Activité	S7 : RESEAUX, TELECOMMUNICATION ET MODES DE TRANSMISSION	
Durée : 8H		

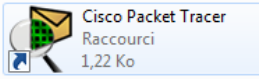
INTRODUCTION AUX RESEAUX - CONFIGURATION D'UN RESEAU DE BASE

Moyens pour réaliser l'activité

Cisco Networking Academy

Utilisation d'ordinateurs connectés à un réseau

Utilisation du logiciel de simulation Cisco Packet Tracer



Utilisation du logiciel Wireshark

Introduction aux réseaux - configuration d'un réseau de base

Introduction

Cette activité est composée de deux parties, la première avec une étude préliminaire dont l'objectif est de vous amener à rechercher des informations sur les savoirs suivants :

S7. Réseaux, télécommunications et modes de transmission

- S7.1 : Concepts fondamentaux de la transmission (support filaire, connectiques, support de transmission hertzien, support de transmission optique)
- S7.2 : Concepts fondamentaux des réseaux (architecture, types de réseaux, topologies, équipements)
- S7.3 : Protocoles de bas niveau (liaison RS232, configuration matérielle/logicielle)
- S7.4 : Transmission sans fil (Type IEEE 802.11 Wifi)
- S7.8 : Système d'exploitation réseau (sécurisation, administration)
- S7.9 : Application utilisateur (http)

La seconde partie consiste à configurer, en parallèle de la première partie, une activité Packet Tracer vous permettant de configurer un réseau de base, grâce aux ressources que vous aurez consultées.

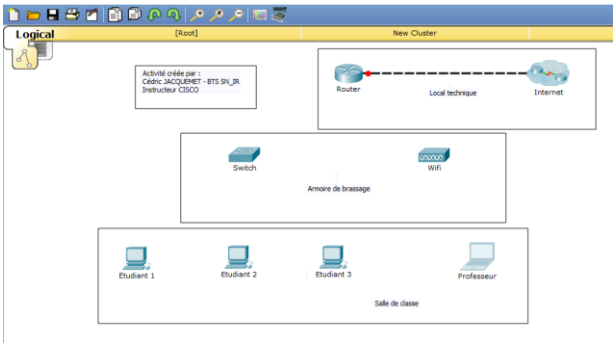
Remarque : La plupart des questions de cette activité nécessitent de nombreuses recherches, soit dans votre cours sur les réseaux, soit dans l'accès en ligne sur le CCNA – Exploration des réseaux, soit sur internet. Vous prendrez un soin particulier à croiser les informations recueillies avant de fournir vos réponses pour vous assurer de la véracité de vos réponses. Les logos suivants indiqueront la nécessité de ce type de recherche :

Pour réaliser cette activité, lancer le fichier « BTS_SN_IR_CJ.pka » en utilisant **Packet Tracer version 6.2 (conseillée) ou supérieure.**

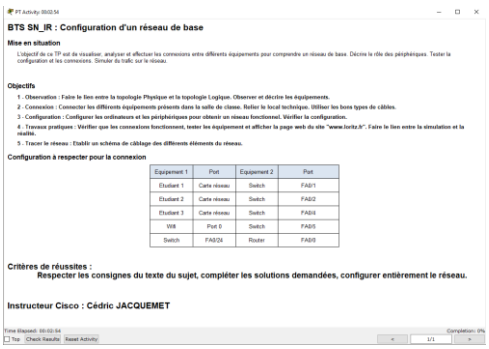
Suivre les instructions au fur et à mesure du texte du sujet, compléter le document présent lorsque que cela est nécessaire.

Au lancement de cette activité, 2 fenêtres s'ouvrent, la fenêtre 1 servant à réaliser le TP, la fenêtre 2 contenant les tâches à réaliser et permettant de tester plus tard votre configuration du réseau :

Fenêtre 1



Fenêtre 2

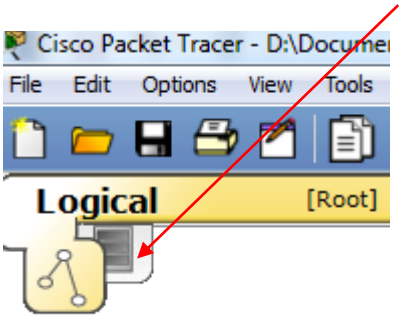


1 – Observation

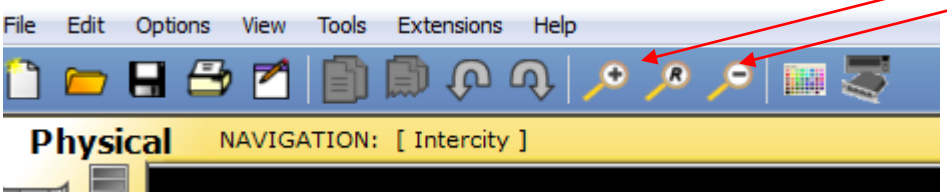
Cette partie du TP va vous permettre de comparer les topologies dites « Physique » et « Logique » pour faire le lien entre la simulation et la réalité.

Dans la fenêtre 1, le travail se fait sur la topologie logique. Toute la configuration et les connexions se feront sur cette vue. Toutefois, cette topologie correspond à une réalité physique.

Cliquer sur l'onglet topologie physique pour passer en vue « intercity »

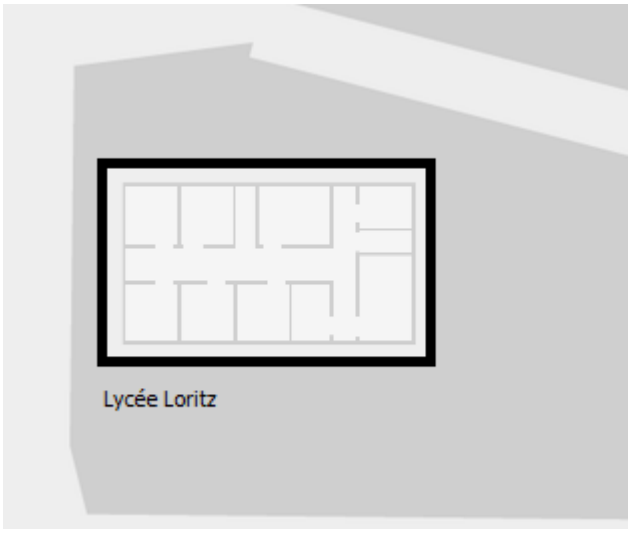


Pour vous déplacer correctement sur les différentes vues, cliquer sur les zooms avant et arrière selon les besoins.

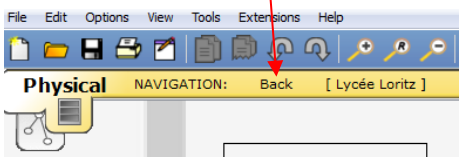


Vous devez maintenant voir la ville de Nancy sur ce plan. Cliquer dessus.

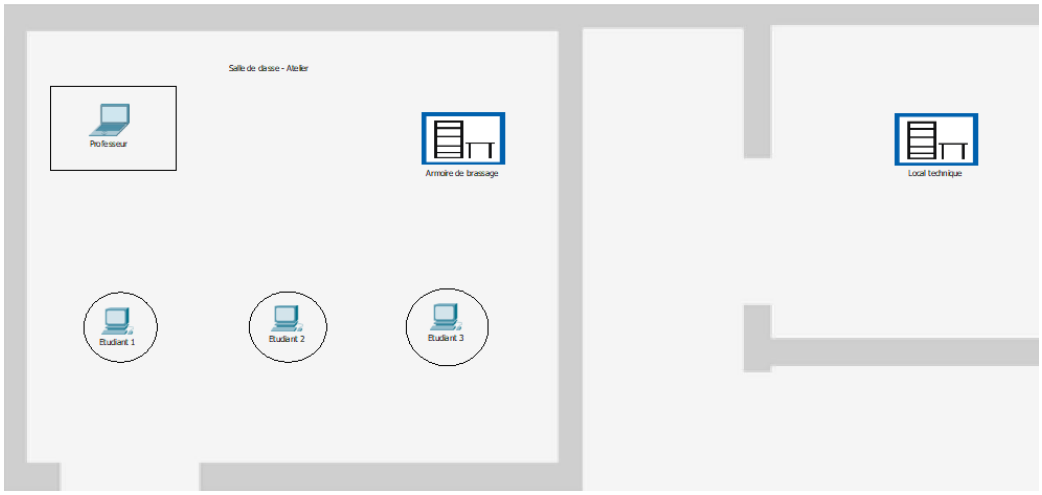
Cliquer sur la ville pour obtenir le Lycée Loritz.



Pour revenir à la vue précédente, il suffit de cliquer sur Back



Cliquer sur le bâtiment du lycée pour accéder à une vue interne qui représente l'emplacement des équipements présents sur la vue logique.



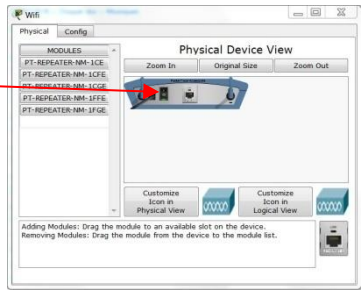
Cliquer sur les PC pour voir physiquement ces équipements.

Cliquer maintenant sur l'armoire de brassage contenue dans la salle de classe.

Q1 : Décrire le contenu du rack

Réponse : Elle contient un point d'accès Wifi et un switch (commutateur en français).

Cliquer sur la borne Wifi. Mettre l'alimentation en service en cliquant sur le bouton Marche/Arrêt.

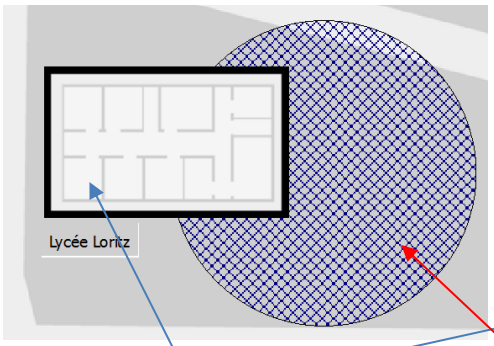


Revenir à la vue précédente.

Q2 : Que constatez-vous ? A quoi correspond ce cercle grisé ?

Réponse : Un cercle grillagé est apparu sur la figure. Ce dernier correspond à la couverture des ondes Wifi. Si un PC Wifi est en dehors de cette zone, il ne pourra pas communiquer avec le réseau.

Dans le lycée :



Dans le bâtiment :

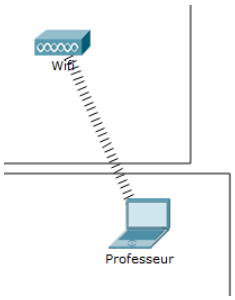
Zones non couvertes.

Zones couvertes

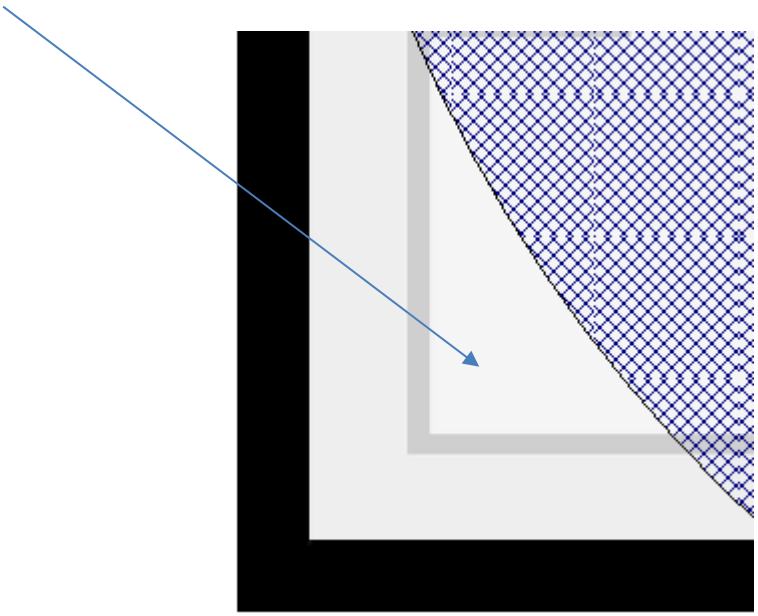
Revenir à la vue logique

Q3 : Que constatez-vous ?

Réponse : Un lien non filaire est établi entre le PC professeur et la borne Wifi.

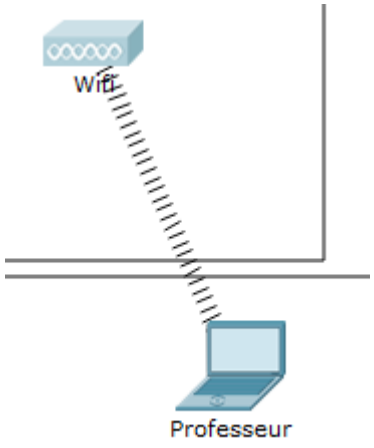


Revenir à la vue physique. Cliquer sur le PC « Professeur » pour le déplacer de manière à le positionner en dehors de la zone grisée. Puis revenir à la vue logique.

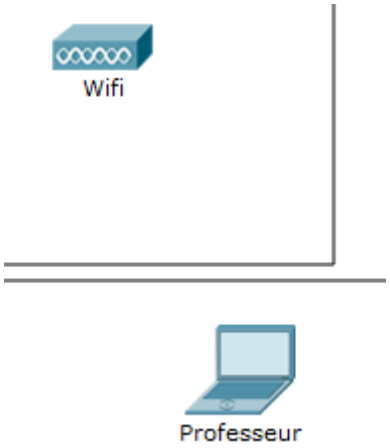


Q4 : Qu'observez-vous ? Pourquoi ?

Réponse : En revenant à la vue logique, on constate que le lien précédant entre le PC professeur et la borne Wifi a disparu. Ceci est dû au fait que le PC n'est plus dans la zone couverte par la borne Wifi.

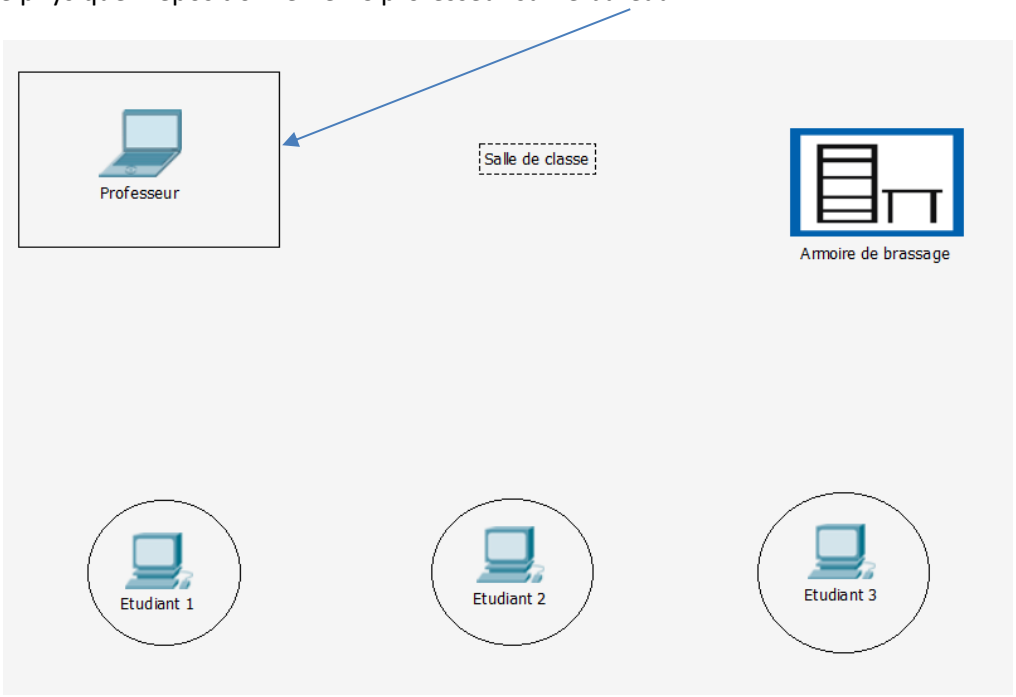


Dans la zone de couverture



En dehors de cette zone de couverture

Revenir à la vue physique. Repositionner le PC professeur sur le bureau.



Q5 : Après avoir effectué les recherches nécessaires, déterminer la norme utilisée pour la communication Wifi. Donner les différentes caractéristiques et indiquer si plusieurs normes existent ainsi qu'une possible rétrocompatibilité entre ces normes.

Réponse : Source CCNA : Présentation des réseaux 5.1

"L'IEEE et les normes de l'industrie des télécommunications pour les communications de données sans fil couvrent à la fois les couches liaison de données et physique.
D'autres technologies sans fil telles que les communications par satellite ou cellulaires peuvent également fournir une connectivité au réseau de données.
Dans chacune de ces normes, des spécifications de couche physique sont appliquées à des domaines comprenant :

- *le codage des données en signal radio.*
- *la fréquence et la puissance de transmission.*
- *les besoins relatifs à la réception et au décodage des signaux.*
- *la conception et la mise en service des antennes.*

Wi-Fi est une marque commerciale de la Wi-Fi Alliance. L'appellation Wi-Fi est utilisée sur des produits certifiés appartenant à des périphériques WLAN basés sur les normes IEEE 802.11. "

Source ITEv6

"Le terme IEEE 802.11, ou « Wi-Fi », fait référence à un ensemble de normes qui spécifient les radiofréquences, les vitesses et autres fonctionnalités des réseaux locaux sans fil. Plusieurs implémentations de la norme IEEE 802.11 ont été développées au fil des ans, comme le montre l'illustration ci-dessous.

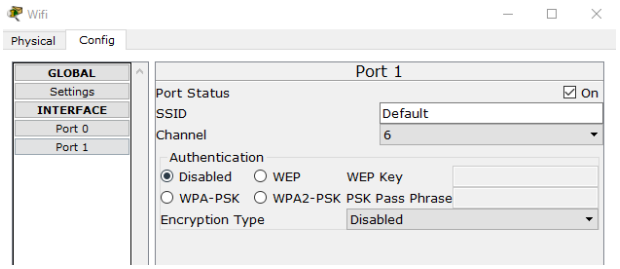
Les normes 802.11a, 802.11b et 802.11g sont dépassées. Les nouveaux réseaux locaux sans fil doivent implémenter des périphériques 802.11ac. Les implémentations des réseaux locaux sans fil existantes doivent mettre en œuvre la norme 802.11ac lors de l'achat de nouveaux périphériques."

