

1^{er} master IDO.

MODULE: systèmes organisationnels.

TP - RÉSEAU LAN - PARTIE 1

Contenu :

- 1-Packet Tracer
- 2-Liaison directe
- 3-Couches matérielles
- 4-Hub
- 5-Switch

La simulation permettra de réaliser facilement certaines opérations sans risque et surtout très rapidement.

Lancer une recherche sur **Cisco Packet Tracer** et s'inscrire sur le site. Cela vous permettra de télécharger les dernières versions et surtout de les utiliser : il faudra vous identifier pour utiliser le logiciel.

Il existe une version 32 bits et une version 64 bits. Pensez à vérifier la configuration de votre système : dans paramètres, chercher système puis informations système.

Il vous faudra une adresse email sur laquelle vous pouvez répondre pour valider votre inscription. Vous trouverez sur leur site une multitude de documentations (en français) et de vidéos (en anglais). Si vous vous rendez compte que les réseaux vous passionnent, c'est le site où vous rendre.

Lien :

<https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html>

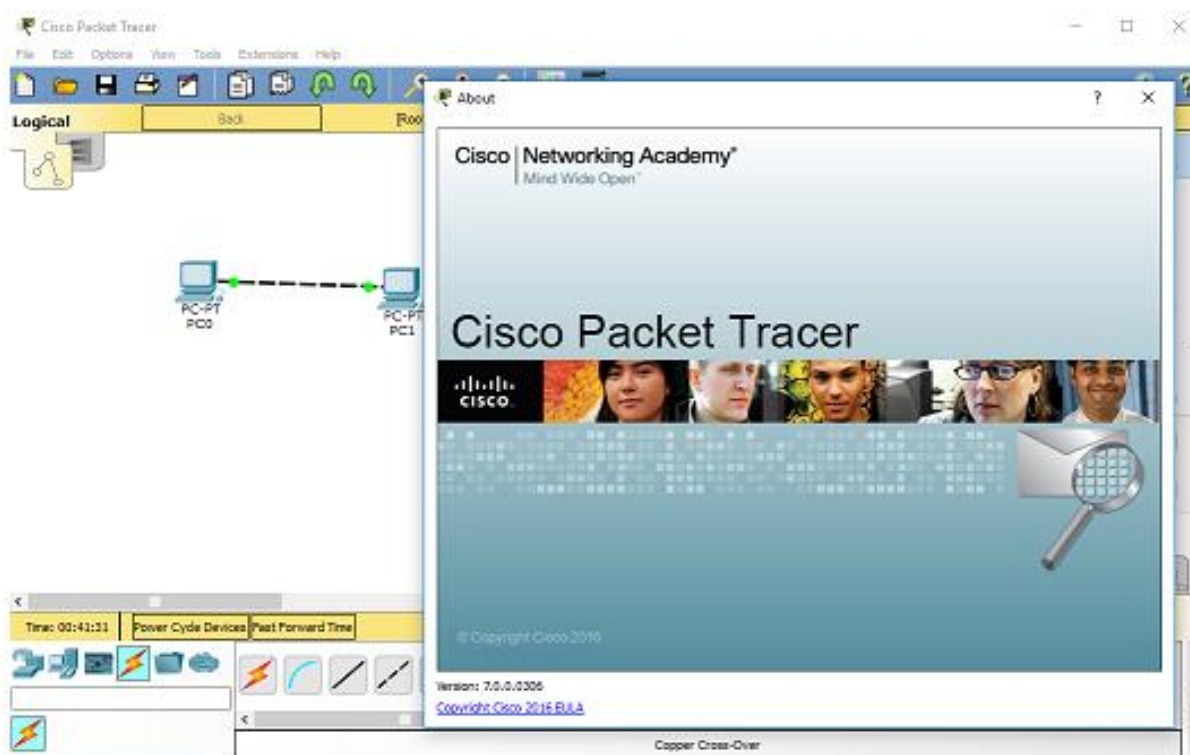
<https://www.filehorse.com/download-cisco-packet-tracer-64/>

Liens vidéo pour introduction à packet tracer :

<https://www.youtube.com/watch?v=meWVYGfQHnI>

<https://www.youtube.com/watch?v=VqMeJ-WH4E0>

° Installer puis lancer le logiciel pour vérifier qu'il fonctionne.



2 - LAN : LOCAL AREA NETWORK EN LIAISON DIRECTE ENTRE DEUX TERMINAUX

Un LAN est un petit réseau local dont les différentes machines sont géographiquement proches.

Les machines d'un même LAN peuvent communiquer entre elles sans passer par Internet.

un réseau local dans sa version minimaliste est un ensemble :

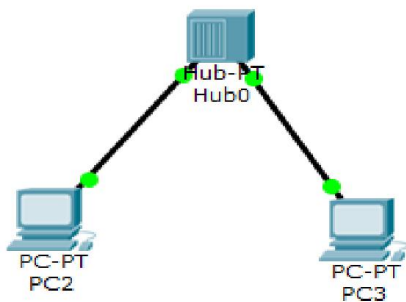
- Des **données** qu'on veut faire transiter et partager
- Des équipements **terminaux** munis d'une carte réseau (ordinateurs, imprimantes...)
- Des équipements de **transfert** permettant la communication entre les terminaux (hub, switch...)

- Des **protocoles** de communication permettant aux appareils de se comprendre (leur langage donc)
- De la connectique physique (ou **support physique**) entre cartes réseaux : câbles de cuivre, fibres optiques, wifi ...

