

Séquence 1 : Introduction et architecture matérielle

Activité 5 : TD/TP Réseaux

1. Activités de TD (à réaliser en autonomie)

1.1 Adressage IP et masque de sous réseau :

Nous avons présenté l'adresse IP dans le cours d'introduction, nous allons désormais introduire la notion de masque de sous-réseau.

Une adresse IP est une double adresse, elle identifie à la fois un réseau et une adresse machine dans ce réseau, mais cette adresse seule ne vaut rien ! car sans le masque, vous ne saurez jamais distinguer la partie réseau et la partie machine de l'adresse. L'adresse IP et le masque sous réseau sont donc liés l'un à l'autre.

Une adresse IPv4 est composée de 4 octets soit 32 bits. La notation couramment utilisée pour représenter ces adresses est notation « décimale pointée » c'est-à-dire elle s'écrit en décimal en séparant chaque octet par des points,

Exemple : 192.168.25.147

L'adresse 10101100 00010000 00000100 00010100 est exprimée en format décimal pointé de la manière suivante : 172.16.4.20

N. B : L'adresse IP est toujours associée à un masque !

Un masque de sous réseau est un séparateur qui permet de distinguer les parties réseau et machine d'une adresse IP.

Comme nous l'avons dit précédemment cette adresse seule ne nous donne pas d'information sur l'adresse réseau ou de la machine.

L'adresse IP est une suite de 4 octets soit 32 bits, chacun de ces bits peut prendre la valeur 1 ou 0, en effet, il nous suffit juste de dire que les bits à 1 représenteront la partie réseau de l'adresse et les bits à 0 la partie machine. Ainsi on fera une association entre une adresse IP et un masque afin de séparer l'adresse IP en deux parties pour identifier à la fois le réseau et l'adresse

Les bits positionnés à 1 dans le masque indiquent la partie réseau de l'adresse.

Par exemple si on associe :

Adresse IP :192.168.25.147

Masque de sous réseau : 255.255.255.0

On peut dire que les 3 premiers octets de l'adresse représentent la partie réseau de l'adresse.

En effet si je transforme le masque en binaire, j'obtiens :

255.255.255.0 = 11111111.11111111.11111111.00000000

On voit bien que les trois premiers octets ne contiennent que des 1 alors que le dernier octet ne contient que des 0.

La définition du masque nous dit donc que les trois premiers octets de l'adresse identifient le réseau.

La partie du réseau de l'adresse est donc : **192.168.25**

La partie machine de l'adresse au sein de ce réseau est donc représentée par le quatrième octet : **147**

Dans cet exemple on remarque que qu'un octet a été réservé pour l'adresse machine ce qui nous donne $2^8 = 256$ adresses disponibles pour les machines sur le réseau **192.168.25**

192.168.25.0 [réservée pour le réseau]

192.168.25.1

192.168.25.2

.....

192.168.25.254

192.168.25.255 [réservée pour le broadcast]

On observe alors que c'est le masque qui détermine le nombre de machines d'un réseau. Ainsi, on verra par la suite qu'on choisit un masque en fonction du nombre de machines que l'on veut installer.

Adresse spécifique :

Il existe des adresses spécifiques au sein d'un réseau, la première adresse d'une plage ainsi que la dernière ont un rôle particulier. La première adresse d'une plage représente **l'adresse du réseau**, celle-ci est très importante car c'est grâce à elle qu'on peut identifier les réseaux et router les informations

d'un réseau à un autre. La dernière adresse est **l'adresse de broadcast** celle-ci permet de faire la diffusion à toutes les machines du réseau. Ainsi quand on veut envoyer une information à toutes les machines, on utilise cette adresse.

Dans notre exemple :

L'adresse du réseau sera la première adresse : 192.168.25.0

L'adresse de **broadcast** est donc la dernière : 192.168.25.255

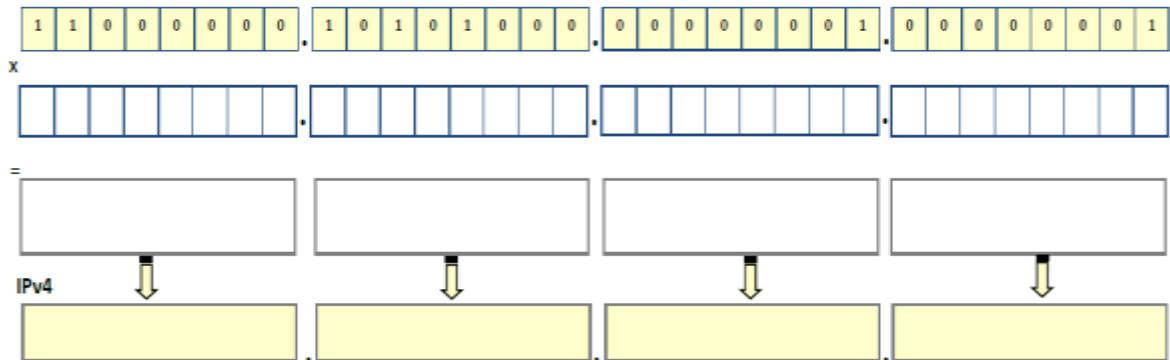
Il nous reste plus que 254 adresses pour identifier nos machines, attention !! Il faudra toujours tenir compte de ces deux adresses ...

1.2 Exercice 1 : Conversion adresse IP binaire/IP décimale pointée

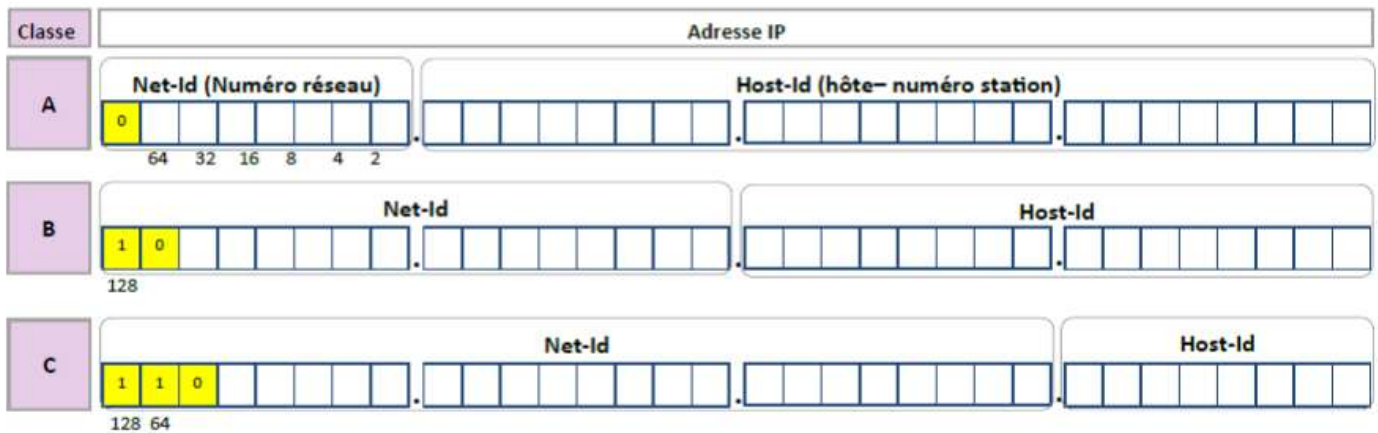
1.2.1 Conversion d'une adresse IP décimale en adresse IP binaire :