Comparaison des normes :

Norme IEEE	Débit maximal	Portée maximale à l'intérieur	Fréquence	Rétrocompatibilité
802.11a	54 Mbit/s	35 m	5 GHz	–
802.11b	11 Mbit/s	35 m	2,4 GHz	–
802.11g	54 Mbit/s	38 m	2,4 GHz	802.11b
802.11n	600 Mbit/s	70 m	2,4 GHz et 5 GHz	802.11a/b/g
802.11ac	1,3 Gbit/s (1 300 Mbit/s)	35 m	5 GHz	802.11a/n

Q6 : Cliquer sur le point d'accès. Dans l'onglet Config, port 1, rechercher le type de cryptage utilisé.

Réponse : A ce moment de l'activité, aucun cryptage n'est défini, on parle de Wifi ouvert.

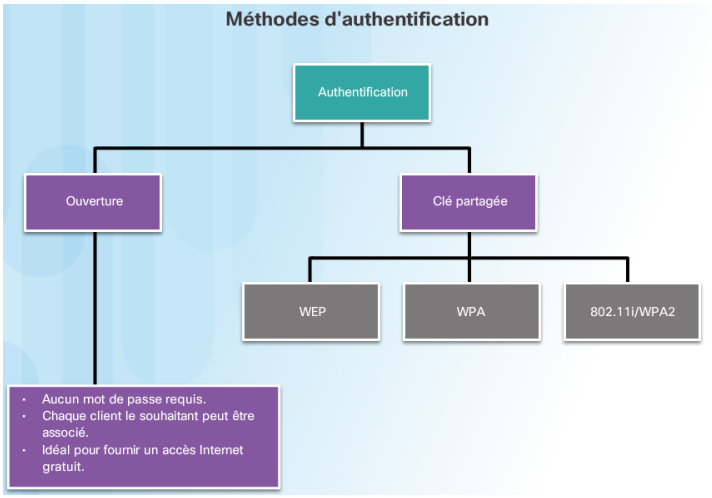


Q7 : Indiquer le type de cryptage disponible pour ce type de connexion. Indiquer la plus recommandée en justifiant votre réponse. 🔍💻

Réponse : Source ITEv6

"Sécurité sans fil

Le meilleur moyen de sécuriser un réseau sans fil consiste à utiliser des systèmes d'authentification et de chiffrement. Deux types d'authentification ont été introduits avec la norme 802.11 d'origine, comme illustré ci-dessous :



- *Authentification Open system - N'importe quel appareil sans fil peut se connecter au réseau sans fil. Cette norme doit être réservée aux situations où la sécurité ne pose pas de problème.*
- *Authentification Shared key - Fournit des mécanismes pour authentifier et chiffrer les données entre un client sans fil et un point d'accès ou un routeur sans fil.*

Les trois techniques d'authentification par clé partagée (Shared key) pour les réseaux locaux sans fil sont les suivantes :

- *Wired Equivalent Privacy (WEP) - Protocole de sécurité 802.11 d'origine pour les réseaux locaux sans fil. Toutefois, la clé de chiffrement ne change jamais lors de l'échange des paquets, ce qui la rend facile à pirater.*
- *WPA (Wi-Fi Protected Access) - Norme utilisant la technologie WEP, mais qui sécurise les données à l'aide d'un algorithme de chiffrement TKIP (Temporal Key Integrity Protocol) bien plus robuste. Le protocole TKIP modifie la clé pour chaque paquet, rendant très difficile son piratage.*
- *IEEE 802.11i/WPA2 - IEEE 802.11i est la norme industrielle de sécurisation des réseaux sans fil. La version Wi-Fi Alliance est appelée WPA2. Les normes 802.11i et WPA2 utilisent toutes deux le mécanisme Advanced Encryption Standard (AES) pour le chiffrement. Le mode de chiffrement AES est actuellement considéré comme étant le protocole de chiffrement le plus puissant.*

Depuis 2006, tout périphérique portant le logo de certification Wi-Fi est également certifié WPA2. Les réseaux sans fil modernes doivent toujours utiliser la norme 802.11i/WPA2."

La version WPA2 est donc la version la plus récente, la plus recommandée et surtout la plus sécurisée, raison pour laquelle nous utiliserons ce cryptage.

Q8 : Que signifie le sigle SSID pour une connexion Wifi ? 🔍💻

Réponse : SSID signifie Secure Set Identifier, il correspond au nom du réseau sans fil. C'est lui qui permet de découvrir et de choisir le réseau auquel on souhaite se connecter lorsque des réseaux Wifi sont disponibles. Noter que la diffusion du SSID peut être désactivée, ce qui oblige l'utilisateur à connaitre ce réseau et à entrer manuellement les informations.

Configurer ce mode de connexion sur le point d'accès, en utilisant les informations suivantes :

SSID : WifiLoritz

Mot de passe : ReseauProfs

Cliquer maintenant sur l'armoire de brassage de la salle de classe.

Q9 : Observer le switch, décrire la vue. Expliquer rapidement son rôle. 🔍💻

Réponse :

Vue : On voit des ports (24) qui servent à connecter des équipements (pc, router, autre switch, imprimante réseau, etc.). Pour le moment, aucun câble n'est connecté à cet équipement.

Rôle : Il travaille essentiellement avec les adresses MAC et les ports connectés. Il permet les échanges de messages (données) sur le réseau auquel il est connecté. Lorsqu'il reçoit un message qui concerne un équipement du réseau, il le transfert sur le port concerné. Si le message ne concerne pas un équipement du réseau, le paquet est rejeté, sauf si une route par défaut est configurée.

Chaque périphérique possède une adresse MAC. C'est elle qui permet au switch de transmettre les messages. Faire des recherches sur internet sur les adresses MAC (aussi appelées adresses physiques).

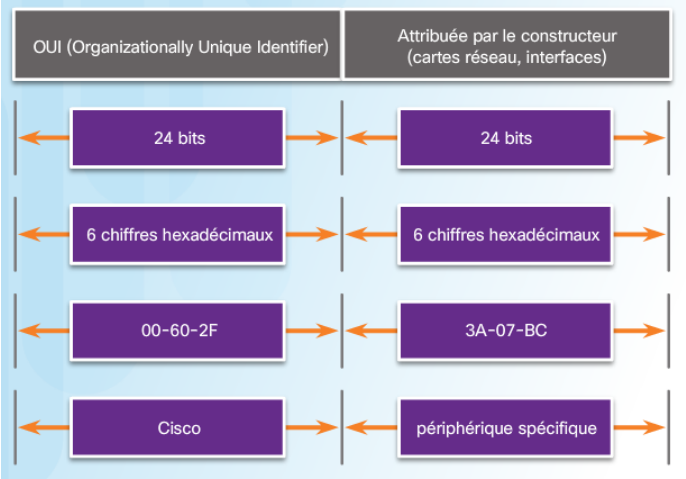
Q10 : Qu'est qu'une adresse MAC ?

Réponse : C'est la carte d'identité d'un périphérique ou d'un équipement (carte Arduino, carte réseau d'un PC, carte WIFI de votre Smartphone, etc.). Elle est unique et se décompose comme suit par exemple :

Source CCNA : Présentation des réseaux 5.1

"00 – 60 – 2F – 3A – 07 – BC

Structure de l'adresse MAC Ethernet



L'adresse MAC est codée en dur sur la carte réseau par le fabricant. Elle reste associée au périphérique, quel que soit le réseau sur lequel il est connecté. Une adresse MAC se compose de 48 bits."

Exemple pour un PC : 48 – 5D – 60 – 81 – 19 – 32

Un constructeur saura donc avec le numéro ci-dessus, qu'il s'agit d'un équipement de sa marque (48 – 5D – 60) dont le numéro unique 81 – 19 – 32 permet d'identifier le type (ici une carte mère) et le numéro de série.

Q11 : En utilisant la commande ipconfig /all dans l'invite de commande de votre PC, donner l'adresse MAC de votre carte réseau.

Réponse : Les réponses varient en fonction des PC. En revanche, il ne peut y avoir deux adresses MAC identiques et doivent avoir un format tel que (Source ITEv6) :

Format d'adresse	Description
00-50-56-BE-D7-87	Deux chiffres hexadécimaux séparés par des tirets
00:50:56:BE:D7:87	Deux chiffres hexadécimaux séparés par deux-points
0050.56BE.D787	Quatre chiffres hexadécimaux séparés par des points

Pour gagner du temps dans les échanges de trames, les différents équipements d'un réseau possède une table de correspondance adresse MAC et adresse IP.

Q12 : Donner le nom de cette table ou protocole. 🔍💻 . Rechercher une commande du Shell qui vous permet d'afficher cette table. Expliquer le contenu de cette table. Effacer cette table en utilisant un autre paramètre de la commande précédente et afficher à nouveau cette table. Que contient-elle ? Faire un ping sur un autre pc de votre salle (demander l'adresse IP de votre voisin), puis afficher de nouveau la table précédente. Que constatez-vous ?

Réponse : Source CCNA : Présentation des réseaux 5.1

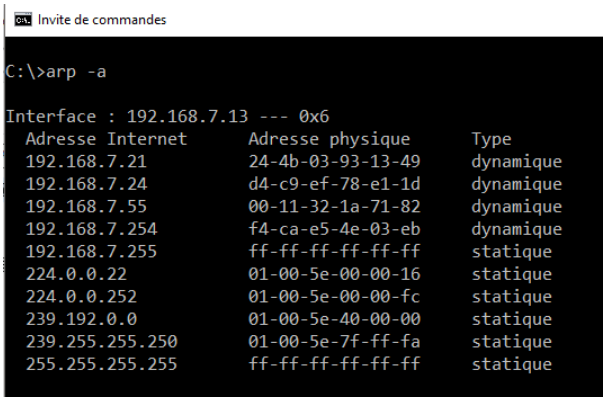
"Présentation du protocole ARP
Souvenez-vous que tout périphérique possédant une adresse IP sur un réseau Ethernet possède également une adresse MAC Ethernet. Lorsqu'un périphérique envoie une trame Ethernet, celle-ci contient deux adresses :

- *l'adresse MAC de destination, c'est-à-dire l'adresse MAC de la carte réseau Ethernet qui correspond soit à l'adresse MAC du périphérique de destination finale soit à celle du routeur.*
- *l'adresse MAC source, c'est-à-dire l'adresse MAC de la carte réseau de l'expéditeur.*

Pour déterminer l'adresse MAC de destination, le périphérique utilise le protocole ARP. Le protocole ARP assure deux fonctions principales :

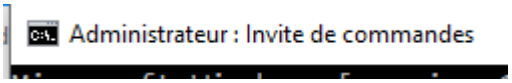
- *la résolution des adresses IPv4 en adresses MAC ;*
- *la tenue d'une table des mappages."*

La commande Shell qui permet d'afficher la table ARP d'un PC est la commande "arp -a" :

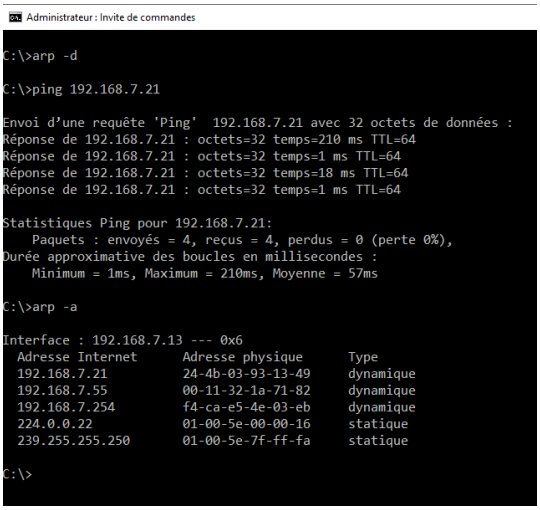


Toutes les adresses dynamiques sont des adresses apprises par le PC et régulièrement rafraichies par les différents périphériques. Les adresses statiques sont des adresses imposées par le PC et seront toujours présentes comme l'adresse de diffusion 192.168.7.255.

Pour effacer cette table, la commande est "arp -d" (pour cela, il faut exécuter l'invite de commande en tant qu'administrateur) :



Voici ce que donne l'effacement de la table arp, puis un ping puis l'affichage de la nouvelle table :



On constate que la table a été vidée des éléments dynamiques. Le ping a fait apparaitre une nouvelle adresse qui a été immédiatement stockée dans la nouvelle table. On constate également que durant les commandes, deux autres adresses ont effectué une requête vers le PC, ce qui fait qu'elles apparaissent de nouveau dans la table. Il s'agit du serveur NAS et de la passerelle du routeur. Les éléments statiques sont restés intactes.

Revenir à la vue physique. Cliquer sur le local technique.

Q13 : Décrire le contenu du rack.

Réponse : On voit sur ce rack, un serveur avec un câble de connexion et un routeur.

Le serveur est un serveur DNS et HTTP.

Q14 : Décrire le rôle d'un serveur de ce type.

Réponse : DNS signifie Domain Name System. C'est un serveur qui permet de traduire une adresse IP en un nom de domaine. Il est effectivement plus facile de se rappeler du nom d'un site plutôt que de son adresse IP.

Exemple : www.loritz.fr a pour adresse IP : 82.165.59.214

Le serveur HTTP, sert à stocker les pages web que les utilisateurs peuvent consulter, avec une relation client/serveur.

Remarque : Le serveur peut être local ou distant. C'est lui qui contient les informations nécessaires (page html, adresse DNS, etc.) pour consulter les pages internet. Ici il est local, même s'il fait partie du nuage internet. Nous verrons dans la dernière partie, qu'en réalité il est distant et nous calculerons le nombre de sauts nécessaires pour l'atteindre. Les sauts en informatique correspondant au nombre de périphériques traversés.

Q15 : Observer le Routeur, décrire la vue. Expliquer rapidement son rôle.

Réponse :

Vue : On constate que cet équipement n'a que 2 ports contrairement au switch qui en possède 24. L'un des deux ports est connecté. Cela correspond à la liaison entre le serveur et le routeur qui est effective sur la vue logique.

Rôle : Comme son nom l'indique, il trouve les autres routes que celles du réseau local auquel appartient le switch. Il travaille essentiellement avec les adresses IP. C'est lui qui permet d'accéder à internet.

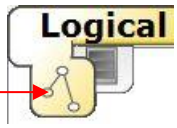
Q16 : En observant une Box équipant les domiciles que pouvez-vous en conclure ?



Réponse : Les Box qui équipent votre maison, sont à la fois des switch permettant de connecter plusieurs équipements (PC, imprimante, etc.), des points d'accès Wifi (tablette, smartphone, TV, etc.) et à la fois des routeurs qui vous permettent de naviguer sur internet.

Bilan intermédiaire

Faire la synthèse des connaissances abordées durant cette partie de l'activité, apporter les éléments de correction nécessaires aux étudiants.

Revenir à la vue logique. 

2 – Connexion

Il faut choisir les bons câbles pour les bons équipements. Les plus courants sont : les RJ45, les câbles coaxiaux et les fibres optiques. Pour utiliser ces deux derniers, il faut des interfaces spécifiques, nous utiliseront donc des câbles RJ45. Il en existe deux sortes, les câbles droits et les câbles croisés.

Q17 : Déterminer l'utilisation des câbles suivants :

- **RJ45 droit**
- **RJ45 croisé**

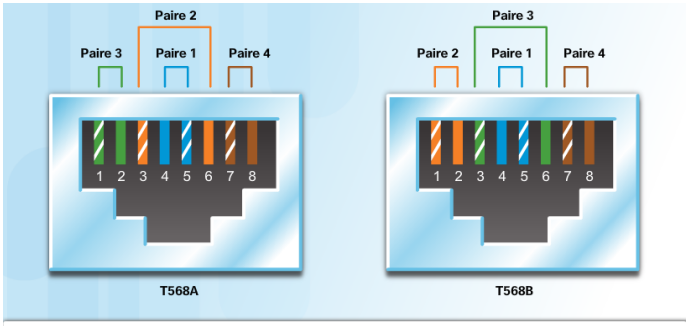
Indiquer en fonction de vos recherches, le type de câble nécessaire pour connecter les PC au switch et le switch au routeur.

Réponse : Source CCNA : Présentation des réseaux 5.1

"Le câblage UTP respecte les normes établies conjointement par la Telecommunications Industry Association (TIA) et l'Electronic Industries Association (EIA). La norme TIA/EIA-568 en particulier, la plus souvent utilisée dans les environnements de câblage LAN, définit le câblage commercial pour les installations de réseau local. Elle définit des éléments tels que :

- *Les types de câbles*
- *Les longueurs de câbles*
- *Les connecteurs*
- *Le raccordement des câbles*
- *Les méthodes de test des câbles*

Les caractéristiques électriques du câblage en cuivre sont définies par l'IEEE (Institute of Electrical and Electronics Engineers). L'IEEE classe le câblage UTP suivant ses performances. Les câbles sont placés dans des catégories en fonction de leur capacité à prendre en charge des débits supérieurs de bande passante. Par exemple, un câble de catégorie 5 (Cat5) est généralement utilisé dans les installations Fast Ethernet 100BASE-TX. Les autres catégories comprennent le câble de catégorie 5 renforcée (Cat5e), la catégorie 6 (Cat6) et la catégorie 6a.
Les câbles des catégories supérieures sont conçus pour prendre en charge des débits de données plus élevés. À mesure que de nouvelles technologies Ethernet avec des débits exprimés en gigabits sont mises au point et adoptées, Cat5e constitue désormais le type de câble minimum acceptable, Cat6 étant recommandé pour les installations de nouveaux bâtiments. "



Type de câble	Standard	Application
Ethernet droit	T568A aux deux extrémités ou T568B aux deux extrémités	Connecte un hôte réseau à un périphérique réseau tel qu'un commutateur ou un concentrateur.
Ethernet croisé	Une extrémité T568A, l'autre T568B	• Connecte deux hôtes réseau. • Connexion de deux périphériques réseau intermédiaires (commutateur à commutateur ou routeur à routeur).

Les câbles croisés (appelés à disparaître) servent essentiellement à interconnecter des équipements de même nature. Par exemple lorsqu'un switch n'a plus de port de disponible, on connecte un autre switch en cascade à

l'aide d'un câble croisé pour ajouter des ports. Ceci n'est pas valable pour des équipements différents, routeur et switch par exemple.

Noter que les nouveau OS permettent de reconnaître le type de câble connecté et de s'adapter en conséquence (à partir de Vista pour Windows). Il en va de même sur les équipements Cisco qui sont équipés du protocole Auto-MDIX.

