

## ABREGÉ sur la table ARP vs LA TABLE DE TRANSFERT dans un switch

### ATTENTION A LA TERMINOLOGIE !

Dans un commutateur de couche deux (L2), il n'y a pas de table ARP, seulement une table de transfert.

Il s'agit d'une idée fautive assez courante ou, plus précisément, d'un problème de terminologie qui fait penser que les Switch L2 ont une table ARP.

Le commutateur enregistre chaque adresse MAC source qu'il voit en entrée **dans la table de transfert** et l'attribue au port afin que les trames avec une adresse MAC destination ne soient envoyées qu'au port connu pour ce MAC.

Beaucoup de gens appellent cela une "table arp" ou "cache arp" même si ce n'est ni l'un ni l'autre.

Dans un commutateur de couche deux administrable (switch L2 administrable), il y a **une table de transfert et une table ARP**, mais cette table ARP est uniquement utilisée pour l'interface de gestion pour parler aux hôtes intéressés (c'est-à-dire le PC que vous utilisez pour configurer le commutateur : Rappelez vous l'exemple de Putty.exe, pour administrer le Switch Avaya de couche 2, en connexion protocole TELNET : via l'adresse ip du switch).

Dans un commutateur de couche 3 (faisant office de routeur) administrable, il y aura **une table de transfert plus une table ARP**, car il en a besoin pour l'interface de gestion et la fonctionnalité de routeur existe pour effectuer le transfert entre les sous-réseaux.

#### Commandes basiques Cisco permettant d'afficher la configuration d'un Switch ou d'un routeur :

Test / Commande	Description	Objectifs
<b>Routeur Cisco</b>		
<b>sh arp</b>	Affiche le cache ARP (adresses IP / MAC)	Vérifier que le cache n'est pas corrompu. Détecter les entrées invalides (adresses <i>incomplète</i> )
<b>sh interface status</b>	Montre l'état et la vitesse des ports	Vérifier si un port est actif, sa vitesse (suite à l'auto-négociation), etc.
<b>sh interface description</b>	Montre l'état et le descriptif des ports	Affiche l'état du port pour un serveur donné
<b>sh ip interface brief</b>	Montre l'état et l'adresse IP par port	Montre les adresses IP configurées pour les ports en mode routé
<b>clear arp-cache</b>	Vide le cache ARP	Vérifier que le niveau 2 remonte correctement
<b>sh interfaces fastEthernet 0</b>	Affiche l'état d'un port	Vérifier la vitesse, les pertes, etc.

## ABREGÉ sur la table ARP vs LA TABLE DE TRANSFERT dans un switch

Test / Commande	Description	Objectifs
<b>Switch Cisco</b>		
<b>sh mac-address-table</b>	Affiche la table de switching (adresses MAC par port du Switch)	Vérifier qu'il n'y a pas de corruption au niveau des adresses MAC
<b>clear arp-cache</b>	Vide le cache ARP	Vérifier que le niveau 2 remonte correctement
<b>clear mac-address-table</b>	Efface la table de commutation	Si le vidage du cache ARP n'a pas donné de résultat
<b>sh interfaces fastEthernet 0</b>	Affiche l'état d'un port	Vérifier la vitesse, les pertes, etc.

### Gestion de la table ARP sous Windows/Linux

Les commandes sont pour la plupart les mêmes, les changements seront évidemment notifiés. La table ARP est une table "cache" qui possède des enregistrements de type association "IP <-> Adresse MAC" ceci pour éviter de refaire une requête ARP "who-is" à chaque fois que l'on souhaite communiquer avec une machine.

#### Afficher la table ARP

La première chose que l'on souhaite généralement faire est d'afficher la table ARP, c'est à dire les enregistrements qui y sont présents, pour cela on peut utiliser la commande "arp -a" tout simplement :

```
C:\Users\Neaj>arp -a
Interface : 192.168.1.21 --- 0x4
Adresse Internet    Adresse physique    Type
192.168.1.30        70-9e-29-4a-d0-81   dynamique
192.168.1.31        84-a6-c8-36-ef-8e   dynamique
192.168.1.254       c8-cd-72-5a-db-bd   dynamique
192.168.1.255       ff-ff-ff-ff-ff-ff   statique
224.0.0.2           01-00-5e-00-00-02   statique
224.0.0.22          01-00-5e-00-00-16   statique
224.0.0.251         01-00-5e-00-00-fb   statique
224.0.0.252         01-00-5e-00-00-fc   statique
224.1.1.1           01-00-5e-01-01-01   statique
226.178.217.5       01-00-5e-32-d9-05   statique
239.255.255.250     01-00-5e-7f-ff-fa   statique
255.255.255.255     ff-ff-ff-ff-ff-ff   statique
```

On voit alors un tableau par interface (ou par IP que l'interface a pu avoir) avec les correspondances IP <-> MAC. Sous Windows, on voit également le type d'enregistrement, à savoir s'il s'agit d'un enregistrement dynamique ou statique.

## Enregistrer une entrée fixe dans la table ARP

Le fait est que mettre un enregistrement de type statique dans une table ARP est une protection contre l'ARP spoofing car cet enregistrement et son association IP <-> MAC ne peut être remplacée par une fausse valeur. Pour cela, on peut utiliser l'option "-s" qui est valable sur Windows comme sur Linux.

### Voici son utilisation sous Windows :

```
arp -s 178.89.87.85 0A-02-03-04-05-06
```

### Et son utilisation sous Linux qui a une syntaxe légèrement différente au niveau de la définition de l'adresse MAC :

```
arp -s 178.89.89.85 0A0203040506
```

On pourra alors vérifier cet enregistrement avec la commande d'affichage de la table ARP vue plus haut.

## Vider la table ARP

Dans certains cas, il peut être utile de vider la table ARP d'une machine cliente. A nouveau, cela s'effectue de la même manière sur Windows et Linux :

```
arp -d
```

On peut également supprimer une entrée bien précise en spécifiant l'IP de cette entrée, par exemple :

```
arp-d 192.168.54.89
```

## Voir la table ARP d'une seule interface réseau

Il peut être plus simple dans certaines situations de n'afficher les entrées ARP que d'une seule interface, pour cela, on peut utiliser l'option "-i" sous Linux :

```
arp -a -i eth0
```

Sous Windows, on utilisera l'option "-N" suivi de l'IP voulue (celle présente sur l'interface que l'on souhaite observer bien évidemment) :

```
arp -a -N 172.16.1.50
```

Voilà, nous avons à présent fait le tour des principales utilisations de la table ARP chez un OS client, vous pouvez toutefois avoir plus d'informations avec les commandes "**arp /?**" sur Windows et "**arp -h**" sous Linux