UTILISER PACKET TRACER

Objectif

Utiliser Packet pour :

- Mettre en oeuvre ses fonctions de base.
- Etudier la commande Ping et les tables MAC sur différents matériels et en utilisant plusieurs méthodes.

Scenario

Deux topologies, une qui utilise un concentrateur (hub) et l'autre qui utilise un commutateur (switch). Ces topologies sont idéales pour étudier ARP (le protocole de resolution d'adresses Ethernet) et ICMP (le protocole de la commande « ping »).

Fichiers nécessaires

- UtiliserConcentrateur.pkt
- UtiliserCommutateur.pkt

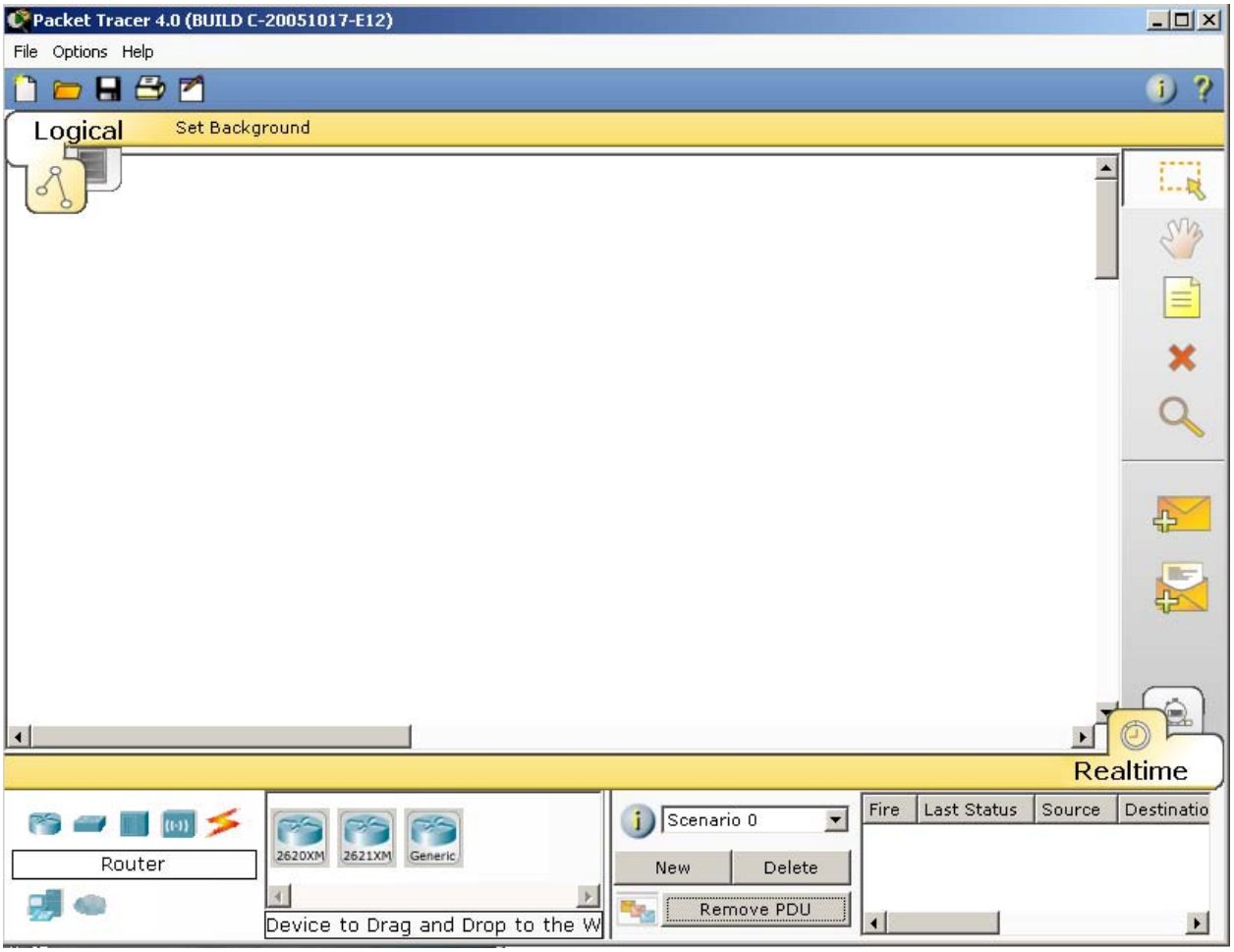
Plan

Introduction.

Packet Tracer est un simulateur de protocoles développé par Cisco Systems. Packet Tracer (PT) met en oeuvre différents protocoles, soit en temps réel, soit en mode simulation. Les protocoles sont de niveau 2 comme Ethernet et PPP, de niveau 3 comme IP, ICMP, ARP, et de niveau 4 comme TCP and UDP. Les protocoles de routage comme RIP peuvent être aussi tracés.

