

1<sup>er</sup> master IDO.

MODULE: systèmes organisationnels.

## TP - RÉSEAU LAN – PARTIE 2

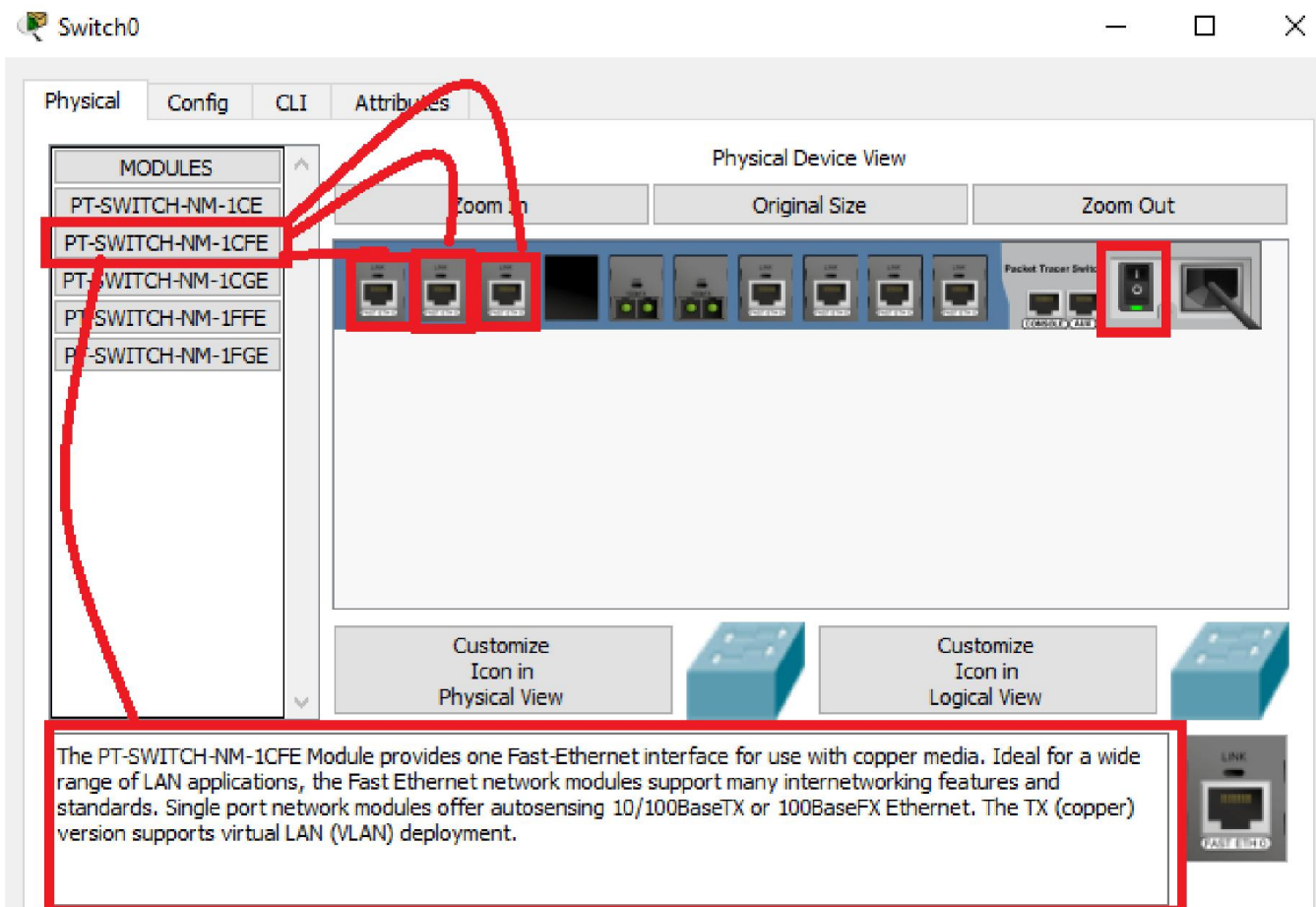
### 5 - SWITCH ( OU COMMUTATEUR EN FRANÇAIS)

Pourquoi ne trouve-t-on plus de hub ou presque ? Parce que le **switch** fait mieux. Et pour pas beaucoup plus cher. En français, on dit **commutateur**.



