MAC et une @IP

Switch lookup table

02 60 8c 12 34 56 Port 2



Switch



1 2 3 4 5 6 7 8 9 10

Ethernet frame



Ethernet frame

Destination address
00 10 4c 39 47 6c

Source address
02 60 8c 12 34 56

Data packet

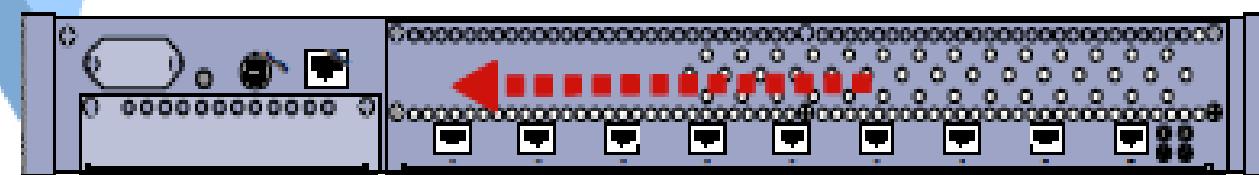
Switch lookup table

00	10	4c	39	47	6c	Port 7
02	60	8c	12	34	56	Port 2

Ethernet frame



Switch



1 2 3 4 5 6 7 8 9 10

Ethernet frame

Ethernet frame



Device A

MAC = 02 60 8c 12 34 56



Device B

MAC = 02 60 8c 34 56 78



Device C

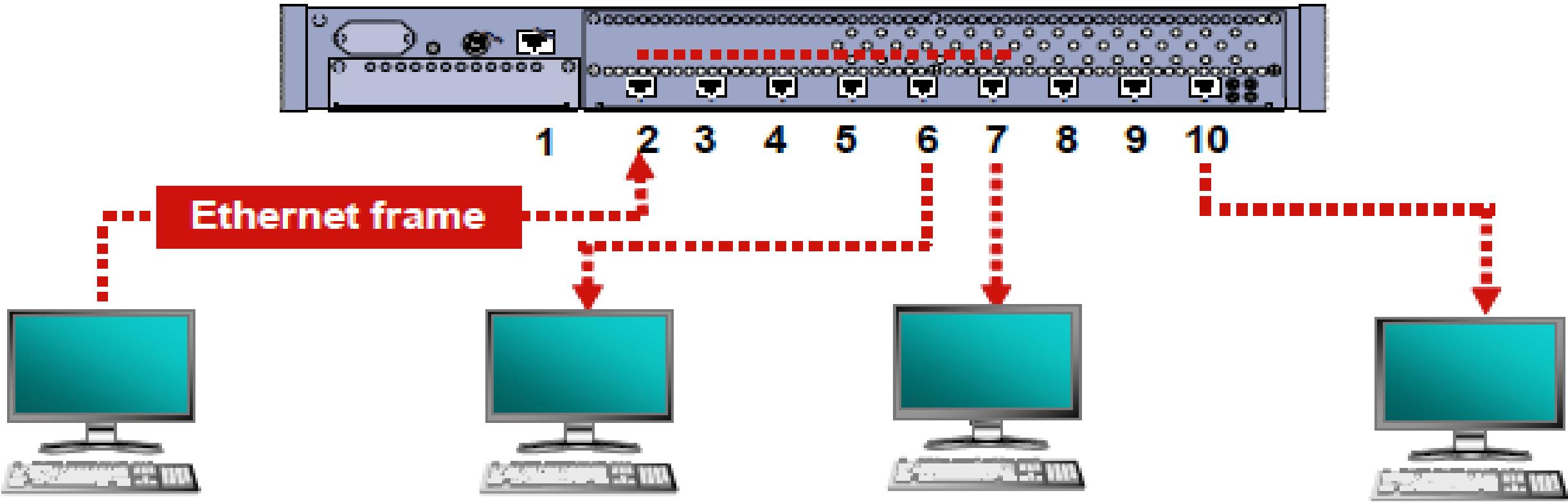
MAC = 00 10 4c 39 47 6c



Device D

MAC = 00 02 67 80 5c 1a

Switch



Ethernet frame



La table CAM (Content-Addressable-Memory)

- ✓ Il existe 3 façons de remplir la table CAM :

Dynamique

Statique

Port-security

// Visualiser la table CAM

Switch# show mac address-table

// Désactiver le remplissage dynamique de la table CAM de l'équipement

Switch(config)# mac address-table learning vlan

// Affecter une entrée statique dans la table CAM

(Solution à mettre en place avec prudence et uniquement lorsque vous n'avez pas d'autres choix !!)

Switch(config)# mac address-table static **xxxx**
vlan **10** interface **Fa0/1**

// Visualiser les adresses MAC saisies avec la méthode Port-security

Switch# show mac address-table secure

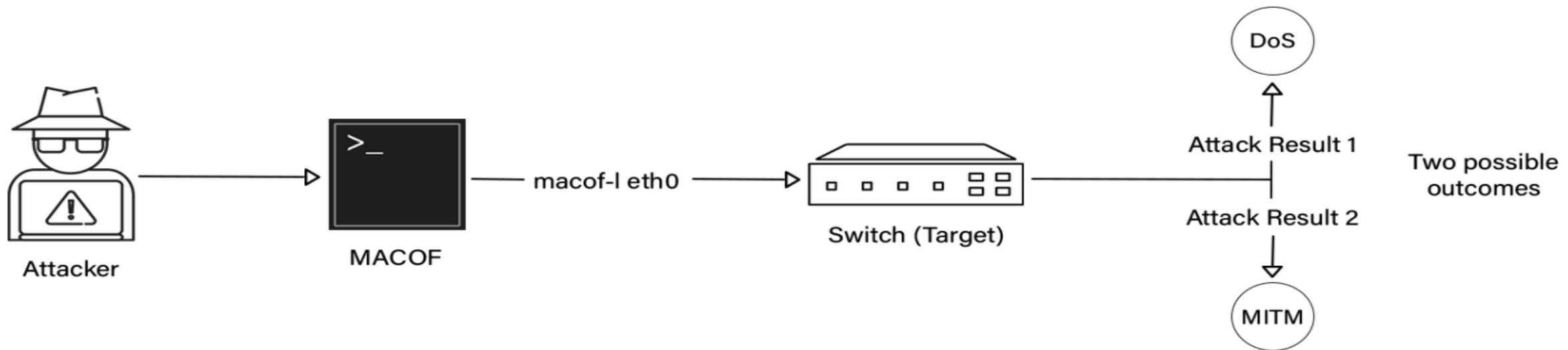
// Changer le temps d'expiration

Switch(config)# mac address-table aging-time **300**

Débordement de la table CAM (mémoire adressable par le contenu)

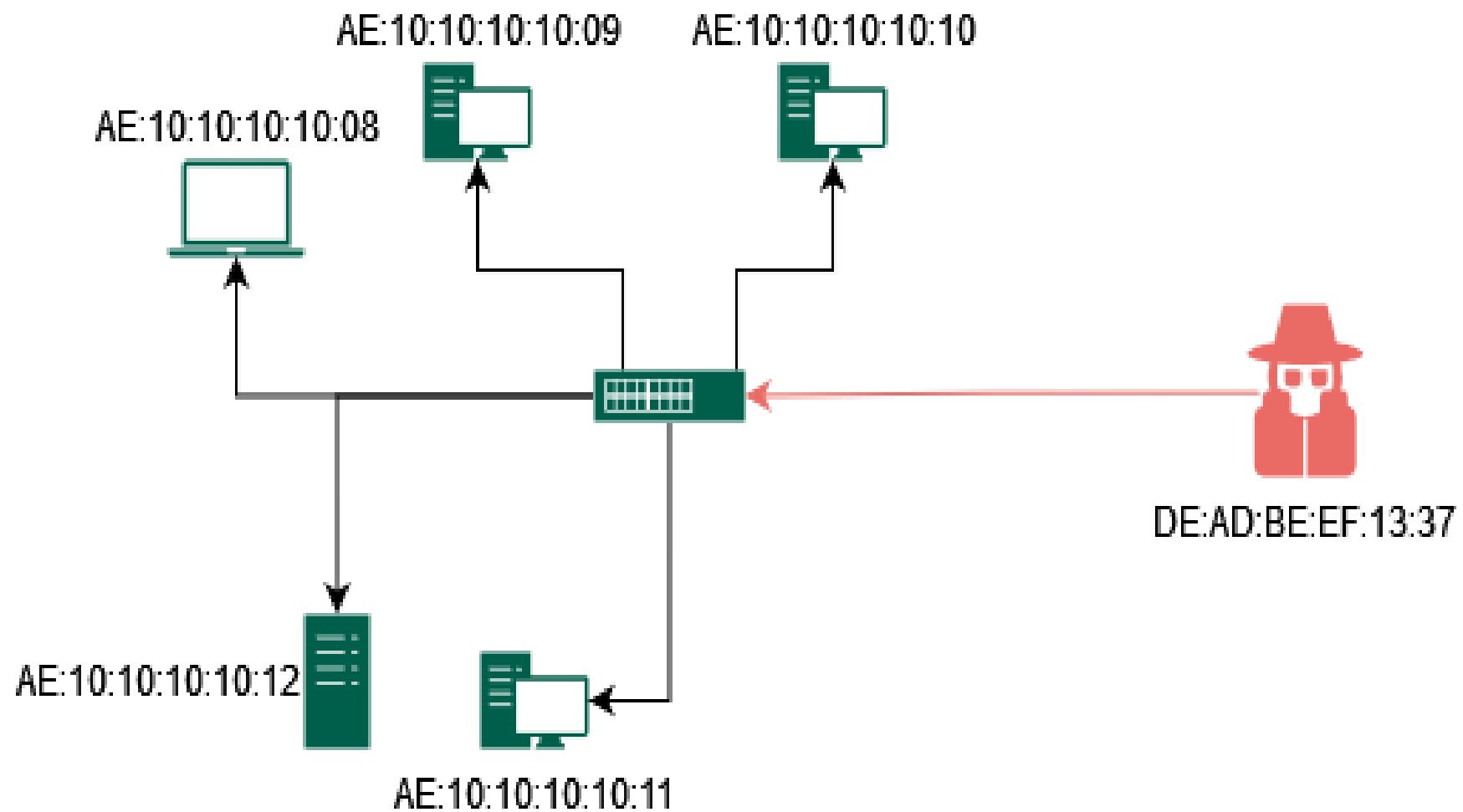
Débordement de la table CAM consiste à envoyer un grand nombre d'adresses MAC générées aléatoirement pour saturer la table CAM du commutateur.

Il faut noter que certains commutateurs n'ont pas de taille de table CAM fixe, ils sont cependant limités par leurs ressources physiques. Si la table est pleine, le switch va alors se transformer en hub.



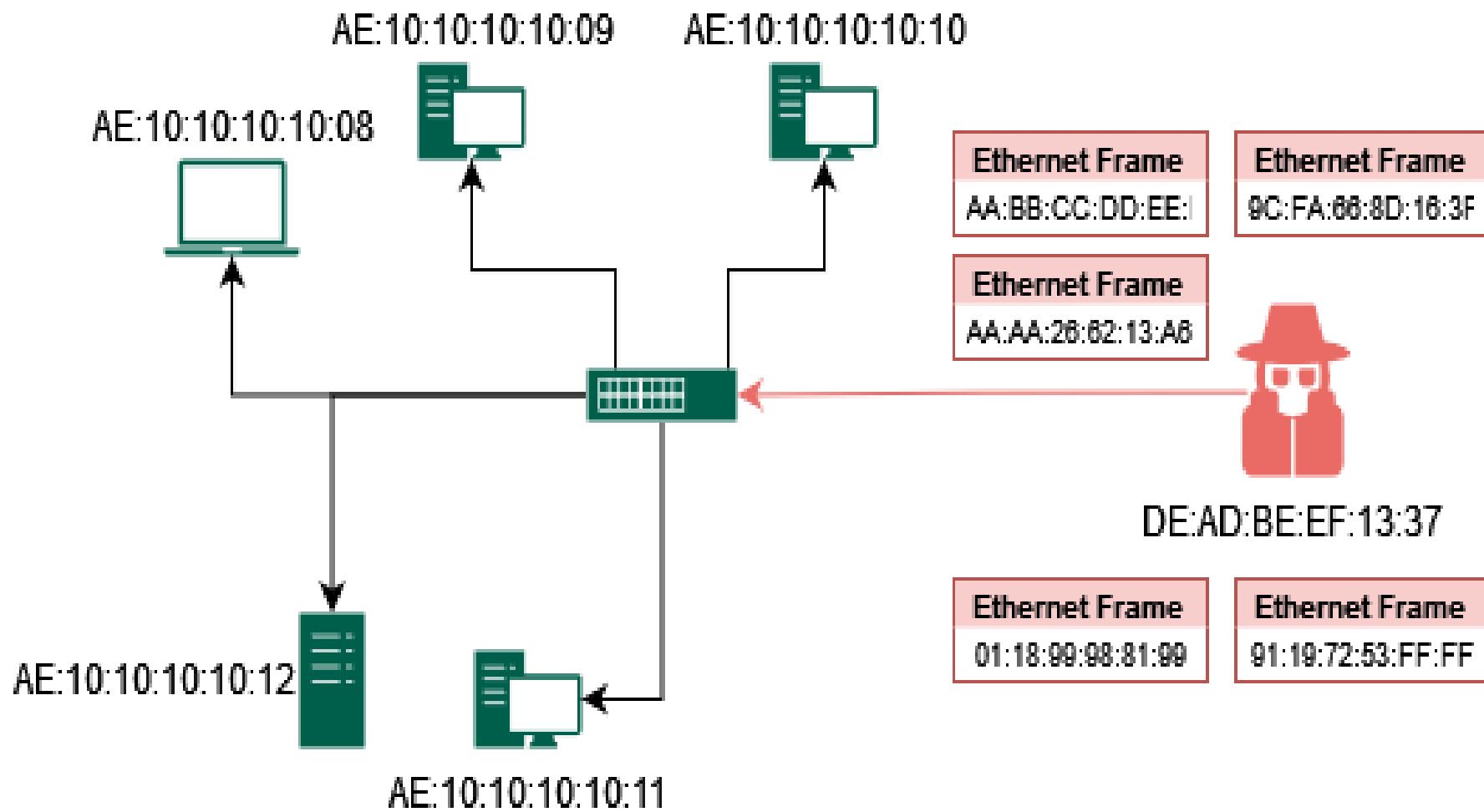
Macof is a tool used to flood the switch on a local network with MAC addresses.