Convertir l'adresse 192.168.1.1 en binaire

1.2.2 Conversion de l'adresse IP binaire ci-dessous en adresse IP décimale :



1.3 Exercice 2 : Ecriture des adresses IP Net-Id et Host-Id selon les classes



Ecriture des adresses IP Net-Id et Host-Id selon les classes :

Ecriture IP concernant le Net-Id

Attention : l'adresse Net-Id 127 (de classe A) est inutilisable car c'est une adresse particulière

Classe	Première adresse IP réseau (bits restant Net-Id à 0)	Dernière adresse IP réseau (bits restant Net-Id à 1)	Nombre de réseaux possibles
			Nombre maximal = $2^{\text{nombre de bits}}$
A	1	$2^7 - 2 = 126$ (car 0 et 127 interdits)
B	
C	

Attention : Pour communiquer directement les stations doivent avoir le même Net-Id

Ecriture IP concernant l'Host-Id

Première adresse : tous les bits sont à « 0 » sauf le bit LSB qui est à « 1 »

Dernière adresse : tout les bits sont à « 1 » sauf le bit LSB qui est à « 0 »

Classe	Première adresse	Dernière adresse	Nombre d'hôtes possibles
	IP HOST-ID	IP HOST-ID	Nombre maximal = $2^{\text{nombre de bits}} - 2$ (réseau-broadcast)
A	
B	
C	

Attention : adresse Host-Id avec tous les bits à « 1 » n'est pas utilisable car c'est une adresse de Broadcast

1.4 Parties réseau et hôte

Pour chaque adresse IPv4, **une partie des bits d'ordre haut** représente l'adresse réseau. Au niveau de la couche 3, **un réseau se définit par un groupe d'hôtes** dont la partie adresse réseau de l'adresse contient **la même configuration binaire**.

Bien que l'ensemble des 32 bits définisse l'adresse IPv4 d'un hôte, un nombre variable de bits constitue la partie hôte de l'adresse. Le nombre de bits contenus dans la partie hôte détermine le nombre d'hôtes possible sur un réseau.

Par exemple, si un **réseau particulier** doit contenir au **minimum 200 hôtes**, il faut utiliser suffisamment de bits dans la partie hôte pour **pouvoir représenter au moins 200 configurations binaires** différentes.


Pour attribuer une adresse unique à 200 hôtes, il convient d'utiliser **le dernier octet dans son intégralité**. Avec 8 bits, nous pouvons obtenir un total de 256 configurations binaires différentes. Nous en déduisons que **les bits des trois premiers octets représentent la partie réseau**.

1.5 Exercice 3 : Comment trouver le numéro d'hôte (ou d'utilisateur)

L'adresse réseau (identifiant réseau) auquel appartient le poste est 172.16.4.0.

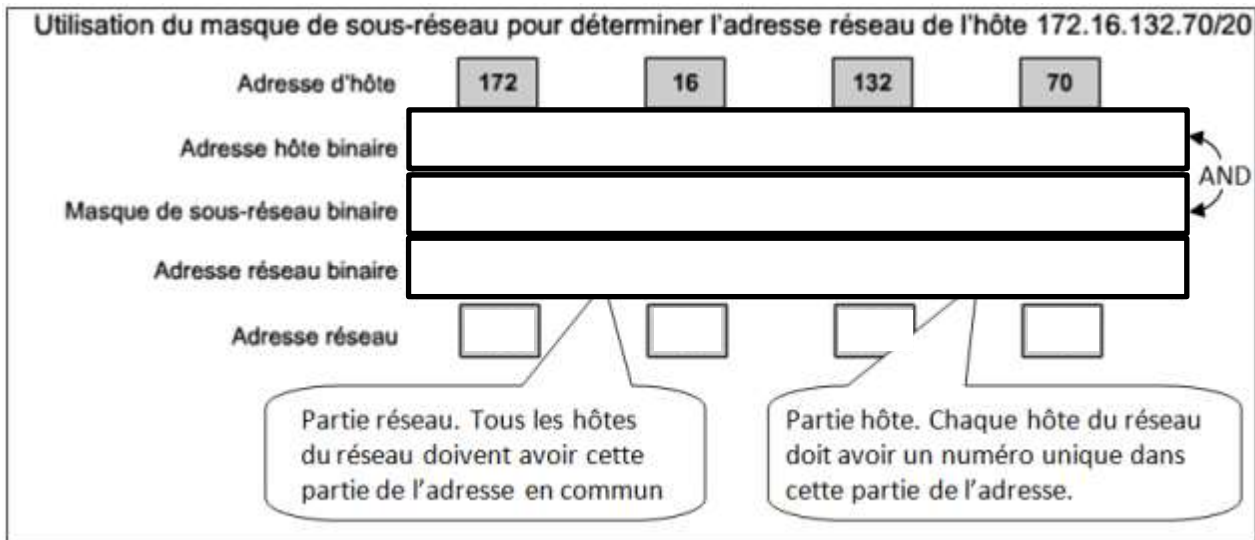
Détermination du numéro de l'hôte : En prenant le complément du masque (inverse logique obtenu avec l'opérateur NON) : **0.0.0.255** et en l'appliquant à l'@IP

1.5.1 Déterminer le numéro d'hôte du poste dans le réseau .

 &	@IP 10101100 . 00010000 . 00000100 . 172.16.4.1 00000001		
Complément du masque			
Résultat & bit à bit			

Le numéro d'hôte de notre poste est :

1.5.2 Déterminer l'adresse de réseau de l'hôte 172.16.132.70/20



1.5.3 Déterminer le numéro de l'hôte 172.16.132.70/20

&	@IP		
	Complément du masque		
	Résultat & bit à bit		

Ce réseau a les caractéristiques suivantes :

Adresse de réseau	172 . 16 . 128 . 0
Adresse du premier hôte	
...	...
Adresse du dernier hôte	
Dernière adresse dans le réseau	

Dernière adresse de réseau = adresse de diffusion

1.6 Exercice 4 :

Un serveur de fichiers a pour adresse IP : **235.198.166.4/24**.

- **L'adresse IP** de ce serveur de fichier est-elle **publique** ou **privée** ?

- **A quel réseau appartient** ce serveur de fichier ?

- Quel est son **numéro d'hôte** dans ce réseau ?

Un serveur WEB a pour **adresse IP : 215.118.106.134/24**.

- **L'adresse IP** de ce serveur de fichier est-elle **publique** ou **privée** ?

- A quel réseau appartient le serveur web ?

- Quel est son **numéro d'hôte** dans ce réseau ?