Regardons comme il fonctionne concrètement. Pour cela, vous allez créer une simulation de réseau en remplaçant le HUB pour un SWITCH.

° Remplacer tous les pc et rajouter un switch. Vous pouvez garder les mêmes adresses IP (192.168.6.21 à 192.168.6.25). Utiliser l'icone Select (deux icones au dessus de Delete) pour sélectionner le Switch.



**Attention** : Quittez le mode simulation pour que le switch puisse se configurer sans que vous ayez besoin de valider chaque étape. Sinon, ça risque de prendre un temps certain

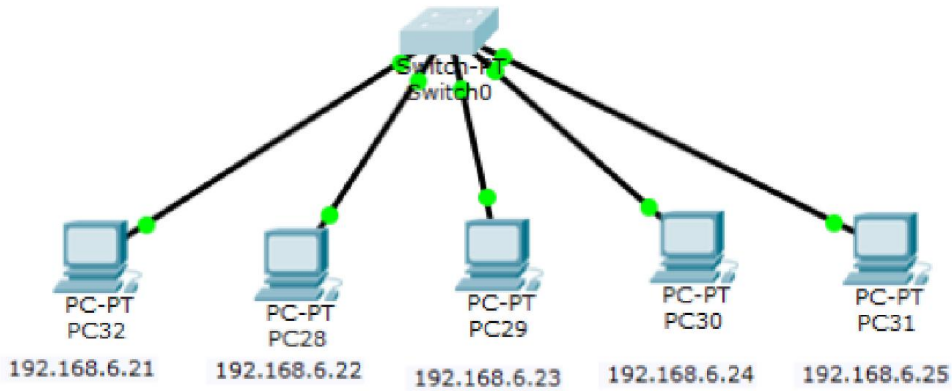
...

° Dans le menu physical, arrêter le switch avec le bouton ON/OFF et rajouter au moins un port Fast Ethernet puisque, de base, notre switch n'en possède que trois. Pour avoir une description des ports que vous pouvez rajouter, il suffit de cliquer sur l'élément. Pour le rajouter, il faut faire un drag-and-drop. Pour le supprimer, il faut faire un drag-and-drop dans l'autre sens. Remettre ensuite le switch sous tension.

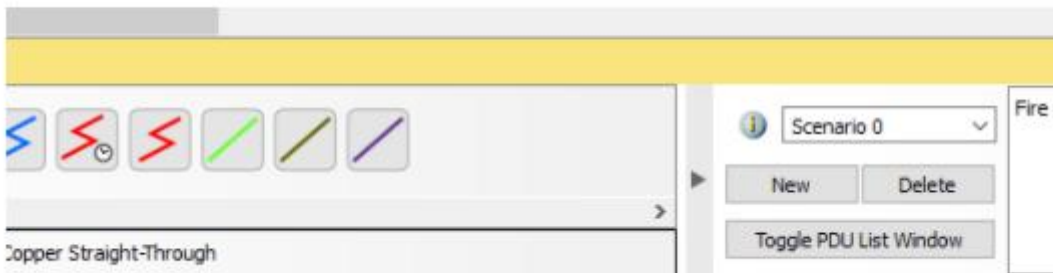
° Connecter les PC au switch avec un câble droit, comme pour le Hub. Le point orangé indique que le switch est en train de configurer ses ports. Attendre qu'ils soient tous passés au vert.