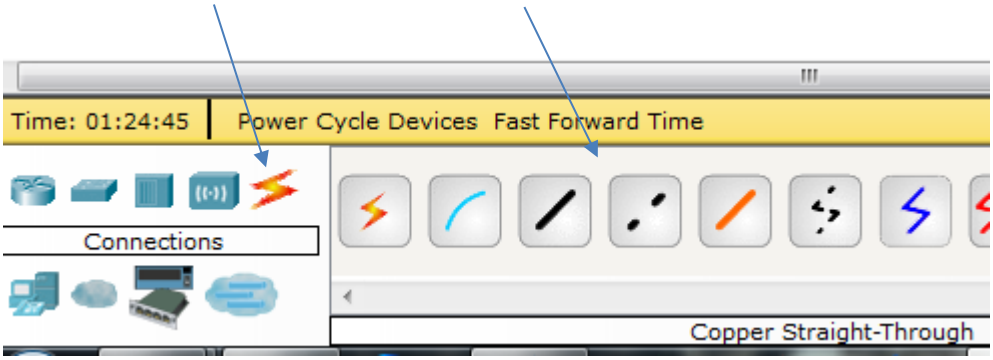
Source CCNA : Présentation des réseaux 5.1

"Outre le paramètre duplex approprié, il est également nécessaire que le type de câble adéquat soit défini pour chaque port. Les connexions entre des périphériques spécifiques, notamment entre deux commutateurs, un commutateur et un routeur, un commutateur et un hôte, et un routeur et des périphériques hôtes nécessitaient au départ l'utilisation de types de câble spécifiques (croisés ou droits). Désormais, la plupart des commutateurs prennent en charge la commande de configuration d'interface mdix auto dans l'interface en ligne de commande (CLI), qui active la fonction auto-MDIX.

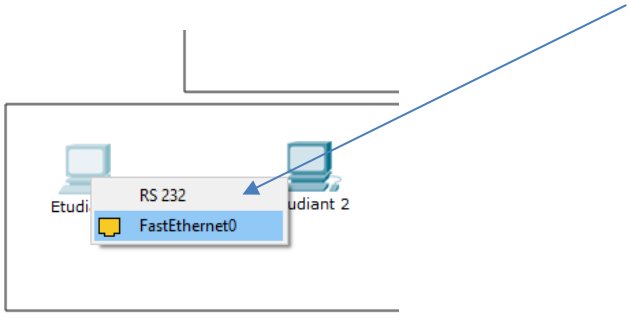
Lorsque vous activez cette fonction, le commutateur détecte le type de câble connecté au port et configure les interfaces en conséquence. Vous devez donc opter pour un câble croisé ou un câble droit pour les connexions sur un port 10/100/1000 cuivre sur le commutateur, quel que soit le type de périphérique à l'autre extrémité de la connexion. "

Connexion du poste « Etudiant 1 » au switch.

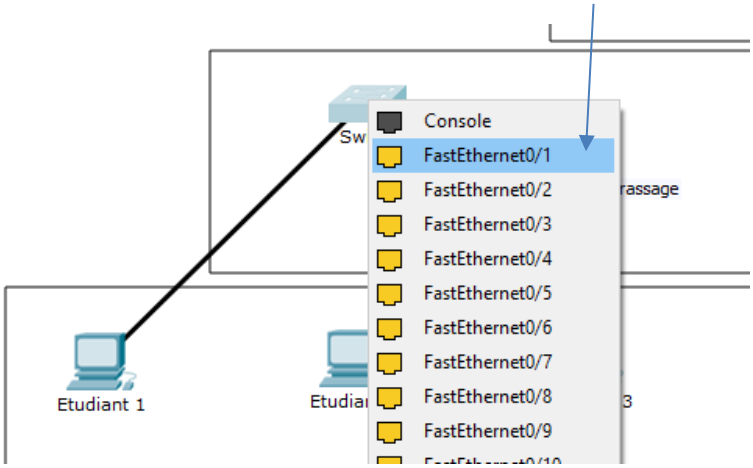
Cliquer sur Connexions puis sur choisir le câble adéquat dans la liste des connexions possibles.



Cliquer ensuite sur le PC « Etudiant 1 », choisir le port « FastEthernet0 ».



Cliquer maintenant sur le switch, choisir le port « FA0/1 ».

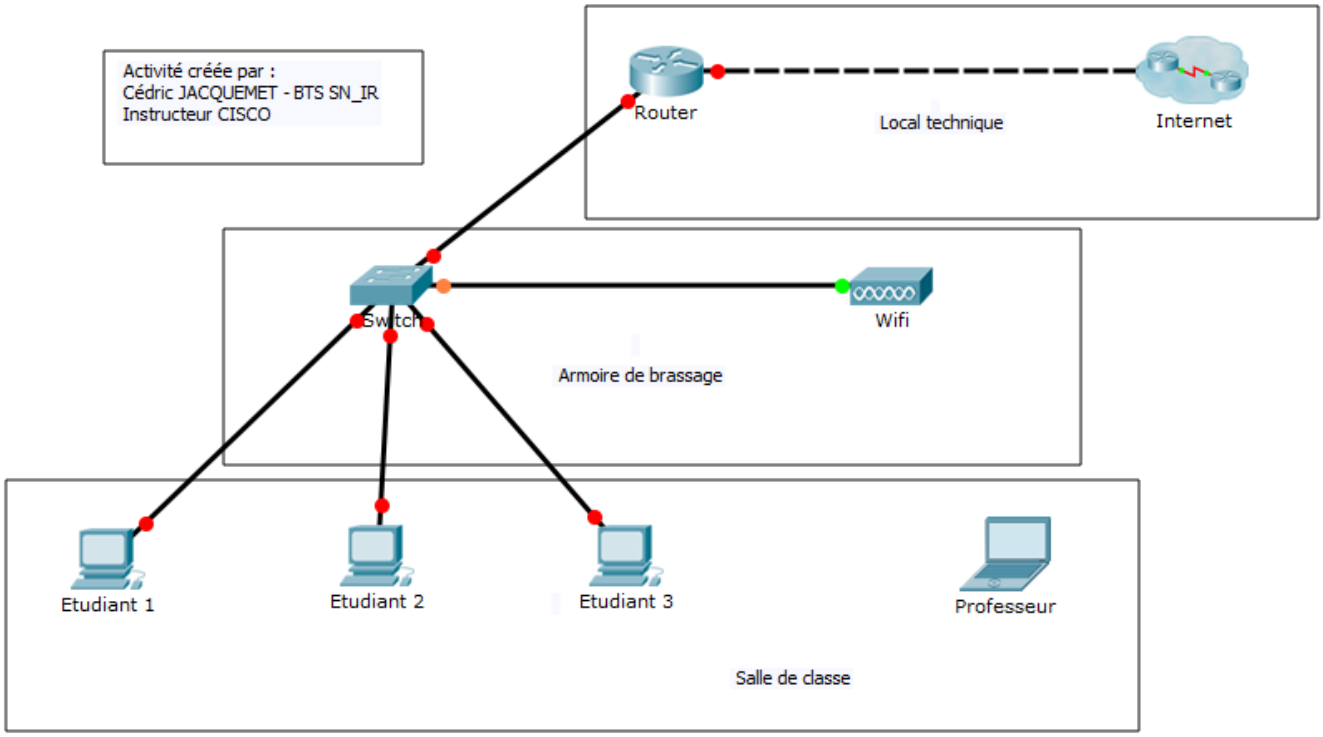


Connecter tous les autres équipements selon la configuration ci-dessous :

Equipement 1	Port	Equipement 2	Port
Etudiant 1	Carte réseau	Switch	FA0/1
Etudiant 2	Carte réseau	Switch	FA0/2
Etudiant 3	Carte réseau	Switch	FA0/4
Wifi	Port 0	Switch	FA0/5
Switch	FA0/24	Router	FA0/0

Q18 : En observant la vue logique et les ports, que constatez-vous ?

Réponse : Toutes les connexions sont en rouge. Sauf entre la borne Wifi et le switch qui alterne orange et vert.



Remarque concernant les couleurs des câbles :

- En Vert, la connexion est correcte, tout va bien.
- En orange, le câble est connecté mais le dialogue ne se fait pas encore. La configuration n'est pas finalisée et nécessite quelques secondes pour être établie (le clignotement correspond au temps réel sur les équipements CISCO).
- En rouge, la communication sera impossible car le support de connexion est incorrect (câble droit au lieu de croisé ou inversement), un problème de protocole (qui permet le dialogue) est survenu ou la configuration de l'équipement est incorrecte.

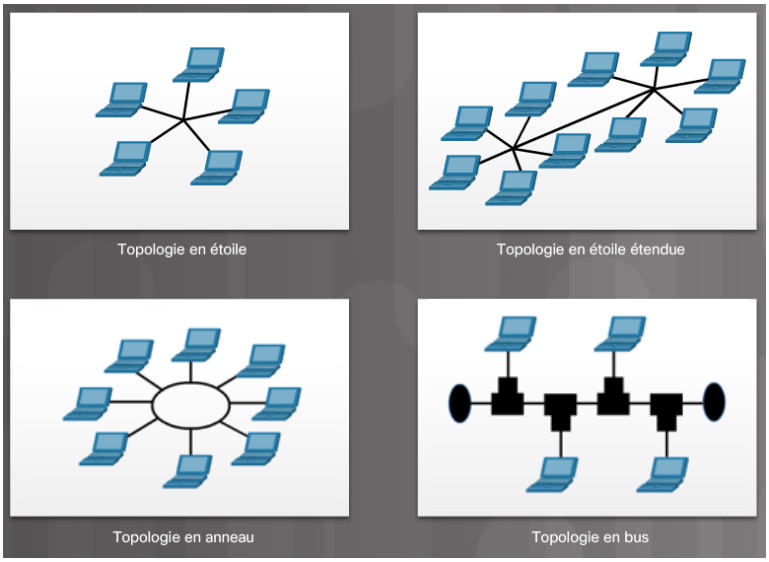
Observer la topologie du réseau que vous venez de créer.

Q19 : Indiquer les différents types de topologie physique existante ainsi que les différents types de réseau (PAN, LAN, MAN et WAN).

Réponse : Source CCNA : Présentation des réseaux 5.1

"La topologie physique définit la façon dont les systèmes finaux sont physiquement interconnectés. Sur les réseaux locaux à supports partagés, les périphériques finaux peuvent être interconnectés selon les topologies physiques suivantes :

- *Topologie en étoile : les périphériques finaux sont connectés à un périphérique intermédiaire central. Dans les premières topologies en étoile, les périphériques finaux étaient interconnectés à l'aide de concentrateurs Ethernet. De nos jours, des commutateurs Ethernet sont utilisés. La topologie en étoile est simple à installer, très évolutive (il est facile d'ajouter et de retirer des périphériques finaux) et facile à dépanner.*
- *Topologie en étoile étendue : dans une topologie en étoile étendue, les périphériques Ethernet supplémentaires sont interconnectés avec d'autres topologies en étoile. Une topologie en étoile étendue est un exemple de topologie hybride.*
- *Topologie en bus : tous les systèmes finaux sont reliés entre eux en formant une chaîne et le réseau est terminé à chaque extrémité par un bouchon de terminaison. Les périphériques d'infrastructure tels que les commutateurs ne sont pas nécessaires pour interconnecter les périphériques finaux. Les topologies en bus sur câbles coaxiaux étaient utilisées dans les anciens réseaux Ethernet en raison de leur faible coût et de leur simplicité d'installation.*
- *Topologie en anneau : les systèmes finaux sont connectés à leur voisin respectif et forment ainsi un anneau. Contrairement à la topologie en bus, l'anneau n'a pas besoin d'être terminé. Les topologies en anneau étaient utilisées dans les réseaux FDDI (Fiber Distributed Data Interface) et Token Ring. "*



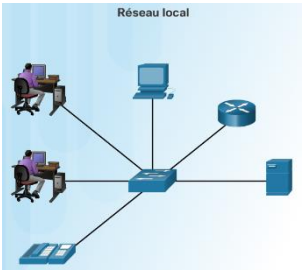
Concernant les différents types de réseau, on peut en recenser 5 principaux types : PAN, LAN, WLAN, MAN et WAN (auquel on peut ajouter Peer to Peer et Client/serveur)

Source ITEv6 :

- PAN (Personal Area Network)

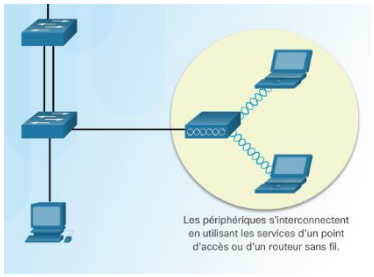
Un réseau personnel relie des périphériques tels que des souris, des claviers, des imprimantes, des smartphones et des tablettes sur une portée très limitée, pour une seule personne. Tous ces périphériques sont dédiés à un seul hôte et utilisent généralement une connexion Bluetooth.

- LAN (Local Area Network)



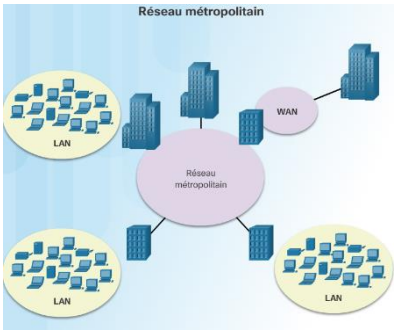
Les réseaux LAN englobent généralement une petite zone géographique. Toutefois, leur principale caractéristique actuellement est d'appartenir à une entité, comme un travailleur à domicile ou une petite entreprise, ou d'être entièrement gérés par un service informatique, comme dans une école ou une grande entreprise. Cet individu ou groupe garantit le respect des politiques de sécurité et de contrôle d'accès sur le réseau.

- WLAN



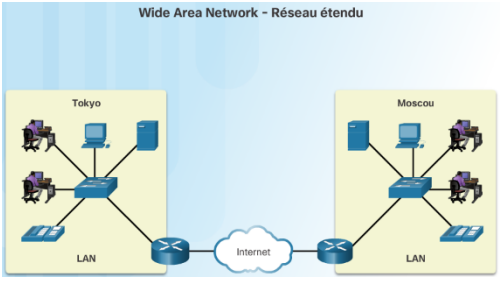
Un réseau local sans fil (WLAN) est un réseau local utilisant des ondes radio pour transférer des données entre les périphériques. Dans un réseau local traditionnel, les périphériques sont interconnectés par le biais d'un câblage en cuivre. Dans certains environnements, l'installation de câbles en cuivre peut être difficile, indésirable, voire impossible. Dans une telle situation, des périphériques sans fil sont utilisés pour transmettre et recevoir les données via les ondes radio. Tout comme pour les réseaux locaux classiques, les réseaux locaux sans fil permettent de partager des ressources telles que les fichiers et les imprimantes, et d'accéder à Internet.

- MAN (Metropolitan Area Network)



Un réseau métropolitain est un réseau qui couvre une vaste zone, comme un grand complexe ou une ville. Il comprend plusieurs bâtiments interconnectés en réseaux fédérateurs sans fil ou à fibres optiques. Dans ce cas, les lignes et équipements de communication appartiennent généralement à un consortium d'utilisateurs ou à un fournisseur d'accès, qui vend ce service aux utilisateurs. Un réseau métropolitain peut être un réseau à haut débit permettant le partage de ressources locales.

- Réseaux étendus



Un réseau étendu (WAN) permet de connecter plusieurs réseaux situés dans des zones géographiques distinctes. Il appartient à un opérateur télécoms. Les particuliers et les entreprises s'abonnent aux services WAN. L'exemple le plus courant de réseau étendu est Internet. Internet est un vaste réseau étendu composé de millions de réseaux interconnectés. Ci-contre, les réseaux de Tokyo et de Moscou sont connectés par Internet.

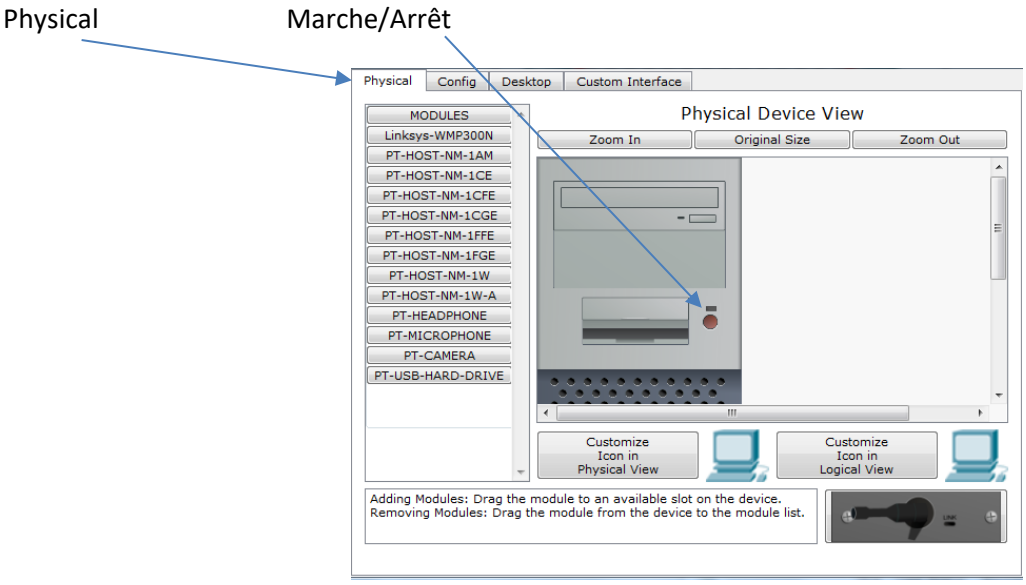
Q20 : En fonction des recherches précédentes, indiquer la topologie du réseau, ainsi que le type de réseau de cette salle de classe.

Réponse : Ce réseau correspond aux réseaux classiques, il s'agit donc d'un réseau LAN avec une topologie en étoile.

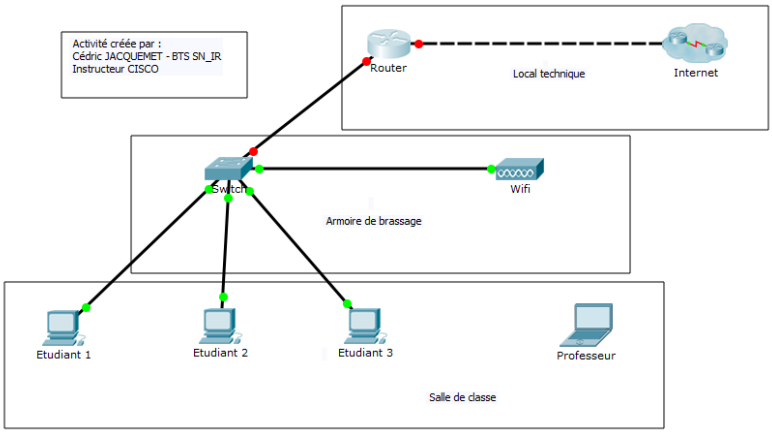
2-1 Alimentation

Mettre en fonctionnement les équipements suivants : PC étudiants 1, 2, 3 et le routeur.