Débordement de la table CAM (mémoire adressable par le contenu)



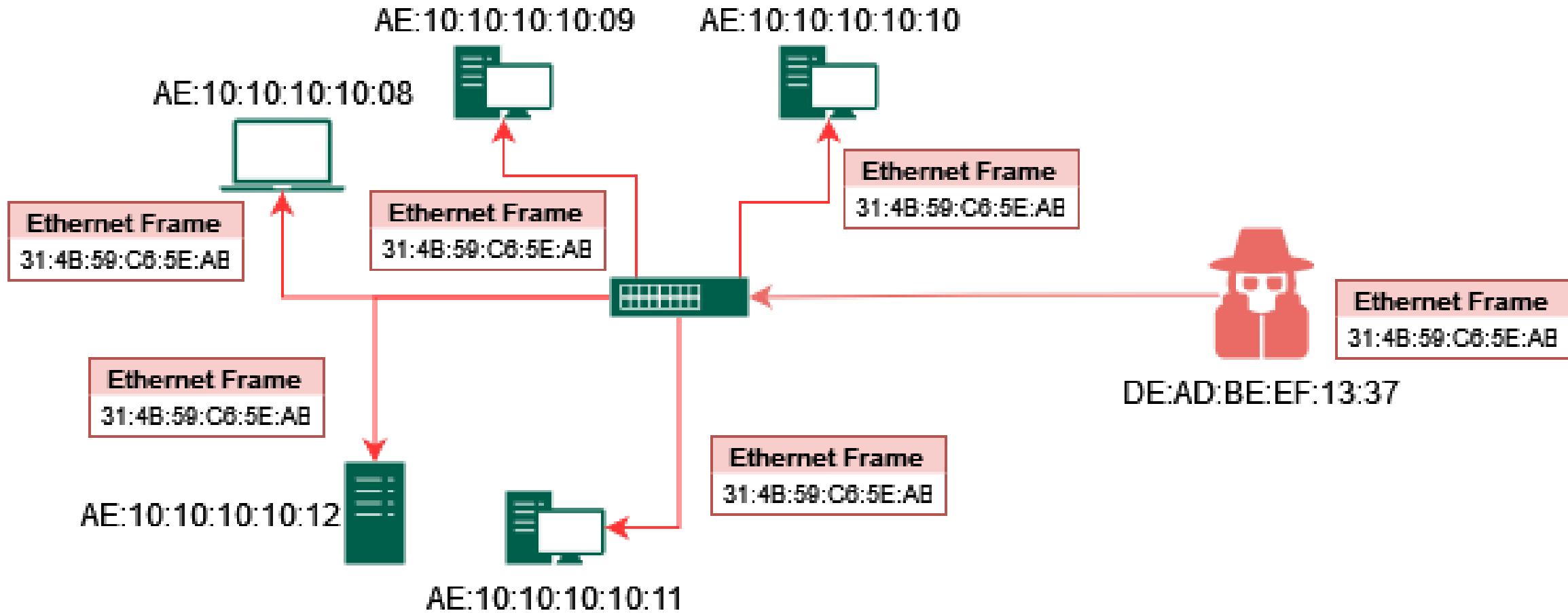
MAC Address Table	
	Capacity: 8
Port 1:	AE:10:10:10:08
Port 2:	AE:10:10:10:09
Port 3:	AE:10:10:10:10
Port 4:	AE:10:10:10:11
Port 5:	AE:10:10:10:12
-	-
-	-
-	-

Débordement de la table CAM (mémoire adressable par le contenu)



MAC Address Table	
Capacity: 8	
Port 1:	AE:10:10:10:08
Port 2:	AE:10:10:10:09
Port 3:	AE:10:10:10:10
Port 4:	AE:10:10:10:11
Port 5:	AE:10:10:10:12
Port 6:	AA:BB:CC:DD:EE:FF
Port 6:	01:18:99:98:81:99
Port 6:	91:19:72:53:FF:FF

Débordement de la table CAM (mémoire adressable par le contenu)



La sécurité sur les ports (Port-security)

La sécurité sur les ports permet de contrôler les adresses MAC autorisées sur un port. En cas de "*violation*", c'est-à-dire en cas d'adresses MAC non autorisées sur le port, une action est prise.

Le port doit être *Access* ou *Trunk* !!

Port-Security

Dynamique

Statique

Violation Mode

Protect

Restrict

Shutdown

La sécurité sur les ports (Port-security)

// Visualiser le nombre des @MAC affectées dans la table CAM

```
Switch# show mac address-table count vlan 10
```

```
Switch(config)# interface G0/1
```

```
Switch(config-if)# switchport mode access
```

// Activation de port-security

```
Switch(config-if)# switchport port-security
```

// Fixer une adresses MAC pour un port (statique)

```
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
```

// Définition du nombre maximal des adresses MAC autorisées (dynamique)

```
Switch(config-if)# switchport port-security maximum 10
```

// Préciser l'action prise en cas de non-respect d'une règle port-security

```
Switch(config-if)# switchport port-security violation {protect | restrict | shutdown}
```

// Afficher la configuration port-security d'un port

```
Switch# show port-security interface G0/1
```

// Afficher les adresse MAC passées par la sécurité des ports

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

// Afficher les details de violation d'un port

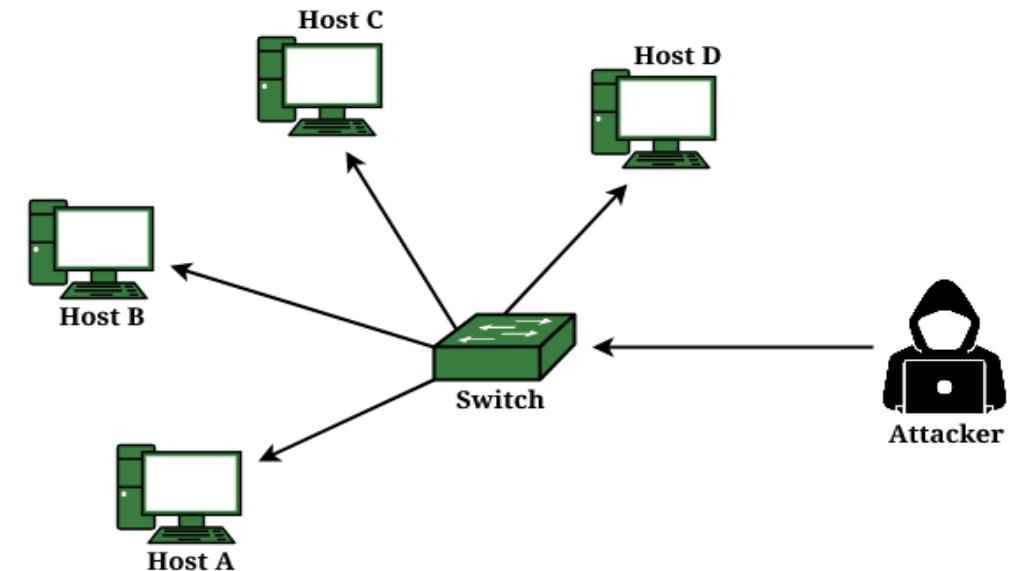
```
Switch# show interface G0/1 status err-disabled
```

Usurpation d'adresse MAC (MAC Spoofing)

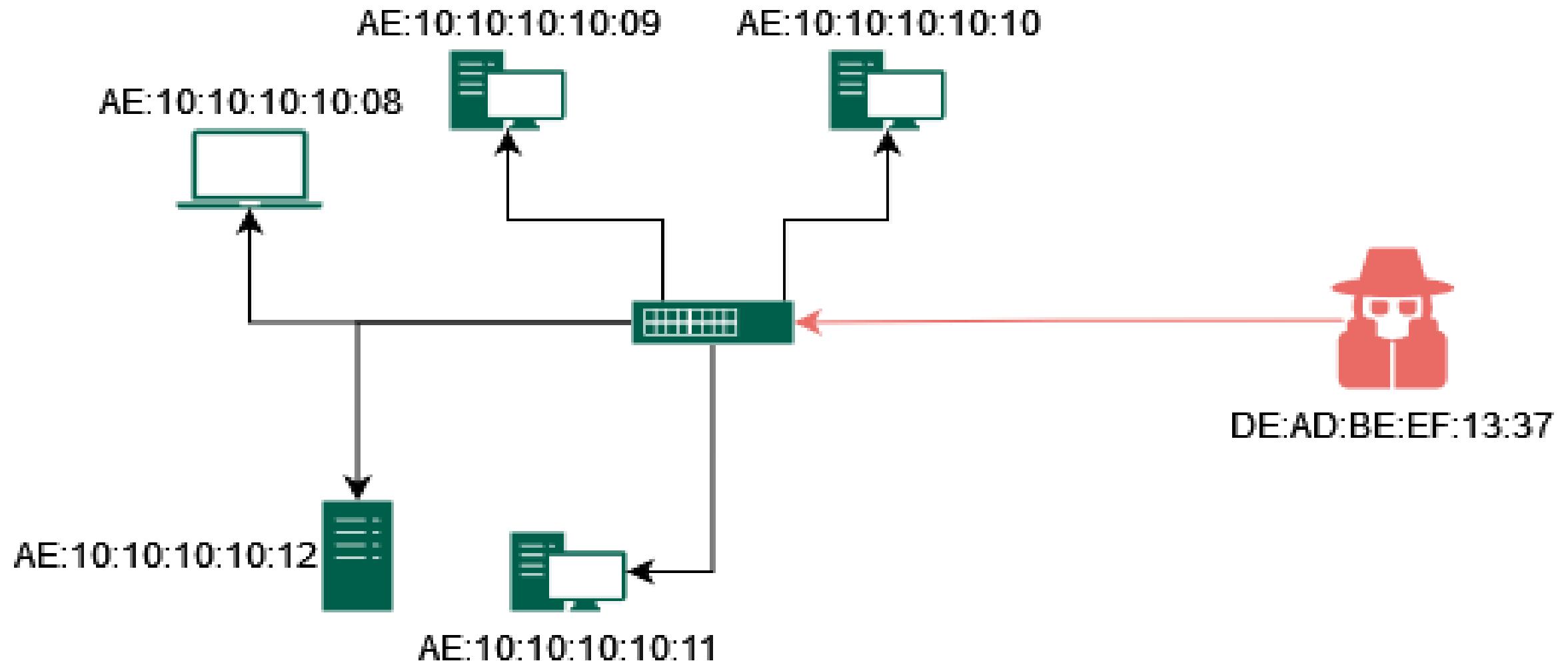
Une attaque d'usurpation d'adresse MAC se produit lorsqu'un pirate modifie l'adresse MAC de son appareil pour qu'elle corresponde à l'adresse MAC d'un autre sur un réseau. Il conduit au vol d'informations sensibles ou à la réalisation d'activités malveillantes.

Pourquoi l'usurpation d'adresse MAC ?

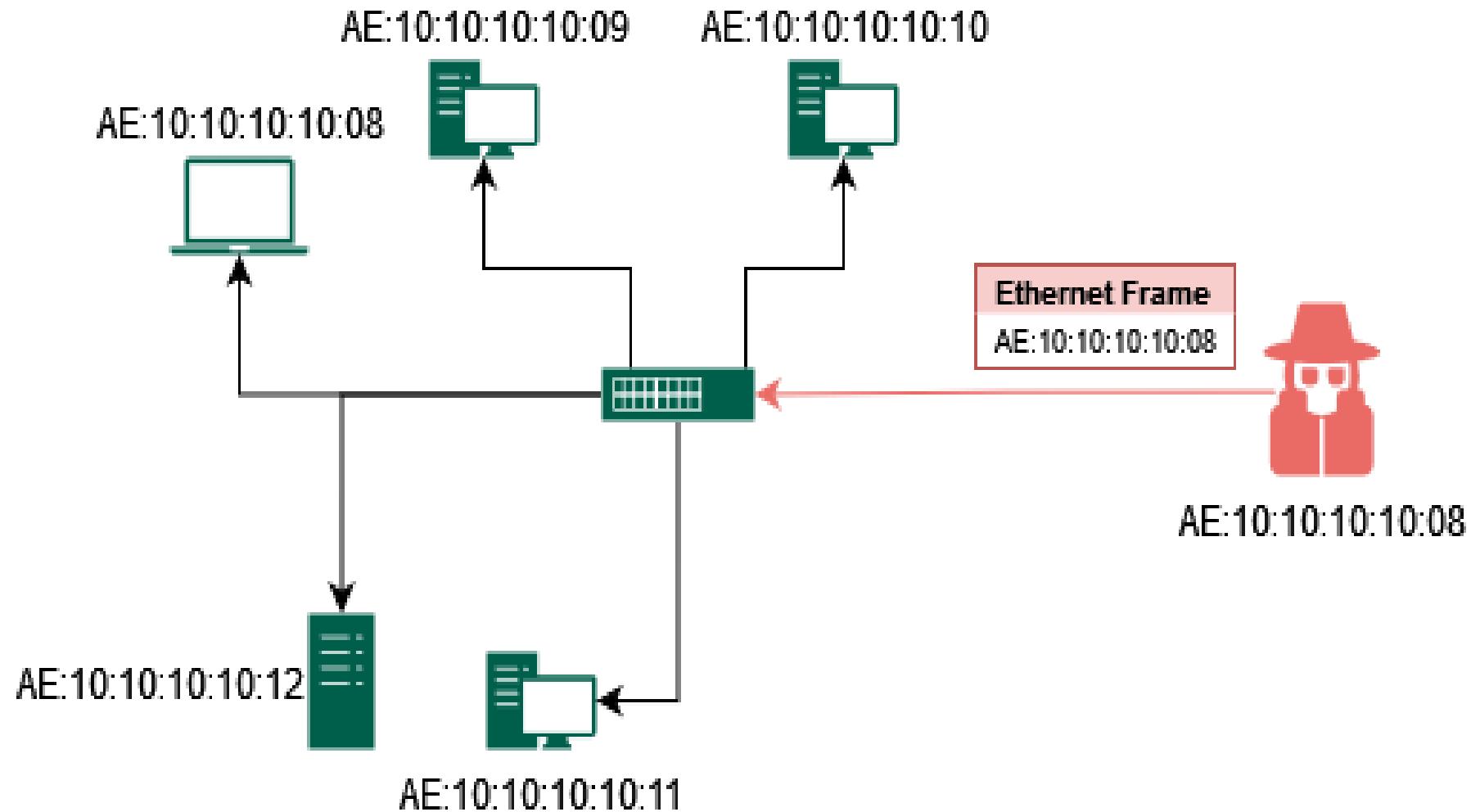
- Cacher son identité.
- Contourner les mesures de sécurité, par ex. les ACLs ou segmentation basée sur les adresses MAC.
- Obtenir un accès non autorisé au réseau.
- Lancer des attaques (MITM).