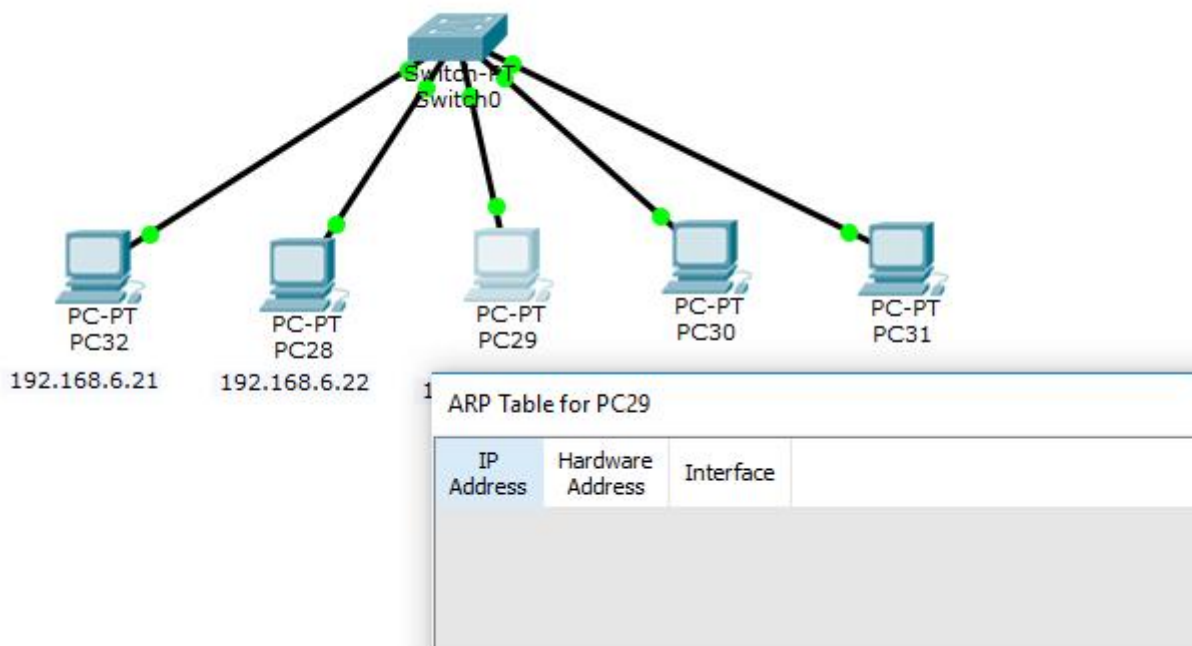
Vous allez obtenir ceci :



° Supprimer les anciennes simulations d'envois avec Delete :



° Utiliser la loupe (Inspect) sur l'un des PC pour afficher sa table ARP (qui est normalement vide) si vous avez bien mis de nouveaux pc).

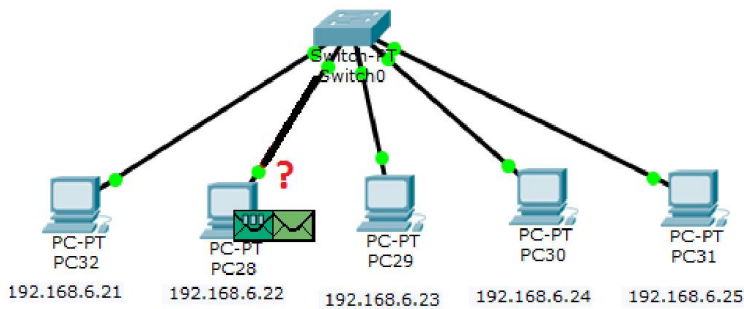


## TABLE ARP

Le cache ARP ou table ARP est une table de correspondance entre adresse IP et adresse Mac pour les pc qui sont dans le même réseau que l'ordinateur. Chaque ordinateur possède sa propre table ARP qu'il crée au fur et à mesure qu'il reçoit des messages dont il connaît l'adresse IP locale et l'adresse MAC de l'expéditeur.

Ainsi lorsque cet ordinateur veut contacter l'une des IP présentes dans la table, il n'a pas besoin de se renseigner sur le réseau : il lui suffit d'indiquer l'adresse MAC qui va bien.

° Faire un envoi d'un pc vers un autre en mode SIMULATION pour voir le fonctionnement. ATTENTION : Activez via EDIT FILTERS le suivi des protocoles ICMP et ARP. Nous allons voir un peu comment fonctionne la reconnaissance des adresses IP / MAC et la création de la table de correspondance.



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC28	ICMP	
	0.000	--	PC28	ARP	

Reset Simulation  Constant Delay

**Etape A** : On voit que le protocole ICMP veut envoyer un message de type 8 de l'IP 192.168.2.22 (PC28) vers l'IP 192.168.6.23 (PC29).

**PARTIE EN OPTION, UN PEU TECHNIQUE MAIS ASSEZ INTÉRESSANTE**

On regarde donc dans la table ARP de correspondance IP/MAC et on constate qu'on ne peut pas atteindre la couche 2 car on ne connaît pas l'adresse MAC de l'IP 192.168.2.22  
 ...