- Le **serveur de fichier** et le **serveur WEB** appartiennent-ils au **même réseau** ?

- Quels **équipements réseau** sont nécessaires pour qu'ils puissent **communiquer** ?

Une notation est souvent utilisée pour représenter les masques. On la rencontre souvent pour la simple raison est qu'elle est plus rapide à écrire. Cette notation permet d'écrire directement le nombre de bits significatifs en décimal, en considérant que la contiguïté est respectée. Ainsi, pour notre exemple 192.168.25.0/255.255.255.0, on peut aussi écrire 192.168.25.0/24, car **24 bits sont significatifs de la partie réseau** de l'adresse.

De même, les écritures suivantes sont équivalentes :

$10.0.0.0/255.0.0.0 = 10.0.0.0/8$

$192.168.25.32/255.255.255.248 = 192.168.25.32/29$

1.7 Exercice 5 : Adressage IP

Pour les adresses suivantes, donner :

ADRESSE N°1 : 172.24.245.25

ADRESSE N°2 : 212.122.148.49

1/ La classe d'adresse.

2/ Le masque réseau par défaut.

3/ L'adresse réseau.

4/ Le masque modifié si les réseaux comportent respectivement (1) 200 et (2) 20 machines.

5/ L'adresse du sous-réseau et son numéro.

6/ Le numéro de la machine sur le sous-réseau.

7/ Les **intervalles d'adresses utilisables** pour les **trois premiers sous-réseaux**.

1.8 Exercice 6 :

Soit l'adresse IP suivante : 172.16.5.32 /24

1/ Donner le **masque du sous-réseau**.

2/ Ecrire ce **masque en binaire**.

3/ Quelle est la **classe du réseau** ?

4/ Sachant que l'**adresse** de ce **sous-réseau** est **172.16.5.0 /24**, quelle est donc l'**adresse de diffusion (broadcast)** de ce **sous-réseau** ?

1.9 Exercice 7 :

Supposons un réseau IP dont l'adresse est **194.170.25.0**.

Vous avez besoin **d'au moins 20 sous-réseaux** avec **au moins 5 hôtes** disponibles par sous-réseau.

1/ Combien de **bits** devez-vous **emprunter** ?

2/ Quel est le **nombre** de **sous-réseau total** dont vous disposez ?

3/ Combien **d'hôtes** par **sous-réseau** avez-vous ?

2. TP avec Cisco Packet tracer

2.1 Introduction

Pour parvenir à ce que deux ordinateurs échangent des informations, nous allons devoir les relier l'un à l'autre tout simplement. Ainsi, nous créons un réseau informatique constitué de deux machines uniquement. Ce type de réseau est appelé un réseau **peer-to-peer**.

Mais relier un ordinateur à l'autre ne suffit pas afin que ceux-ci communiquent. Chaque ordinateur doit pouvoir être identifié de façon unique sur le réseau.

De la même façon que votre domicile comporte une adresse unique, un ordinateur (ou toute autre machine informatique reliée à un réseau) comporte une adresse **unique**.

Notre premier objectif est de découvrir cette adresse.

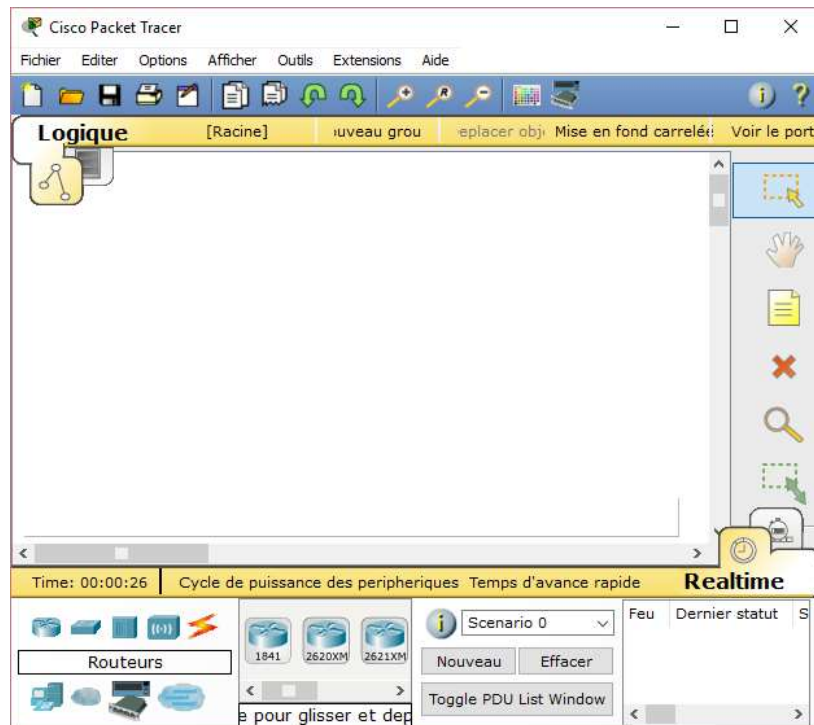
2.2 Simuler une communication entre deux ordinateurs

Afin de découvrir cette adresse et construire notre réseau, nous allons utiliser le logiciel « Cisco Packet Tracer »

Lancez le logiciel en cliquant sur



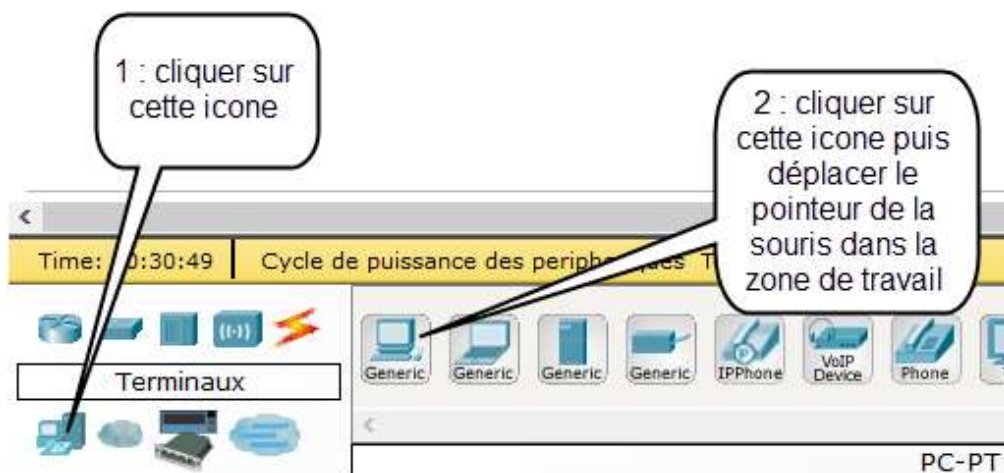
Vous obtenez un écran qui ressemble à :