Procéder comme suit, cliquer sur un équipement (exemple PC Etudiant 1), puis cliquer sur le bouton marche arrêt :



Vous devez alors obtenir le schéma logique suivant :

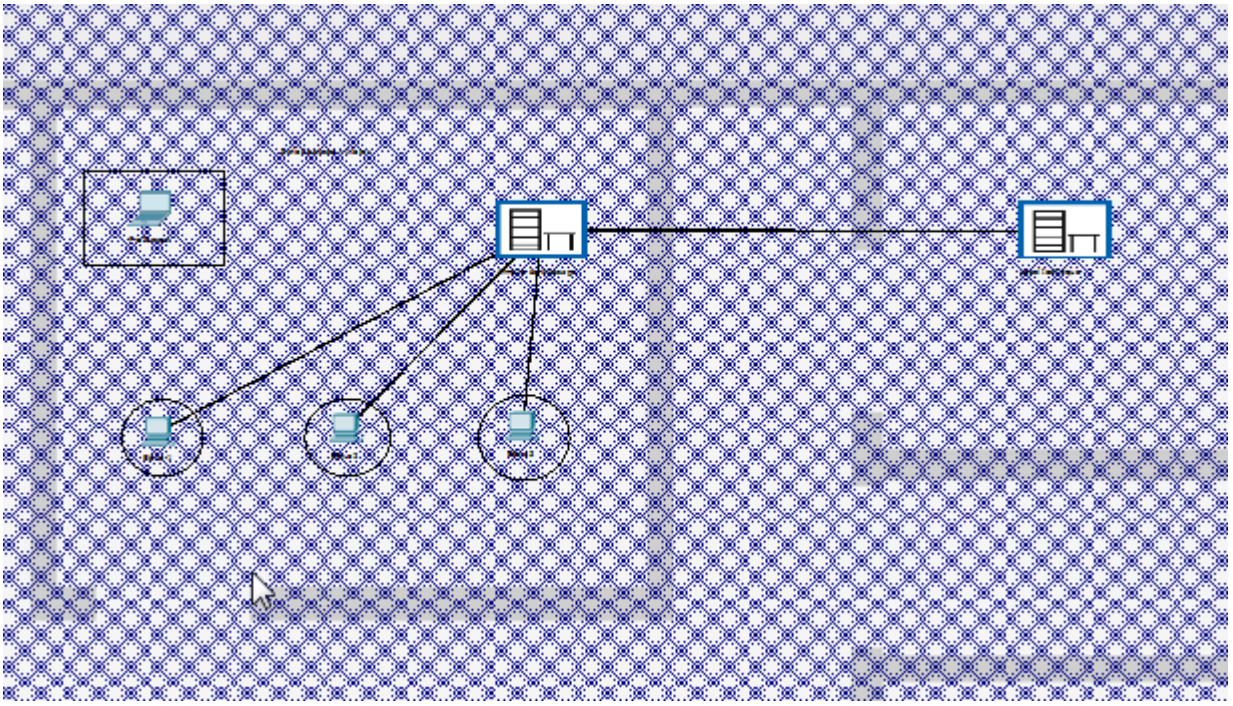


Changer de topologie et passer en mode physique.

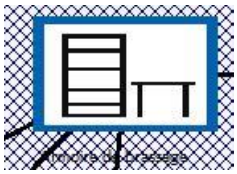
Aller dans le lycée Loritz.

Q21 : Que constatez-vous en plus de la zone grisée ?

Réponse : Les câbles sont désormais présents entre les équipements, ainsi que la couverture Wifi.

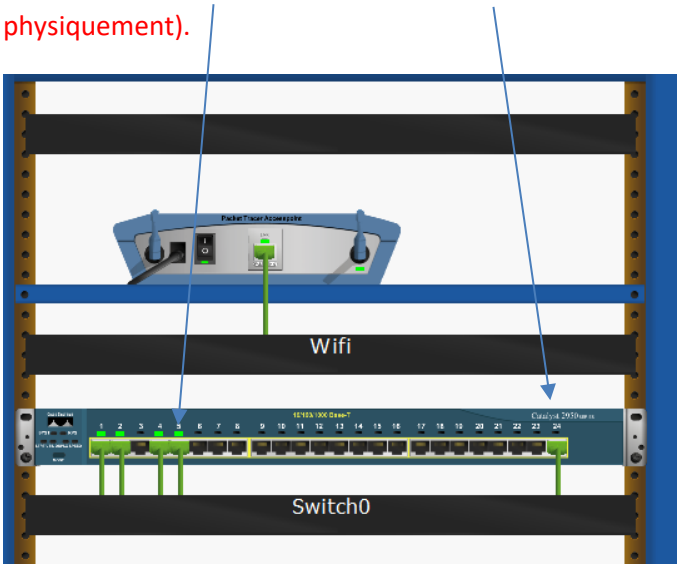


Cliquer ensuite dans l'armoire de brassage de la salle de classe.



Q22 : Qu'est-ce qui a changé ?

Réponse : On constate que les câbles RJ45 ont été ajoutés aux bons ports du switch, ainsi que la couleur des connexions (vertes pour tous les ports sauf FA0/24 qui est en rouge sur le schéma logique et donc éteint physiquement).



Dans la vue logique la couleur rouge pour les ports reliés au routeur est normale. Le problème est dû à l'absence de configuration du routeur. Dans la vue physique, ce port est considéré comme éteint.

Bilan intermédiaire

Faire la synthèse des connaissances abordées durant cette partie de l'activité, apporter les éléments de correction nécessaires aux étudiants.

3 – Configuration de base

Il existe plusieurs types de configuration des équipements. De la configuration de base ou les équipements peuvent communiquer à leur guise, aux configurations spécifiques et complexes, qui créent des sous réseaux, des interdictions d'adresses mac, des listes d'accès de contrôle, et du routage dynamique (ou statique).

Dans notre exemple, nous allons effectuer une configuration de base qui vous permettra de communiquer sur le réseau local entre PC puis d'accéder à internet.

3-1 Configuration des PC

Bien qu'obsolète depuis la fin des années 1990, la plupart des réseaux fonctionnent sur le principe des classes d'adressage.

Q23 : Rapidement, définir les réseaux publics et privés.

Réponse : Source CCNA : Présentation des réseaux 5.1

*"**Adresses IPv4 publiques et privées***
Les adresses IPv4 publiques sont acheminées de manière globale entre les routeurs des FAI (fournisseurs d'accès à Internet). Toutefois, toutes les adresses IPv4 disponibles ne peuvent pas être utilisées sur Internet. Certains blocs d'adresses appelés adresses privées sont utilisés par la plupart des entreprises pour attribuer des adresses IPv4 aux hôtes internes.
Les adresses IPv4 privées ont été créées au milieu des années 1990 en raison de la pénurie d'espace d'adresses IPv4. Les adresses IPv4 privées ne sont pas uniques et peuvent être utilisées par un réseau interne.
Les blocs d'adresses privées sont les suivants :

- *10.0.0.0 /8 ou 10.0.0.0 à 10.255.255.255*
- *172.16.0.0 /12 ou 172.16.0.0 à 172.31.255.255*
- *192.168.0.0 /16 ou 192.168.0.0 à 192.168.255.255*

Il est important de savoir que les adresses appartenant à ces blocs ne sont pas autorisées sur Internet et doivent être filtrées (rejetées) par les routeurs Internet."

Dans l'invite de commande de votre PC, taper la commande ipconfig /all

Q24 : Donner, en fonction du résultat, les adresses IP de votre PC.

Réponse : En fonction de la version de l'OS de votre PC, il peut y avoir 2 adresses IP, l'une IPv4 et l'autre en IPv6.

Par exemple :

```
Adresse IPv6 de liaison locale. . . . .: fe80::5890:df3a:7354:80b6%6(préféré)
Adresse IPv4. . . . . . . . . . . . . .: 192.168.7.13(préféré)
Masque de sous-réseau. . . . . . . . . : 255.255.255.0
```

Q25 : Indiquer si votre PC appartient à un réseau public pour privé.

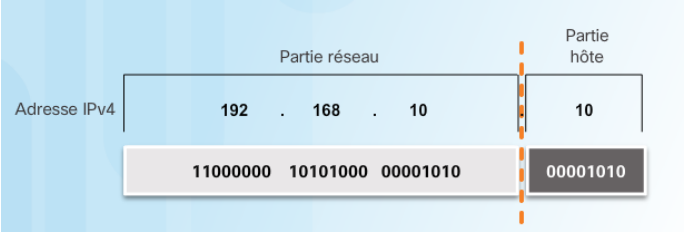
Réponse : L'adresse des PC étant comprise dans la plage 192.168.0.0 /16 ou 192.168.0.0 à 192.168.255.255, ce PC appartient à un réseau privé, son adresse n'est donc pas routable sur internet.

Q26 : Donner la différence entre IPv4 et IPv6. Donner la dénomination d'une adresse IPV4. Donner la dénomination d'une adresse IPv6.

Réponse : IPv4 correspond à la version 4 du protocole internet, et IPv6 à la version 6. IPv4 est codé sur 32 bits alors qu'IPv6 est codé sur 128 bits.

Source CCNA : Présentation des réseaux 5.1

"Il est important de comprendre la notation binaire pour déterminer si deux hôtes se trouvent sur le même réseau. Rappelez-vous qu'une adresse IPv4 est une adresse hiérarchique qui se compose d'une partie réseau et d'une partie hôte. Lorsque vous déterminez la partie réseau et la partie hôte, il est nécessaire d'examiner le flux de 32 bits. Dans le flux de 32 bits, une partie des bits constitue la partie réseau et une autre partie des bits compose la partie hôte, comme le montre la figure ci-dessous :"



Dans le cas d'une adresse IPv4, on parle de notation décimale pointée. Elle est donc représentée par 4 nombres décimaux compris entre 0 et 255, séparés par des points.

Source : CCNA : Présentation des réseaux 5.1

"Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales. Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique ; pour un total de 32 valeurs hexadécimales, comme l'illustre la figure ci-dessous. Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.
…
*Le format privilégié pour noter une adresse IPv6 est x:x:x:x:x:x:x:x, où chaque « x » est constitué de quatre valeurs hexadécimales. Pour faire référence aux 8 bits d'une adresse IPv4, nous utilisons le terme « octet ». Pour les adresses IPv6, **« hextet »** est le terme officieux qui désigne un segment de 16 bits ou de quatre valeurs hexadécimales. Chaque « x » équivaut à un hextet, 16 bits, ou à quatre caractères hexadécimaux."*

Q27 : Donner le nombre d'hôte maximum avec une adresse IPv4. Donner le nombre d'hôtes maximum avec une adresse IPv6.

Réponse :

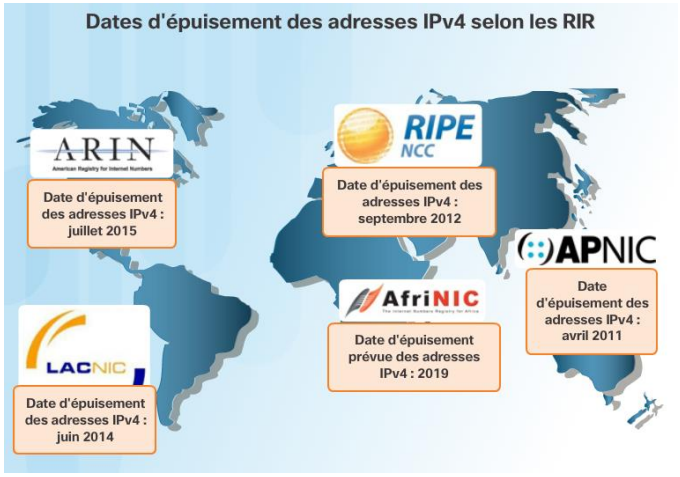
Le protocole IPv4 est codé sur 32 bits, le nombre d'hôtes "maximum" est donc de 2^{32} soit environ 4,3 milliard d'adresses (certaines adresses n'étant pas disponibles).

Le protocole IPv6 est codé sur 128 bits pour un total de 340 undécillions d'adresses soit 340 suivi de 36 zéros. Techniquement, on estime que les adresses IPv6 ne seront jamais épuisées.

Q28 : Expliquer pourquoi IPv6 remplace progressivement IPv4. Donner un avantage et un inconvénient de chaque type d'adressage (IPv4 et IPv6).

Réponse : Source CCNA : Présentation des réseaux 5.1

"Nécessité du protocole IPv6
Le manque d'espace d'adressage IPv4 a été le facteur le plus décisif pour la transition vers l'IPv6. À mesure que les connexions à Internet augmentent en Afrique, en Asie et dans d'autres parties du monde, les adresses IPv4 deviennent insuffisantes pour prendre en charge cette croissance. Comme l'illustre la figure, quatre des cinq RIR se sont trouvés à court d'adresses IPv4.
Théoriquement, l'IPv4 est limité à 4,3 milliards d'adresses. Les adresses privées, en association avec la traduction d'adresses réseau (NAT), ont été utilisées pour ralentir le manque d'espace d'adressage IPv4. Toutefois, la fonction NAT endommage de nombreuses applications et comporte des restrictions qui gênent fortement les communications peer-to-peer.
Internet of Everything
Par rapport au dernière décennies, l'Internet d'aujourd'hui est sensiblement différent. Désormais, Internet est principalement utilisé pour les e-mails, les pages web et le transfert de fichiers entre ordinateurs. Internet évolue pour devenir un « Internet des objets ». Les appareils pouvant accéder à Internet ne sont plus seulement des ordinateurs, des tablettes et des smartphones. Demain, les appareils connectés et équipés de capteurs concerneront tous les objets du quotidien, notamment les automobiles, les équipements biomédicaux, l'électroménager et même les écosystèmes naturels.
Avec l'utilisation croissante d'Internet, un espace limité d'adresses IPv4, des problèmes liés à la fonction NAT et l'Internet of Everything, le moment est venu d'entamer la transition vers IPv6."



L'avantage des adresses IPv4 est leur format simple à comprendre et la facilité qui en découle à configurer un réseau. L'inconvénient est la pénurie de ses adresses.

L'avantage du protocoles IPv6 est le nombre d'adresses disponibles 340.10^{36}, l'inconvénient est que la format Hextet le rend difficile à comprendre et à configurer.

Q29 : Qu'est-ce qu'un masque de sous réseau. Déterminer les réseaux en fonction des classes d'adresses. Indiquer le nombre d'hôte possible dans un réseau de classe C.

Réponse : Un masque de sous réseau est une adresse de la forme d'une adresse IP qui permet de déterminer l'adresse du réseau ainsi que l'adresse de l'hôte. En utilisant des opérateurs logiques tel que la And et le Or, nous pouvons facilement déterminer ces deux informations.

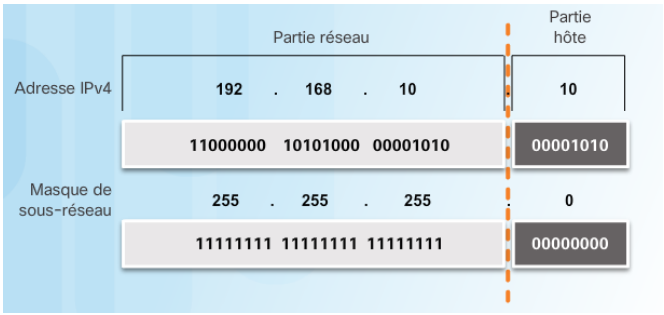
Source CCNA : Présentation des réseaux 5.1

"Masque de sous-réseau
Comme le montre la figure ci-dessous, la configuration IPv4 d'un hôte comprend trois adresses IPv4 décimales à point :

- *l'adresse IPv4, qui est l'adresse IPv4 unique de l'hôte,*
- *le masque de sous-réseau, qui sert à identifier la partie réseau et la partie hôte d'une adresse IPv4,*

- *la passerelle par défaut, qui indique la passerelle locale (c'est-à-dire l'adresse IPv4 de l'interface du routeur local) permettant d'atteindre les réseaux distants.*

Pour identifier les parties réseau et hôte d'une adresse IPv4, chaque bit du masque de sous-réseau est comparé à l'adresse IPv4, de gauche à droite, comme le montre la figure ci-dessous. Les 1 dans le masque de sous-réseau représentent la partie réseau, et les 0 représentent la partie hôte. Notez que le masque de sous-réseau ne contient pas réellement la partie réseau ou hôte d'une adresse IPv4 : il indique uniquement à l'ordinateur où rechercher ces parties dans une adresse IPv4 donnée.
En réalité, le processus utilisé pour identifier la partie réseau et la partie hôte est appelé l'opération AND."



"Longueur de préfixe
Il peut devenir fastidieux d'exprimer les adresses réseau et les adresses d'hôtes avec l'adresse du masque de sous-réseau au format décimal à point. Heureusement, il existe une méthode plus rapide d'identification du masque de sous-réseau, appelée la longueur de préfixe.
En fait, la longueur de préfixe correspond au nombre de bits définis sur 1 dans le masque de sous-réseau. Elle est notée au moyen de la « notation de barre oblique », soit le signe « / » suivi du nombre de bits définis sur 1. Il suffit donc de compter le nombre de bits du masque de sous-réseau et d'y ajouter une barre oblique."

Masque de sous-réseau	Adresse 32 bits	Longueur de préfixe
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Avant la fin des année 1990, les réseaux étaient décomposés en classes.

Source CCNA : Présentation des réseaux 5.1

"Ancien système d'adressage par classe
En 1981, les adresses IPv4 Internet étaient attribuées à l'aide de l'adressage par classe, comme défini dans le document RFC 790, Assigned Numbers. Les clients ont reçu une adresse réseau basée sur l'une des trois classes, A, B ou C. Le RFC a divisé les plages monodiffusion en classes spécifiques, respectivement appelées :

- *Classe A (0.0.0.0/8 à 127.0.0.0/8) : créée pour prendre en charge les réseaux de très grande taille, comportant plus de 16 millions d'adresses d'hôte. Elle utilisait un préfixe /8 fixe avec le premier octet identifiant l'adresse réseau et les trois derniers octets identifiant les adresses d'hôte. Toutes les adresses de classe A nécessitaient que le bit de poids fort du premier octet soit un zéro, pour créer 128 réseaux de classe A au total.*
- *Classe B (128.0.0.0 /16 à 191.255.0.0 /16) : créée pour répondre aux besoins des réseaux de taille moyenne ou de grande taille comportant jusqu'à 65 000 adresses d'hôtes environ. Elle utilisait un préfixe /16 fixe avec les deux octets d'ordre haut pour indiquer l'adresse réseau et les trois derniers octets identifiant les*

adresses d'hôte. Les deux bits de poids fort de l'octet d'ordre haut doivent être 10 pour créer plus de 16 000 réseaux.