Usurpation d'adresse MAC (MAC Spoofing)

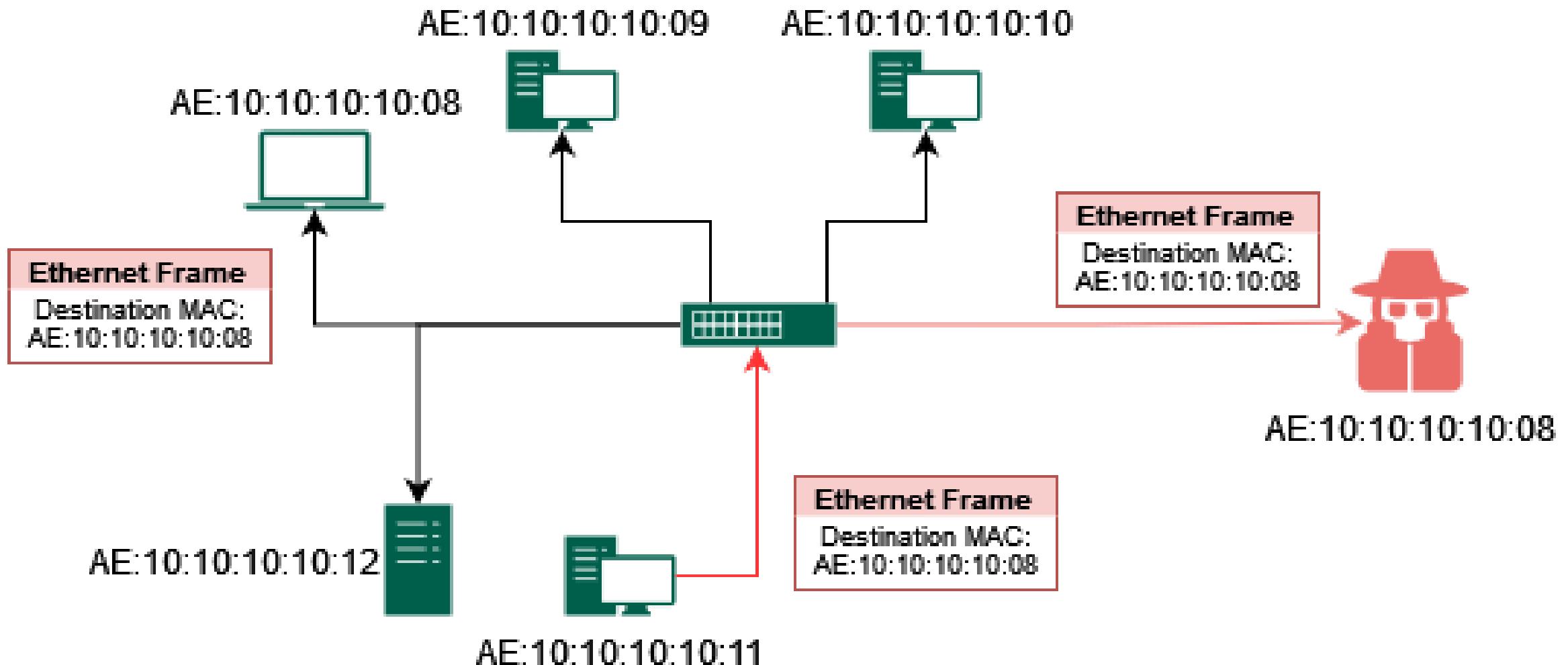


Usurpation d'adresse MAC (MAC Spoofing)



MAC Address Table Capacity: 8
Port 1: AE:10:10:10:08
Port 2: AE:10:10:10:09
Port 3: AE:10:10:10:10
Port 4: AE:10:10:10:11
Port 5: AE:10:10:10:12
Port 6: AE:10:10:10:08

Usurpation d'adresse MAC (MAC Spoofing)



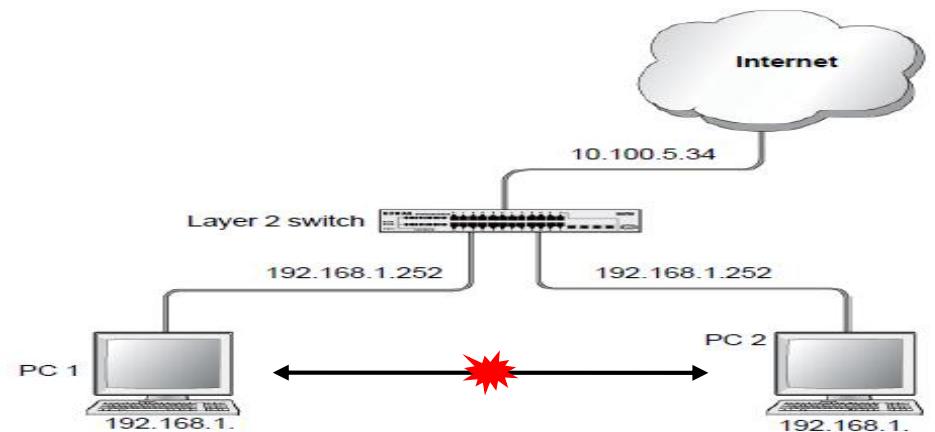
Les ports protégés (Protected Ports)

Un port protégé ne transfère aucun trafic (monodiffusion, multidiffusion ou diffusion) vers un autre port qui est également un port protégé. Le trafic de données ne peut pas être transféré entre les ports protégés de la couche 2.

Tout le trafic de données transitant entre les ports protégés doit être transféré via un périphérique de couche 3.

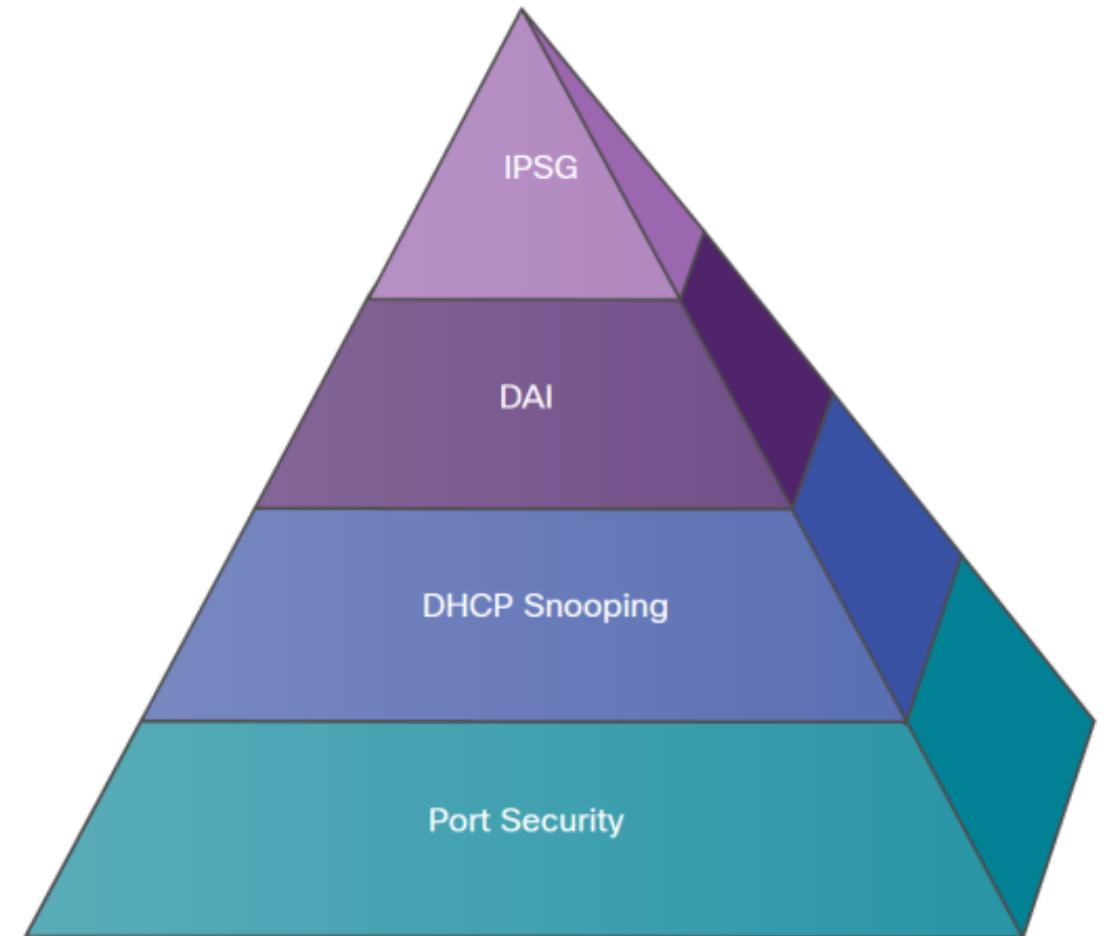
// Configurer l'interface pour être protégée

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport protected
Switch(config-if)# end
```



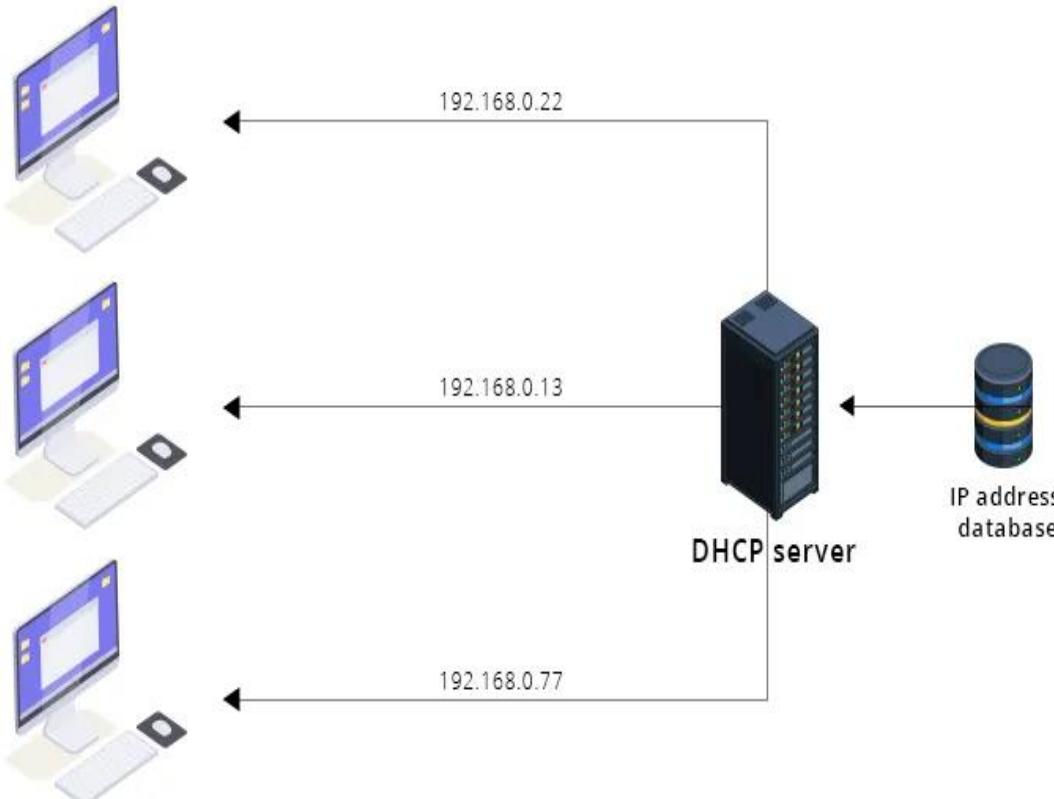
PLAN / Attaques et Contre-mesures

- Attaques MAC**
- Attaques DHCP**
- Attaques ARP**
- Attaques Généraux**

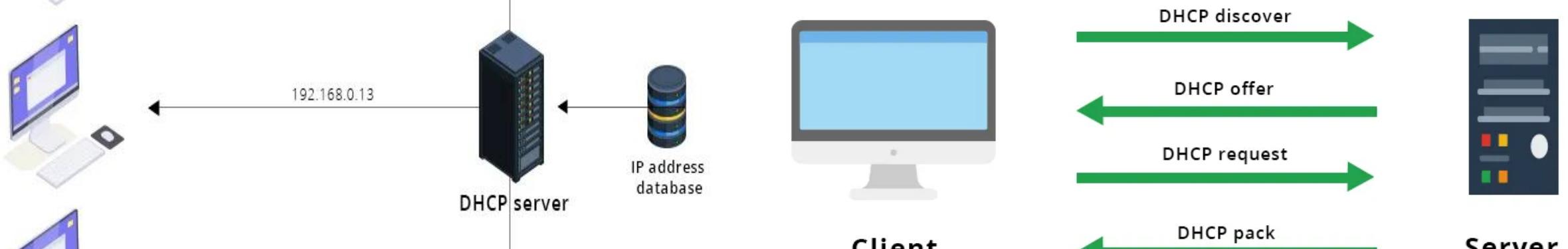


Le protocole DHCP (Dynamic Host Configuration Protocol)

Il automatise la tâche de configuration IP banale de l'administrateur réseau en automatisant efficacement les allocations IP et en minimisant le gaspillage IP et les conflits IP.



Les 4 étapes de DHCP :
Le processus DORA



Le protocole DHCP (Dynamic Host Configuration Protocol)

Le client DHCP demande le bail IP au premier serveur DHCP offrirons un bail IP !

Allocation serveur DHCP

Automatique

Dynamique

Manuel

Client DHCP

Adresse IP

Passerelle par-défaut

Serveur DNS

Le protocole DHCP (Dynamic Host Configuration Protocol)

// Exclure les adresses IP de l'attribution par DHCP à l'aide de l'adresse exclue `dhcp ip FIRST_IP LAST_IP`

```
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

// Créez un nouveau pool DHCP avec la commande `ip dhcp pool NAME`

```
Router(config)# ip dhcp pool Master_DCC
```