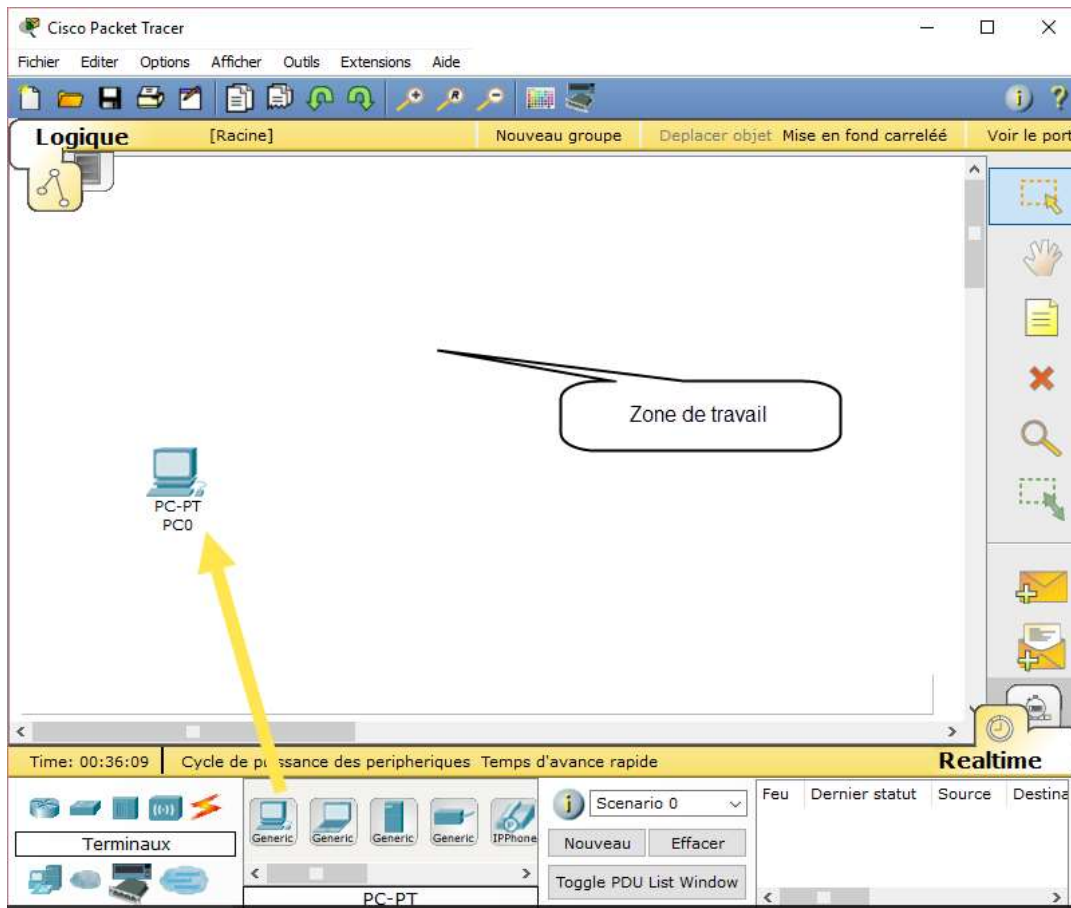


Maintenant, nous allons créer notre réseau « peer-to-peer » constitué de 2 ordinateurs.

Étape n°1 : Insertion d'un terminal dans le réseau

Commençons par insérer dans notre réseau le premier ordinateur en procédant comme ceci :

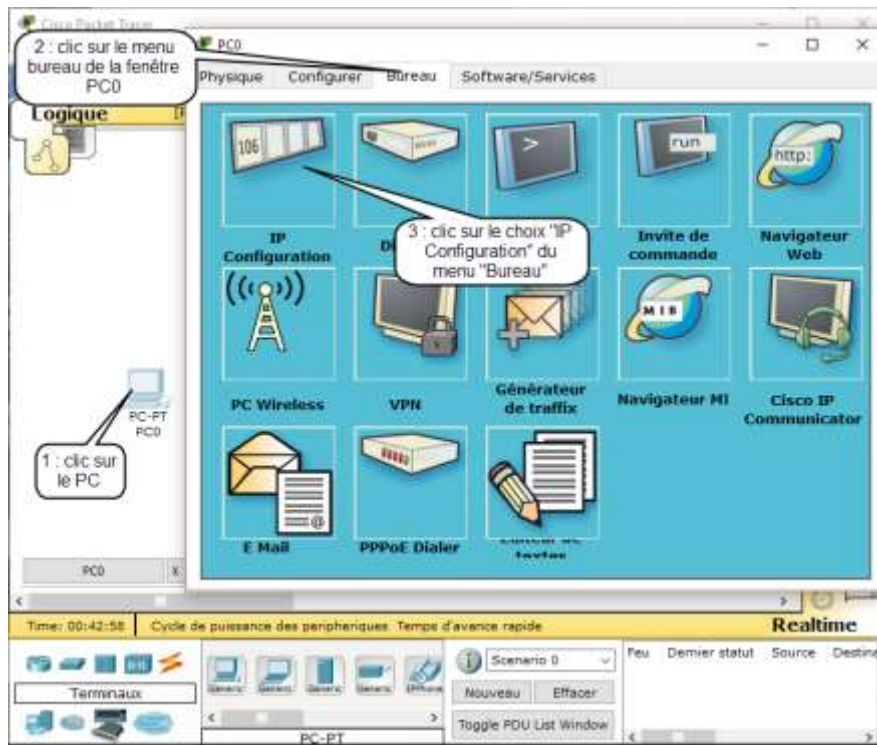




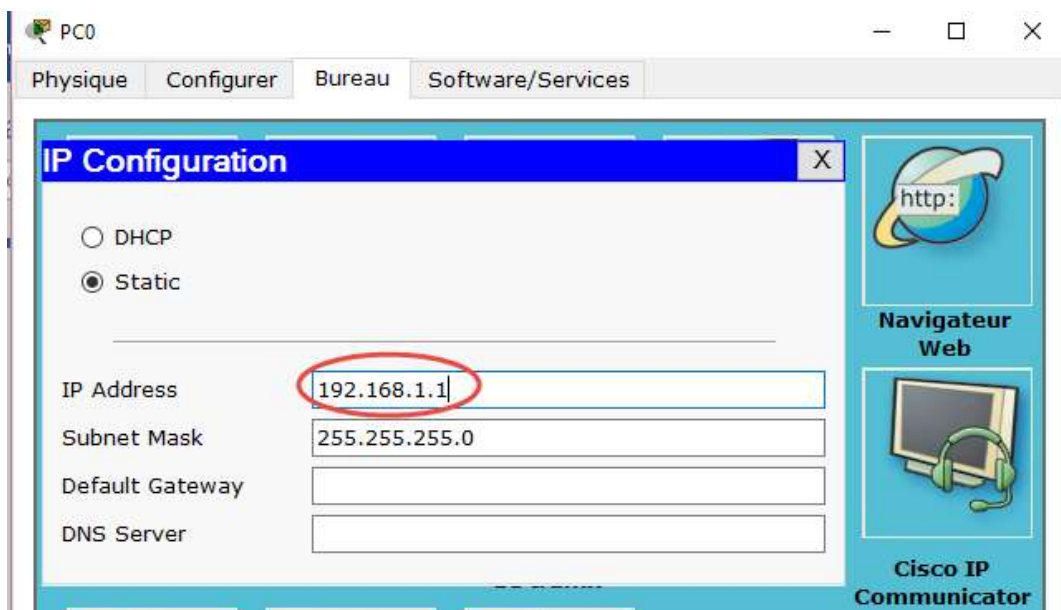
Le premier ordinateur de notre réseau « PC0 » est maintenant positionné. Nous allons maintenant lui attribuer une adresse.