- *Classe C (192.0.0.0 /24 à 223.255.255.0 /24) : créée pour répondre aux besoins des réseaux de petite taille comportant 254 hôtes maximum. Elle utilisait un préfixe /24 fixe avec les trois premiers octets identifiant le réseau et l'octet restant identifiant les adresses d'hôte. Les trois bits de poids fort de l'octet d'ordre haut doivent être 110 pour créer plus de 2 millions de réseaux. La figure ci-dessous résume la classe C.*

Remarque : il existe également un bloc d'adresses de multidiffusion de classe D de 224.0.0.0 à 239.0.0.0 et un bloc d'adresses expérimentales de classe E de 240.0.0.0 à 255.0.0.0.

Spécifications de la classe C	
Bloc d'adresses	192.0.0.0 à 223.255.255.0
Masque de sous-réseau par défaut	/24 (255.255.255.0)
Nombre maximal de réseaux	2 097 152
Nombre d'hôtes par réseau	254
Bit d'ordre haut	110xxxxx.___.___.___

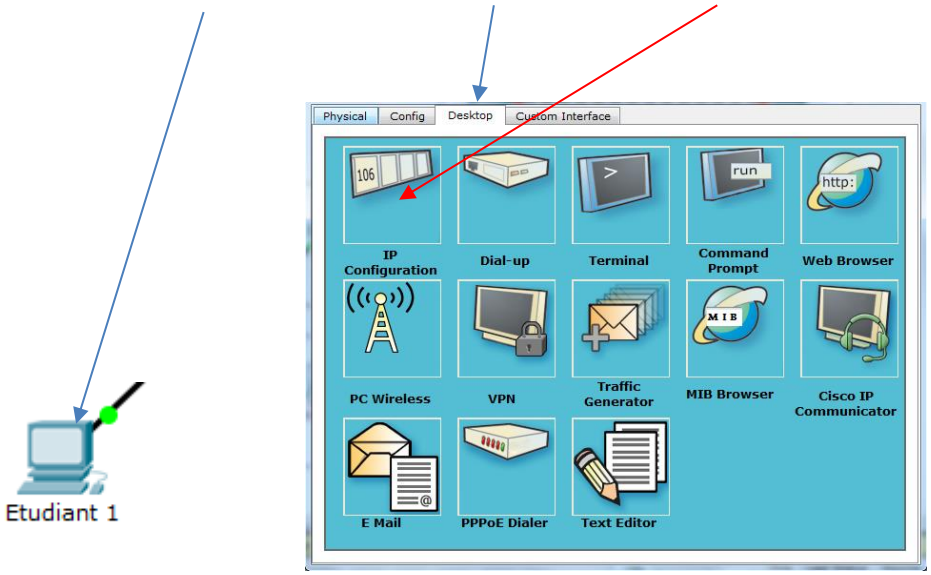
En dehors de l'adresse du serveur DNS qui est fourni, déterminer les adresses des PC étudiants, sachant qu'ils appartiennent au réseau 192.168.10.0 et que la passerelle occupe la première adresse IP disponible, le Vlan1 la seconde et que les PC étudiants prennent les suivantes dans l'ordre croissant en finissant par l'ordinateur de l'enseignant qui prend la dernière adresse disponible de ce réseau. S'agissant d'un réseau privé de classe C, indiquer également le masque de sous réseau standard :

- Adresse IP du Serveur DNS : 172.16.1.5
- Adresse de la passerelle par défaut : 192.168.10.1
- Adresse interface Vlan1 : 192.168.10.2
- Adresse IP du PC Etudiant 1 : 192.168.10.3
- Adresse IP du PC Etudiant 2 : 192.168.10.4
- Adresse IP du PC Etudiant 3 : 192.168.10.5
- Adresse IP du PC professeur : 192.168.10.254
- Masque de sous-réseau standard : 255.255.255.0

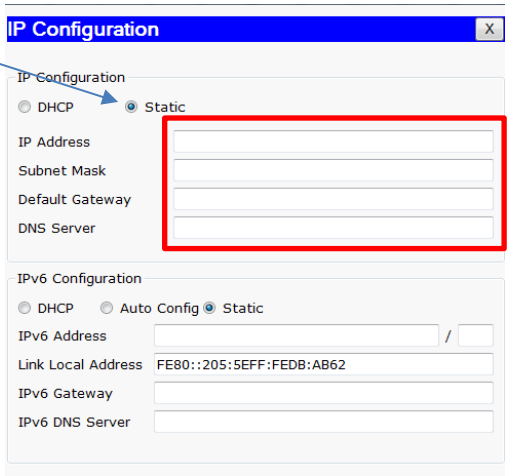
Q30 : Déterminer le masque de sous-réseau à implémenter.

Réponse : La classe utilisée ici est la classe C puisque l'adresse du réseau (192.168.10.0) est comprise entre 192.0.0.0 et 223.0.0.0, le masque est donc 255.255.255.0

Pour configurer les PC, cliquer sur le PC, puis sur l'onglet Desktop, enfin sur l'icône IP Configuration :

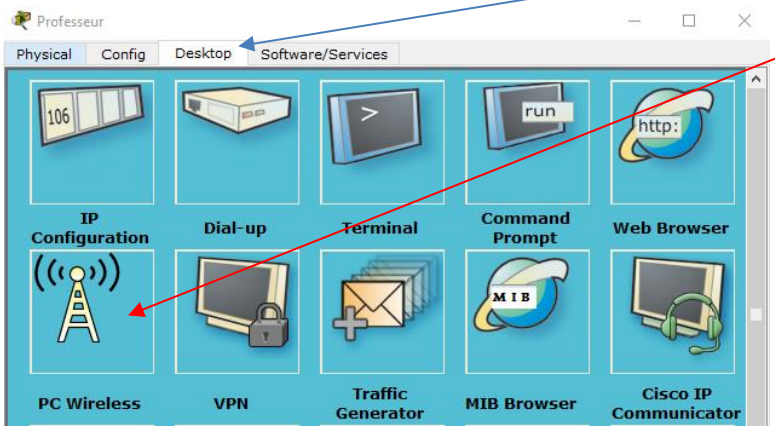


En mode "Static", renseigner la zone suivante pour finaliser la configuration de tous les PC :

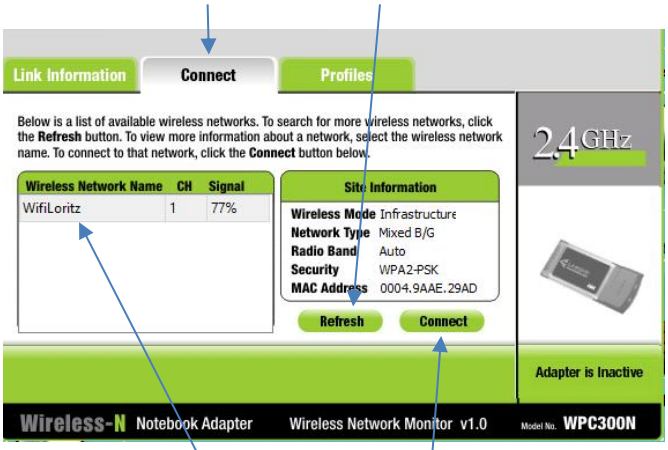


Etablir maintenant la connexion Wifi entre le PC professeur et le point d'accès.

Cliquer sur le PC Professeur et sélectionner l'onglet Desktop, puis cliquer sur PC Wireless.

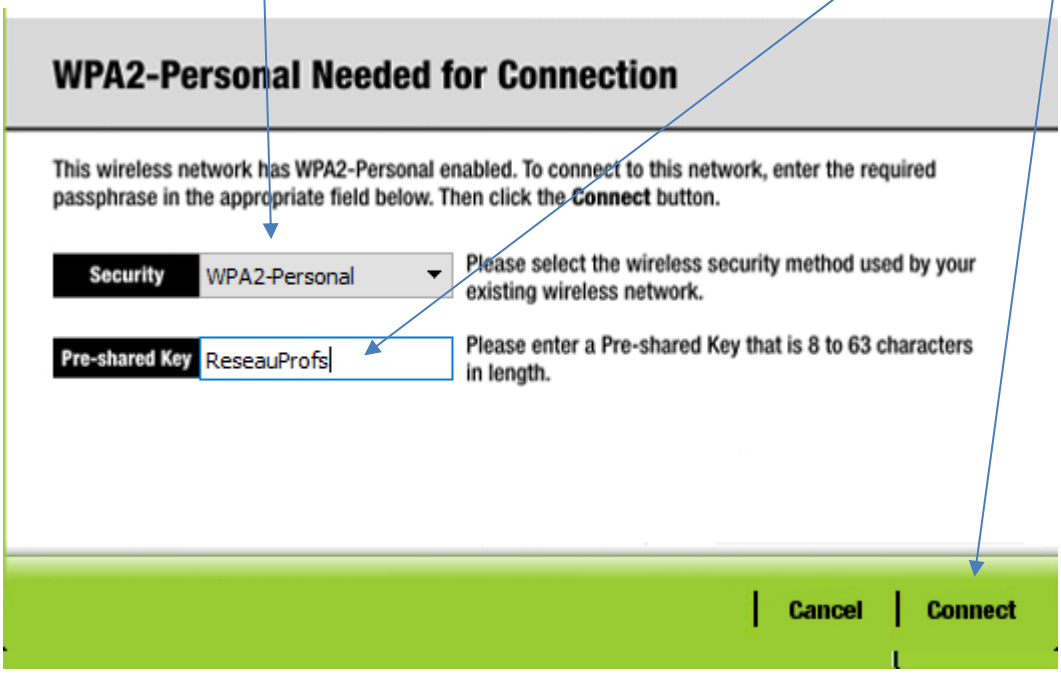


Cliquer sur Connect puis sur Refresh.

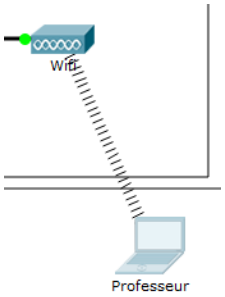


Choisir le bon SSID et cliquer sur Connect.

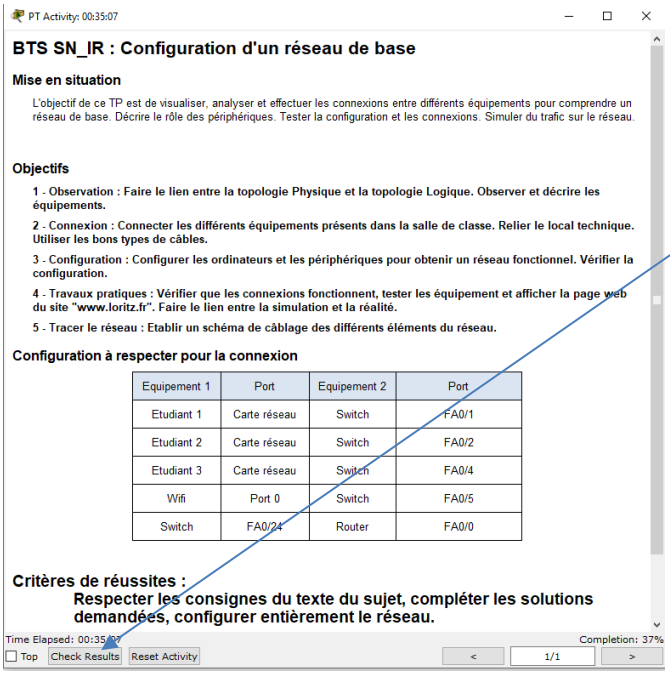
Choisir le type de cryptage correct et renseigner le mot de passe : ReseauProfs, puis Connect.



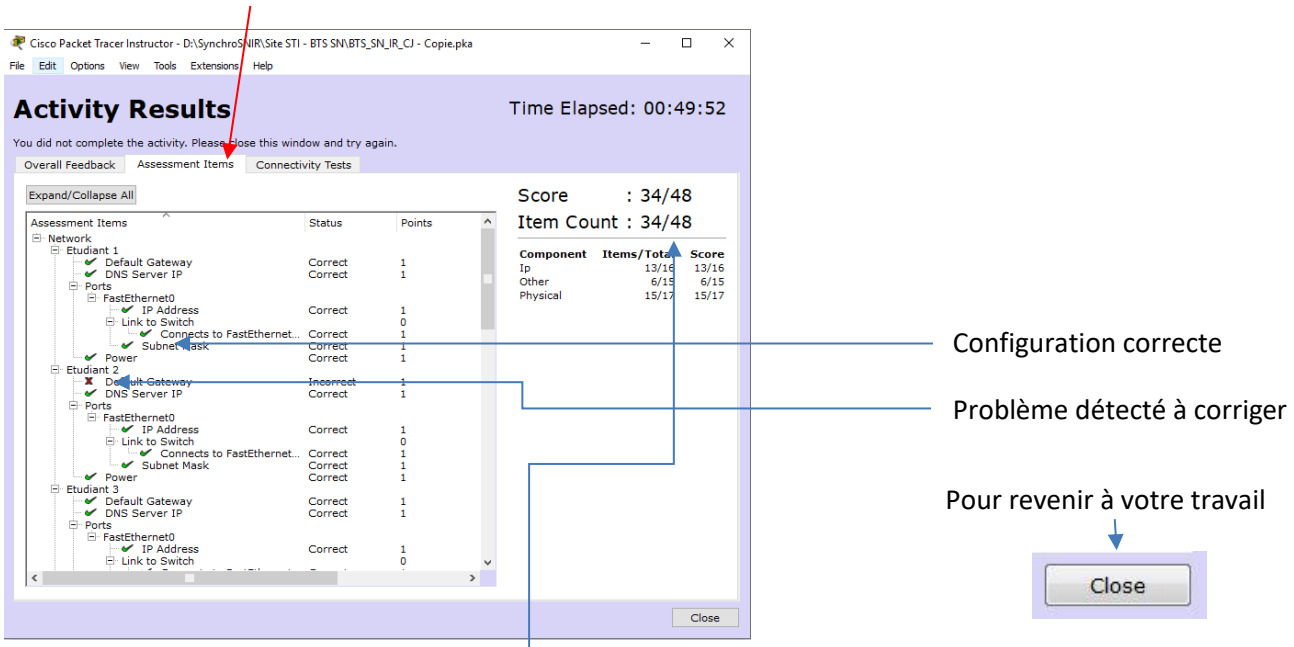
En cliquant sur Link Information on constate que la connexion est établie.



Vérifier votre configuration actuelle. Pour cela, ouvrir la fenêtre suivante, et cliquer sur Check Results :



Puis cliquer sur Assessment Items



A ce stade du TP, votre score doit être de 35/48, toutes les coches des PC doivent être vertes. Si ce n'est pas le cas, reprendre la partie 3-1 et vérifier l'ensemble des PC. Vous pouvez vous aider des encoches rouges pour déterminer les problèmes. Ici, le problème vient du PC Etudiant 2 qui a un problème de passerelle par défaut (default gateway).

Bilan intermédiaire

Faire la synthèse des connaissances abordées durant cette partie de l'activité, apporter les éléments de correction nécessaires aux étudiants.

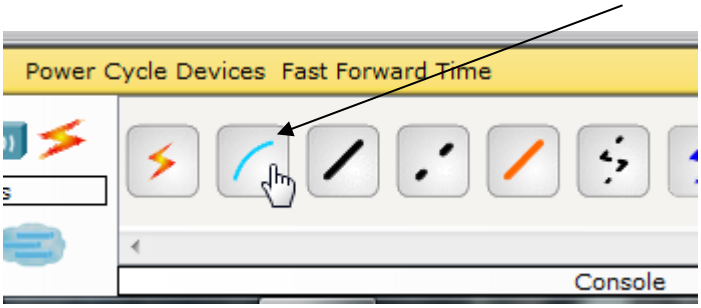
3-2 Configuration du commutateur (switch)

La configuration du switch est assez simple pour une configuration standard. Cette configuration va consister à nommer le commutateur, sécuriser les accès pour des modifications ultérieures et définir des adresses de passerelle par défaut ainsi qu'une adresse de Vlan (*Virtual LAN)*.

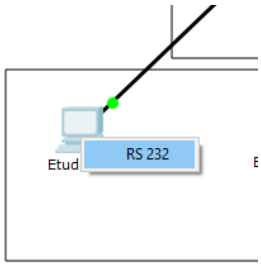
La configuration se fera uniquement en commande IOS, langage standard utilisé par le matériel Cisco.

La première étape consiste à connecter un ordinateur au switch pour accéder à la console qui permet la configuration.

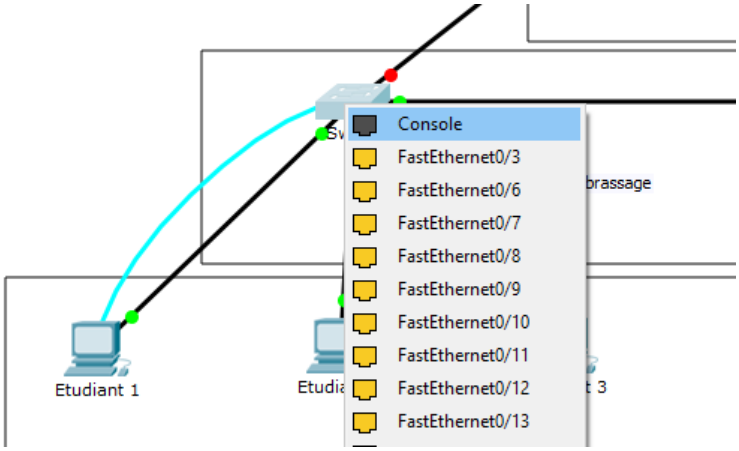
Cliquer sur le symbole connexion, puis sur le câble bleu ciel qui permet de relier le port console :



Cliquer ensuite sur le PC Etudiant 1 et connecter le port RS232 :



Cliquer sur le switch, choisir le port console :

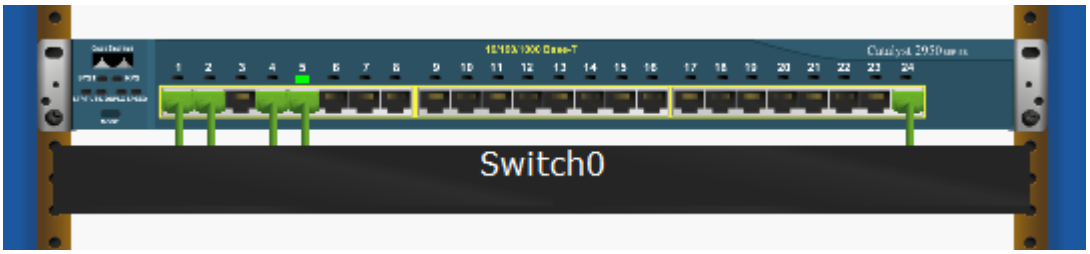


Un câble bleu ciel est maintenant connecté au port série du PC, liaison permettant de communiquer avec le switch.