// Définissez un sous-réseau qui sera utilisé pour attribuer des adresses IP aux hôtes avec la commande réseau `SUBNET SUBNET_MASK`.

```
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
```

// Définissez la passerelle par défaut avec la commande IP du routeur par défaut

```
Router(dhcp-config)# default-router 192.168.1.1
```

// Définissez le serveur DNS avec la commande d'adresse IP du serveur DNS.

```
Router(dhcp-config)# dns-server 8.8.8.8
```

```
Router(dhcp-config)# exit
```

// Configurez le nombre de jours d'affectation d'adresse IP

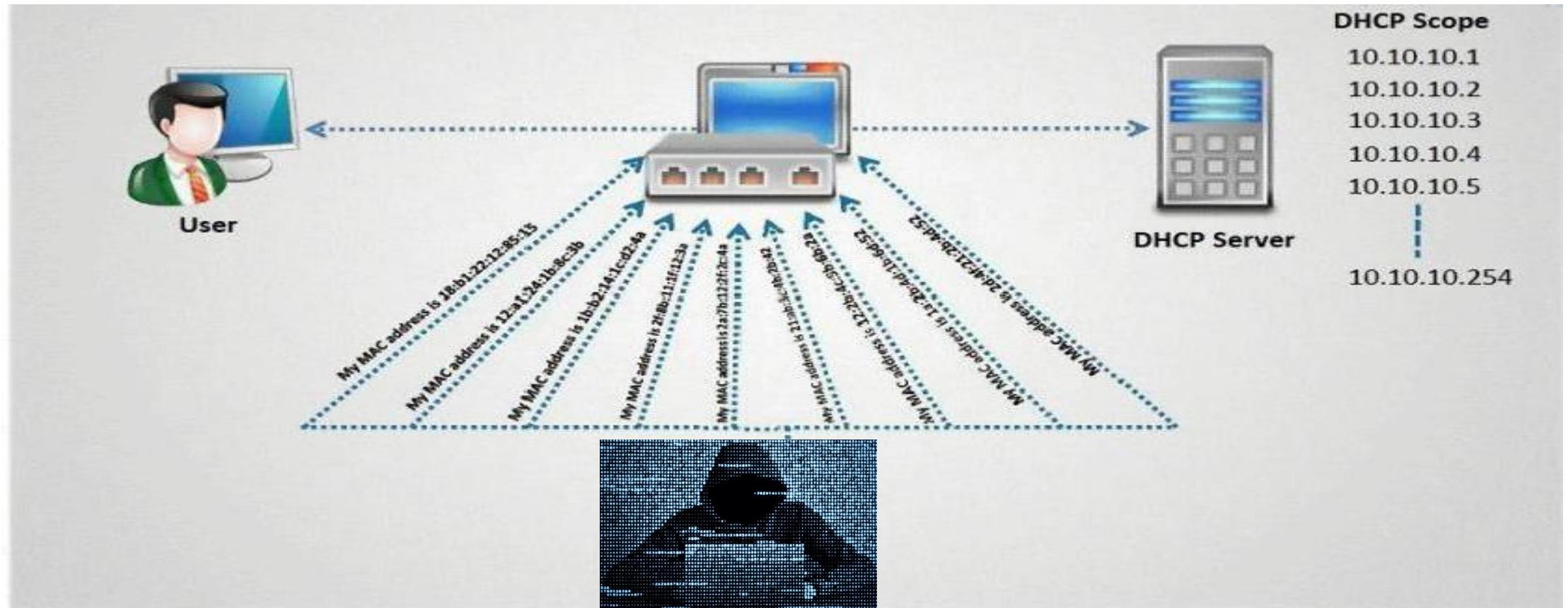
```
Router(config)# lease 7
```

// Afficher des informations sur les adresses actuellement louées, vous pouvez utiliser la commande de liaison `show ip dhcp`

```
Router#show ip dhcp binding
```

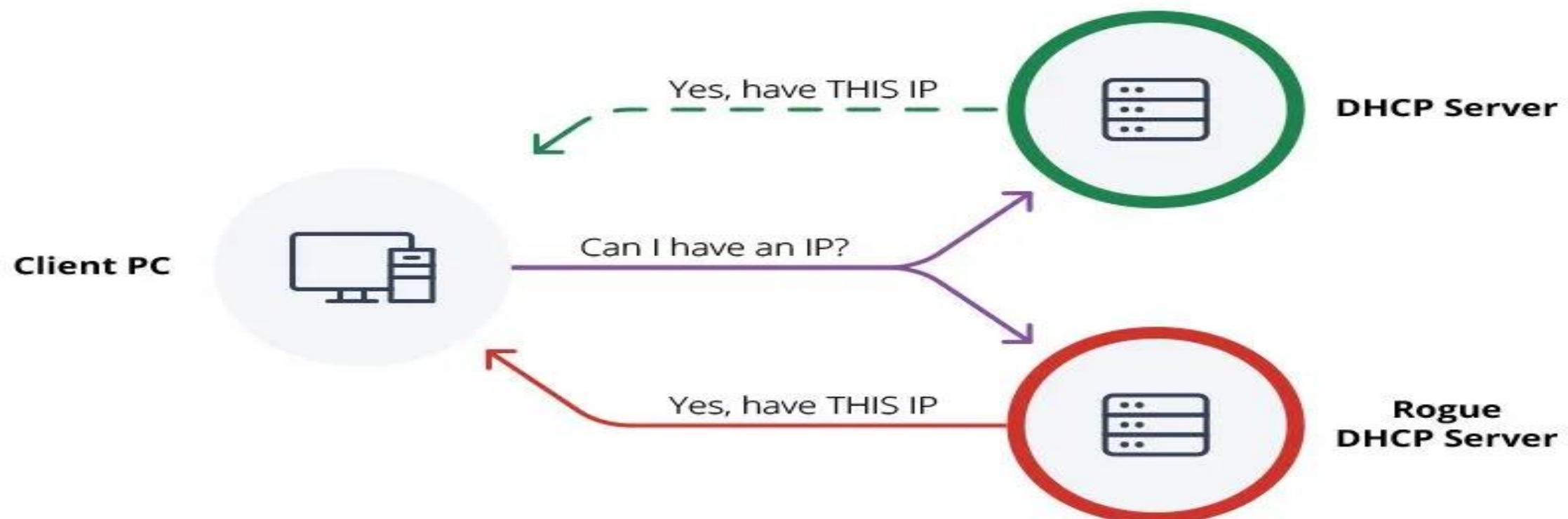
Attaque par épuisement de ressources (DHCP Starvation)

Les vrais clients ne pourront plus obtenir d'adresse IP : le trafic réseau sera *paralysé* !



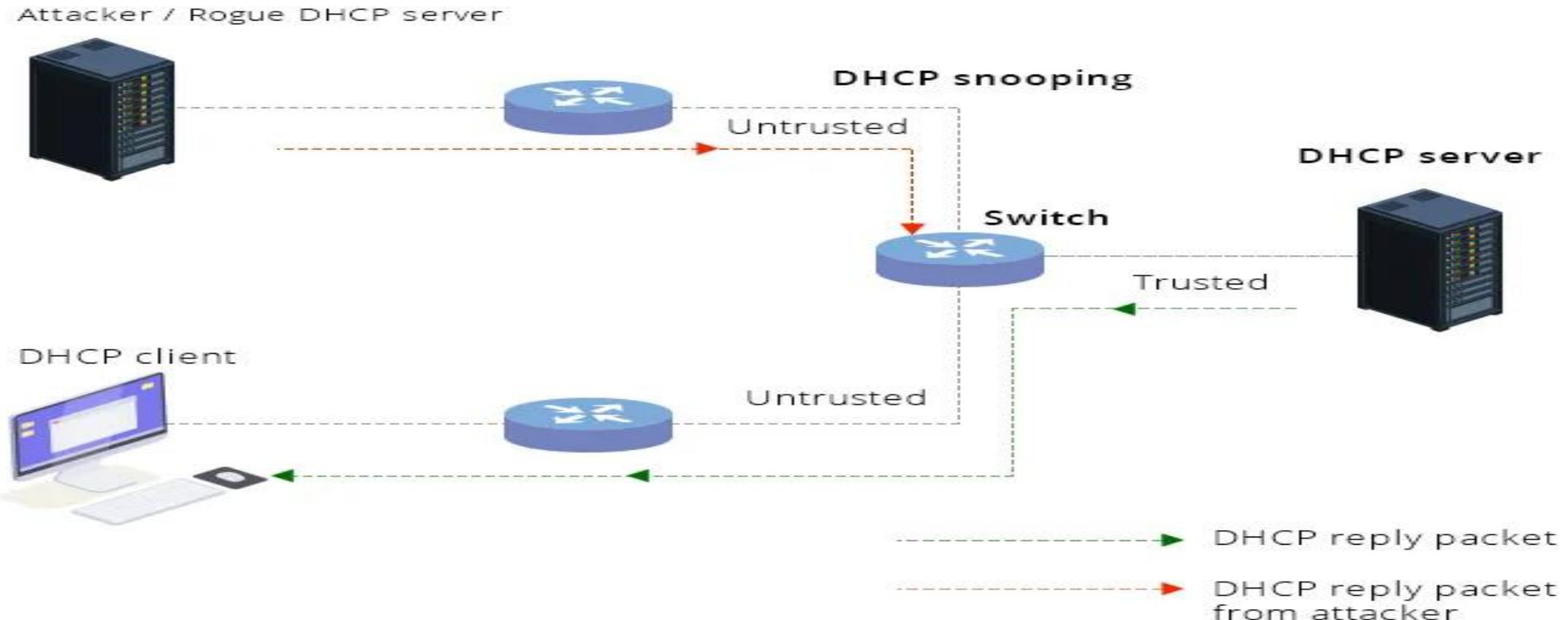
Usurpation d'identité DHCP (Rogue DHCP server)

La raison habituelle de cette attaque est de forcer les clients à utiliser de faux serveurs DNS ou Windows Internet Naming Service (WINS) et d'inciter les clients à se faire passer pour l'attaquant ou une machine sous le contrôle de l'attaquant à utiliser comme étant passerelle par-défaut.



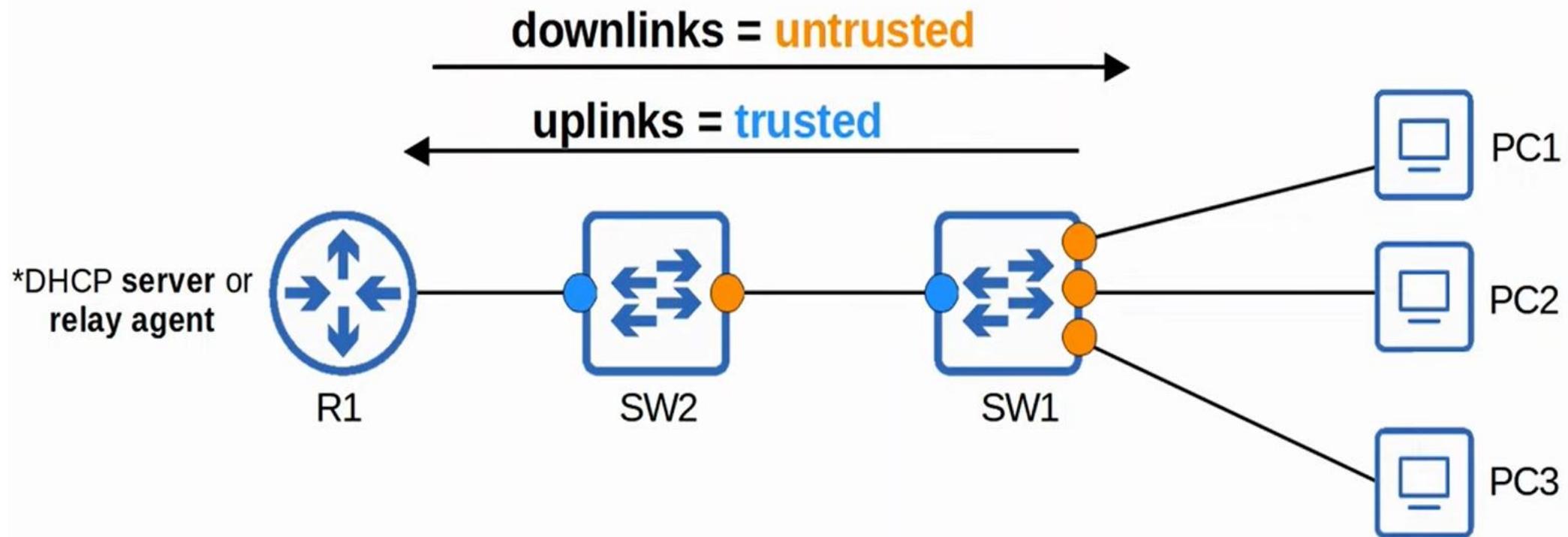
Les ports fiables (DHCP Snooping/Trusted ports)

Le DHCP Snooping n'est applicable qu'aux utilisateurs câblés !