Les terminaux du réseau peuvent être reliés directement entre eux :

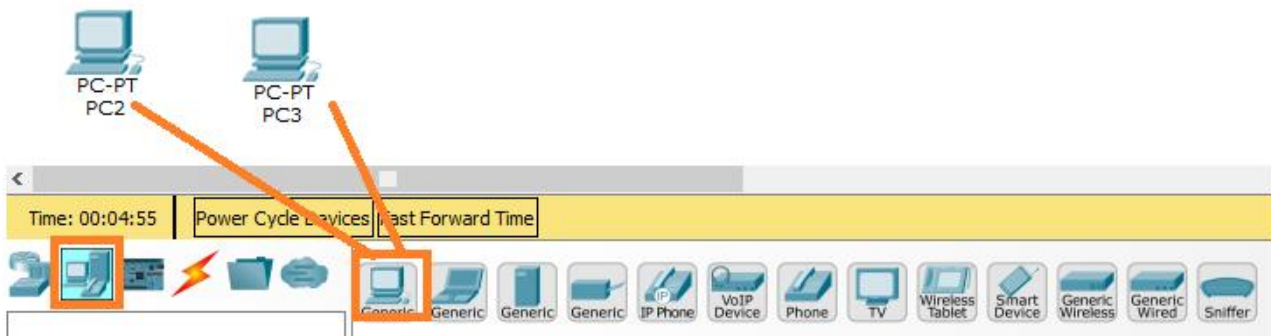


Ils peuvent être reliés entre eux à travers des appareils de communication (ici un hub) :

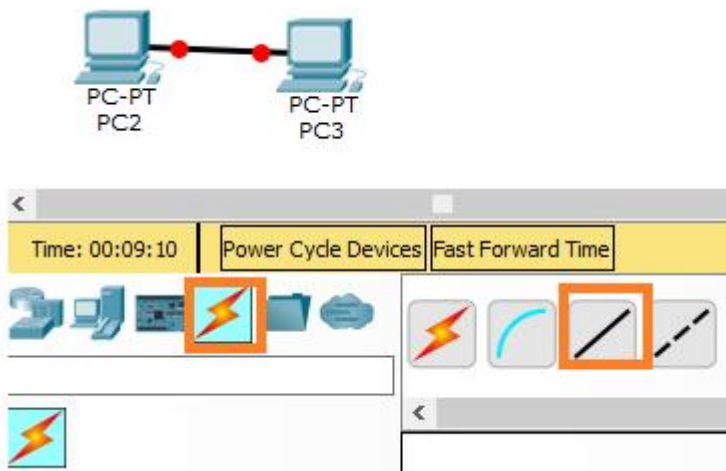


Ce type de connections permet des échanges typiquement d'au moins 100 Mb/s, 100 Mega Bits par seconde : en puissance de 10, cela donne $100 \cdot 10^6$ bits par seconde. Cela correspond à 100 millions de bits par seconde.

Utiliser **Packet Tracer** pour placer deux terminaux sur votre réseau.



°Relier les deux pc (via les prises Ethernet) avec un fil "copper straight-through" : ce sont des câbles droits (straight-through) RJ45 en cuivre(copper) .



Les points-rouges vous indiquent que la liaison n'est pas bonne ! Les deux pc ne peuvent pas communiquer entre eux. Pourquoi ? Il faut regarder la liaison physique pour cela.

CÂBLES DROITS ET CÂBLES CROISÉS

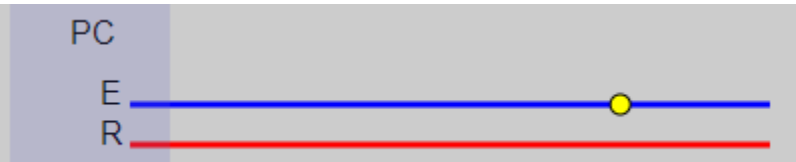
Les câbles dits RJ5 de façon usuelle portent en fait le nom de la prise comme nous l'avons dit. Leur vrai petit nom est 8P8C (8 positions et 8 contacts électriques). Ils sont utilisés par le port Ethernet mais également en téléphonie (avec une prise légèrement différente).

Ils sont composés de 8 fils fonctionnant par pair : 4 fils servent à l'émission d'information et 4 fils servent à la réception des informations.

Sur les réseaux 100 Mb/s, on n'utilise d'ailleurs que 2 fils en émission et 2 fils en réception. Les 4 autres ne servent que sur les réseaux 1 Gb/s.

Attention, je n'utilise pas ici les vraies couleurs : si vous voulez comprendre le vrai câblage interne, renseignez-vous sur Internet, plein de sites techniques l'expliquent. Je considère ici une connectique sur l'ordinateur telle que la première borne est la bornes d'émission et l'autre la borne de réception.

Très grossièrement donc, et avec 2 fils uniquement car ça fait moins de dessins à faire, un câble droit, c'est ça :



A gauche, on voit donc que mon premier ordinateur possède une borne de sa carte réseau dédiée à l'émission (E) et une borne dédiée à la réception (R).

Si je branche un second ordinateur de l'autre côté du câble, le branchement donne ceci :

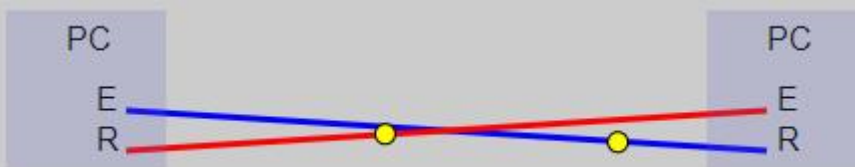


On voit donc qu'avec un câble droit, ça ne fonctionne pas entre deux PC : on branche un port d'émission sur un port d'émission. Si on rajoute le fait que le second PC peut lui aussi émettre et créer des interférences avec l'autre signal, on se rend bien compte que le câble droit n'est pas adapté à la situation.