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC28	ICMP	

**PDU Information at Device: PC28**

OSI Model    Outbound PDU Details

At Device: PC28  
Source: PC28  
Destination: PC29

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer 3: IP Header Src. IP: 192.168.6.22, Dest. IP: 192.168.6.23 ICMP Message Type: 8
Layer2	Layer 2:
Layer1	Layer1

1. The next-hop IP address is a unicast. The ARP process looks it up in the ARP table.  
2. The next-hop IP address is not in the ARP table. The ARP process tries to send an ARP request for that IP address and buffers this packet.

Du coup, l'ordinateur lance une requête ARP pour connaître l'adresse MAC de l'IP qui appartient au même réseau que notre ordinateur.

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC28	ARP	

**PDU Information at Device: PC28**

OSI Model    Outbound PDU Details

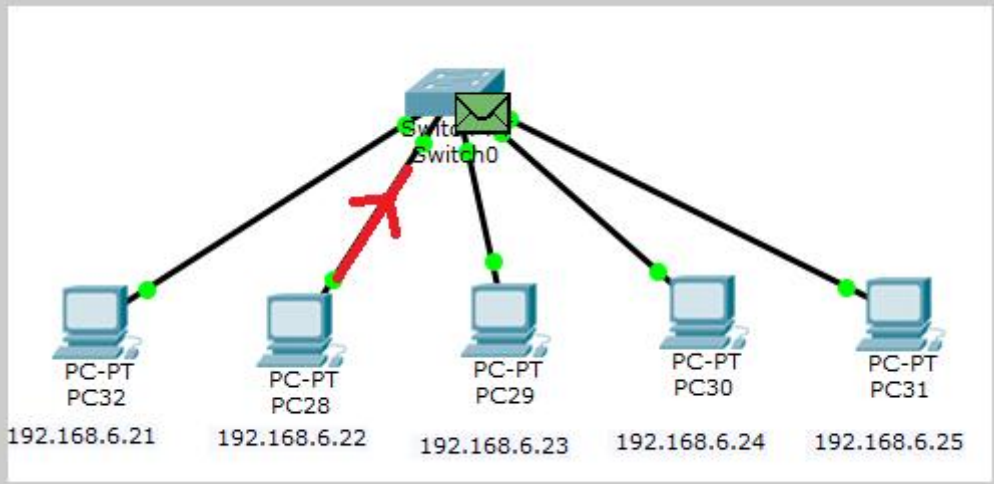
At Device: PC28  
Source: PC28  
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2	Layer 2: Ethernet II Header 0030.A3C6.E1E1 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.6.22, Dest. IP: 192.168.6.23
Layer1	Layer 1: Port(s): FastEthernet0

1. The ARP process constructs a request for the target IP address.  
2. The device encapsulates the PDU into an Ethernet frame.

On voit qu'on lance une requête ARP de l'adresse MAC du PC 28 vers l'adresse MAC **FFFF.FFFF.FFFF**.. Cela correspond à un **broadcast** : on diffuse l'appel à tous les pc en communication avec le notre. Le protocole précise l'adresse IP voulue de façon à ce que le bon pc réponde à la demande ARP.

On envoie la requête via le port Ethernet et on atteint ainsi le Switch.



Si on regarde de plus près la requête :

The screenshot shows a network simulation interface with the following details:

- 0.001 PC28 Switch0 ARP
- PDU Information at Device: Switch0
- OSI Model: Inbound PDU Details
- At Device: Switch0
- Source: PC28
- Destination: Broadcast

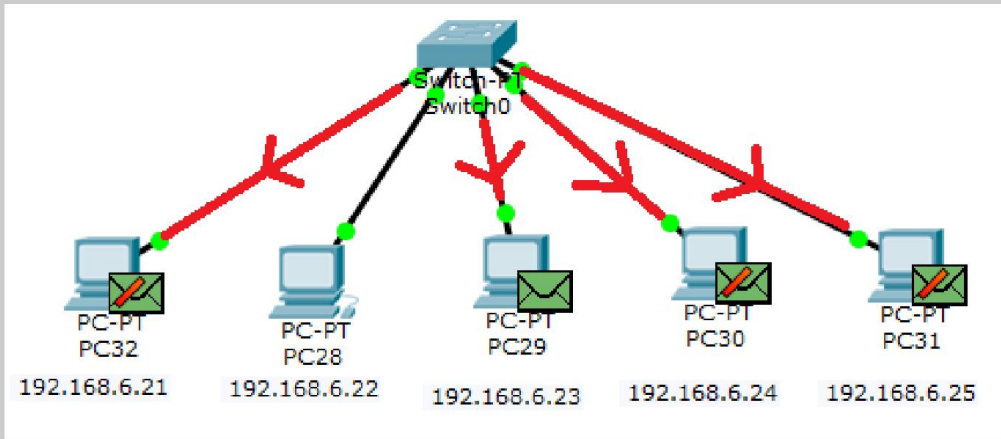
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 0030.A3C6.E1E1 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.6.22, Dest. IP: 192.168.6.23	Layer 2: Ethernet II Header 0030.A3C6.E1E1 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.6.22, Dest. IP: 192.168.6.23
Layer 1: Port FastEthernet1/1	Layer 1: Port(s): FastEthernet0/1 FastEthernet2/1 FastEthernet3/1 FastEthernet9/1