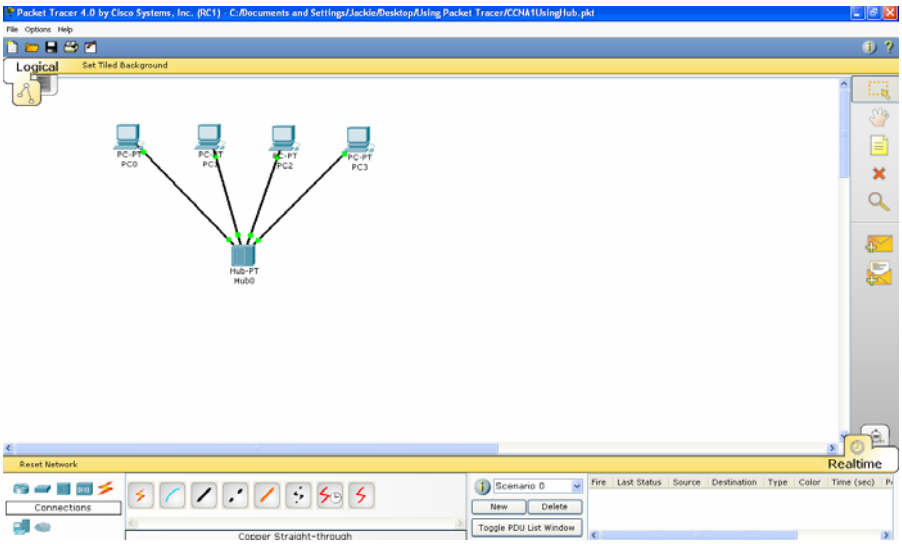
1° partie : Utiliser un concentrateur.

1° étape : Démarrer Packet Tracer et activer le mode simulation



2° étape : Utiliser une topologie existante.

- Cliquer sur le bouton Ouvrir sur la barre d'outils..
- Ouvrir le fichier UtiliserConcentrateur.pkt.



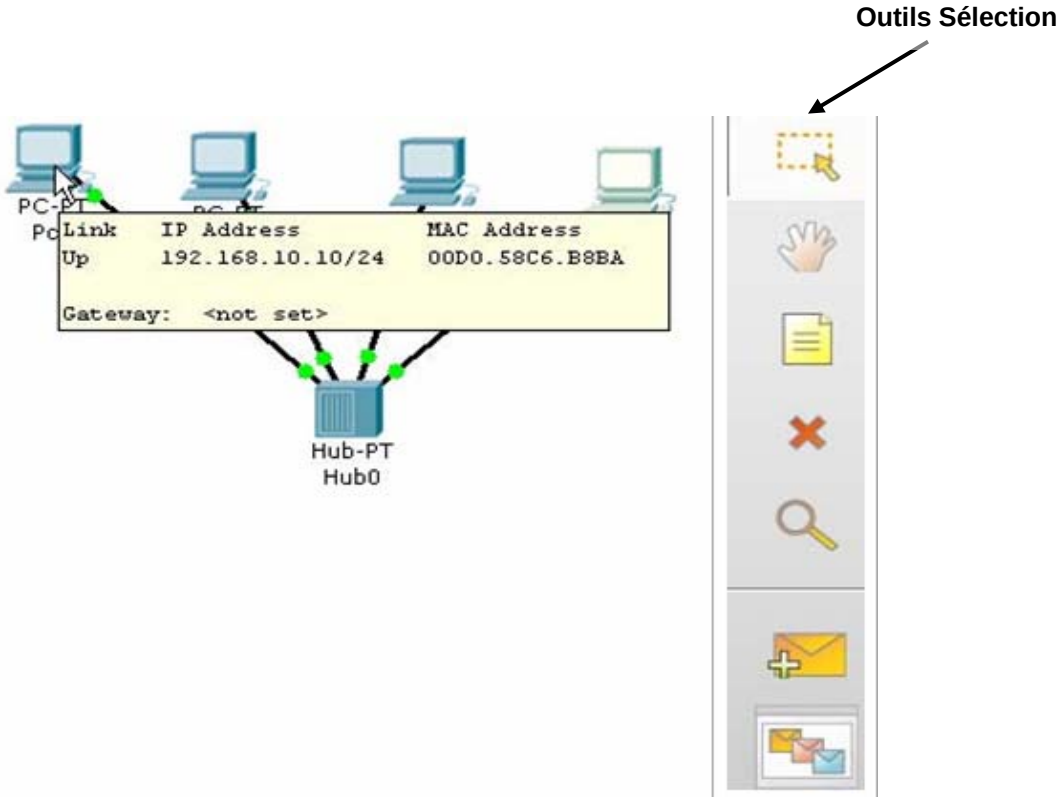
Par défaut, la topologie est ouverte en mode **temps réel**.

Le mode **Simulation** permet de voir une série d'évènements associés à une communication entre deux ou plusieurs matériels.

Le mode **temps réel (Realtime)** fournit cette séquence d'évènements comme en réalité.

L**'aide** (help) peut être obtenue en utilisant le menu Aide. Il y a une aide en ligne et un didactitiel disponibles. Il faut les utiliser.

Pour voir l'adresse IP, le masque de sous-réseau, la passerelle par défaut, l'adresse MAC d'un poste, mettre le curseur de la souris sur l'image d'un hôte. S'assurer que l'outil Sélection est sélectionné.



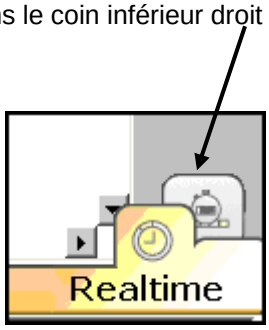
3° étape : Pinguer PC1 à partir de PC0.