Comment reconnaître un câble droit ? C'est simple : si vous regardez les deux broches de votre fil, vous devez voir les mêmes couleurs dans le même ordre.

Nous allons voir que le fil RJ-45 droit sert à relier un PC à un Hub ou à un Switch.

On utilise un câble croisé, c'est à dire un câble dont on inverse l'ordre de certains fils sur les deux bornes extrêmes :



Comment reconnaître un tel câble ? L'ordre des fils n'est plus le même et donc les couleurs ne doivent pas être dans le même ordre des deux côtés de votre câble.

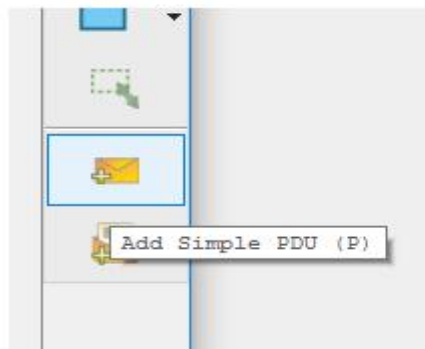
° Avec la croix rouge, supprimez le câble droit que vous aviez placé et remplacez le avec un **copper cross-over** qui est donc un câble croisé.

➤ Normalement, la connexion passe au vert.



Nous allons maintenant faire communiquer les deux pc entre eux. Pour cela, le logiciel permet d'envoyer un message d'un pc vers un autre : il s'agit de l'icône **enveloppe** : Add Simple PDU.

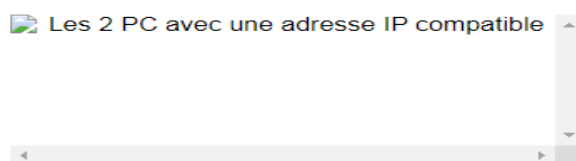
° Utiliser ce bouton et sélectionner le pc 2 puis le pc 1 pour envoyer votre message.



Ca ne fonctionne toujours pas ! C'est normal : les pc n'ont pas d'adresse ip de base. Aucun service ne donne d'adresse Ip à vos ordinateurs dans cette simulation.

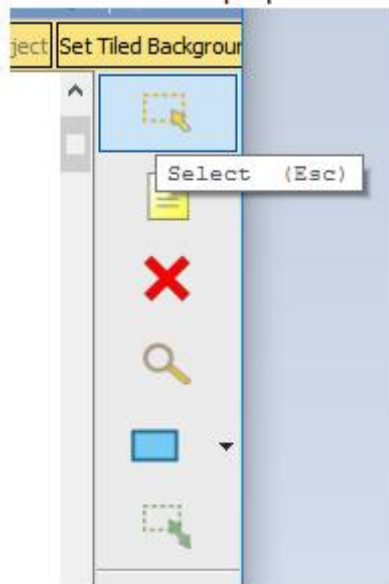
Commençons par leur donner les deux adresses suivantes :

- 192.168.0.10
- 192.168.0.20

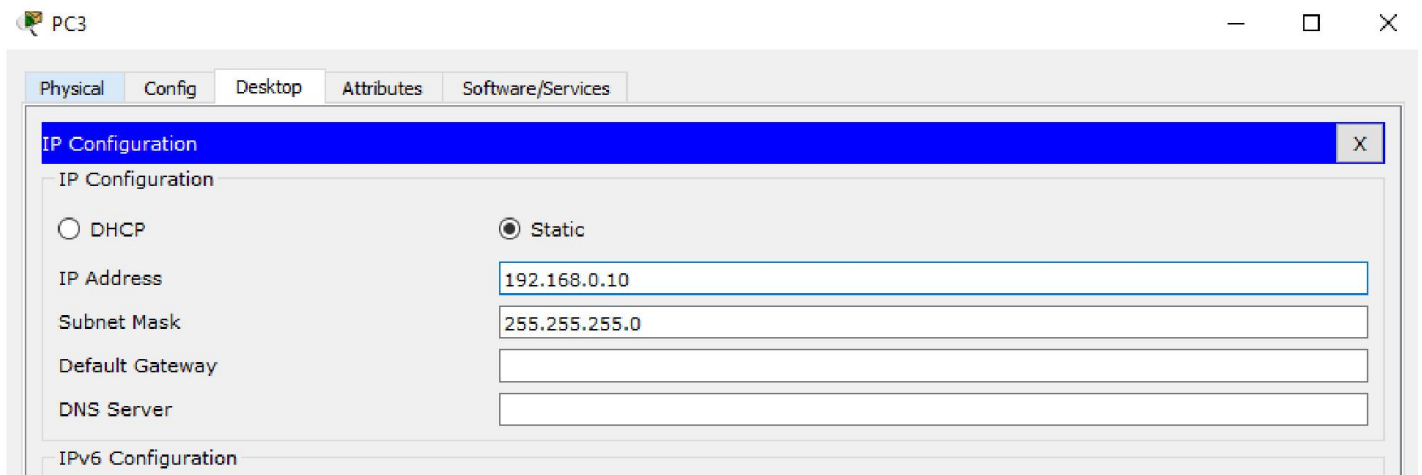


° Utiliser l'icône **Select** et configurer des adresses statiques en sélectionnant le pc puis en utilisant **IP configuration** et

Icône Select



Icône Select



Configuration de l'Ip en mode Desktop

Configuration de l'Ip en mode Desktop

Comme vous pouvez le voir, vous obtenez un remplissage automatique de la partie masque de sous-réseau. Il vous place automatiquement 255.255.255.0.