1. FastEthernet1/1 receives the frame.



Comme le switch reçoit une adresse MAC de diffusion de broadcast, il va envoyer la demande sur tous les ports connectés (hormis celui qui a fait la demande).

Tous ces pc sont alors contactés mais seul le pc dont l'IP est bien 192.168.6.23 va traiter la demande. Il s'agit du PC 29 sur l'image.



Le PC29 d'IP 192.168.6.23 renvoie donc un message au switch pour qu'il soit transféré vers le PC d'IP 192.168.6.22 dont il connaît l'adresse MAC puisqu'elle était encapsulée dans le message que le PC29 a reçu. Vous pouvez voir dans la description des transferts qu'il ne s'agit pas d'un message en broadcast mais bien d'un message destiné à un ordinateur en particulier :

The diagram shows the same network setup as above. A packet capture window is open on the switch, displaying the following information:

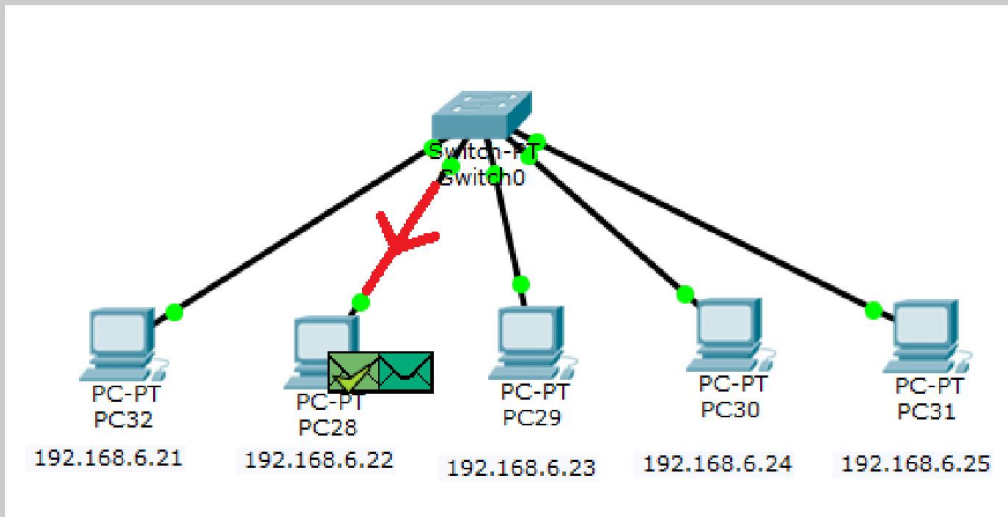
At Device: Switch0  
Source: PC28  
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 000B.BEE7.43CE >> 0030.A3C6.E1E1 ARP Packet Src. IP: 192.168.6.23, Dest. IP: 192.168.6.22	Layer 2: Ethernet II Header 000B.BEE7.43CE >> 0030.A3C6.E1E1 ARP Packet Src. IP: 192.168.6.23, Dest. IP: 192.168.6.22
Layer 1: Port FastEthernet2/1	Layer 1: Port(s): FastEthernet1/1

1. FastEthernet2/1 receives the frame.

Le switch va donc (contrairement au hub) renvoyer le message uniquement au destinataire du message :