La commande Ping génère un paquet IP qui est encapsulé dans un message Echo Request du protocole ICMP. C'est un outil qui permet de tester le niveau 2 et 3 d'un communication entre deux hôtes. Quand un utilisateur emploie la commande ping, la plupart des systèmes d'exploitation envoie quatre ou cinq messages Echo. Quand l'hôte de destination a reçu le message Echo Request, il envoie un message Echo Reply.

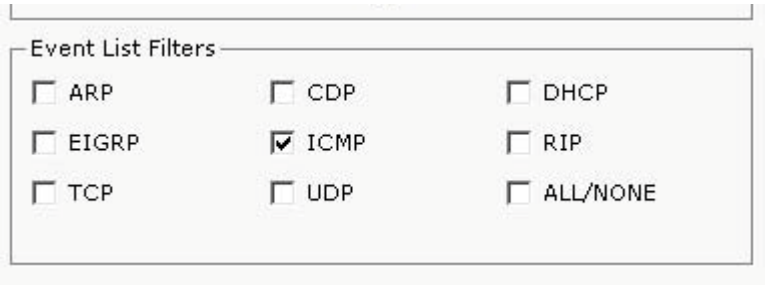
La commande à taper sur PC0 est : **ping 192.168.10.37**

Packet Tracer permet soit d'utiliser la commande dans une console, soit d'utiliser l'outil "Add Simple PDU". Nous allons mettre en œuvre les deux méthodes.

Pour entrer en mode simulation, cliquer sur l'onglet "Simulation Mode", dans le coin inférieur droit de la fenêtre.



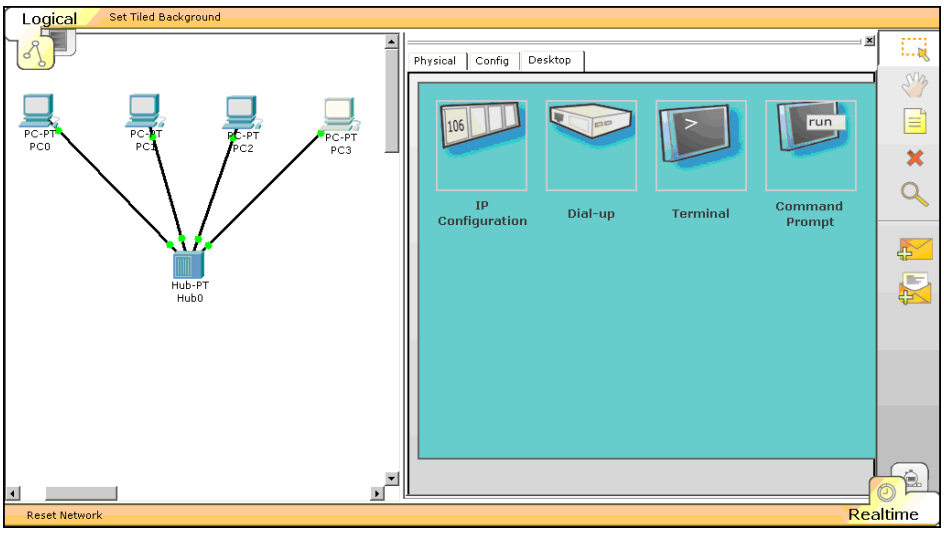
De façon à ne voir que les “pings”, dans **Event List**, cliquer sur **ALL/NONE** pour effacer tous les protocols, puis cliquer sur **ICMP** pour sélectionner ce protocole seulement.



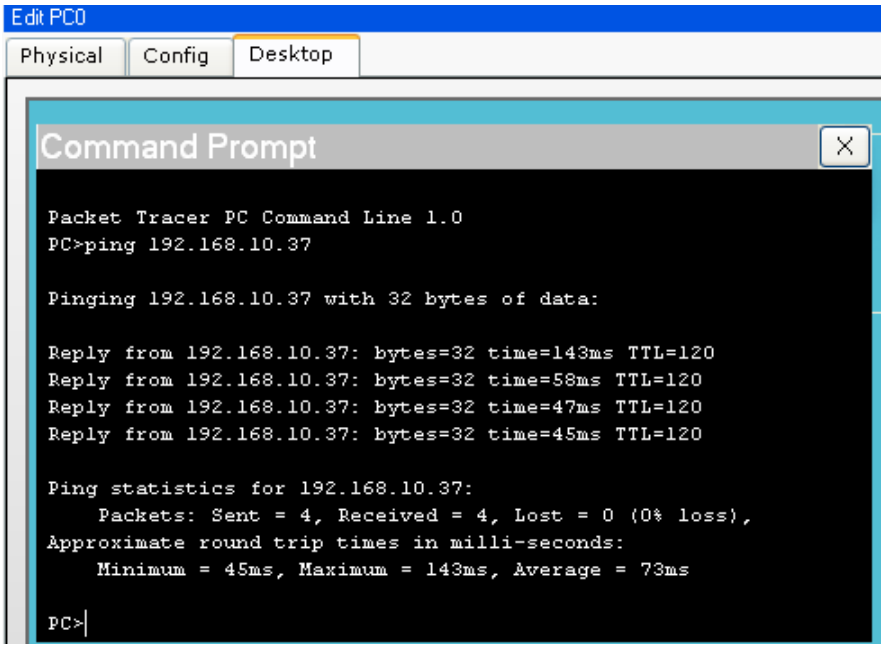
Ping: Utiliser la ligne de commande en mode reel

Retourner en mode reel en cliquant sur l'onglet "Realtime" dans le coin inférieur droit de l'écran.