- **Utiliser les 2 modes : real time et simulation**



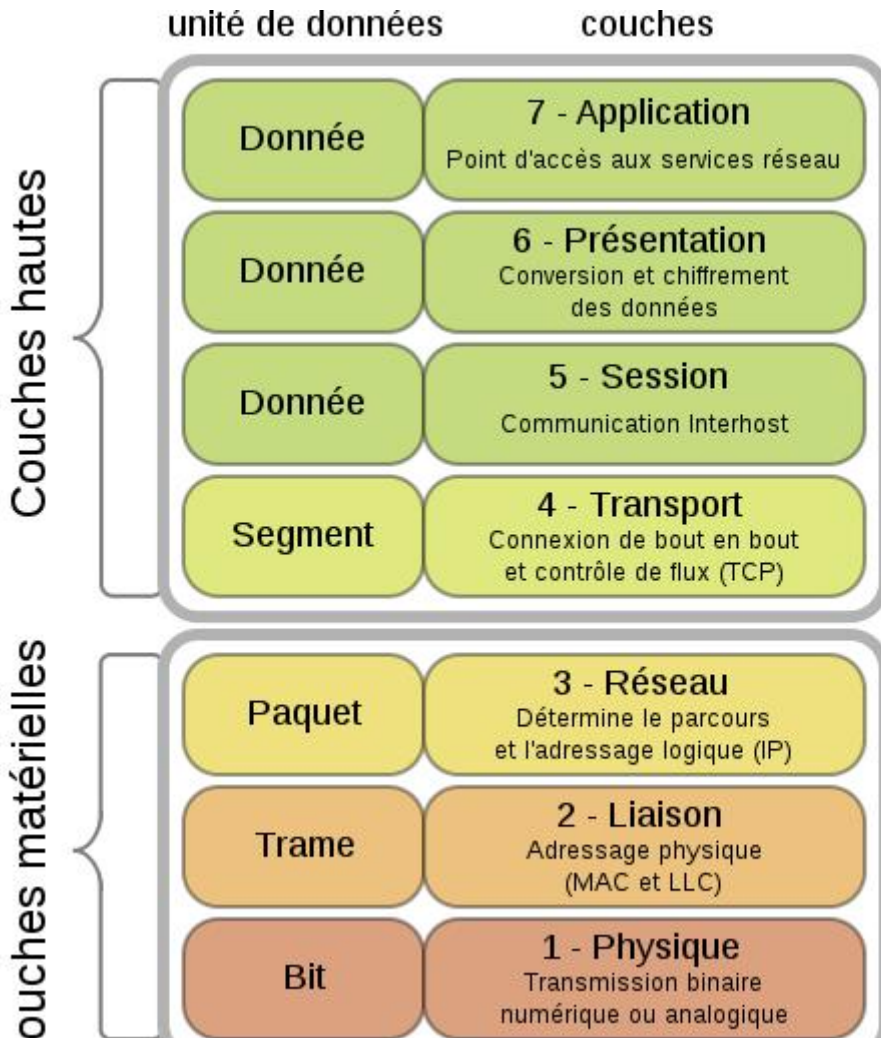
3 - LES COUCHES MATÉRIELLES DU MODÈLE ISO

Le **PDU** de la question précédente veut dire **Protocol Data Unit** : il s'agit de la plus petite unité d'information qu'on puisse transmettre lors d'une communication.

Les communications entre les machines se font par couches de plus en plus concrètes d'un point de vue matériel :

- La machine émettrice dispose d'une adresse IP et envoie un message via la **couche réseau (la couche 3)**. C'est cette couche qui va gérer l'adresse IP pour savoir où envoyer le message. Le PDU du message s'appelle alors un **paquet** ou **packet** en anglais.
- On passe à la **couche liaison (la couche 2)**. Cette couche n'utilise plus les adresses IP (les "titres") mais des adresses dites MAC propres à chaque machine : on contacte désormais le véritable destinataire dont on a cherché à connaître le nom. Le PDU de cette couche se nomme **trame** ou **frame** en anglais.
- On arrive alors au plus près de la communication : la communication physique via le support physique. C'est la **couche physique (la couche 1)** qui s'occupe de

transférer correctement le PDU de ce niveau : le **bit** d'information. Cette couche s'occupe donc réellement des transferts électriques ou optiques. Cette couche est totalement "matérielle" ou "physique" : c'est ici qu'on traduit les bits (informations 0 ou 1) en un signal qui va être transmis réellement.



Auteur de l'image : Offnopt — Travail personnel / Domaine Public

Une fois que les bits sont envoyés vers la machine suivante, on fait la même chose dans l'autre sens :

- La **couche physique (la couche 1)** se charge de transformer le signal physique reçu en bits d'informations.
- La **couche liaison (la couche 2)** assemble les bits pour recréer une **trame** et communique avec la couche suivante en lui transmettant le paquet encapsulé dans la trame :