Étape n°2 : Attribution d'une adresse

Pour ce faire, à l'aide de votre souris, vous cliquez sur l'ordinateur PC0 (1 :) puis réalisez les opérations 2 : puis 3 :



Ensuite, vous attribuerez l'adresse « 192.168.1.1 » au PC0 en saisissant cette adresse dans le champ « IP adress » comme ceci :



Puis cliquer « gauche » sur le champ « Subnet Mask » et vous constatez que ce dernier est renseigné automatiquement.

INTERPRETATION :

192.168.1.1 est l'adresse IP affectée au PC0.

IP signifie « Internet Protocol » (Protocole Internet)

255.255.255.0 est le « Subnet Mask » ou « masque de sous-réseau ». Nous avons étudié sa signification au début du TD.

Étape n°3 : Vérification de l'adresse

Nous allons à présent vérifier que nous avons bien affecté une adresse à PC0. Pour ce faire, nous allons activer la fenêtre de commande du PC et saisir la commande « ipconfig ». Voici la manipulation à effectuer :

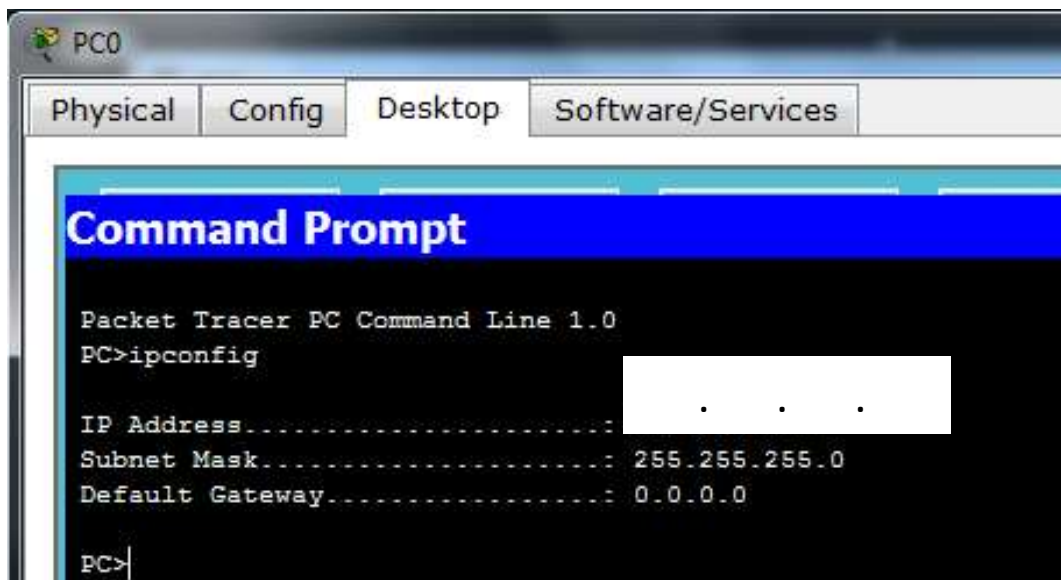
1 : clic gauche de la souris sur le PC0 dans la zone de travail.

2 : clic gauche sur l'onglet « Bureau » de la fenêtre PC0

3 : clic gauche sur l'icône « invite de commande » (command prompt)

4 : au prompt PC>, saisir la commande « ipconfig » puis enfoncer la touche « entrer »

5 : Compléter le champ « IP Adress » ci-dessous :



6 : au prompt PC>, saisir la commande « ipconfig /all » puis enfoncer la touche « entrer »

Une nouvelle adresse apparait. Notez là ci-dessous.

Adresse physique PC0 : _ _ _ . _ _ _ . _ _ _

Il s'agit de l'adresse physique de la carte « réseau » du PC0. On l'appelle communément l'adresse « MAC ».

Définitions :

L'adresse MAC est l'adresse physique unique d'un matériel d'interface réseau. Précisément, il s'agit de la partie qui assure la connexion entre un terminal utilisateur et un réseau. La première moitié de l'adresse MAC indique le constructeur. Ainsi une carte réseau, un routeur, un switch, une Clé USB Wifi ... possèdent une adresse MAC.

À quoi sert l'adresse MAC ?

Uniquement sur le réseau local, l'adresse est transmise à chaque paquet d'information pour faciliter la transmission. Elle peut également permettre aussi de filtrer des accès de tout appareil voulant se connecter dans un réseau.

Étape n°4 : Insertion du deuxième ordinateur puis attribution d'une adresse

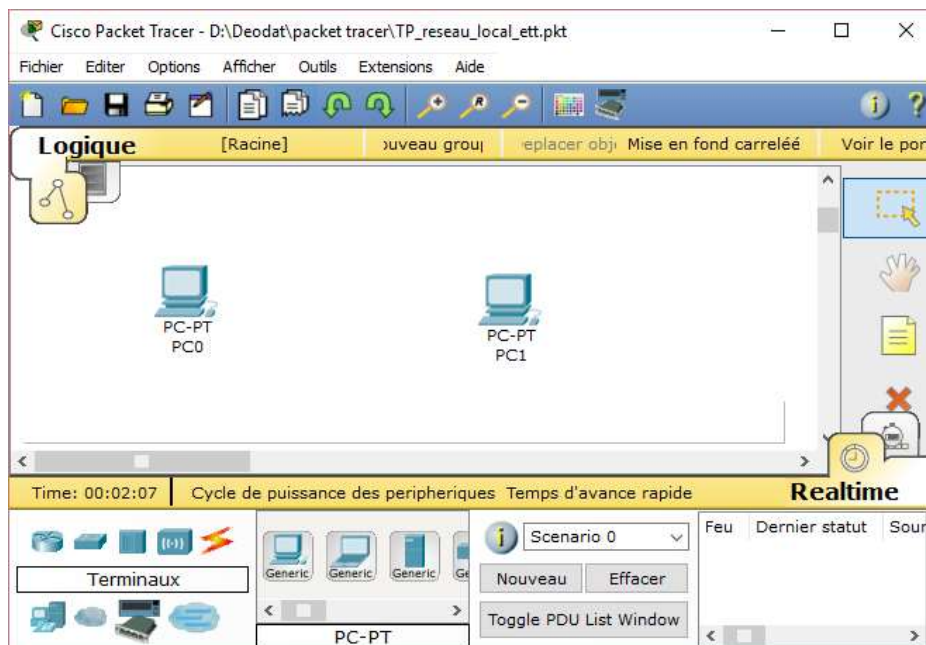
Nous allons maintenant insérer le deuxième ordinateur dans notre réseau. Pour ce faire, vous reprendrez les étapes n°1 et n°2. Vous attribuerez au deuxième ordinateur l'adresse IP 192.168.1.2.