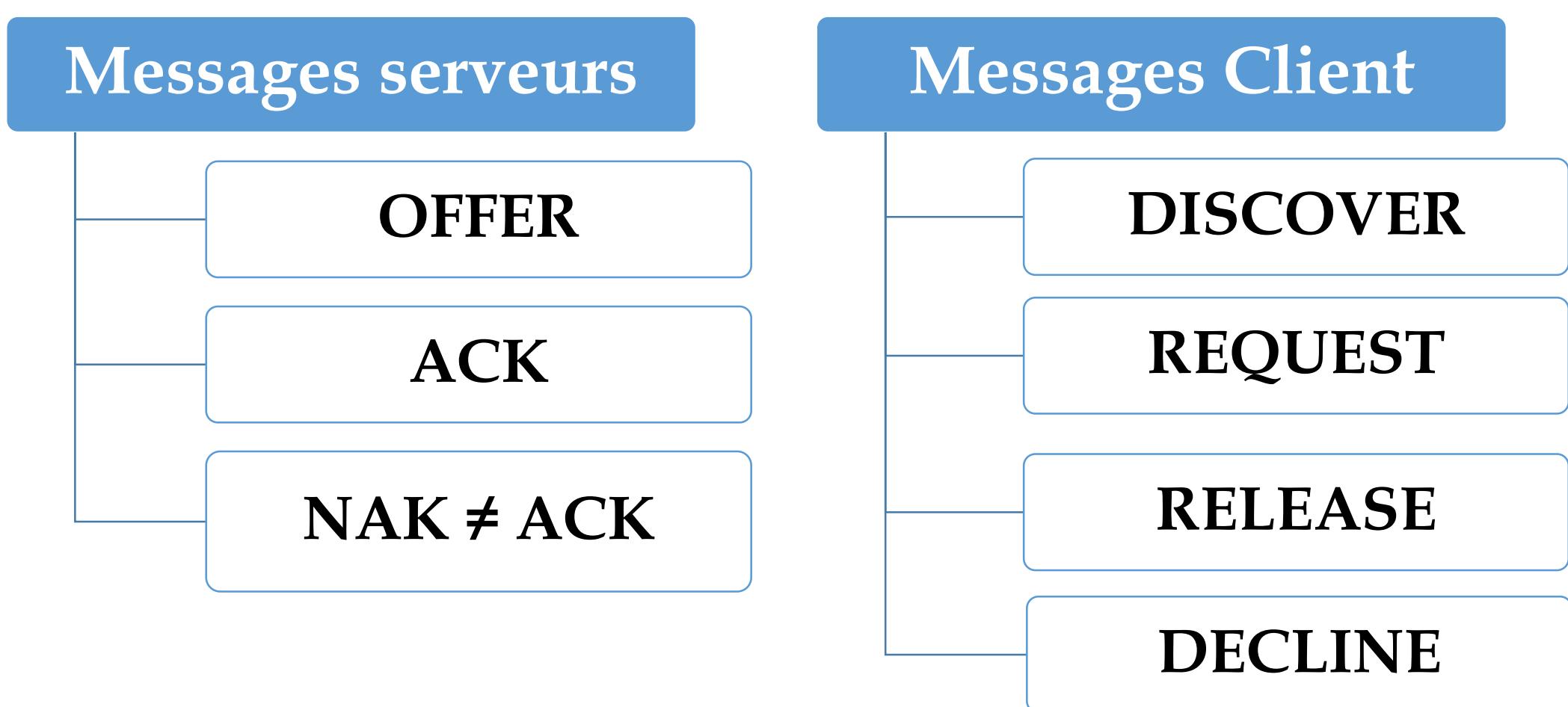


Les ports fiables (DHCP Snooping/Trusted ports)

DHCP Snooping est une fonctionnalité de sécurité des commutateurs utilisée pour filtrer les messages DHCP reçus sur des ports untrusted.



DHCP Snooping/Filtrage des messages DHCP



DHCP Snooping/Filtrage des messages DHCP

- Si un message DHCP est reçu sur un port trusted ? transférez-le normalement sans inspection.
- Si un message DHCP est reçu sur un port untrusted ? inspectez-le et agissez comme suit :
 - S'il s'agit d'un message du serveur DHCP ? jetez-le.
 - S'il s'agit d'un message DHCP client ? effectuez les vérifications suivantes :
 - Messages **DISCOVER/REQUEST**: Vérifiez si l'adresse **MAC** source de la trame et les champs **CHADDR** du message DHCP sont correspondant ? Correspondance = transfert, contradiction = rejet.
 - Messages **RELEASE/DECLINE**: Vérifiez si l'adresse **IP** source du paquet et **l'interface** de réception correspondent aux entrées dans la table **DHCP Snooping Binding Table** ? Correspondance = transfert, contradiction = rejet.

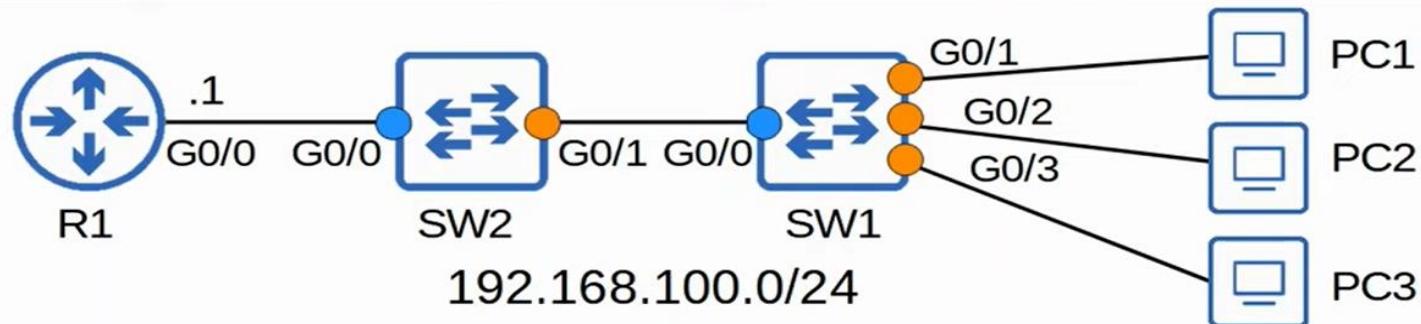
Les ports fiables (DHCP Snooping/Trusted ports)

```
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
```

```
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
-----  -----
0C:29:2F:18:79:00  192.168.100.10
0C:29:2F:90:91:00  192.168.100.11
0C:29:2F:67:E9:00  192.168.100.12
Total number of bindings: 3
```

RELEASE/DECLINE messages will be checked to make sure their IP address/interface ID match the entry in the DHCP snooping table.

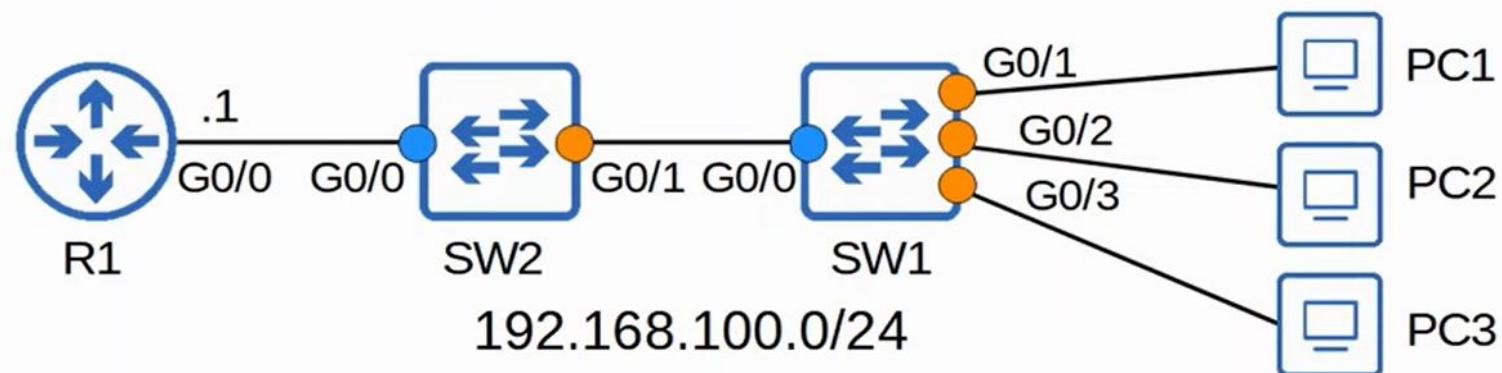


DHCP Snooping rate-limiting

DHCP Snooping peut limiter la vitesse à laquelle les messages DHCP sont autorisés à entrer dans une interface.

```
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
```