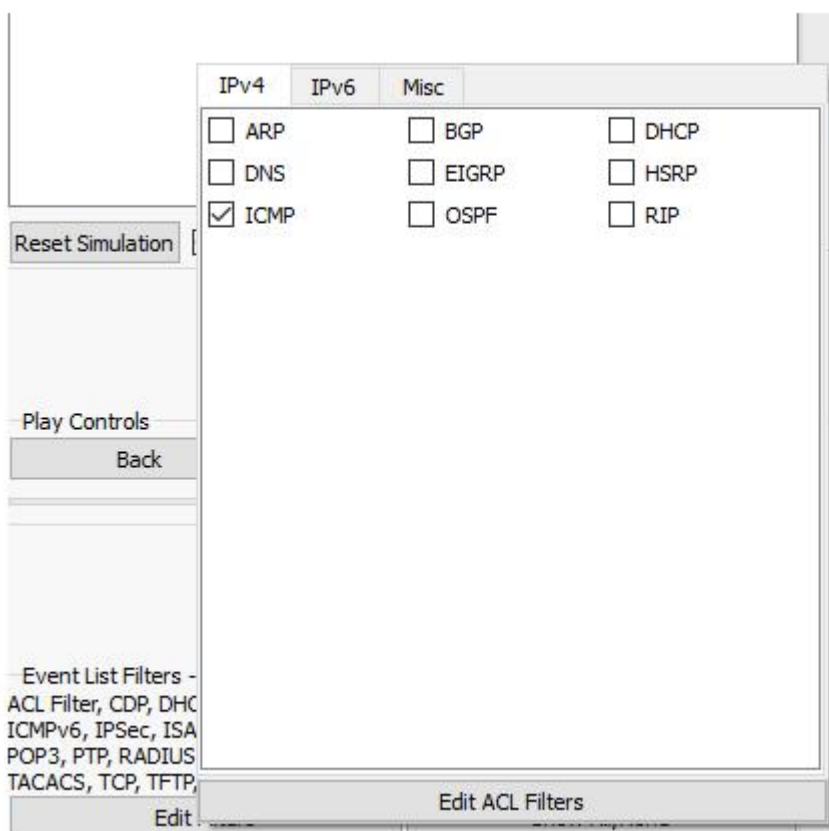
- La **couche réseau (la couche 3)** se charge de déterminer le message à traiter à l'aide de la trame. S'il faut discuter avec un logiciel, on atteint les couches dites hautes dont la première est la **couche transport (la couche 4)**.

Pour tenter de comprendre la notion de couches, nous allons utiliser le mode **simulation** du logiciel.

- Passer en mode simulation en cliquant en bas à droite :



- Utiliser le bouton **Edit Filter** pour ne sélectionner que le protocole ICMP.



Le protocole ICMP que nous gardons va nous permettre de savoir s'il y a des erreurs de transmission ou non :

Le protocole ICMP (**Internet Control Message Protocol**) est un protocole qui informe les machines sur les erreurs lors des transmissions. Le protocole ICMP communique avec les autres protocoles.

° Recommencer à envoyer un message avec **Add Simple PDU**. En appuyant sur **capture/forward** vous allez pouvoir voir le déroulement de l'envoi et voir la communication entre les machines. Pour obtenir les infos, cliquer sur l'icône colorée. Si vous n'avez pas l'écran avec les différents transferts, appuyer sur **Event List**.

Vous devriez obtenir :

Première étape :

The screenshot shows a network simulation interface. On the left, a network diagram displays two PC-PT nodes, PC01 and PC02, connected by a dashed line. A red circle labeled 'A,B,C' highlights the PC01 node. Below the diagram is an 'Event List' table with columns for 'Vis.', 'Time(sec)', 'Last Device', 'At Device', 'Type', and 'Info'. The first row shows an ICMP event at 0.000 seconds from PC01. A purple arrow points from the 'Info' icon in this row to the 'PDU Information at Device: PC01' window on the right. This window shows 'Outbound PDU Details' with 'At Device: PC01', 'Source: PC01', and 'Destination: PC02'. It lists 'In Layers' (Layer7 to Layer2) and 'Out Layers' (Layer7 to Layer2). Layer 3 is highlighted in yellow and contains the text: 'Layer 3: IP Header Src. IP: 192.168.0.10, Dest. IP: 192.168.0.20 ICMP Message Type: 8'. A red arrow points to this layer, with a red 'A' next to it. Layer 2 contains the text: 'Layer 2: Ethernet II Header 0090.0C69.BE2D >> 00D0.D321.A83A'. A red arrow points to this layer, with a red 'B' next to it. The 'Info' icon in the event list is also marked with a red 'C'.

- A-Couche réseau(3) : on indique les adresses IP de l'émetteur et du destinataire. Le message utilise le protocole ICMP, avec un message de type 8.
- B-Couche liaison(2) : on y trouve deux adresses étranges. Nous verrons qu'il s'agit des adresses MAC des appareils correspondant aux IP précédentes : ce sont les adresses qui permettent d'identifier sans équivoque des machines à proximité. En effet, une adresse IP peut correspondre à plusieurs machines dans certains cas. C'est ici qu'on envoie le frame.
- C-Couche physique(1) : on y trouve le nom du port utilisé pour envoyer concrètement le message.

° Rechercher sur Internet la signification d'un message code 8 avec l'ICMP.

Deuxième étape :

The screenshot displays a network simulation interface. On the left, a 'Simulation Panel' shows an 'Event List' with the following entries:

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC01	ICMP	
	0.001	PC01	PC02	ICMP	

On the right, the 'OSI Model' window shows 'Inbound PDU Details' for PC02. The message is identified as an ICMP message from PC01 to PC02. The layers are detailed as follows:

Layer	Details
Layer 3	IP Header Src. IP: 192.168.0.10, Dest. IP: 192.168.0.20 ICMP Message Type: 8 (Label F)
Layer 2	Ethernet II Header 0090.0C69.BE2D >> 00D0.D321.A83A (Label E)
Layer 1	Port FastEthernet0 (Label D)

The 'Out Layers' section shows the message being sent back from PC02:

Layer	Details
Layer 3	IP Header Src. IP: 192.168.0.20, Dest. IP: 192.168.0.10 ICMP Message Type: 0 (Label G)
Layer 2	Ethernet II Header 00D0.D321.A83A >> 0090.0C69.BE2D (Label H)
Layer 1	Port(s): FastEthernet0 (Label I)

- D-Couche physique(1) : on y trouve le nom du port utilisé pour recevoir les bits et reformer le frame.
- E-Couche liaison(2) : l'adresse MAC de destination est compatible avec celle de l'ordinateur. Il transfère alors le frame à la couche réseau qui y lit son paquet.
- F-Couche réseau(3) : on retrouve les adresses IP de l'émetteur et du destinataire. On voit qu'on utilise le protocole ICMP, avec un message de type 8.