En reprenant l'étape n°3 :

- Vérifier l'adresse IP
- Noter l'adresse MAC ci-dessous :

Adresse physique PC1 : _ _ _ . _ _ _ . _ _ _

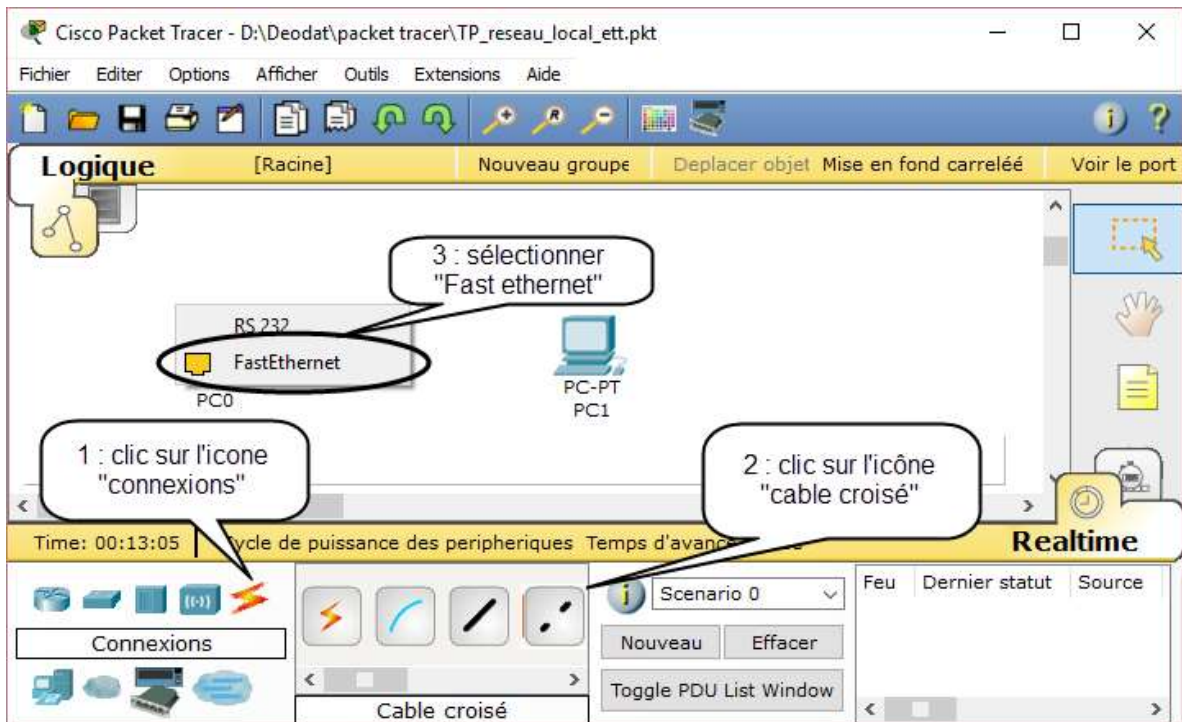
À l'issue de cette étape, vous obtenez l'architecture suivante :



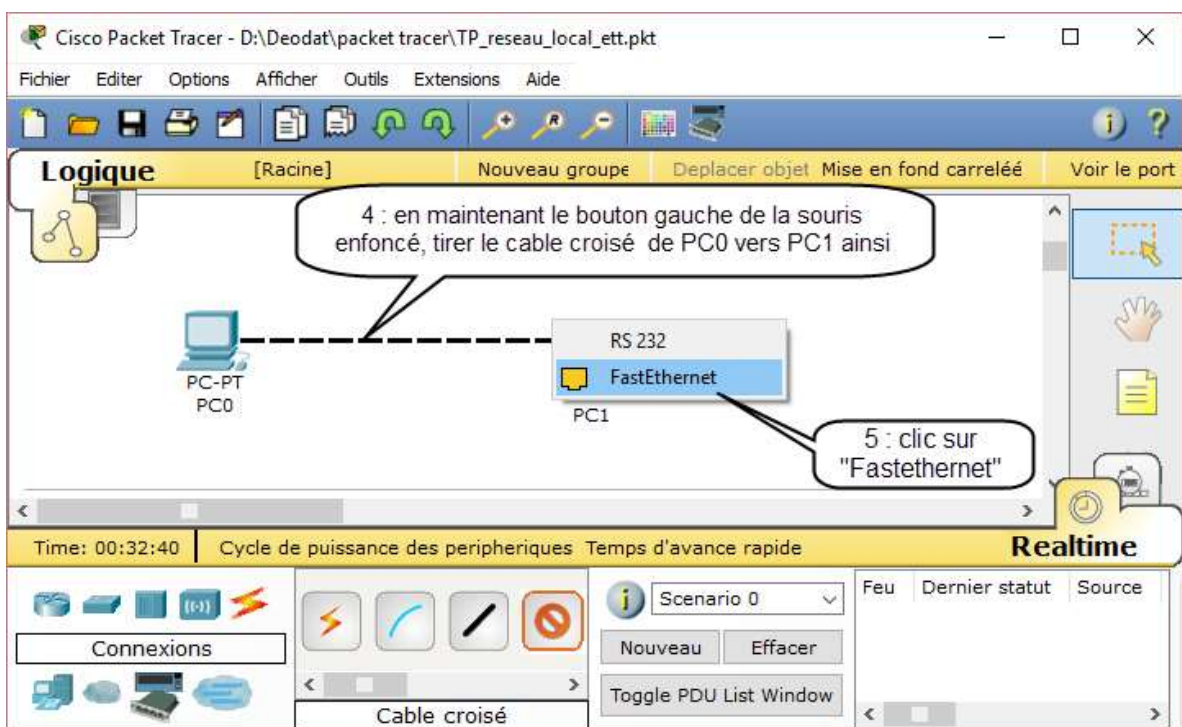
Maintenant nous devons relier les PC l'un à l'autre afin qu'ils puissent échanger de l'information.