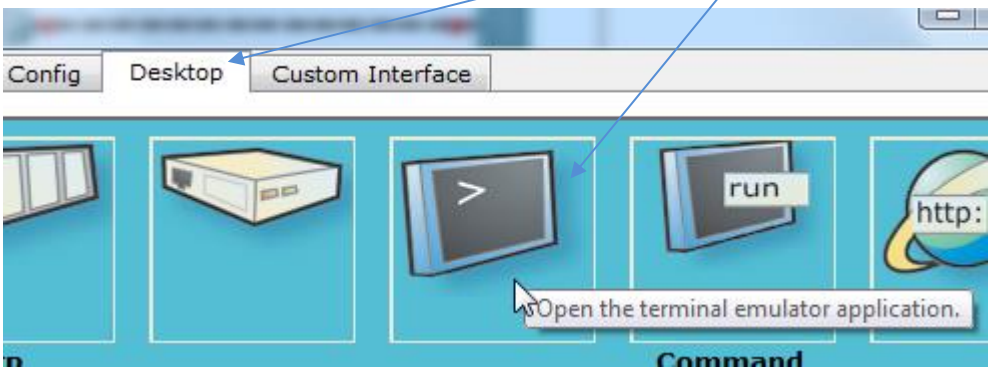
Passer en mode Physique et visualiser le switch dans l'armoire de brassage.

Q31 : Un câble a-t-il été ajouté ?

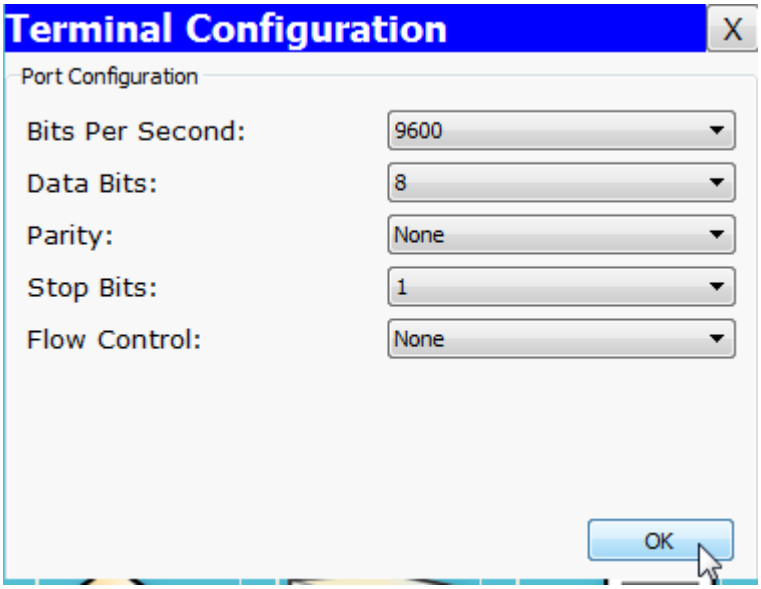
Réponse : Non, on ne visualise aucun câble supplémentaire car il s'agit de la face avant du switch. Ce câble a été connecté par l'arrière de l'appareil.



Cliquer maintenant sur le PC Etudiant 1, puis Desktop, puis Terminal :



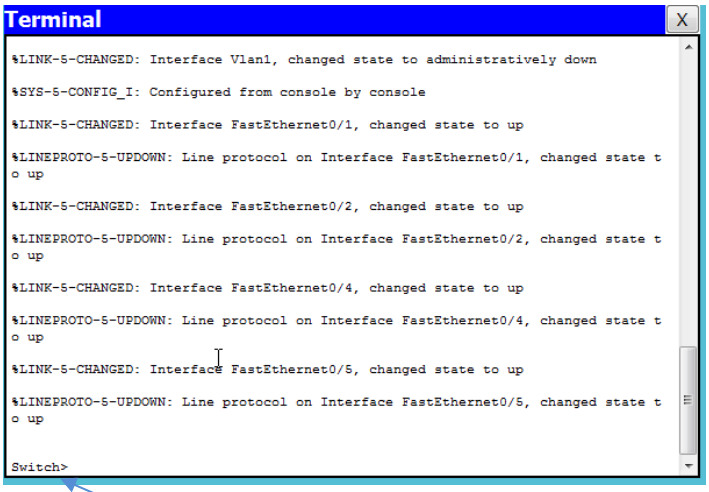
Une fenêtre s'ouvre pour configurer la communication entre les deux équipements via la liaison série RS232 :



Q32 : Déterminer la configuration standard pour une liaison série RS232 et comparer les valeurs par défaut. Indiquer s'il convient de modifier ces valeurs.

Réponse : On retrouve la vitesse de transmission (9600 bauds), le nombre de bit par trame (8), la parité, bit de stop et contrôle du flux. Cette configuration étant la configuration standard dans une communication RS232, il suffit de valider par OK.

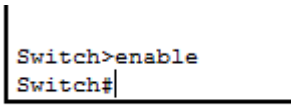
On obtient alors la fenêtre qui permet de configurer le switch, la communication est établie entre le switch et le PC :



La seconde étape consiste à entrer les commandes pour configurer le switch.

Dans un premier temps, il convient de passer en mode privilégié, c'est-à-dire en mode **administrateur**. Le fait que l'invite de commande affiche « Switch> » montre que nous sommes en mode utilisateur simple.

Taper la commande suivante : « enable »



« Switch# » indique que nous sommes en mode privilégié.

3-2-1 Configuration du nom

Pour configurer un terminal, il faut indiquer le mode de configuration du terminal.

Taper : « configure terminal » le switch affiche maintenant Switch(config)# qui prouve que la configuration est activée.

Changer le nom du switch

Taper : « hostname S1 » le nom a changé en S1(config)#

3-2-2 Sécuriser le mode privilégié

Il faut indiquer un mot de passe crypté pour interdire l'accès non autorisé au switch. Le mot de passe sera « class ».

Taper : « enable secret class »

3-2-3 Accès au port console

Pour modifier ultérieurement votre configuration, vous devez autoriser l'accès au port console du switch. Cet accès sera sécurisé par le mot de passe « cisco ».

Taper : « line console 0 » vous obtenez S1(config-line)#

Activer le mot de passe

Taper : « password cisco » Le mot de passe étant cisco

Activer la ligne

Taper : « login »

Sortir du mode line console 0

Taper : « exit »

Chiffrer le mot de passe

Taper : « service password-encryption »

Ainsi le mot de passe n'apparaitra pas en clair si vous avez laissé le mode privilégié sans surveillance.

3-2-4 Prévenir d'un accès sécurisé

Ne jamais souhaiter la bienvenue à un utilisateur non autorisé (Hacker), indiquer que cet accès est réservé ou interdit.

Taper : « banner motd #Acces interdit# »

3-2-5 Configuration du Vlan

Ceci permet un accès au vlan par un port du réseau local (FA0/1 à FA0/24).

Taper : « interface vlan1 »

Indiquer l'adresse IP et son masque de sous réseau

Taper : « ip address 192.168.10.2 255.255.255.0 »

Activer le vlan

Taper : « no shutdown »

Sortir du mode de configuration du vlan1

Taper : « exit »

3-2-6 Passerelle par défaut

Q33 : Déterminer ce qu'est une passerelle. 🔍💻

Réponse : Pour sortir du réseau local et accéder à un autre réseau ou à internet, il faut indiquer si un routeur est présent et donner son adresse d'accès. C'est la passerelle par défaut. Tous les messages ayant une adresse différente du réseau 192.168.10.0 seront transmis à cette passerelle.

Taper : « ip default-gateway 192.168.10.1 »

Sortir du mode de configuration

Taper : « exit »

3-2-7 Sauvegarde de la configuration

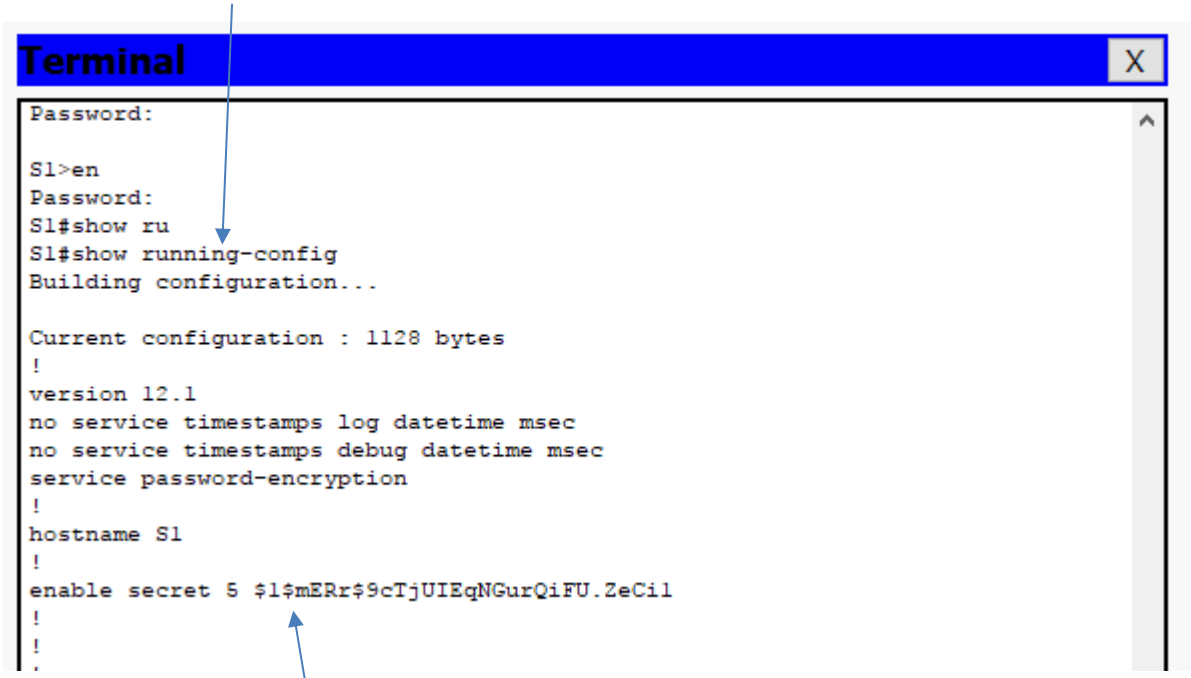
En cas de coupure de courant, cette configuration sera perdue. Il convient donc d'en faire la sauvegarde en mémoire.

Avant de sauvegarder la configuration courante, il convient de vérifier qu'il n'y a pas d'erreur dans les adresses, mots de passe, etc.

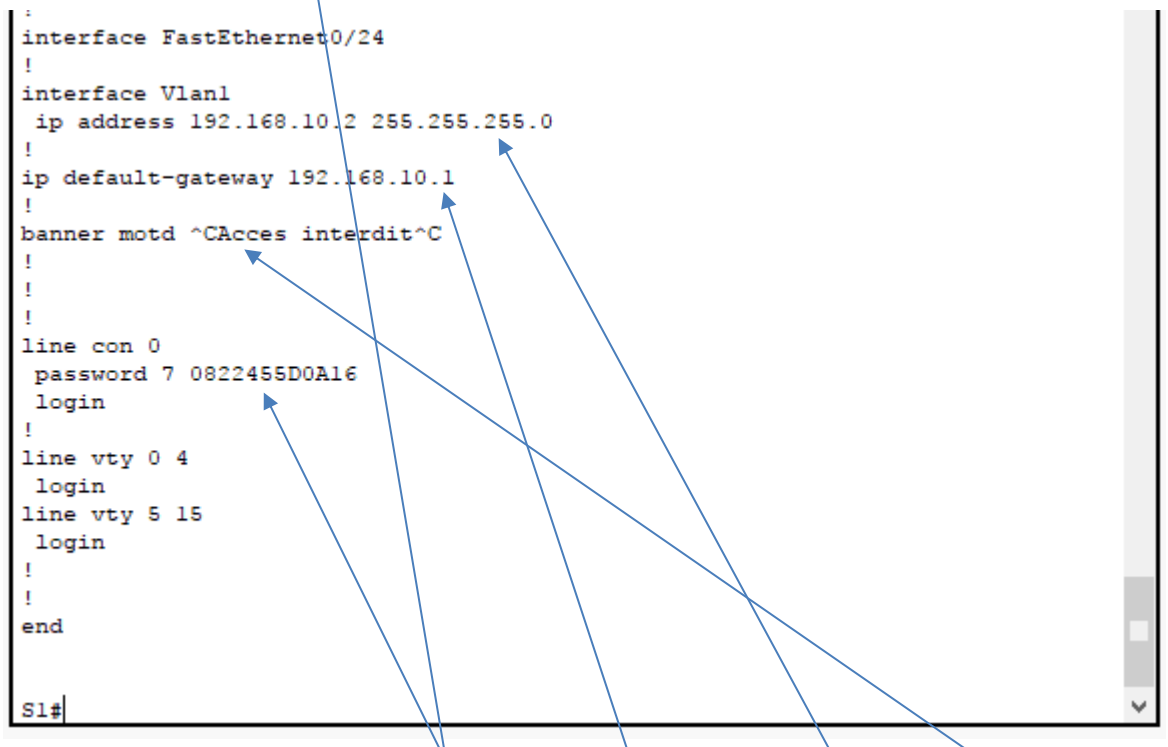
Vous devez avoir l'invite suivant : S1#

Sinon, appuyer sur « ctrl + c »

Taper : « show running-config »



…



Vérifier que les mots de passe sont cryptés, la passerelle par défaut, l'adresse Vlan, etc.

Si la configuration actuelle correspond à celle attendue, passer à la sauvegarde, sinon corriger votre configuration.

Taper : « copy running-config startup-config » confirmer par appui sur la touche entrée

La configuration actuelle est enregistrée.

Sortir du mode privilégié

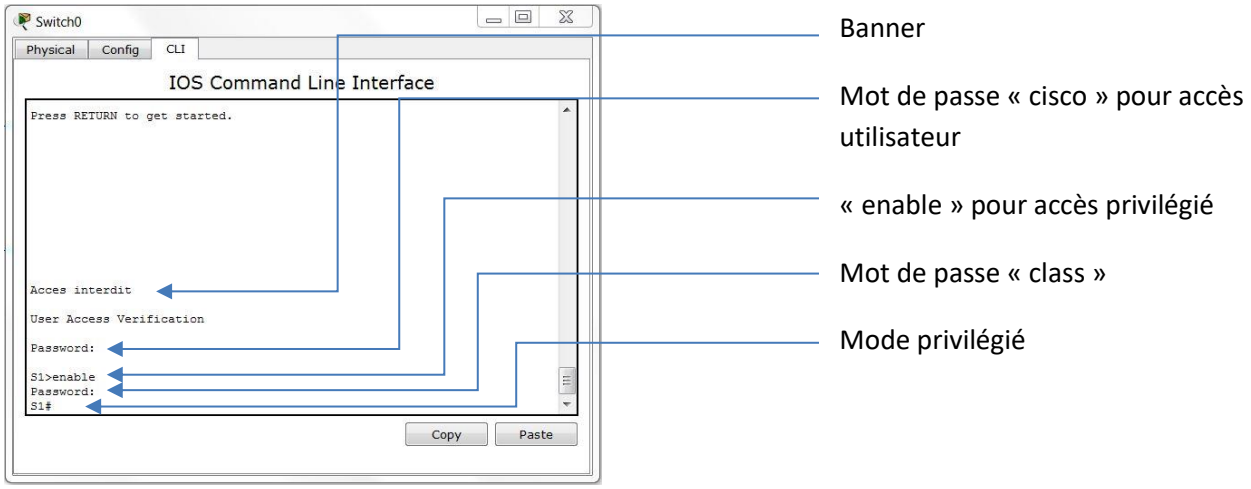
Taper : « exit »

3-2-8 Test de configuration

Appuyer sur entrée, la banner s'affiche (Acces interdit) puis un mot de passe vous est demandé (cisco).

Taper « enable » pour accéder au mode privilégié, un autre mot de passe vous est demandé (class).

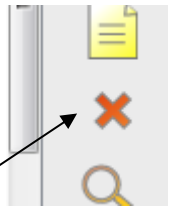
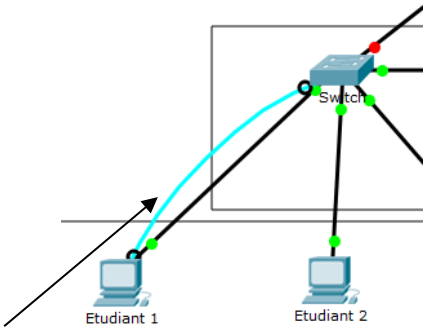
Comme le montre la capture ci-dessous :



Tester votre configuration en cliquant sur Check Results. Votre score à ce moment du TP doit être de 41/48.

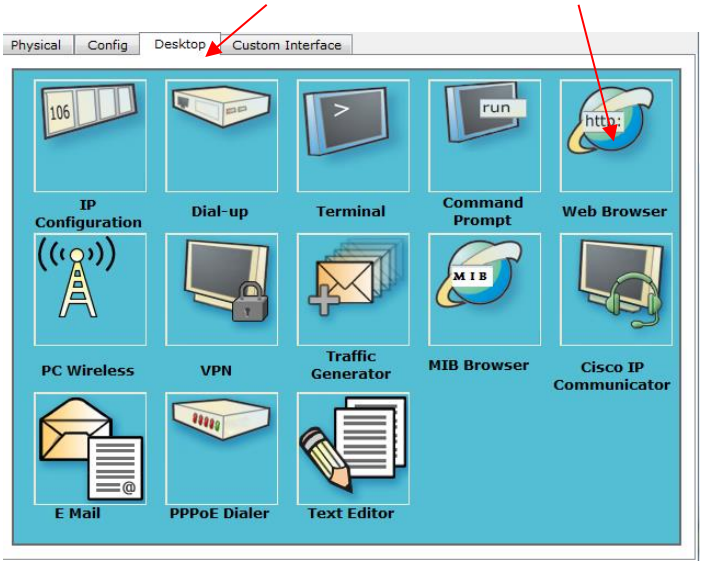
Si ce n'est pas le cas, reprendre la configuration depuis le début du chapitre 3-2. Vous pouvez vous aider des coches rouges pour déterminer le problème.

Si votre score est bien de 41/48, débrancher le câble console, enregistrer votre fichier.