La machine interprète alors le message : le type 8 en ICMP veut dire que la machine émettrice attend qu'on lui réponde en lui renvoyant un paquet ICMP de type 0.

- G-Couche réseau(3) : on crée le paquet et on y indique les adresses IP du nouveau émetteur et du destinataire (celui qui avait envoyé le ICMP type 8. Le message utilise le protocole ICMP, avec un message de type 0.
- H-Couche liaison(2) : on forme le frame à partir du paquet. On y trouve les adresses MAC de l'émetteur et du récepteur attendu du message.
- I-Couche physique(1) : on y trouve le nom du port utilisé pour envoyer concrètement le message.

° Quelle est la machine destinatrice du nouveau message d'après les étapes G et H ?

Troisième étape :

The screenshot displays a network simulation environment. At the top, a diagram shows two PCs, PC01 and PC02, connected by a dashed line. PC01 is circled in red, and an orange arrow points from it towards PC02. Below the diagram is the 'Simulation Panel' with an 'Event List' table:

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC01	ICMP	
	0.001	PC01	PC02	ICMP	
	0.002	PC02	PC01	ICMP	

To the right, the 'PDU Information at Device: PC01' window is open, showing 'OSI Model' and 'Inbound PDU Details'. The details are as follows:

- At Device: PC01
- Source: PC01
- Destination: PC02
- In Layers**
- Layer 7
- Layer 6
- Layer 5
- Layer 4
- Layer 3: IP Header Src. IP: 192.168.0.20, Dest. IP: 192.168.0.10 ICMP Message Type: 0
- Layer 2: Ethernet II Header 00D0.D321.A83A >> 0090.0C69.BE2D
- Layer 1: Port FastEthernet0

Red arrows point to the Layer 3 and Layer 2 information, and a purple arrow points to the event list entry at 0.002s.

- J-Couche physique(1) : on y trouve le nom du port utilisé pour recevoir les bits et reformer le frame.
- K-Couche liaison(2) : l'adresse MAC de destination est compatible avec celle de l'ordinateur. Il transfère alors le frame à la couche réseau qui y lit son paquet.
- L-Couche réseau(3) : on retrouve les adresses IP de l'émetteur et du destinataire. On voit qu'on utilise le protocole ICMP, avec un message de type 0.

Bon. Nous venons en réalité de montrer une des quatre étapes d'un ping, l'instruction qui permet de tester la connectivité entre deux ordinateurs. Le ping fait ça quatre fois de suite.

° A l'aide de la commande `ipconfig /all`, retrouvez l'adresse physique MAC de votre terminal.

ADRESSE MAC ET IP

L'adresse MAC (**Media Access Control**) est un identifiant physique qui est stocké et lié dans une carte réseau (que ce soit celle d'un ordinateur, d'une imprimante, d'une caméra...). Elle est normalement unique au monde.

Elles sont attribuées par une association de professionnels, l'IEEEA : Institute of Electrical and Electronics Engineers.

Elles sont parfois appelées : Adresse ethernet , MAC-48

L'adresse MAC-48 est constituée de 48 bits (6 octets puisque $6 \times 8 = 48$). Il y a donc potentiellement 2^{48} , soit plus de 280 000 milliards d'adresses différentes. C'est moins que l'IPv6 et ses 16 octets mais c'est déjà pas mal.

Elle est donnée sous forme hexadécimale en séparant les octets par un tiret ou un double point.

Par exemple 30-E1-71-47-27-D8 ou 30:E1:71:47:27:D8.

On n'utilise pas uniquement les adresses MAC sur un réseau. La réponse est simple lorsqu'on y pense : si on utilise l'adresse MAC uniquement, tout changement de matériel devient problématique puisque l'adresse MAC de la nouvelle machine sera différente de celle de l'ancienne. C'est pour cela qu'on utilise plutôt l'adresse IP qui correspond à une adresse "logique" et pas une adresse "matériel". Ainsi, l'adresse IP du poste prof pourra être 192.178.6.10 quelque soit l'ordinateur placé à cet endroit.

° Rajouter deux ordinateurs dont les IP seront 192.168.3.15 et 192.168.7.12. Les relier avec un câble croisé puis tenter une communication entre les deux.



Vous devriez constater que ça ne passe pas. En allant observer les informations sur la couche 3 (la couche réseau), vous devriez constater qu'aucun message ne part car l'émetteur détecte que le récepteur n'appartient pas au même réseau.