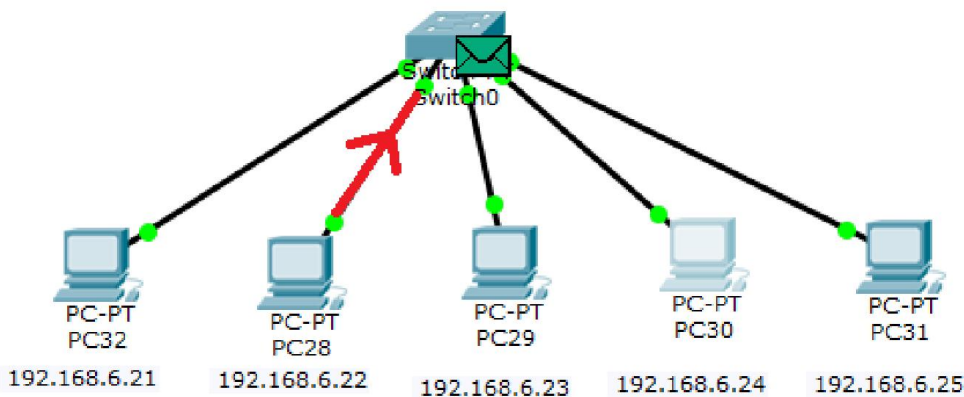


Et maintenant, le PC28 connaît l'adresse MAC du PC29 d'adresse IP 192.168.6.23 !

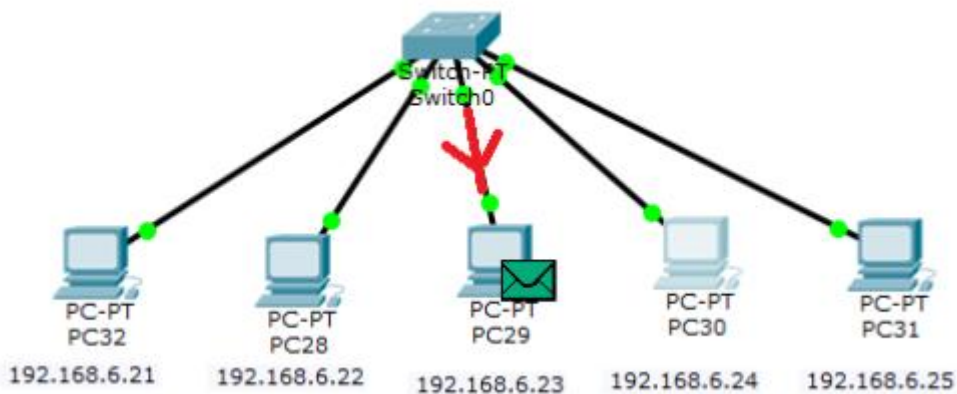
° Utiliser la loupe pour inspecter les tables ARP des différents PC de votre réseau :

Normalement, vous devriez constater que les PC 28 et 29 ont l'autre dans leurs tables ARP.

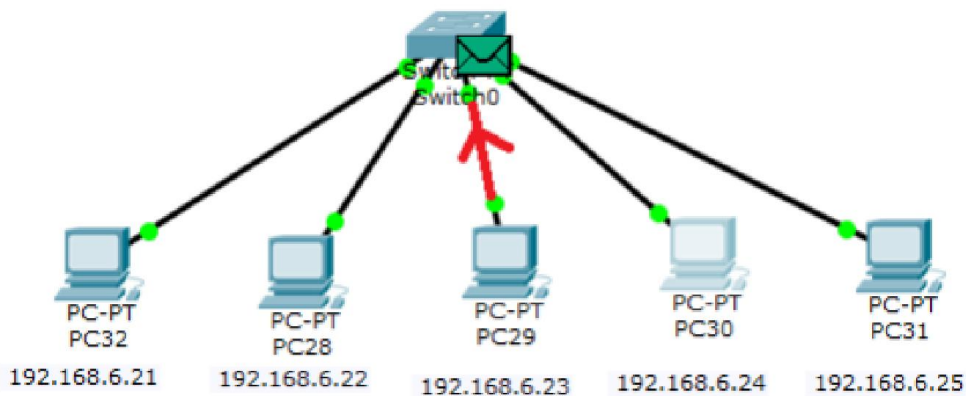
**Etape B** : Le PC 28 revient à son protocole ICMP d'origine : il envoie maintenant un ICMP de type 8 vers l'adresse IP du réseau local et il connaît l'adresse MAC de l'ordinateur destinataire.