1. Faire un simple clic sur **PC0** avec le bouton gauche de la souris.
2. Cliquer sur l'onglet **Desktop**
3. Cliquer **Command Prompt**.



Cliquer après l'invite de commandes **PC**, taper **ping 192.168.10.37** puis valider.

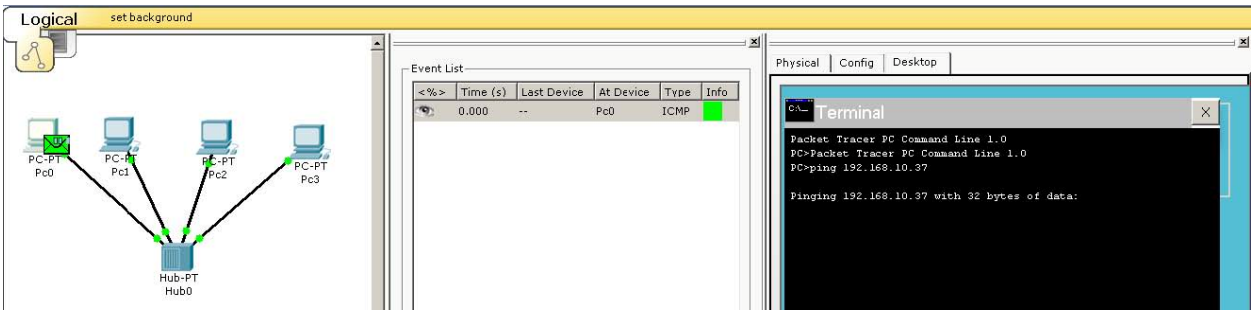


Ping: Utiliser le mode Simulation

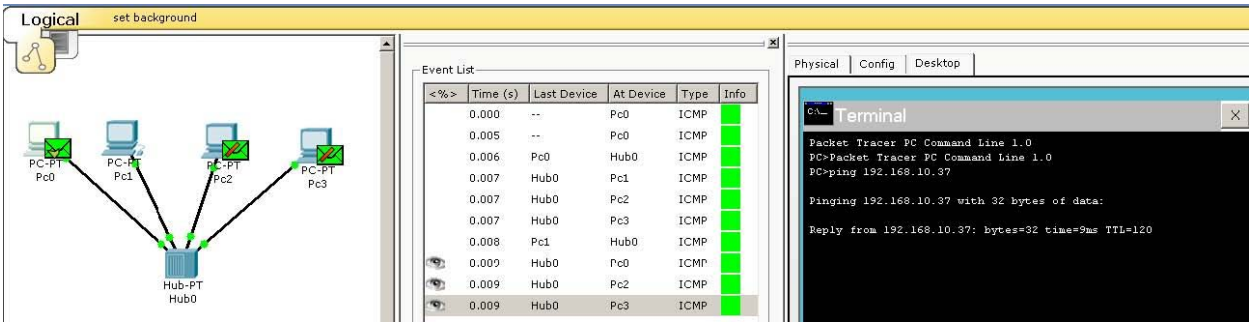
Cliquer sur l'onglet **Simulation** dans le coin inférieur droit de l'écran.

Si la fenêtre de la topologie n'est pas visible, fermer celle de la liste d'évènements.
Taper de nouveau la commande ping dans un **Terminal** (frapper la touche flèche haut pour répéter la dernière commande).

Un paquet ICMP est maintenant prêt à quitter PC0 (écran gauche) et c'est visible aussi sur l' **Event List** (écran du milieu).



Pour voir l'exécution pas à pas de la commande ping, cliquer sur le bouton **Capture / Forward** dans **Play Controls (la barre jaune sous la fenêtre)**.
Cliquer sur chaque évènement pour noter comment le concentrateur traite chaque trame (trame Ethernet , paquet IP , and message ICMP). Remarquer que chaque évènement est lister dans la fenêtre **Event List**. Remarquer également que la commande ping affiche le "Echo reply" du protocole ICMP retourné par PC1 à PC0.



Continuer à cliquer le bouton Capture / Forward button jusqu'à ce que toutes les trames soient expédiées. ***Noter que le concentrateur diffuse la trame sur tous ses ports à l'exception du port par lequel elle est entrée.***

Quand la commande ping est totalement exécutée, en envoyant quatre "Echo Request", on reçoit le message suivant :

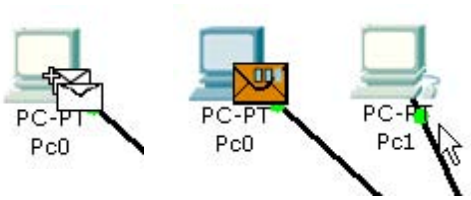
Utiliser l'outil "Simple PDU"

Une autre méthode pour pinguer un hôte est d'utiliser l'outil **Simple PDU**. Cet outil founit le ping sans avoir besoin de taper la commande. Avant d'en arriver à ce stade, fermer la bureau (Desktop) de PC0 en cliquer sur "**X**" dans le coin supérieur droit.

Afficher si nécessaire l' **Event List**, en cliquant "Event List" sur la barre jaune à gauche et cliquer sur le bouton **Reset Simulation**.