DHCP Snooping rate-limiting

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

```
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]

Rate-limiting can be very useful to protect against DHCP exhaustion attacks.

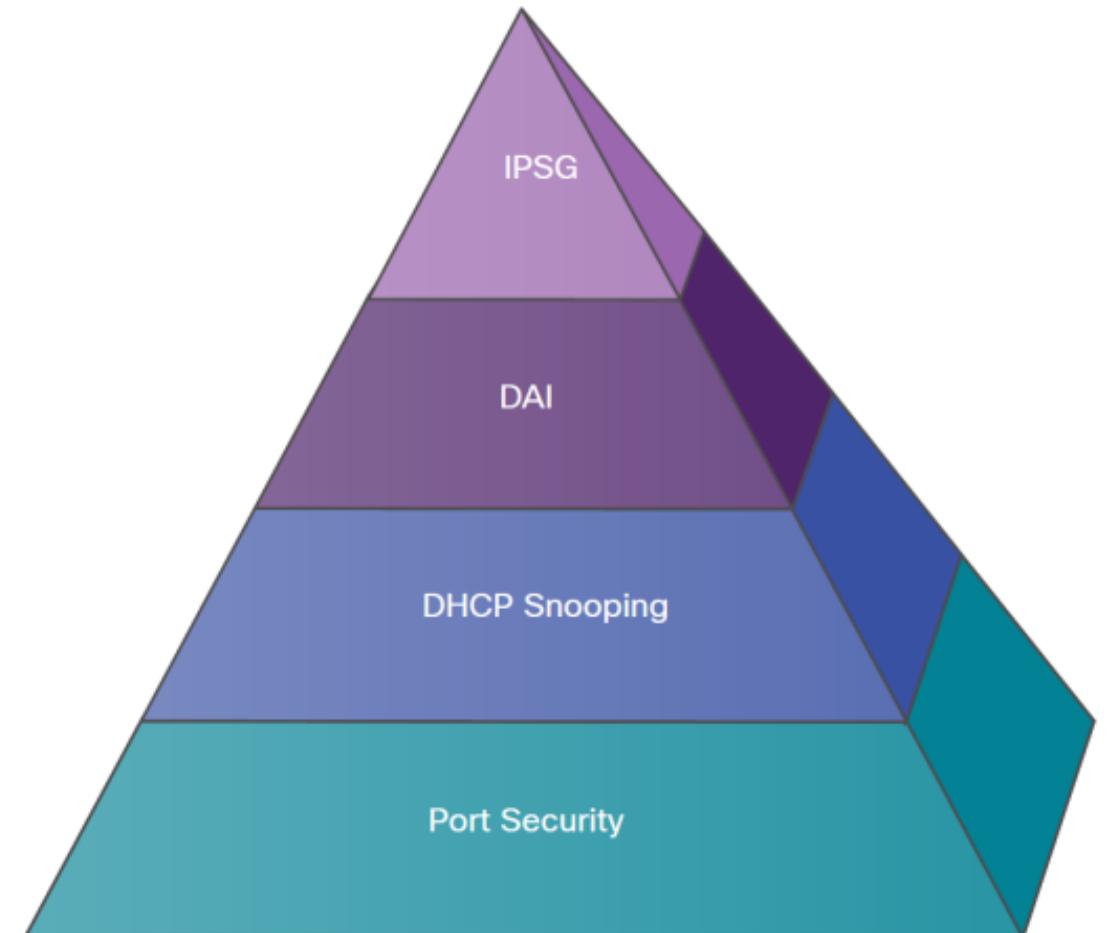
Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

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

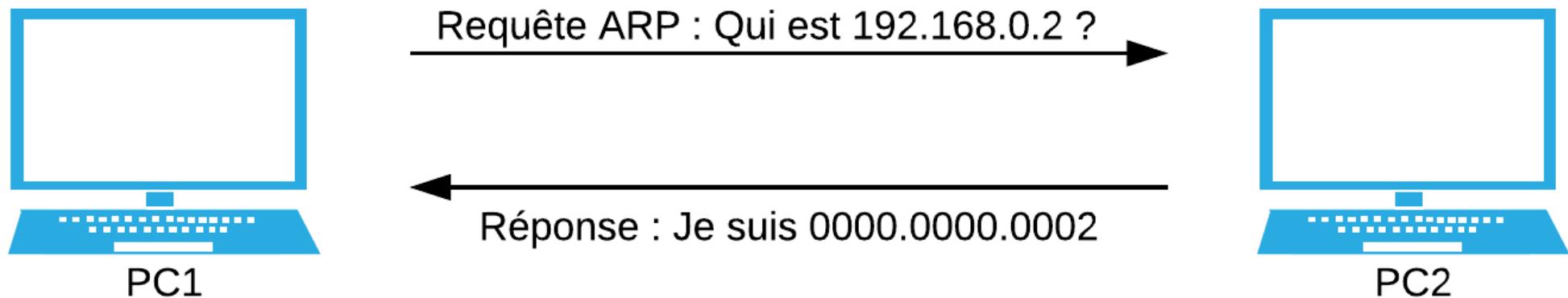
PLAN / Attaques et Contre-mesures

- Attaques MAC**
- Attaques DHCP**
- Attaques ARP**
- Attaques Généraux**



Le protocole ARP (Address Resolution Protocol)

Le protocole de résolution d'adresse (ARP) est un protocole ou une procédure qui relie une adresse IP en constante évolution à une adresse de machine physique fixe.



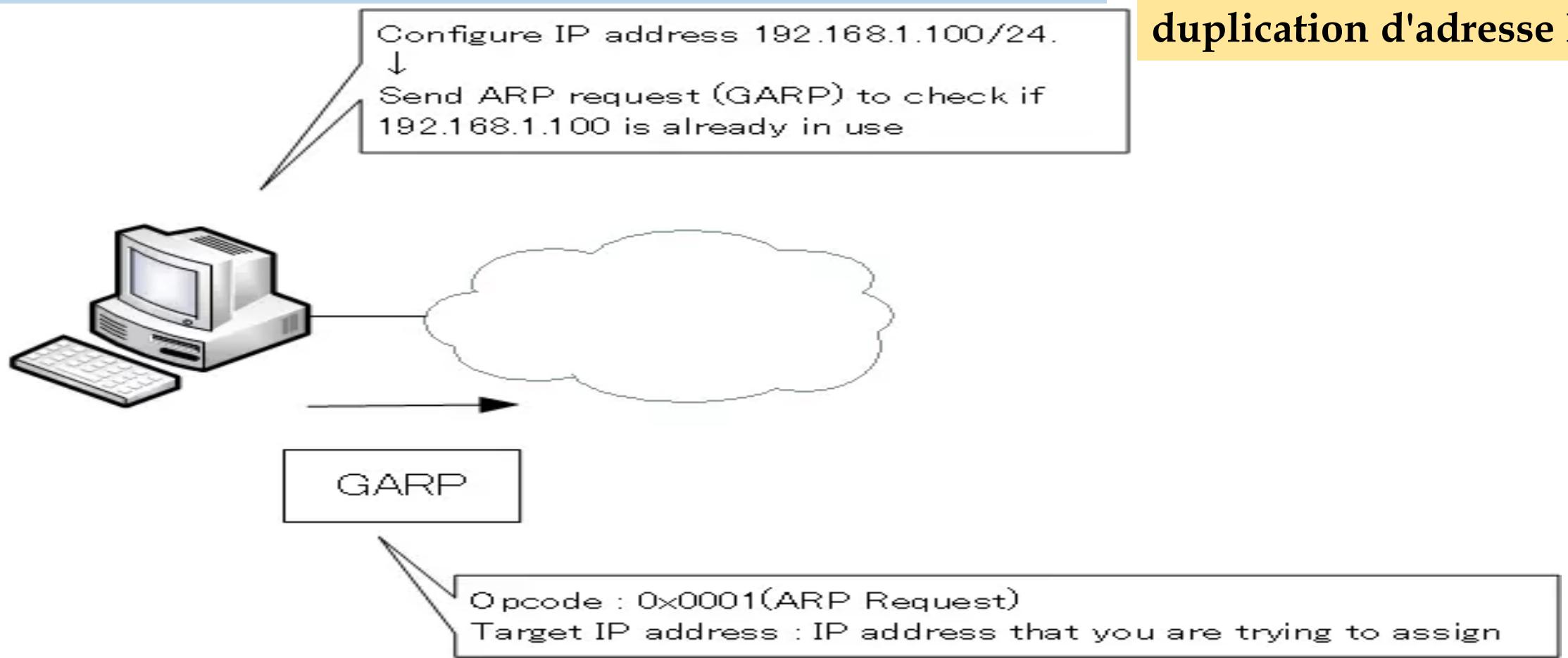
Adresse IP : 192.168.0.1
Adresse MAC :0000.0000.0001

Adresse IP : 192.168.0.2
Adresse MAC :0000.0000.0002

Gratuitous ARP

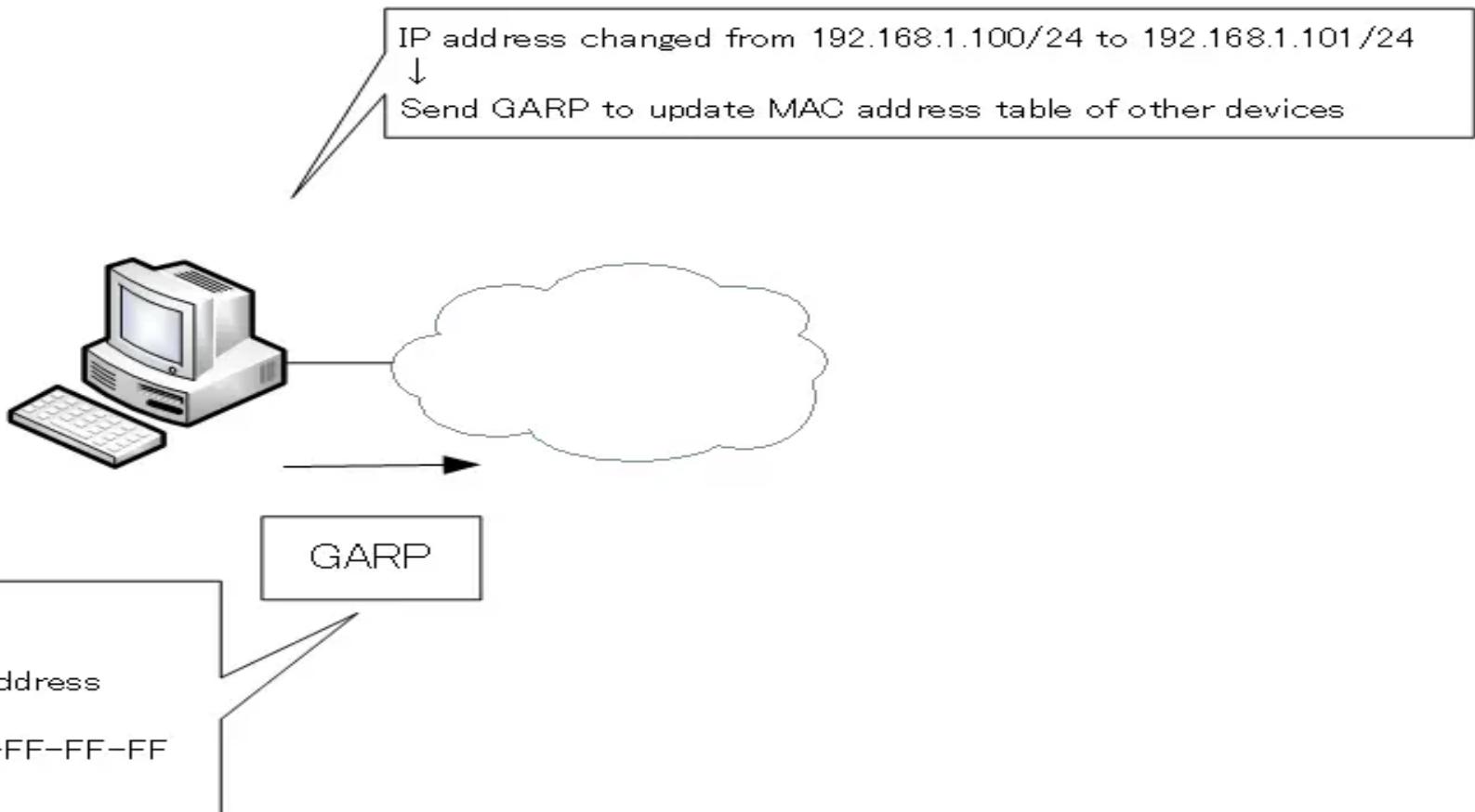
Un message Gratuitous ARP est une réponse ARP envoyée sans recevoir de requête ARP.

La Détection de duplication d'adresse IP.



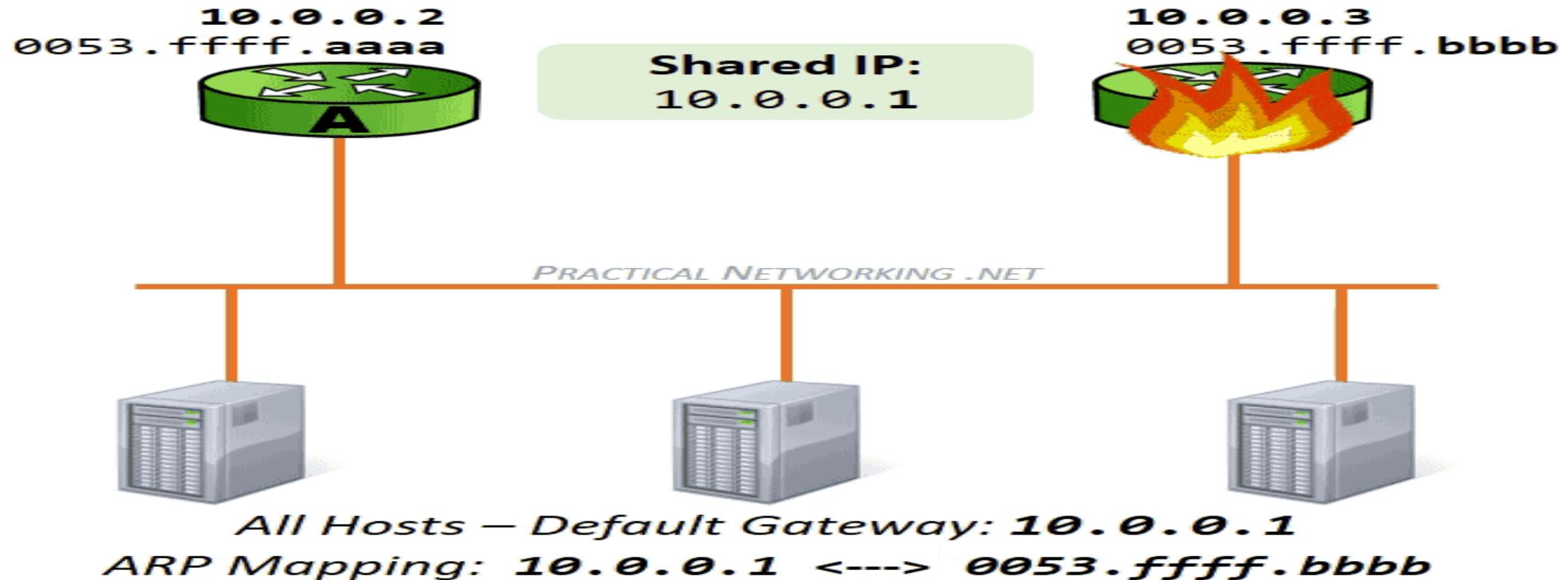
Gratuitous ARP

La mise à jour de cache ARP et la table d'adresses MAC.



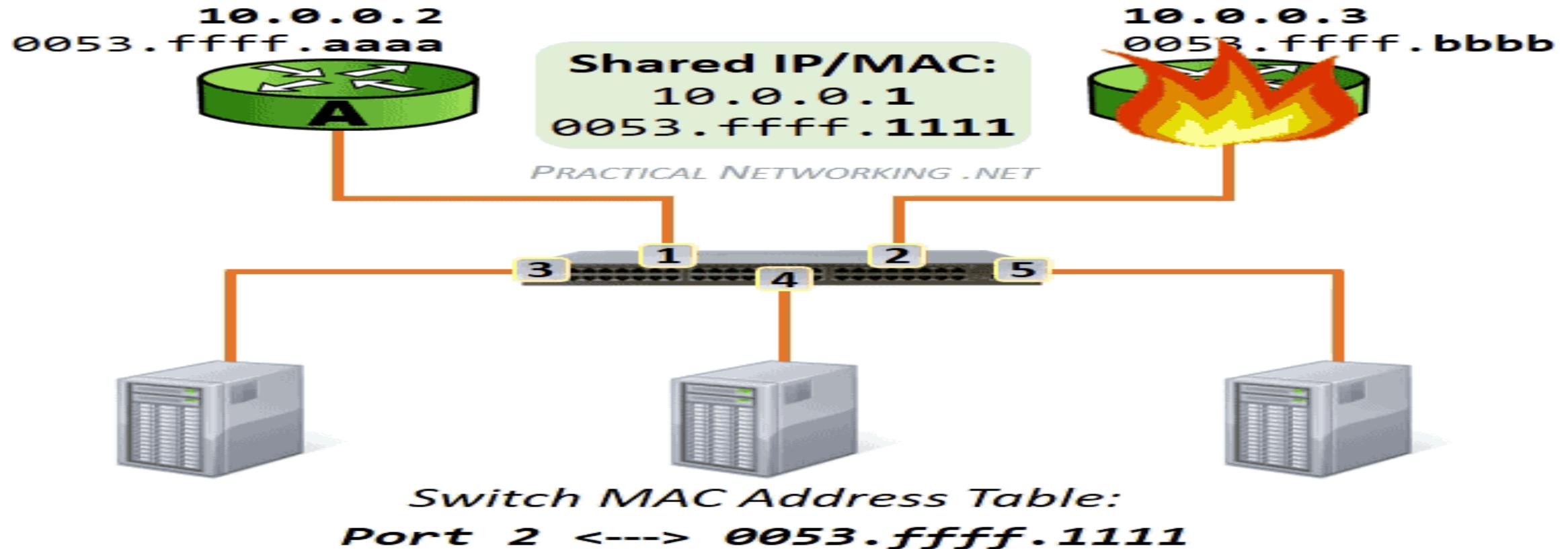
Gratuitous ARP

La redondance d'adresses IP.



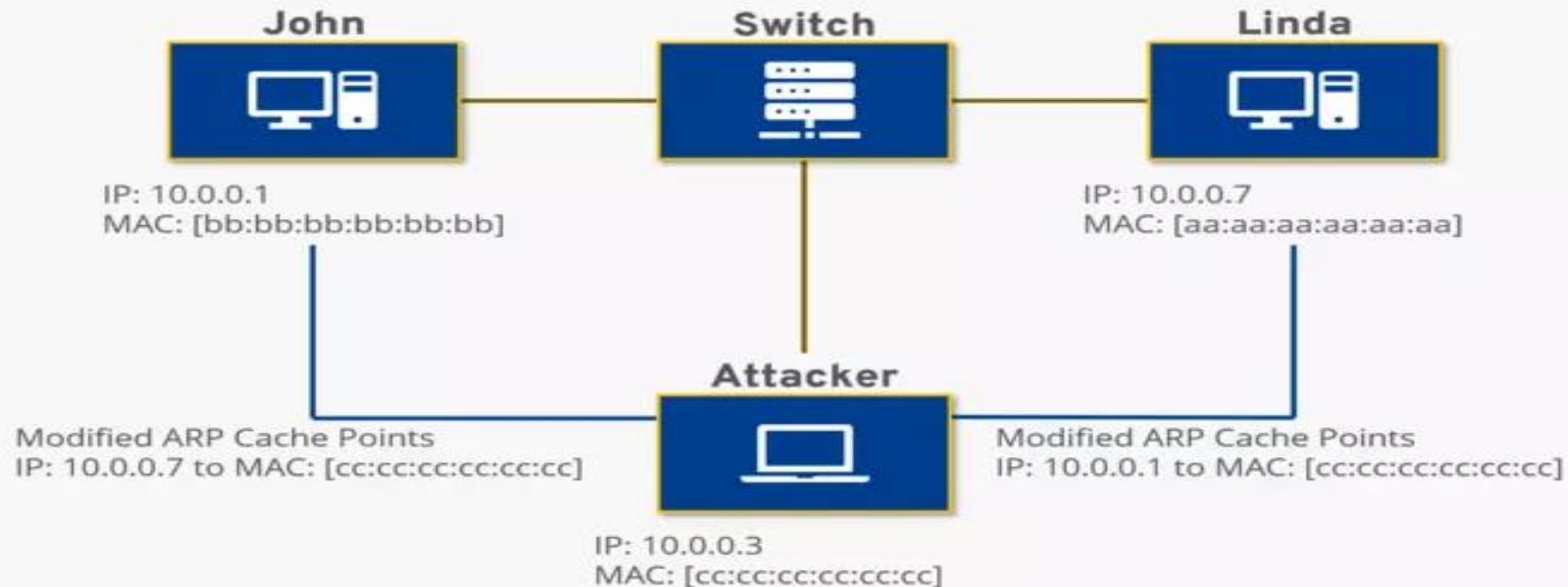
Gratuitous ARP

La redondance d'adresses IP et adresse MAC.



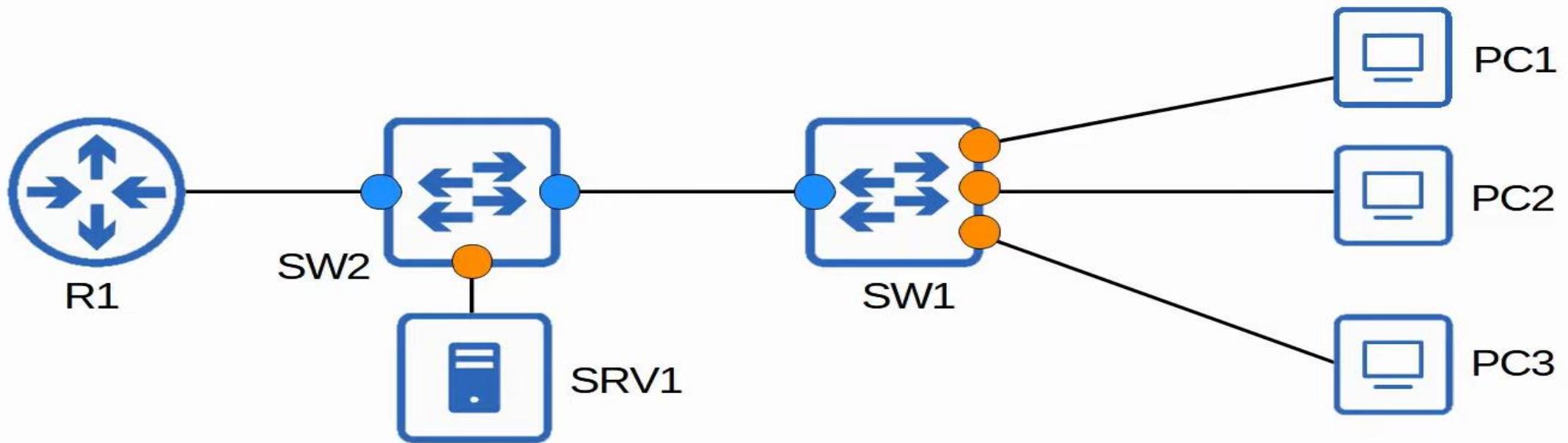
Usurpation du protocole ARP (ARP Poisoning Attacks)

Lorsqu'une réponse ARP est élaborée, un pirate de réseau peut faire apparaître son système comme l'hôte de destination recherché par l'expéditeur.



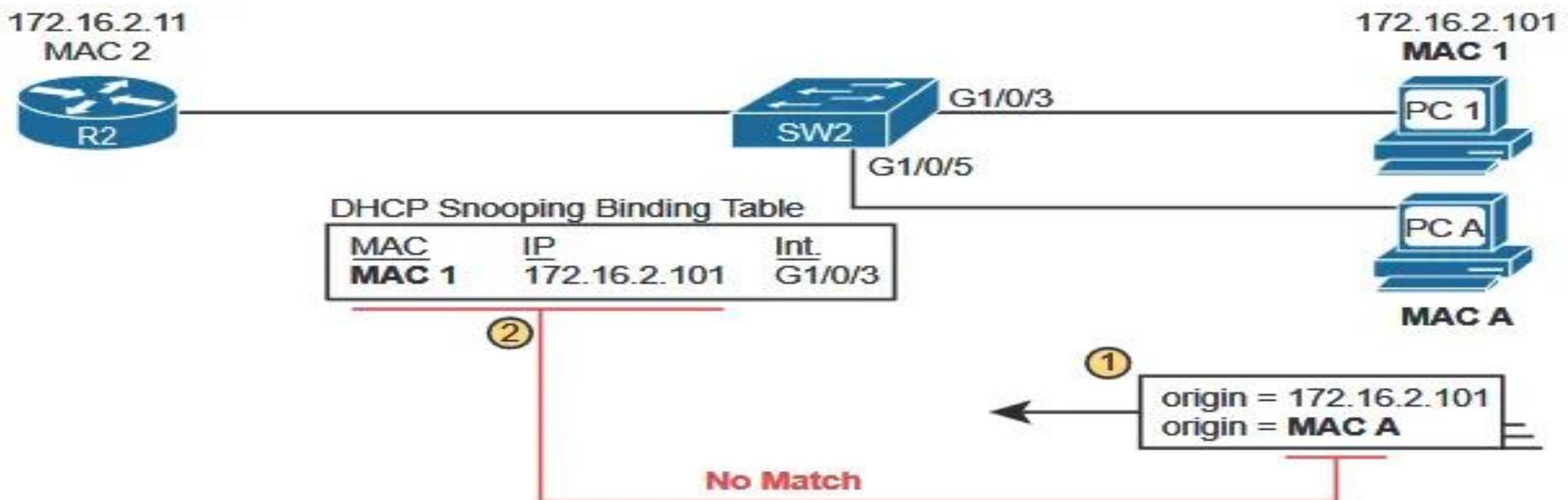
Dynamic ARP Inspection (Trusted/Untrusted Ports)

Généralement, tous les ports connectés à d'autres périphériques réseau (commutateurs, routeurs) doivent être configurés comme étant *trusted*, tandis que les interfaces connectées aux hôtes finaux doivent être *untrusted*.