PDU Information at Device: PC4

OSI Model Outbound PDU Details

At Device: PC4
Source: PC4
Destination: PC5

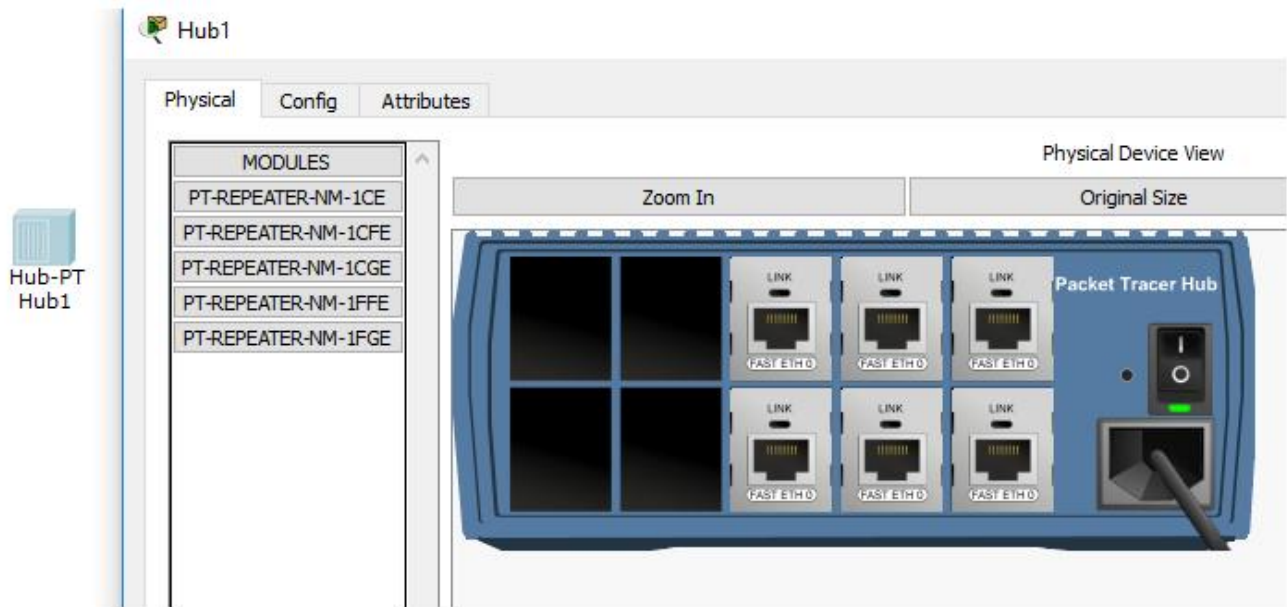
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer 3: ICMP Message Type: 8
Layer2	Layer2
Layer1	Layer1

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The device sets TTL in the packet header.
5. The destination IP address is not in the same subnet and is not the broadcast address.
6. The default gateway is not set. The device drops the packet.

➤ Expliquer pourquoi ça n'a pas marché ?

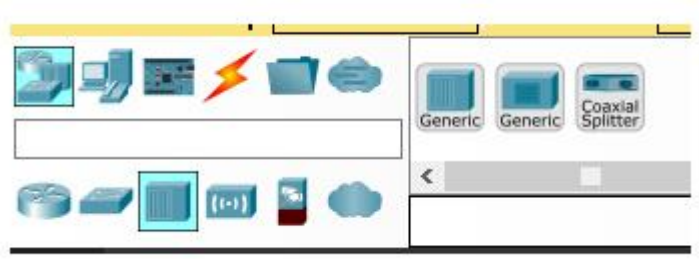
4 - HUB (OU CONCENTRATEUR EN FRANÇAIS)

Le **Hub** ou **Concentrateur** en français est l'un des dispositifs les plus basiques qui soit pour garantir la communication entre plusieurs ordinateurs d'un même réseau.

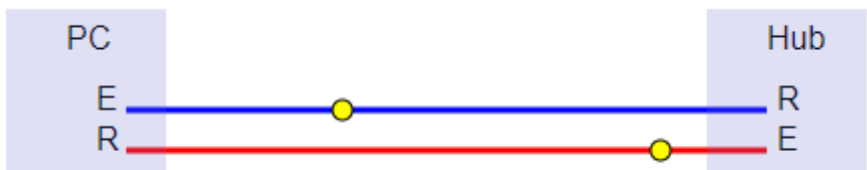


Nous allons voir le principe du Hub mais il n'est plus utilisé..

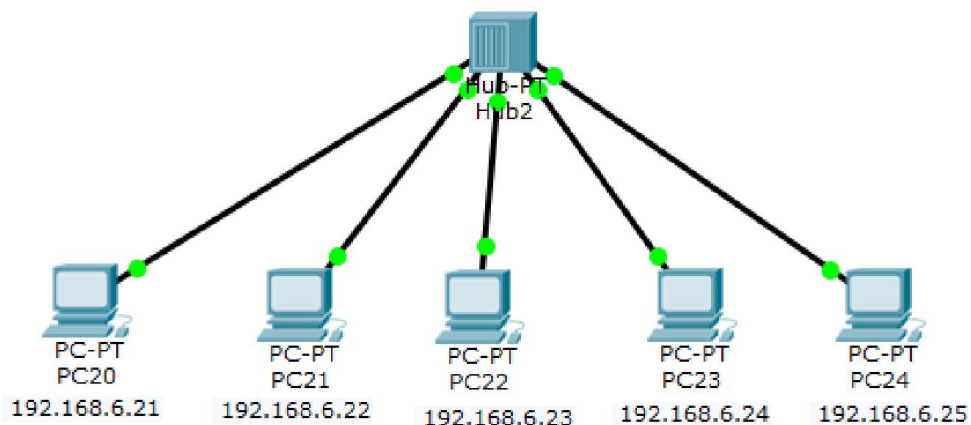
- ° Rajouter 5 pcs ayant des adresses IP de 192.168.6.21 à 192.168.6.25
- ° Rajouter un Hub en allant dans le menu du bas et en sélectionnant **Network devices** puis **Hubs**.