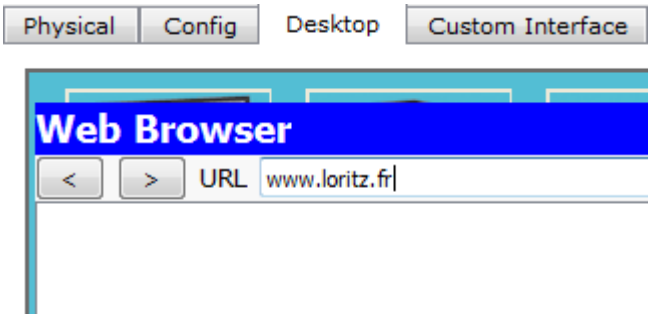
Clic sur  puis sur le câble 

Le réseau local (LAN) étant maintenant configuré, nous allons essayer d'accéder à internet.

Cliquer sur n'importe quel PC, puis sur l'onglet Desktop et enfin sur l'icône http :

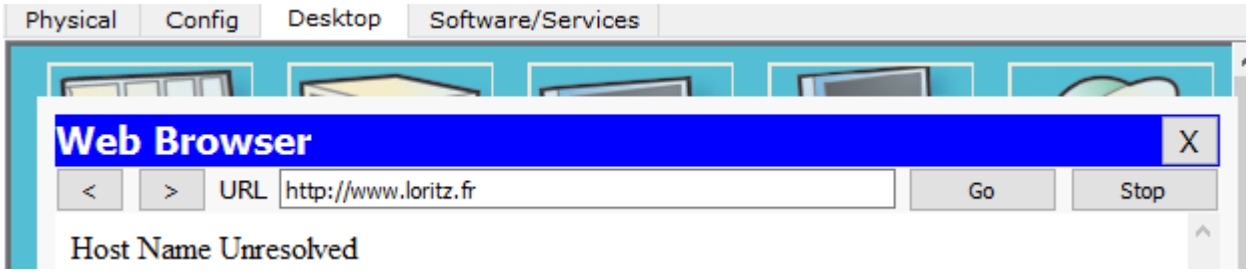


Taper l'adresse suivante : www.loritz.fr



Q34 : Que constatez-vous ?

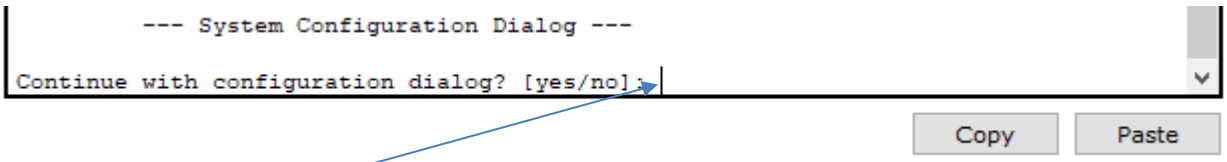
Réponse : Le PC ne peut pas atteindre l'adresse demandée. Le réseau local est effectivement configuré, mais comme le routeur qui permet d'accéder à internet n'est pas encore activé, nous ne pouvons atteindre la page web demandée.



3-3 Configuration du routeur

La configuration du routeur va être très similaire sur certains points. Seul l'adressage des interfaces sera différent.

Lors de l'établissement de la connexion (câble bleu ciel) entre le routeur et le PC, l'interface pose la question suivante :



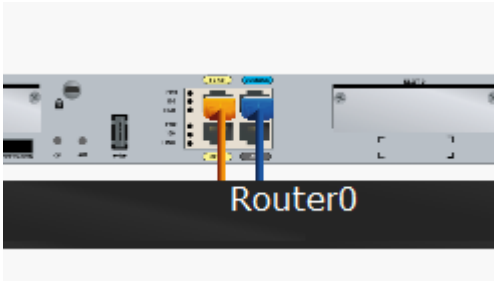
Répondre no

De manière autonome, **connecter le routeur à un PC Etudiant grâce à une câble console (même procédure que pour le switch)**, puis configurer, les points suivants (les commandes sont identiques à celles du switch) :

- Changer le nom du router en « R1 »
- Sécurisation du mode privilégié avec le mot de passe « class »
- Accès au mode line console 0 avec le mot de passe « cisco » qui sera crypté
- Banner avec la phrase « Acces interdit **!!!** », respecter bien le texte imposé.

Q35 : Après avoir connecté le câble console, passer en mode Physique et visualiser le Routeur. Que constatez-vous ?

Réponse : Cette fois on constate un câble supplémentaire, effectivement, le raccordement du port console se trouve de ce côté de la façade du routeur contrairement au switch.



3-3-1 Configuration des interfaces

Il ne reste plus qu'à configurer les deux interfaces du routeur, avec les adresses de chaque réseau auquel il est connecté.

Interface FA0/0, c'est elle qui sert de passerelle au réseau local, elle transmet au réseau suivant tous les paquets n'ayant pas une adresse correspondant au réseau 192.168.10.X. Son adresse, que nous avons configurée sur les PC est donc 192.168.10.1

Appuyer sur « ctrl + c » pour obtenir l'invite suivant R1#

Taper : « configure terminal »

Sélectionner l'interface à configurer

Taper : « interface fa0/0 » on obtient R1(config-if)#

Donner l'adresse IP et son masque de sous réseau.

Taper : « ip address 192.168.10.1 255.255.255.0 »

Activer le port

Taper : « no shutdown »

Sortir de la configuration de fa0/0

Taper : « exit »

Vous constatez alors, que la couleur de la liaison entre le routeur et le switch a changé, elle est passée du rouge au vert.

L'interface FA0/1 permet de communiquer avec le réseau suivant. Son adresse doit donc appartenir à ce réseau.

Taper : « interface fa0/1 »

Configurer l'adresse

Taper : « ip address 172.16.1.1 255.255.255.0 »

Activer le port

Taper : « no shutdown »

Sortir de la configuration de fa0/1

Taper : « exit »

Vous constatez alors, que la couleur de la liaison entre le routeur et le serveur Loritz a changé, elle est passée du rouge au vert.

Taper : « ctrl + c »

Vérifier votre configuration, même méthode qu'avec le switch en tapant « show running-config », la modifier en cas d'erreur sinon passer à la sauvegarde.

Sauvegarder votre configuration.

Taper : « copy running-config startup-config » confirmer par appui sur la touche entrée

Vérifier votre score en cliquant sur Check Results, votre configuration étant terminée, vous devez obtenir 48/48.

Si ce n'est pas le cas, reprendre la configuration du chapitre 3-3 et vous aider des coches rouges.

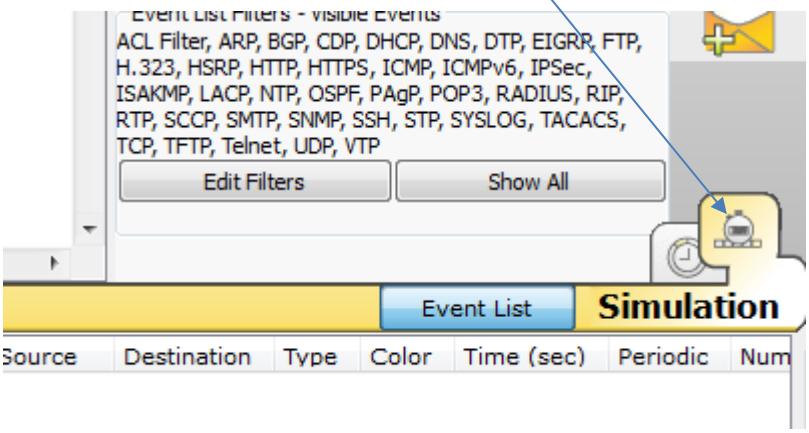
Si votre score est bien de 48/48, débrancher le câble console du routeur, enregistrer votre fichier.

4 – Test de connexion

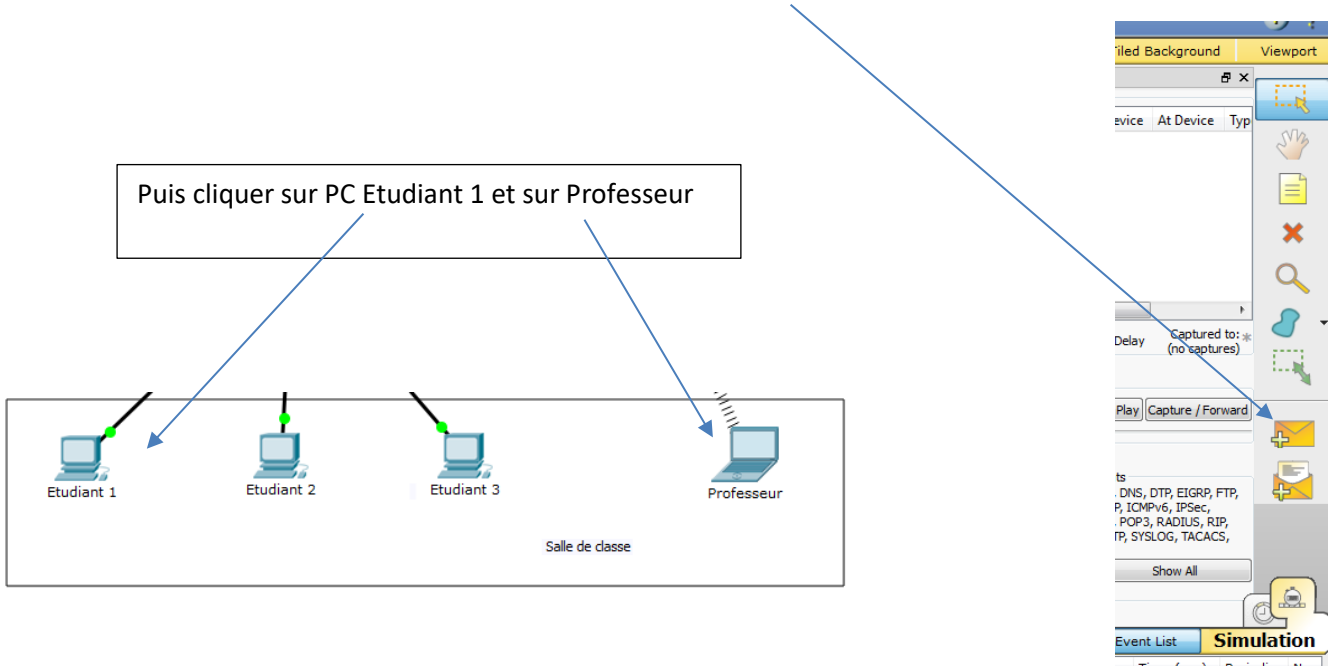
4-1 Réseau local simulé

Pour tester si votre configuration est correcte, nous allons tester des communications avec les équipements qui appartiennent au réseau local, dont l'adresse correspond à 192.168.10.X

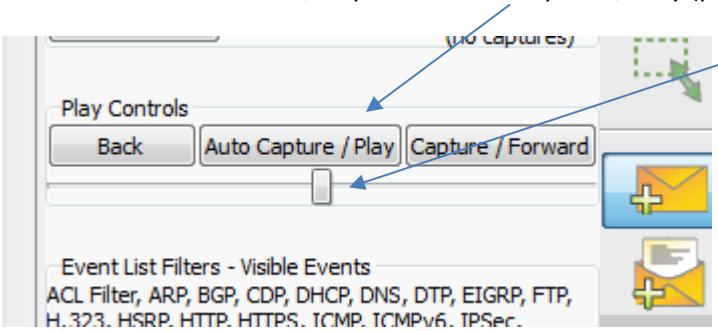
Le meilleur moyen de tester une communication est l'utilisation de la fonction ping. Pour bien comprendre le processus de cette commande, nous allons passer en mode simulation. Cliquer sur Simulation (en bas à droite de la feuille de travail) :



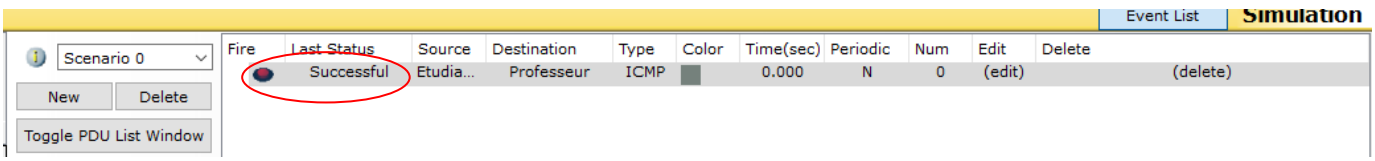
Puis pour envoyer un ping entre deux équipements, cliquer sur l'enveloppe :



Pour visualiser l'animation, cliquer sur Auto Capture / Play (pour régler la vitesse)



Regarder l'animation jusqu'à avoir le résultat suivant :



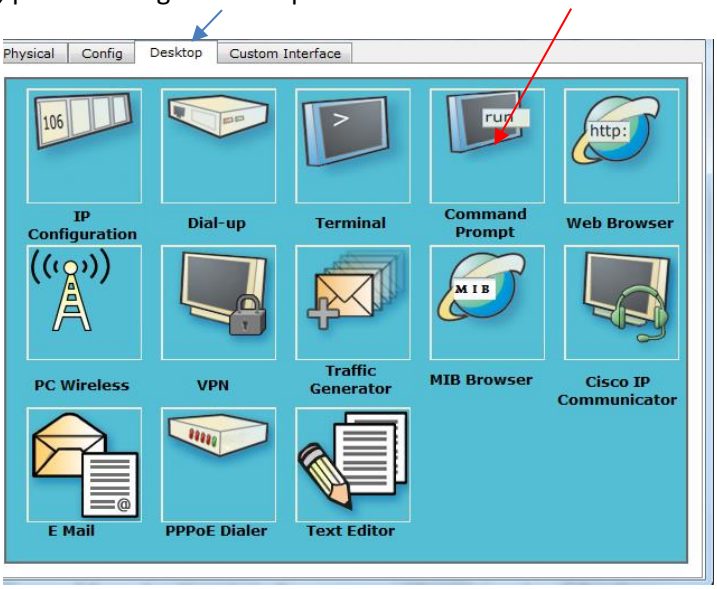
Cliquer à nouveau sur Auto Capture / Play pour interrompre la simulation.

Q36 : Expliquer le fonctionnement du ping au démarrage d'un réseau.

Réponse : Le switch reçoit le ping sur le port Fa0/1. Ne connaissant pas encore le destinataire, il ne peut transmettre la demande. Il envoi alors un message (Requête ARP) à tous les hôtes du réseau pour savoir lequel se trouve à l'adresse demandée. Tous les hôtes non concernés rejettent la demande (croix rouge sur l'enveloppe) sauf le périphérique concerné qui renvoi un message au switch, avec confirmation de son adresse IP ainsi que son adresse MAC. Le switch stocke alors cette information dans une table ARP et sait maintenant que les messages destinés à ce périphérique se trouvent sur le port Fa0/5. La commande ping étant diffusée 4 fois, le premier ping revient en erreur, en revanche, les 3 autres ping seront validés et auront une réponse (Echo). Cette situation n'est valable que la première fois, tant que la table ARP du routeur et du PC est vide.

Tester toutes les connexions en effectuant des ping sur tous les PC, y compris celui du professeur dont l'adresse IP est 192.168.10.6

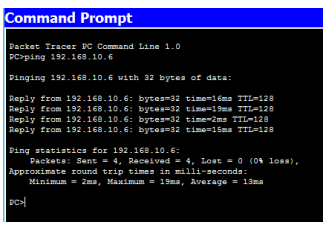
Cliquer sur le PC Etudiant 1, puis sur l'onglet Desktop et enfin sur l'icône Command Prompt :



Dans la fenêtre qui s'ouvre, taper « ping 192.168.10.4 » pour savoir si la communication avec le PC Etudiant 2 est possible. Faire de même avec les autres adresses et reproduire ceci sur tous les PC de la salle de classe.

Q37 : Insérer des captures d'écrans prouvant que les requêtes ping ont abouti.

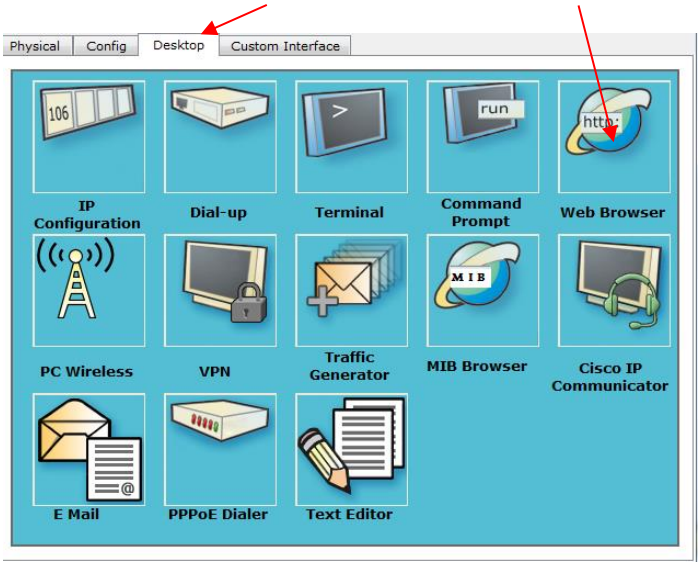
Réponse :



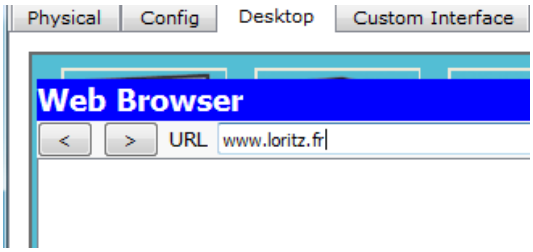
4-2 Accès internet

Les PC peuvent communiquer entre eux, mais nous devons vérifier que le routeur nous permet d'accéder à un autre réseau.

Cliquer sur n'importe quel PC, puis sur l'onglet Desktop et enfin sur l'icône http :



Taper l'adresse suivante : www.loritz.fr



Q38 : Que constatez-vous ?

Réponse : La fenêtre s'ouvre et donne accès à une page web. Un message indique que la configuration est correcte. La page web du lycée Loritz s'affiche.