Dynamic ARP Inspection (Trusted/Untrusted Ports)

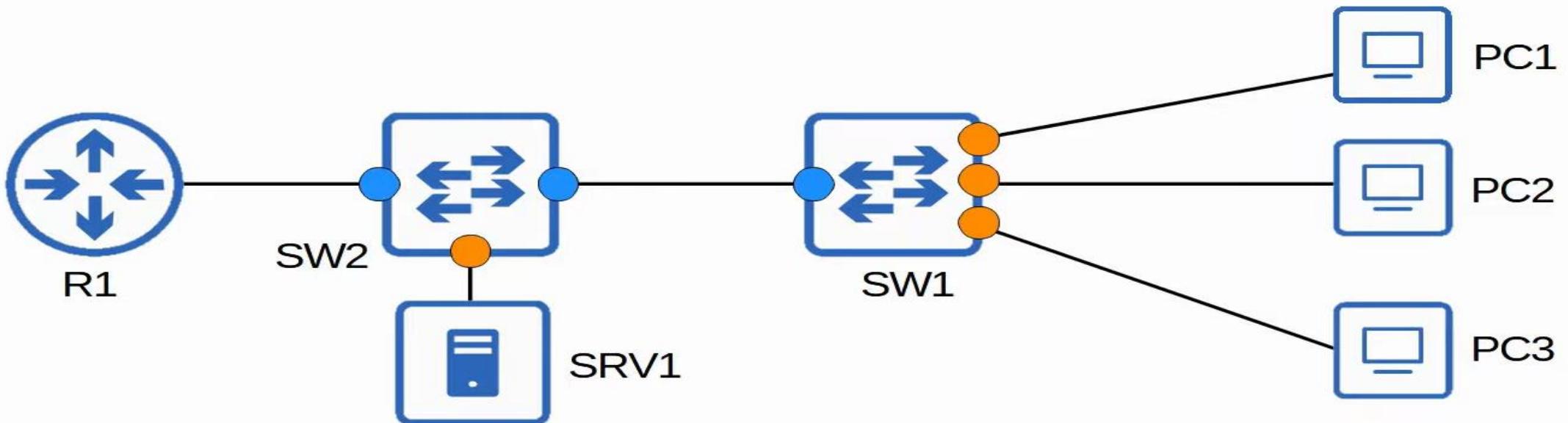
DAI compare les champs d'adresse IP d'origine et d'adresse MAC d'origine du message ARP à la table DHCP Snooping Binding Table. S'il est trouvé dans le tableau, DAI autorise le passage de l'ARP, mais sinon, DAI rejette l'ARP.



Dynamic ARP Inspection (Trusted/Untrusted Ports)

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

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



Dynamic ARP Inspection rate-limiting

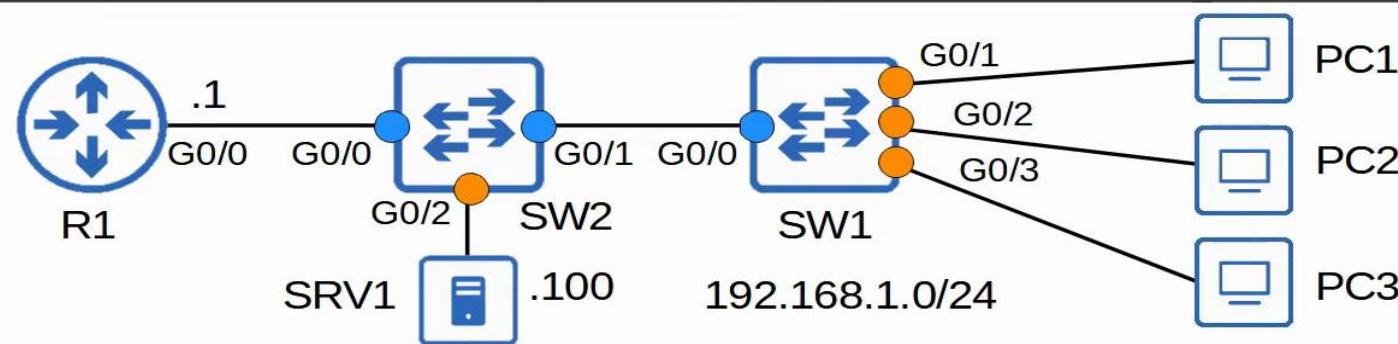
```
SW1#show ip arp inspection interfaces
```

Interface	Trust State
Gi0/0	Trusted
Gi0/1	Untrusted
Gi0/2	Untrusted
Gi0/3	Untrusted
Gi1/0	Untrusted
Gi1/1	Untrusted
Gi1/2	Untrusted
Gi1/3	Untrusted
Gi2/0	Untrusted
Gi2/1	Untrusted
Gi2/2	Untrusted
Gi2/3	Untrusted
Gi3/0	Untrusted
Gi3/1	Untrusted
Gi3/2	Untrusted
Gi3/3	Untrusted

DAI rate limiting is enabled on untrusted ports by default with a rate of 15 packets per second.
It is disabled on trusted ports by default.
*DHCP snooping rate limiting is disabled on all interfaces by default.

DHCP snooping rate limiting is configured like this:
x packets per second.

The DAI **burst interval** allows you to configure rate limiting like this:
x packets per y seconds



Dynamic ARP Inspection rate-limiting

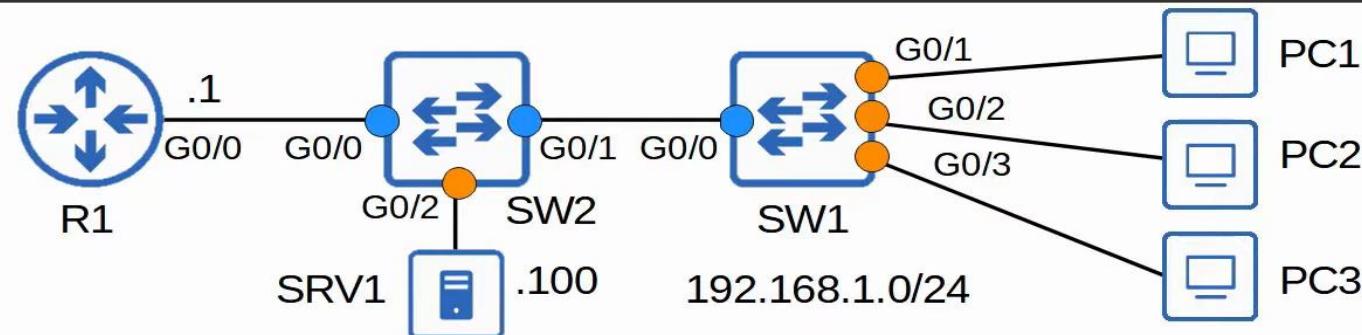
```
SW1(config)#interface range g0/1 - 2
SW1(config-if-range)#ip arp inspection limit rate 25 burst interval 2
SW1(config-if-range)#interface range g0/3
SW1(config-if)#ip arp inspection limit rate 10
SW1(config-if)#do show ip arp inspection interfaces
```

The burst interval is optional. If you don't specify it, the default is 1 second.

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]			

If ARP messages are received faster than the specified rate, the interface will be err-disabled. It can be re-enabled in two ways:
1: **shutdown** and **no shutdown**
2: **errdisable recovery cause arp-inspection**