Choisir l'outil **Add Simple PDU** dans la boite à outils :

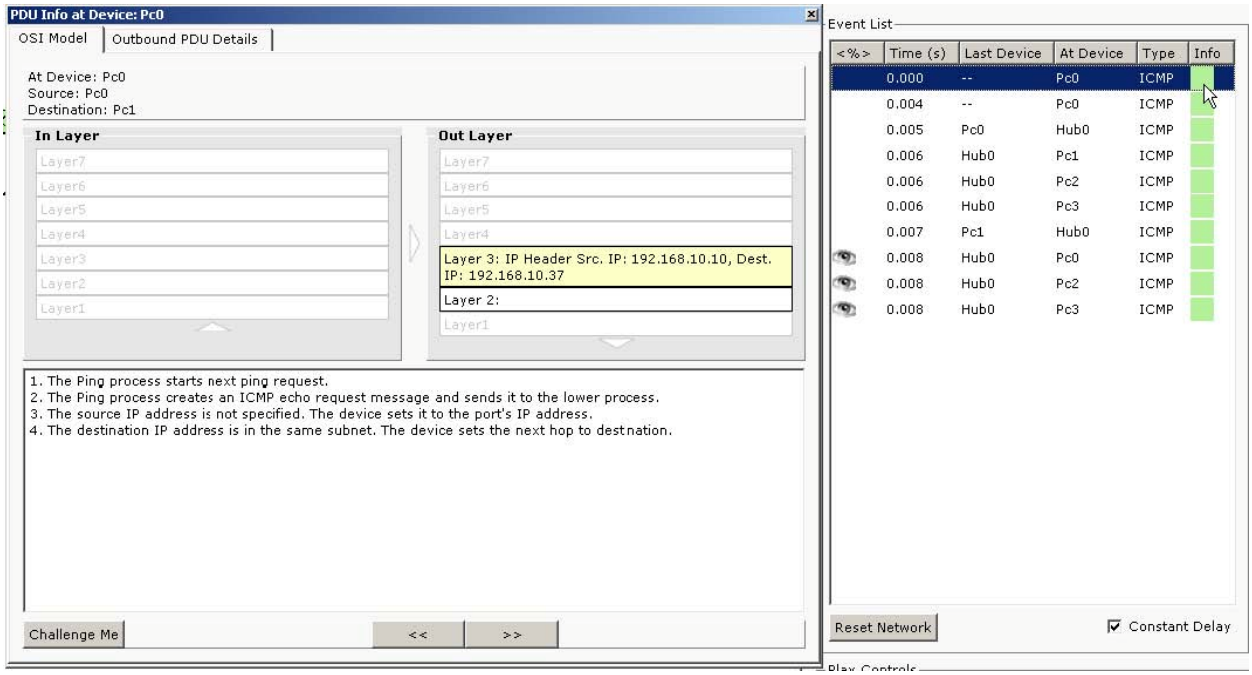
Cliquer un fois sur PC0, l'hôte qui expédie le ping (ICMP Echo Request), puis cliquer une fois sur PC1(la destination de l' ICMP Echo Request).

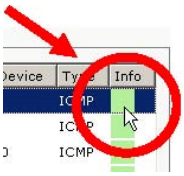


Cliquer le bouton Capture / Forward et regarder l' "Echo Requests" et l' "Echo Replies"du protocole ICMP.
Remarque : Cet outil expédie un seul "Echo Request" au lieu de quatre, en utilisant la commande ping dans une console.

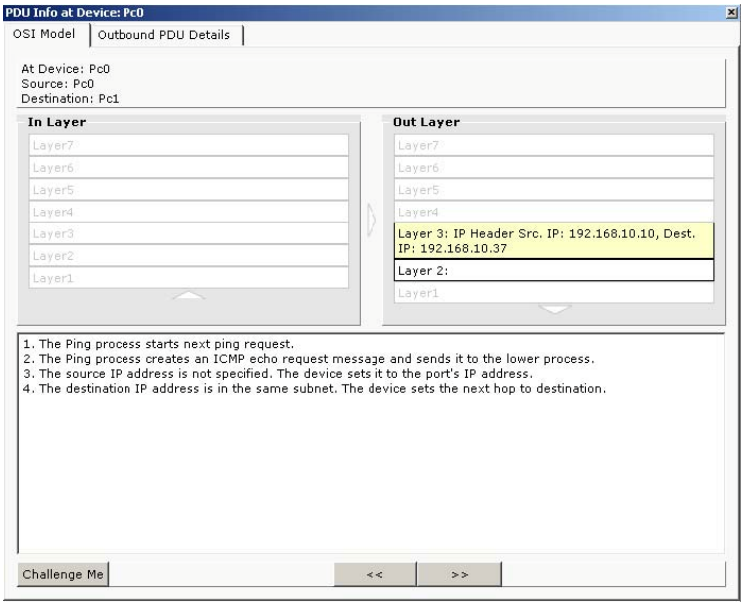
4° étape : Voir une trame en utilisant l'analyseur de protocole.

Pour examiner le protocole qui est en train d'être utilisé, cliquer sur la boite **Info** de couleur dans l' **Event List**.