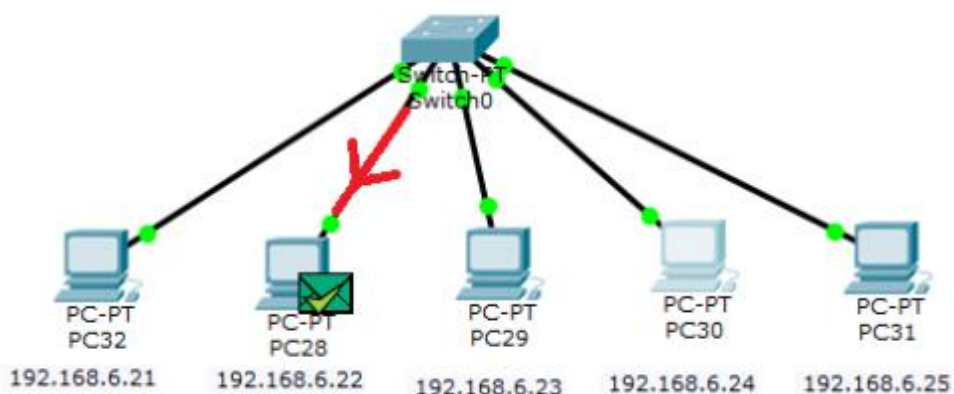
**Etape C** : Le Switch reçoit le message et parvient (contrairement au hub) à rediriger la requête vers le port correspondant à la bonne adresse MAC : le PC29.



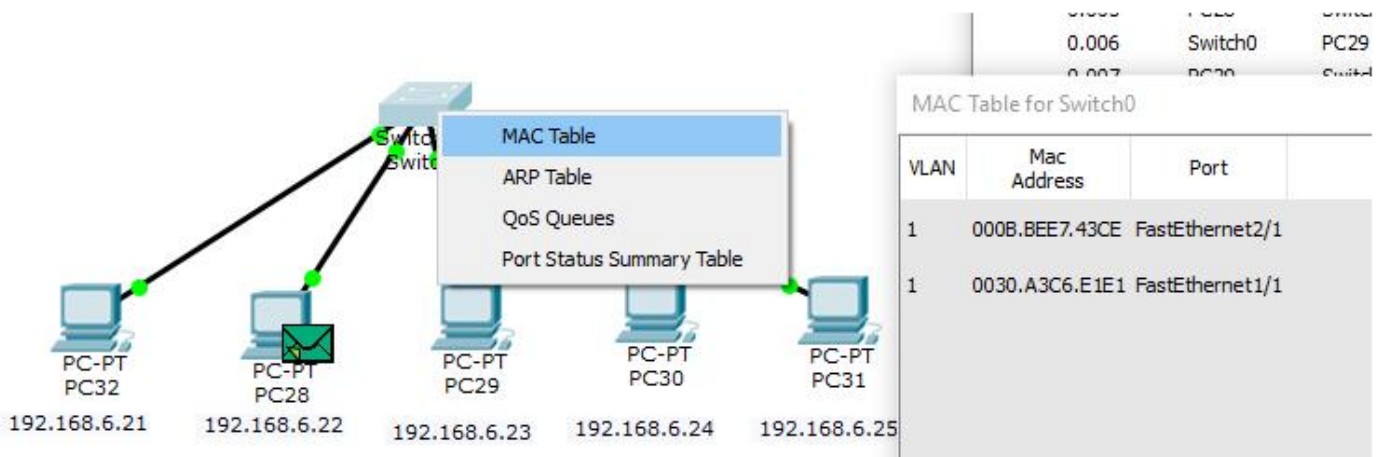
**Etape D** : Le PC29 reçoit la demande ICMP type 8 et renvoie le message ICMP type 0 vers le switch en insérant l'adresse IP et l'adresse MAC du destinataire :