```
SW1(config)#errdisable recovery cause arp-inspection
SW1(config)#do show errdisable recovery
ErrDisable Reason          Timer Status
arp-inspection              Enabled
![output omitted]
```



Dynamic ARP Inspection

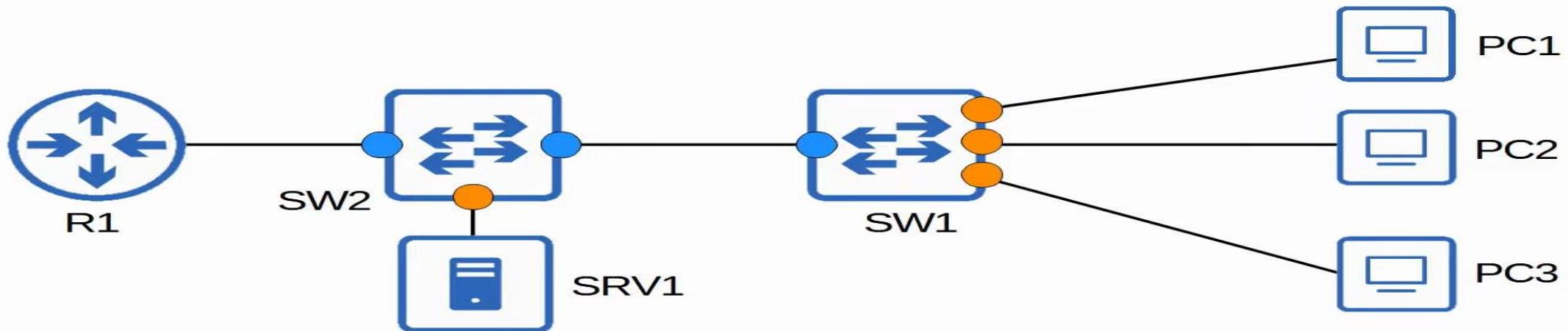
Contrôles optionnelles

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

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

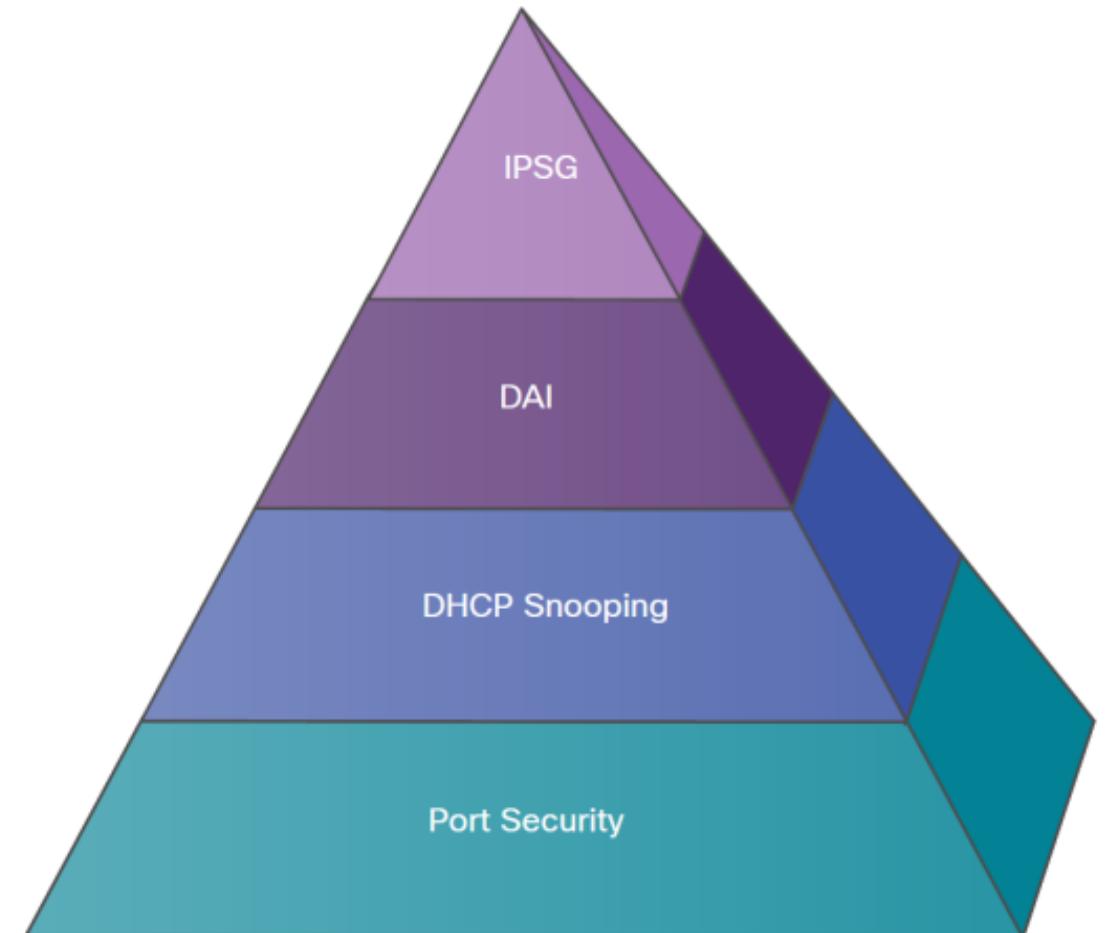
SW1(config)#ip arp inspection validate ip src-mac dst-mac

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

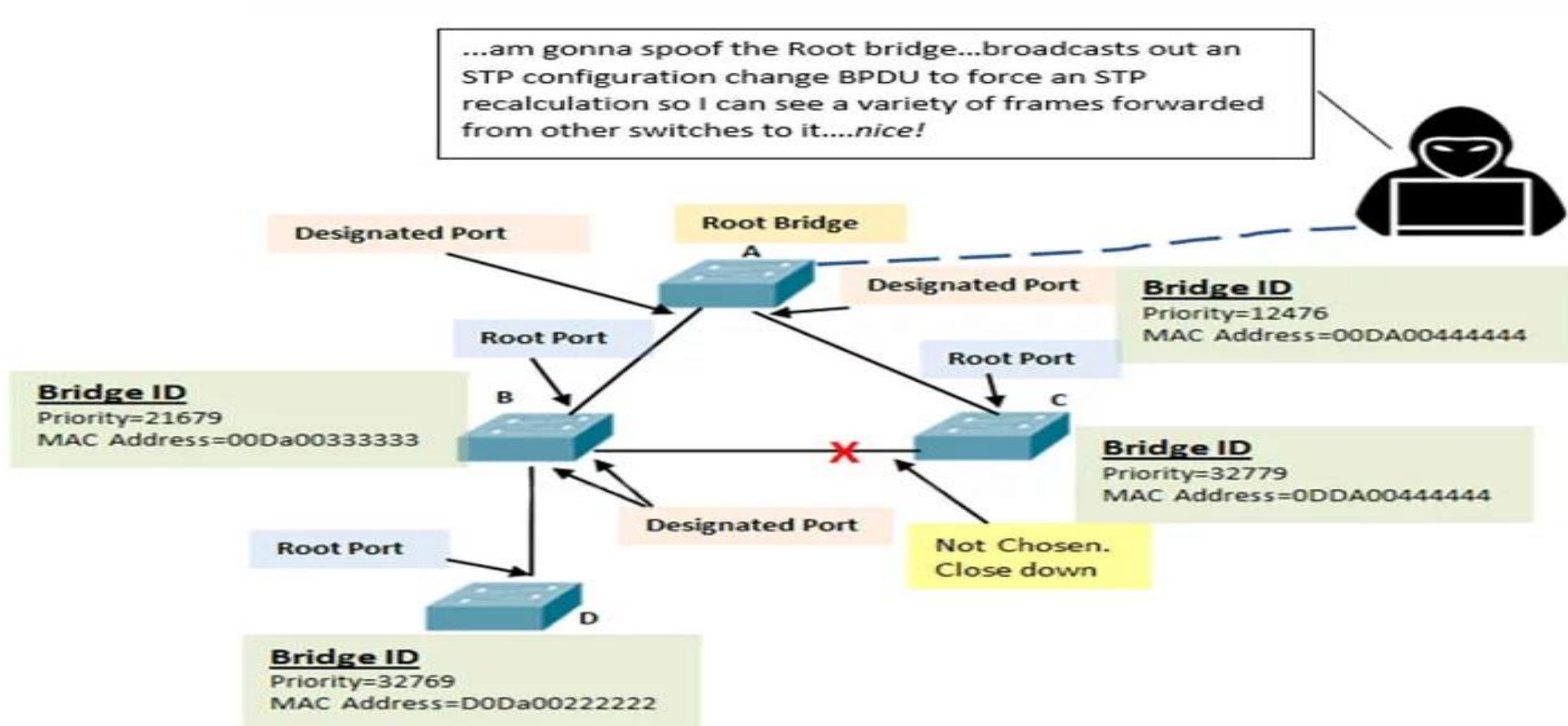


PLAN / Attaques et Contre-mesures

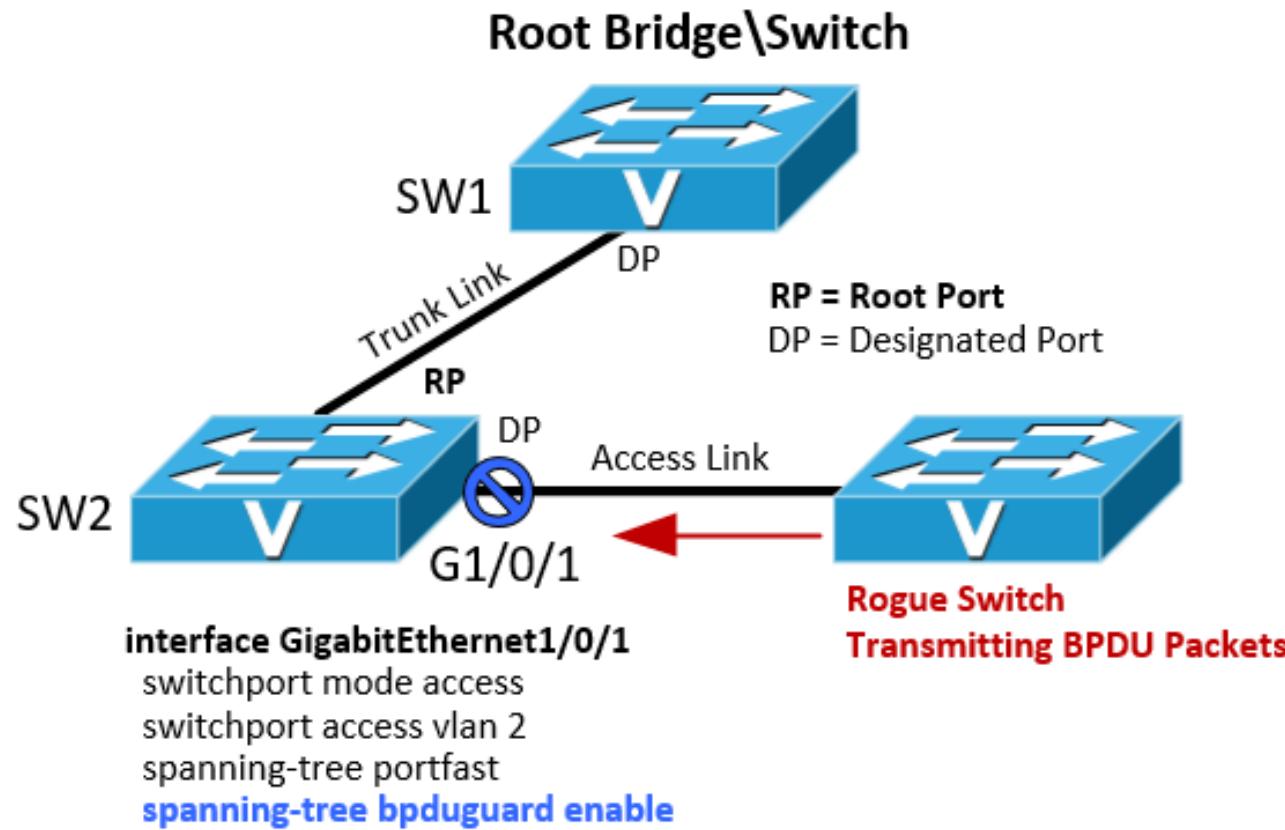
- Attaques MAC
- Attaques DHCP
- Attaques ARP
- Attaques Généraux



Attaques Spanning-Tree



Spanning Tree BPDU Guard

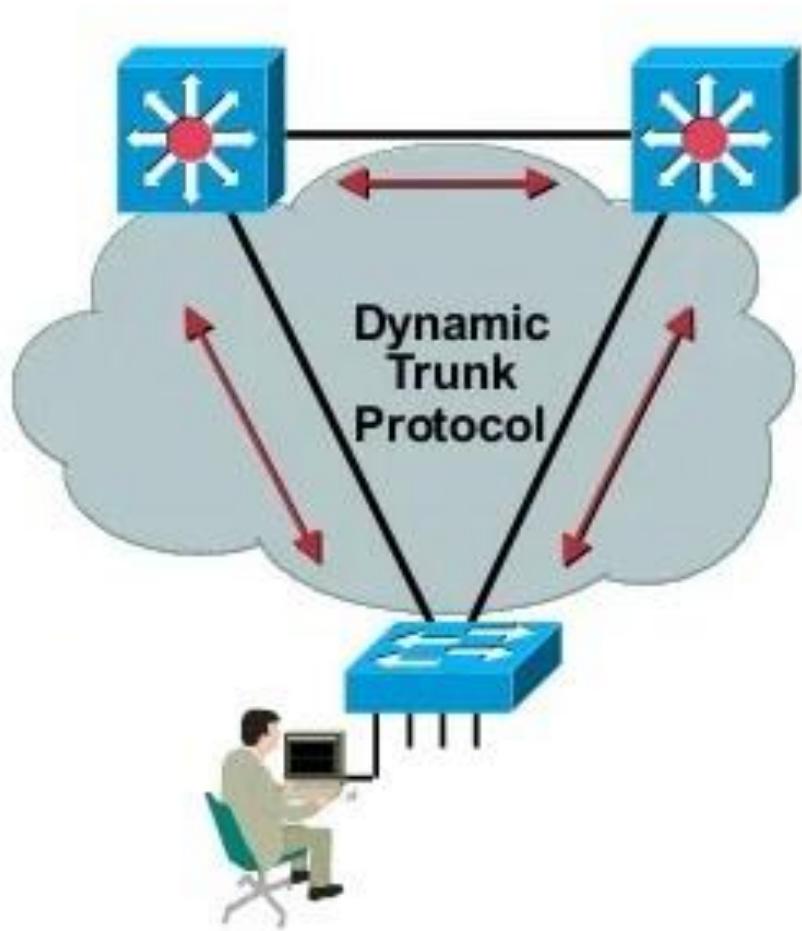


// Configurer BPDU Guard en mode de configuration globale.
Switch(config)# spanning-tree portfast bpduguard default

// Configurer BPDU Guard sur l'interface.
Switch(config)# interface **GigabitEthernet1/0/1**
Switch(config-if)# spanning-tree bpduguard enable

// Afficher la configuration
interface GigabitEthernet1/0/1
switchport mode access
switchport access vlan 2
spanning-tree portfast
spanning-tree bpduguard enable

Dynamic Trunk Protocol (DTP)



- DTP synchronizes the trunking mode on end links
- DTP state on 802.1q/ISL trunking port can be set to “Auto”, “On”, “Off”, “Desirable”, or “Non-Negotiate”

Meilleures pratiques de sécurité pour VLAN et Trunking

- Utilisez toujours un ID de VLAN dédié pour tous les ports trunk
- Désactivez les ports inutilisés et placez-les dans un VLAN inutilisé
- Soyez paranoïaque : n'utilisez pas le VLAN 1 pour quoi que ce soit
- Désactiver l'auto-trunking sur les ports orientés utilisateur (DTP-off)
- Configurer explicitement les liaisons trunk sur les ports d'infrastructure
- Utiliser tous les modes balisés pour le VLAN natif sur les liaisons trunk
- Utilisez l'accès VLAN vocal PC sur les téléphones qui le soutiennent

responsabilité

Ces pratiques et les informations qu'elles contient sont uniquement destinés à des fins d'information.

Si vous savez mieux comment fonctionnent ces attaques, vous pourrez mieux vous défendre contre elles.