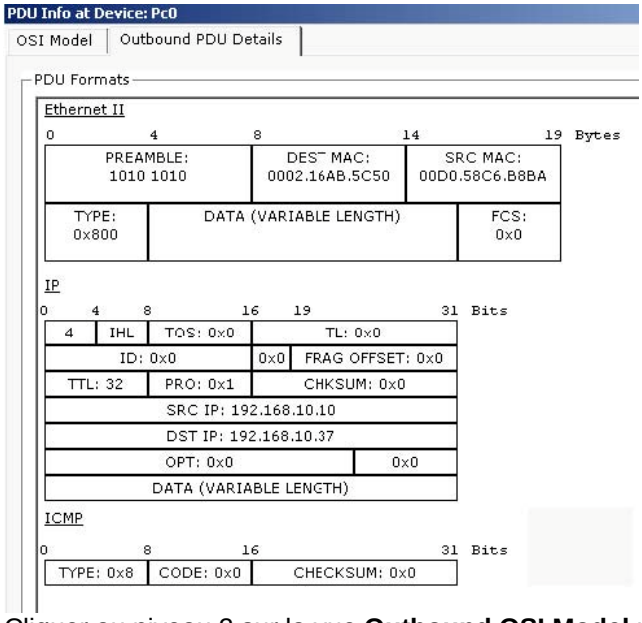




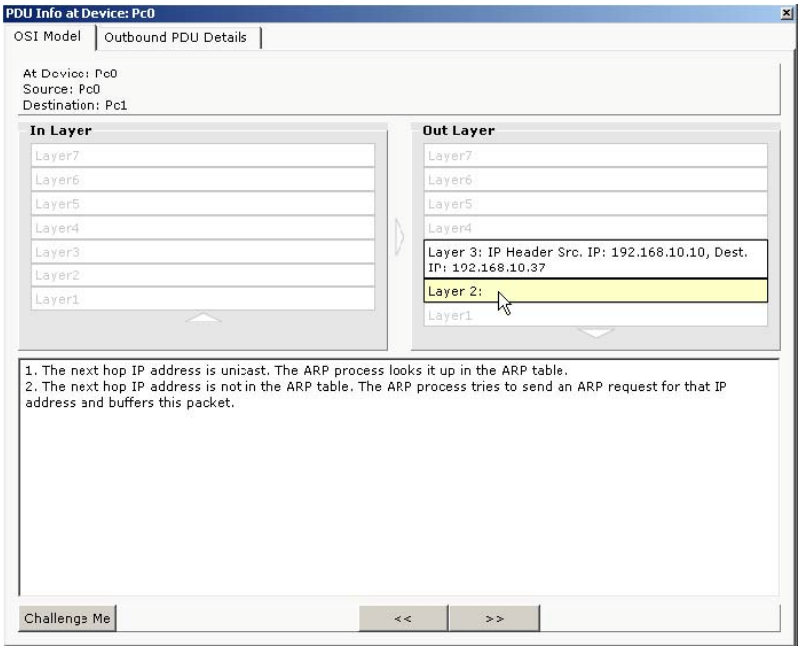
Par défaut, c'est le niveau 3 du modèle OSI qui est vu avec une description succincte du paquet :



Cliquer sur l'onglet **Outbound PDU Details** pour voir la trame Ethernet de niveau 2, le paquet IP de niveau 3 et le message ICMP.



Cliquer au niveau 2 sur la vue **Outbound OSI Model** pour avoir une description brève de ce qui se passé au niveau 2view :



2° PARTIE : Etudier l'algorithme de commutation et la table d'adresses MAC

1° étape :

Ouvrir le fichier **UtiliserCommutateur.pkt**. Ne pas sauvegarder le réseau courant. Le concentrateur de niveau 1 a été remplacé par un commutateur de niveau 2.
Cliquer sur l'icône **Simulation** pour activer le mode simulation.

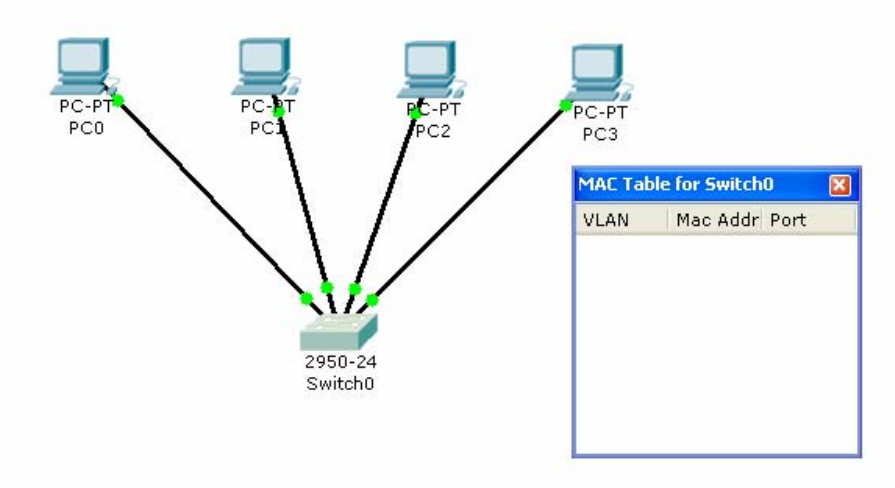
2° étape : Voir la table d'adresses MAC du commutateur.

Utiliser l'outil **Select** pour voir l'adresse IP et MAC pour différents hôtes.

Utiliser l'outil **Inspect** pour voir la table d'adresses MAC du commutateur.