Étape n°5 : relier les deux ordinateurs avec un câble

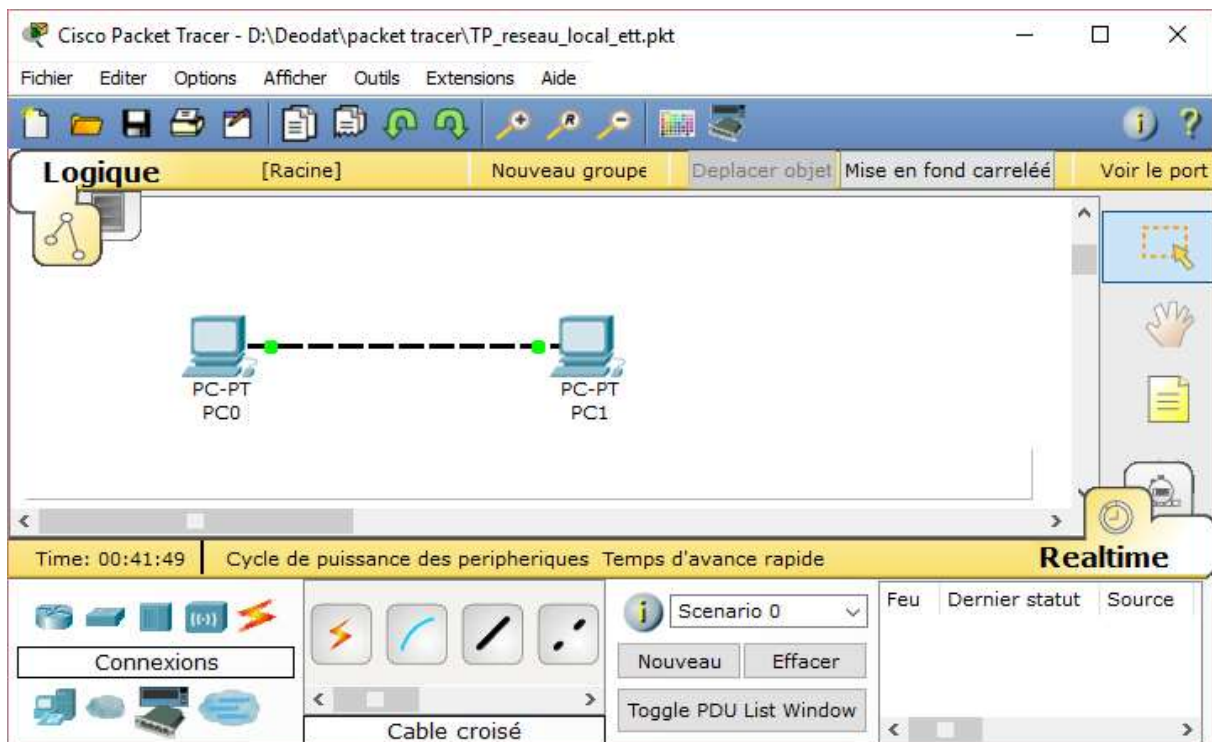
Réaliser les opérations suivantes :



Puis :



Nous obtenons alors un réseau « peer-to-peer » (pair à pair) prêt à fonctionner. Les « points » verts attestent d'une connexion réussie :



Interprétation :

Les postes ont été reliés par un câble. Ce câble sert de support de transmission ou de canal de communication.

Afin de relier des postes directement entre eux (sans utiliser d'éléments matériels intermédiaires), il faut utiliser un **câble réseau croisé** car les deux machines appartiennent à la même catégorie : les PC(s).

Définitions :

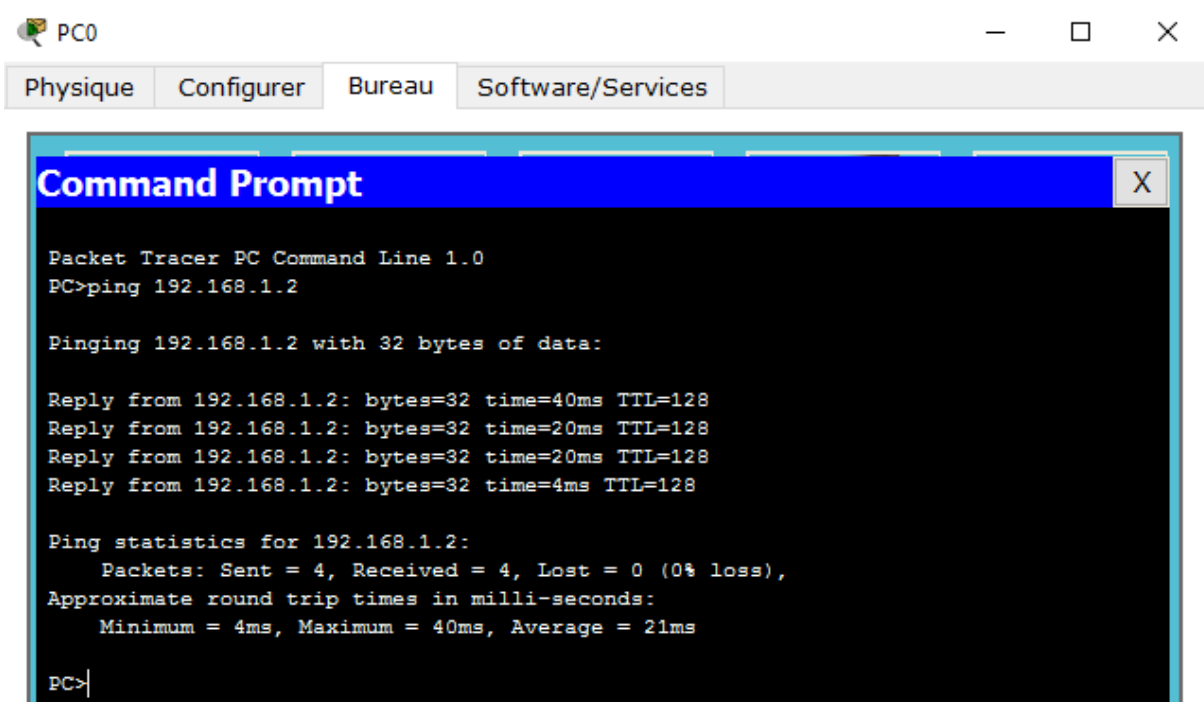
Un réseau Peer-to-Peer (pair à pair) permet de mettre en relation deux ordinateurs clients afin de partager directement leurs fichiers (son, image, données, logiciels) sans passer par un serveur central (qui centralise toutes le données). Le matériel nécessaire est donc minimal.

Nous allons utiliser plusieurs méthodes afin de tester notre connexion.

Étape n°6 : Test de la connexion avec la commande « ping »

Voici la manipulation à effectuer :

- 1 : clic gauche de la souris sur le PC0 dans la zone de travail.
- 2 : clic gauche sur l'onglet « Bureau » de la fenêtre PC0
- 3 : clic gauche sur l'icône « invite de commande » (command prompt)
- 4 : au prompt PC>, saisir la commande « ping 192.168.1.2 ». Vous obtenez le résultat suivant :



Questions (d'après le résultat de la commande ci-dessus) :

Quel ordinateur a joué le rôle de l'émetteur ? :

Quel ordinateur a joué le rôle du récepteur ? :

Quel type d'information les deux ordinateurs se sont-ils échangés ?

Que signifie le terme « Byte » (Aidez-vous d'une recherche « internet » si besoin) :

.....

Dans cette communication, quelle est la taille d'un paquet en bytes ? en octets ?

.....

Quel est le temps moyen pris par l'envoi d'un paquet ?

.....

L'ordinateur récepteur a-t-il reçu toutes les données ?