° Relier les PC au Hub avec un câble **droit** : le Hub est fait pour discuter avec les PC et ses ports sont donc dans le bon sens :



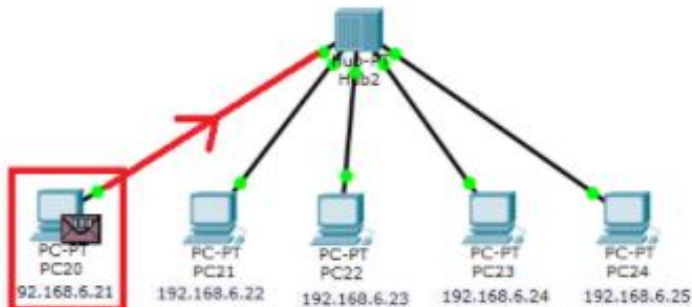
Vous devriez obtenir ceci :



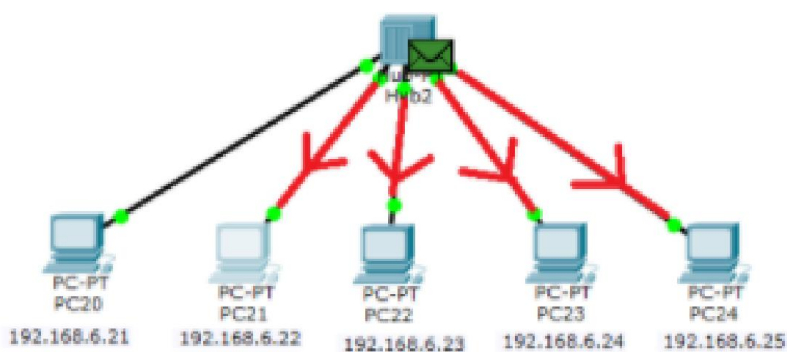
° Créer une simulation pour envoyer un message d'un pc à un autre. Regarder qui le reçoit et regarder qui traite la réponse. Le Hub cible-t-il l'ordinateur possédant la bonne IP ou diffuse-t-il le message à tous les PC qui dépendent de lui ?

Voici le résultat en images :

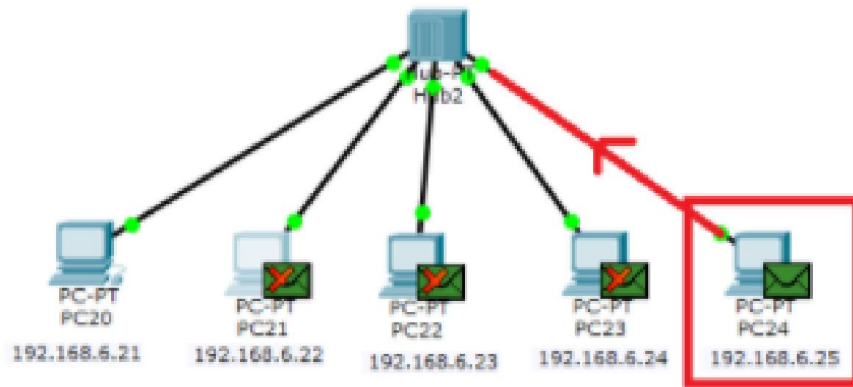
- Le PC d'IP 192.168.6.21 envoie un message pour 192.168.6.25



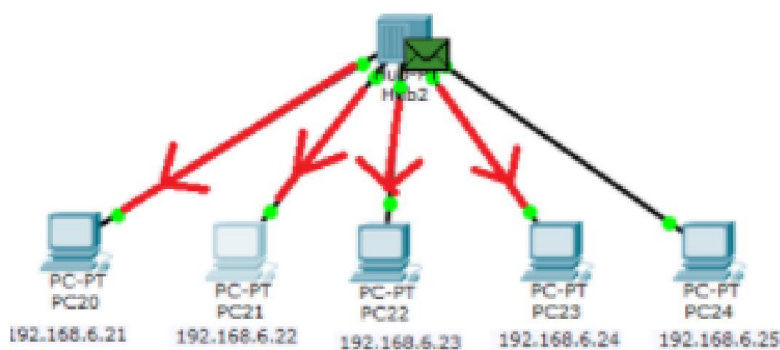
- Le Hub reçoit le message et le diffuse à tous les PC qui sont branchés sur lui (hormis l'émetteur initial).



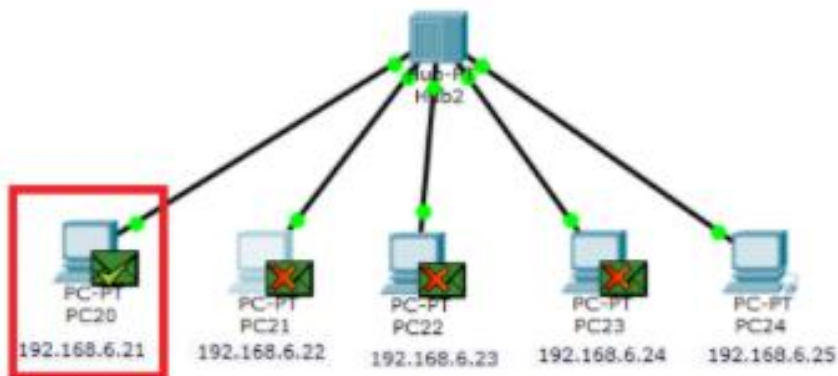
- Les Pc n'ayant pas la bonne adresse reçoivent le message mais n'y donne pas suite. Le PC d'IP 192.168.6.25 lui va renvoyer une réponse ICMP de type 0 à l'ordinateur d'IP 192.168.6.21



- Le Hub reçoit encore le message et le diffuse à tous sauf l'émetteur 192.168.6.25



- Les PC n'ayant pas la bonne adresse reçoivent le message mais lui donne pas suite. Le PC d'IP 192.168.6.21 reçoit le message en le traite puisqu'il est l'émetteur initial de l'ICMP de type 8.



C'est donc le problème principal du hub : lorsqu'il reçoit un message, il le diffuse à tous les ordinateurs. Votre réseau peut donc rapidement devenir très lent car de nombreux messages partent mais ils sont filtrés à l'arrivée uniquement : votre ordinateur reçoit plein de messages et c'est lui qui va décider s'il doit traiter la demande ou non, en fonction de l'adresse IP notée comme destinataire du message.

° Refaire un envoi pour vérifier que cela fonctionne encore de la même façon.