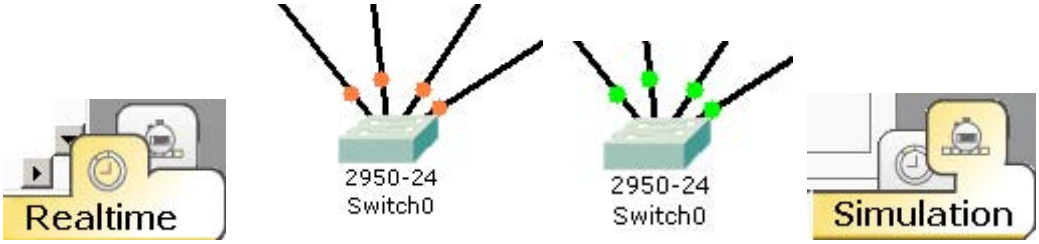
La table d'adresses MAC est vide tant que le commutateur n'a pas appris l'adresse source MAC de la trame Ethernet.

Il y a aussi une colonne VLAN dans cette table qui sera étudiée plus tard.



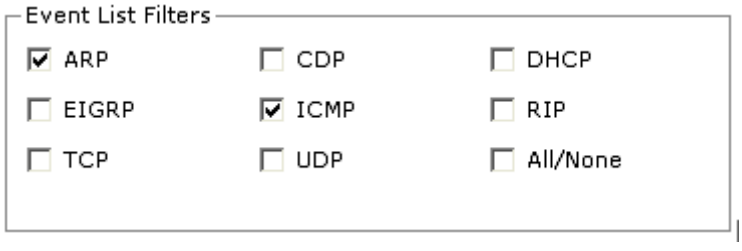
En attente de STP

REMARQUE : Compte-tenu de la manière de traiter le "Spanning Tree Protocol", Packet Tracer met les interfaces du commutateur en rouge en mode réel. Pour corriger cela, cliquer sur l'icône **Realtime** , attendre que la lumière passe au vert, puis cliquer sur l' icône **Simulation**.



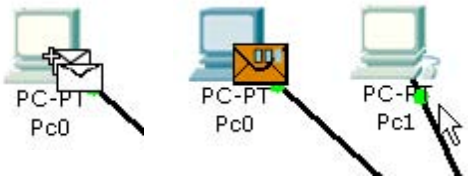
3° étape : Exécuter un ping et voir la table des addresses MAC

Positionner **Event List Filters** de la manière suivante :

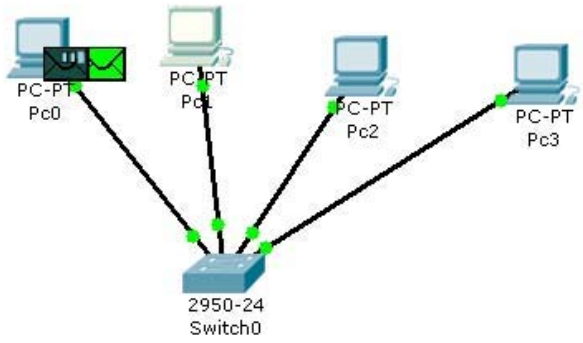


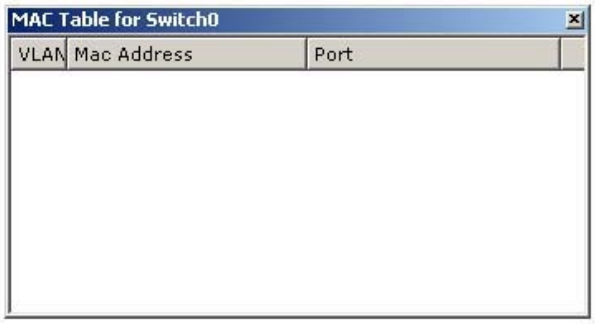
ARP est utilisé pour montrer l'encapsulation d'un paquet IP dans une trame Ethernet. Le paquet ARP précède le paquet ICMP.
ARP is used to learn the MAC address to use to encapsulate the IP packet in an Ethernet frame. The ARP packet will precede the ICMP packet.
Choisir l'outil **Add Simple PDU** dans la boite à outils :

Cliquer sur PC0, l'hôte qui execute le ping (qui expédie un paquet "Echo Request" avec le protocole ICMP) puis cliquer sur PC1 qui est la destination de l' "Echo Request".

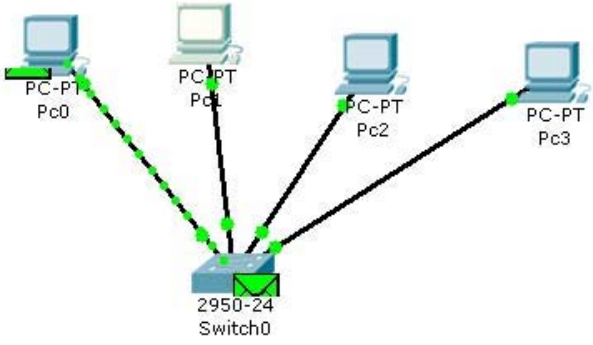


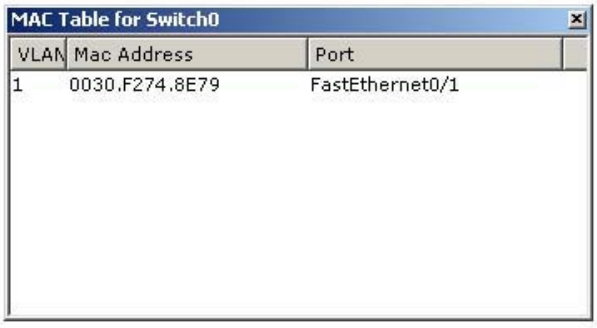
Réaliser une simulation en utilisant le bouton **Capture / Forward**.
PC0 transmet la trame qui contient la requête ARP au Switch0 :