**Etape E** : Le switch transfère vers le bon destinataire car il connaît l'adresse MAC de destination :

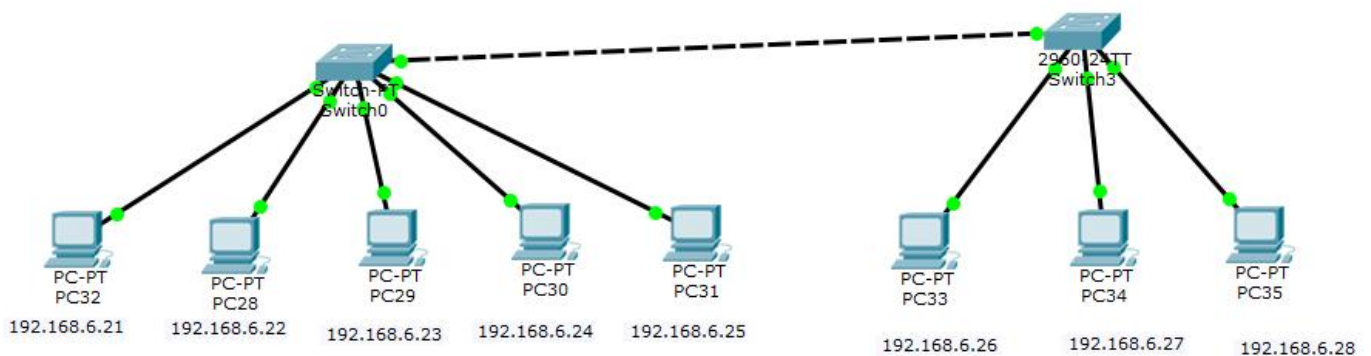


° Utiliser la loupe sur le Switch pour comprendre comment le Switch fait le lien entre l'un de ses ports et une adresse MAC : recherche la table MAC du Switch :



C'est donc le secret du fonctionnement du Hub : pour chacun de ses ports de connexion, il garde en mémoire l'adresse MAC de la carte réseau qui à l'autre bout du fil. Ainsi, contrairement au hub, il n'a pas besoin d'envoyer son message à tous les ordinateurs en espérant que le bon PC détecte que c'est lui qui doit répondre.

petit exercice : configurer le réseau suivant :



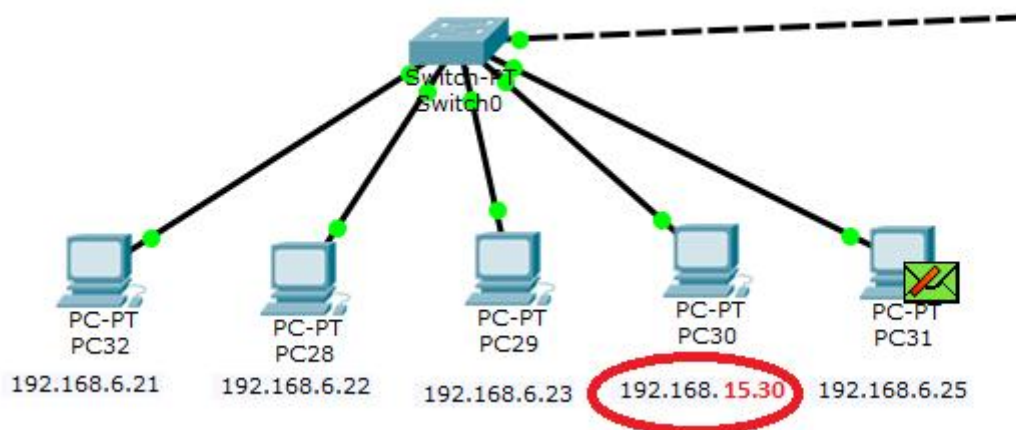
Comme vous pouvez le voir, la liaison entre les deux switches est un câble croisé : c'est normal, les deux switches ont leurs bornes dans le même sens, il faut donc croisé les fils pour qu'une borne d'émission discute avec une borne de réception. En gros.

N'oubliez pas d'éteindre les switches pour rajouter les pc ...

Il ne vous reste plus qu'à simuler les communications entre les pc d'un même switch ou les pcs connectés sur deux switches différents. Commencez par n'observer que le protocole ICMP.

Le protocole STP (Spanning Tree Protocol) est un protocole qui permet d'éviter des chemins bouclés entre deux pc : pour passer de l'un à l'autre, il doit n'y avoir qu'un chemin. Les liaisons sont doublées mais le chemin secondaire ne doit être emprunté que si le chemin principal est hors service. Mettez le de côté pour l'instant.

° Changer le nom d'une des adresses IP. Utiliser plutôt 192.168.15.30 par exemple. Que constatez-vous ? La liaison est-elle encore possible ?



Nous allons voir dans l'activité suivante pourquoi la communication n'est plus possible alors que l'adresse semble finalement assez proche. Cela est lié au masque de sous-réseau.

- **Refaire le même travail (connexion deux lan ) avec les composants suivants :**
  - **Répéteur**
  - **pont**