Dans l'affirmative, quelle information vous le confirme ?

Étape n°7 : Test de la connexion avec l'envoi d'un « PDU »

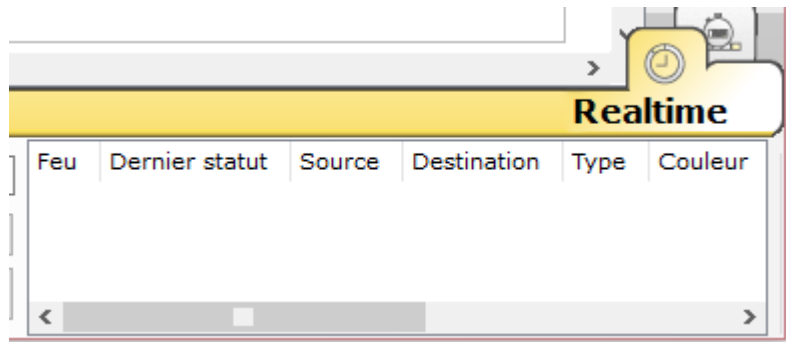
Lorsqu'un ordinateur envoie des données à un autre ordinateur connecté au réseau, on dit qu'il émet un PDU (block of data). Un PDU désigne un bloc d'informations qui circule sur un support de transmission (câble réseau Ethernet, ...).

Le **Protocol Data Unit** ou *Unité de données de protocole (PDU)* est un terme générique qui désigne l'ensemble des informations échangées. Dans le contexte décrit ci-dessous, le PDU constitue le message, c'est-à-dire l'objet de la communication entre les deux PC(s).

Voici la première manipulation à réaliser :

1 : Cliquer sur l'icône « Add simple PDU » 

2 : Cliquer ensuite dans l'ordre sur le poste émetteur de l'information puis sur le destinataire. Cette fois le résultat de l'envoi pourra être lu dans la fenêtre située au-dessous de l'icône « Realtime »



Questions :

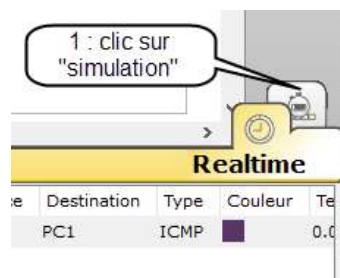
Le PDU a-t-il bien été reçu par le destinataire ?

Quelle information vous permet de le vérifier ?

Avez-vous eu le temps de voir quelque chose ? Pourquoi selon vous ?

Nous allons maintenant réaliser la même manipulation que précédemment mais en mode « Simulation ». Pour ce faire, procéder ainsi :

1 : clic sur l'icône « Simulation »



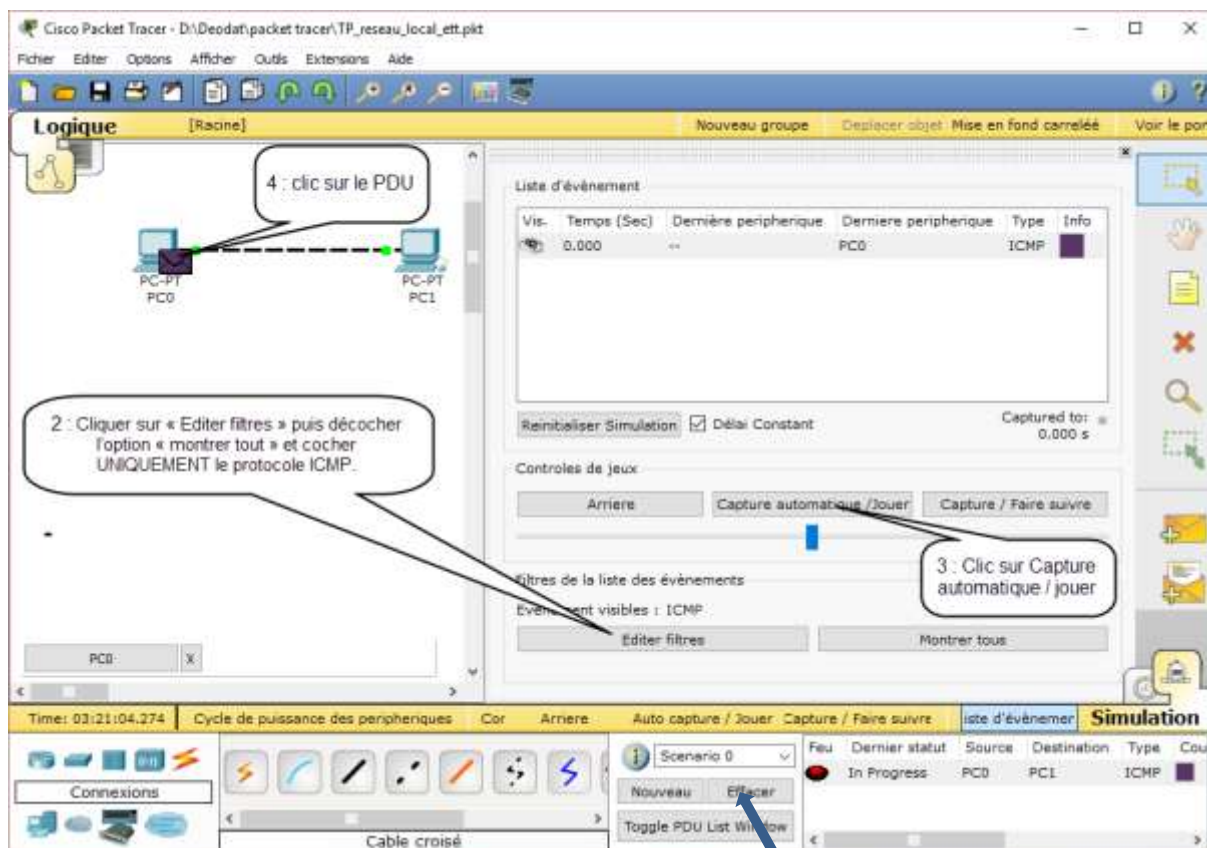
Puis :

2 : Cliquer sur « Editer filtres » puis décocher l'option « montrer tout » et cocher UNIQUEMENT le protocole ICMP



tout » et

3 : Cliquer sur « capture automatique/jouer » et observer l'animation entre les 2 postes. Si vous le souhaitez, vous pouvez réinitialiser la simulation et la rejouer.



Si vous souhaitez rejouer la simulation à partir de zéro, cliquer en bas sur « Effacer » au niveau du « scénario 0 ».

Enfin, L'option « capture/ faire suivre » correspond à un mode « pas à pas » où il faut cliquer à chaque fois pour voir les échanges de données entre les postes.

Questions :

Qu'observez-vous ? Décrivez ce qu'il se passe.

.....

.....

.....

Combien d'échanges y-a-t-il eu ?

.....

4 : Lorsque l'échange est terminé (coche verte clignotante sur l'enveloppe PDU), clic gauche sur le PDU pour l'ouvrir.