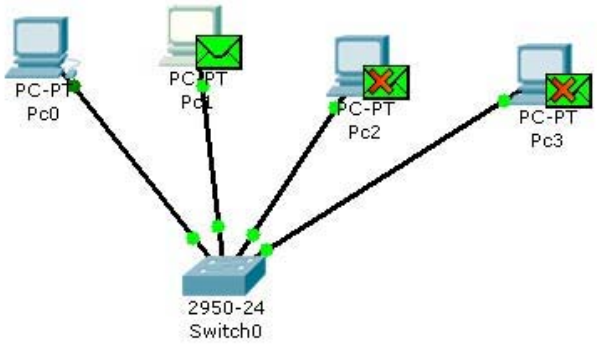


On peut remarquer que le commutateur apprend l'adresse source MAC de la trame :





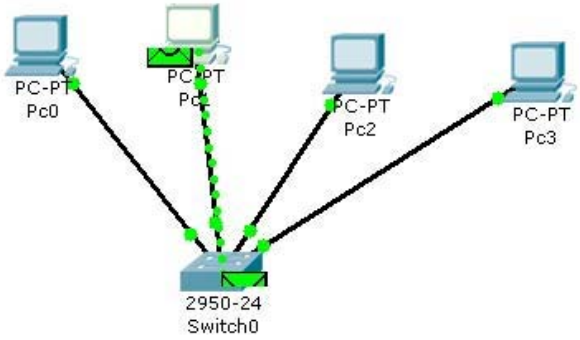
The packet is flooded out all ports because the Switch's MAC Address Table does not contain the Destination Address of the Ethernet frame. PC2 and PC3 disregard the frame:



MAC Table for Switch0

VLAN	Mac Address	Port
1	0030.F274.8E79	FastEthernet0/1

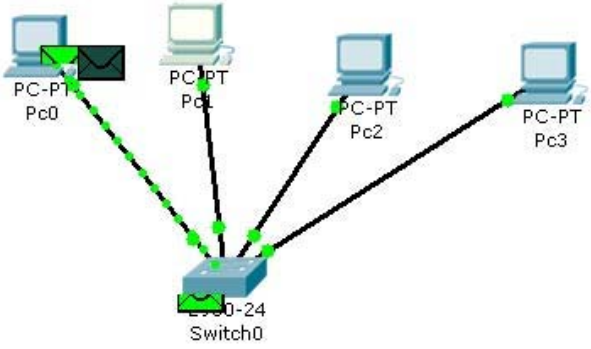
PC1 retourne la réponse ARP. Switch0 apprend l'adresse source MAC de PC1:



MAC Table for Switch0

VLAN	Mac Address	Port
1	0001.C798.4163	FastEthernet0/2
1	0030.F274.8E79	FastEthernet0/1

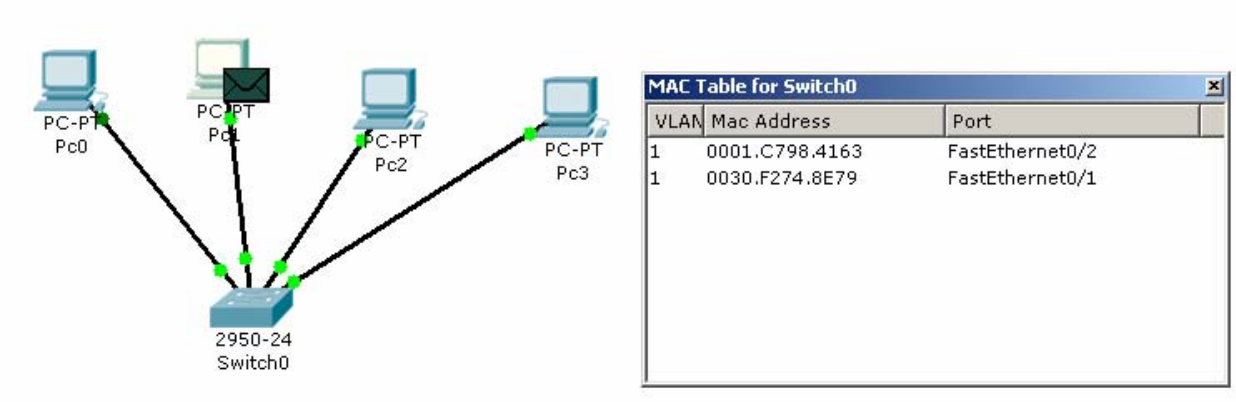
C'est parceque l'adresse MAC de PC0 a été apprise précédemment, que le Switch0 filtre la trame en l'expédiant uniquement sur le port 0/1 FastEthernet.



MAC Table for Switch0

VLAN	Mac Address	Port
1	0001.C798.4163	FastEthernet0/2
1	0030.F274.8E79	FastEthernet0/1

Toutes les autres trames liées à la commande ping sont désormais filtrées par le commutateur et directement envoyé sur le port approprié.



4° étape : Créer différents scénarios

La meilleure façon d'apprendre est d'expérimenter. Il vous reste à essayer différents outils, voir plusieurs protocoles et **utiliser l'aide et le didactitiel**.