4-3 Tracer votre réseau

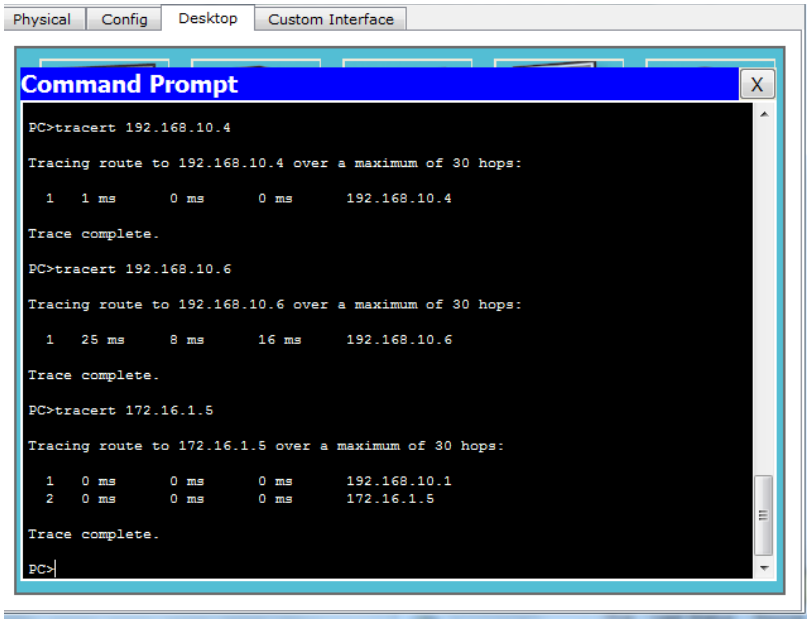
Il existe parmi les commandes « Shell » une commande qui permet de « tracer » les équipements. Contrairement au ping vu précédemment, la commande « **tracert** » détermine le nombre de sauts qu'il faut pour atteindre la cible et donc le nombre d'équipements à traverser pour arriver au périphérique final.

Depuis le PC Etudiant 1, utiliser la commande **tracert** pour trouver la route du PC Etudiant 2, le PC Professeur et le serveur Loritz (172.16.1.5).

Taper : « tracert 192.168.10.4 » dans la fenêtre "invite de commande" pour tracer le PC Etudiant 2.

Q39 : Donner les captures d'écran de vos résultats.

Réponse :



Q40 : En analysant votre topologie logique, expliquer les captures d'écran notamment en identifiant les différents équipements du réseau.

Réponse :

Entre PC Etudiant 1 et PC Etudiant 2 on ne constate qu'un saut. Ce qui veut dire qu'il n'y a qu'un seul équipement entre les deux PC. Il s'agit ici du switch S1.

Entre Etudiant 1 et PC Professeur, là encore, un seul saut, donc un seul équipement. En fait, la borne Wifi connectée au switch est transparente, mais il y a bien deux équipements, le switch et le point d'accès Wifi.

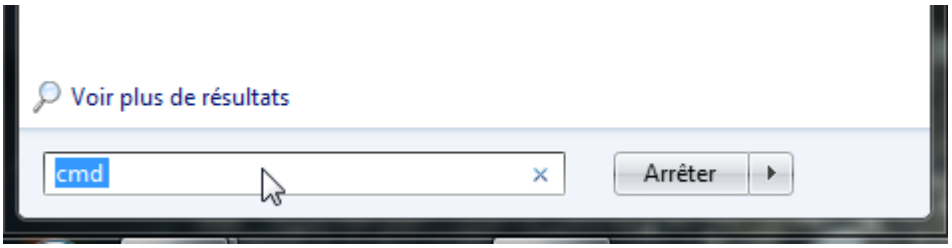
Entre PC Etudiant 1 et le serveur Loritz, on constate deux sauts, donc deux équipements. Le premier correspond au switch S1 et transmet à la passerelle (192.168.10.1). Le second correspond au routeur, sur lequel le serveur est directement connecté (172.16.1.5)

Remarque : Certains équipements utilisent des pares-feux qui ne laissent pas passer la fonction « tracert ». Dans ce cas, la trace est incomplète. Il existe aussi des logiciels plus performants, qui déterminent avec précision les équipements traversés.

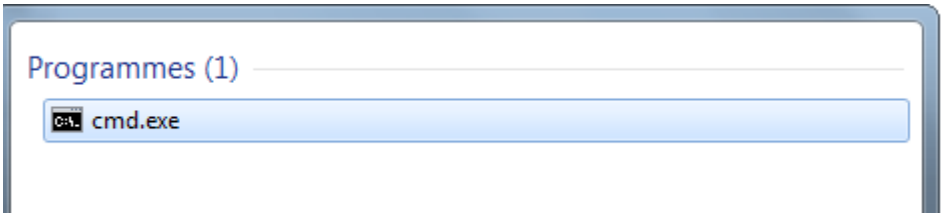
5 – Topologie Réelle

5-1 Tester le réseau de votre salle de classe

Dans le menu démarrer de votre PC, taper "cmd" dans rechercher les programmes et fichiers :



Cliquer sur le résultat obtenu :



Comme pour le réseau testé sous Packet Tracer, votre PC est configuré avec des nom, adresse IP, adresse MAC…

Q41 : En utilisant la fonction « ipconfig /all », relever les informations suivantes :

- **Adresse IP**
- **Masque de sous-réseau**
- **Adresse MAC**
- **Nom du PC**
- **Serveur DNS**
- **Adresse de passerelle**

Réponse :

Cette réponse dépend des PC des étudiants.

Par exemple :

```
Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . : Hades
   Suffixe DNS principal . . . . . . :
   Type de noeud. . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . : Non
```

```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7260
   Adresse physique . . . . . . . . . . . : 80-19-34-[redacted]
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::5890:df3a:7354:80b6%6(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.7.13(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : mercredi 22 novembre 2017 18:38:05
   Bail expirant. . . . . . . . . . . . . : jeudi 23 novembre 2017 06:38:05
   Passerelle par défaut. . . . . . . . . : 192.168.7.254
   Serveur DHCP . . . . . . . . . . . . . : 192.168.7.254
   IAID DHCPv6 . . . . . . . . . . . : 58726708
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-1B-F4-0C-32-54-A0-50-89-DB-D0
   Serveurs DNS. . .  . . . . . . . . . . : 192.168.7.254
```

5-1 Tester les connexions

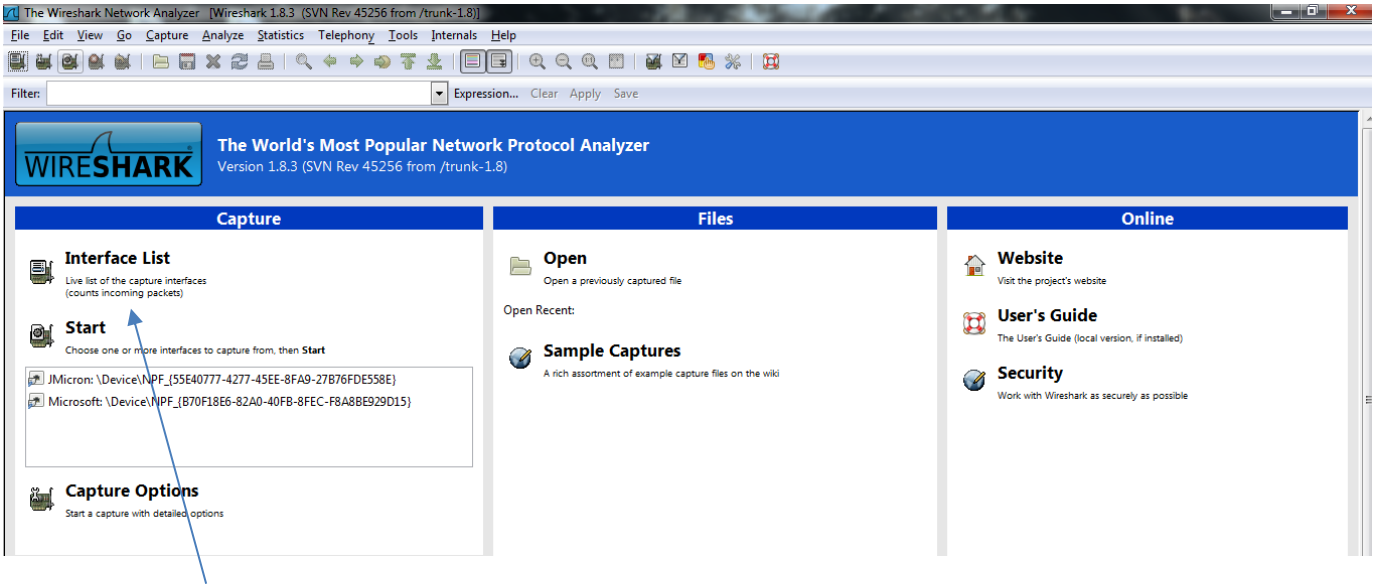
Demander à deux autres étudiants de vous donner leur adresse IP, ainsi qu'au professeur.

Faire un ping sur chaque équipement pour vérifier que les connexions fonctionnent.

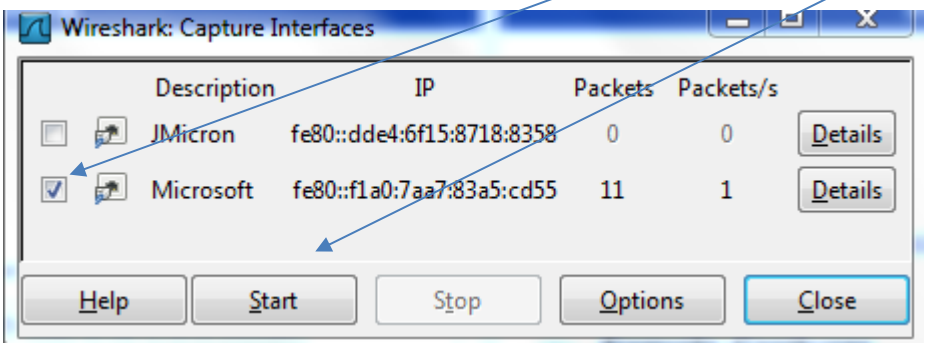
Pour vérifier le fonctionnement réel de la fonction ping, nous allons utiliser le logiciel Wireshark qui permet de capturer les trames présentes sur le réseau auquel est connecté le PC.

Lancer le logiciel : 

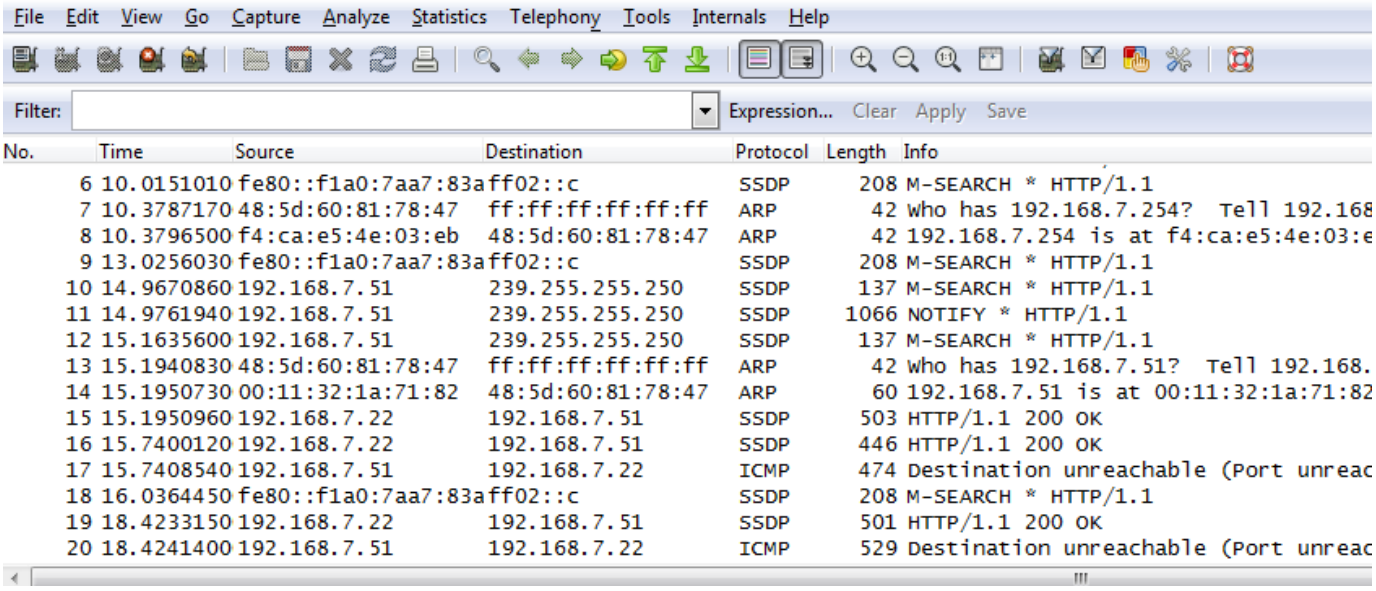
L'application peut changer selon la version de Wireshark utilisée.



Cliquer sur Interface List, puis cocher l'interface Microsoft, cliquer sur Start.

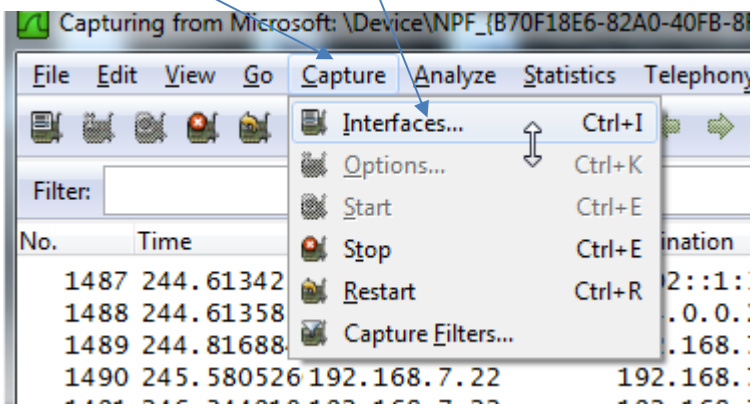


La capture de trames commence, mais tous les échanges apparaissent.

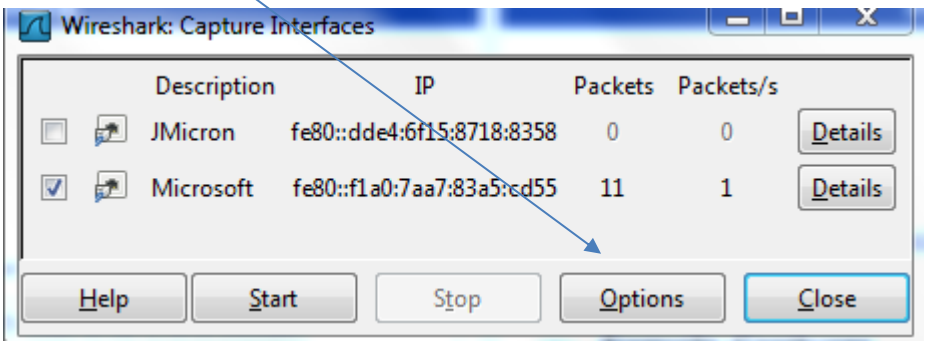


Nous allons affiner notre recherche en réglant quelques options.

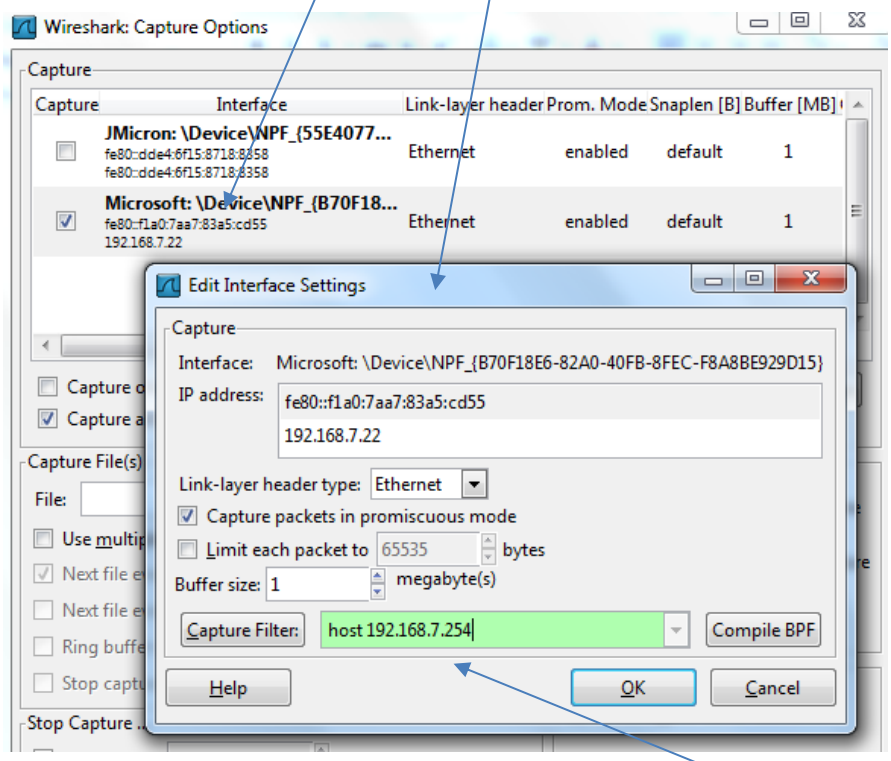
Cliquer sur Capture puis Interfaces.



Cliquer sur Options.

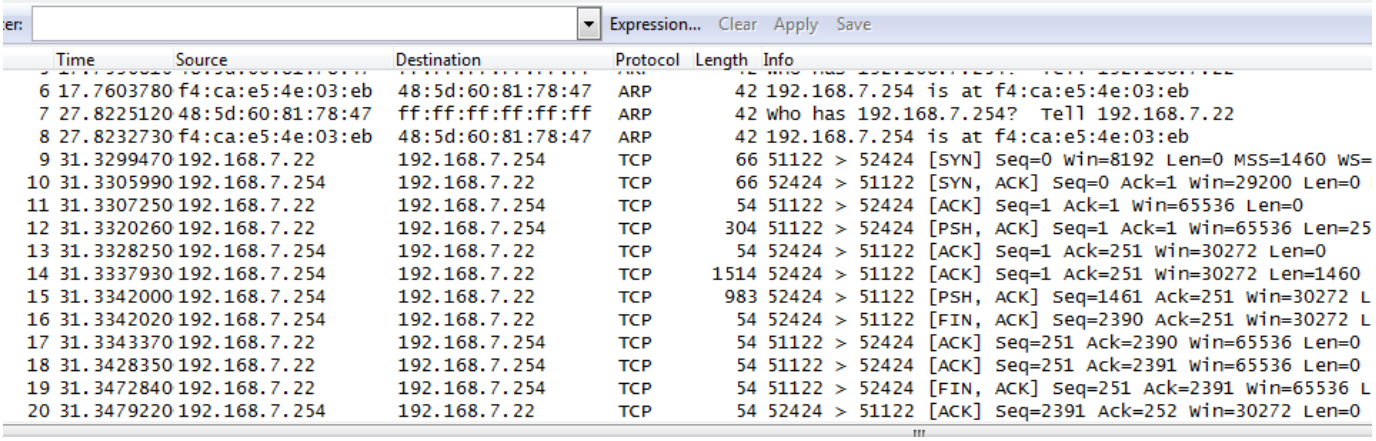


Double cliquer sur l'interface. Edit interface Settings s'ouvre.

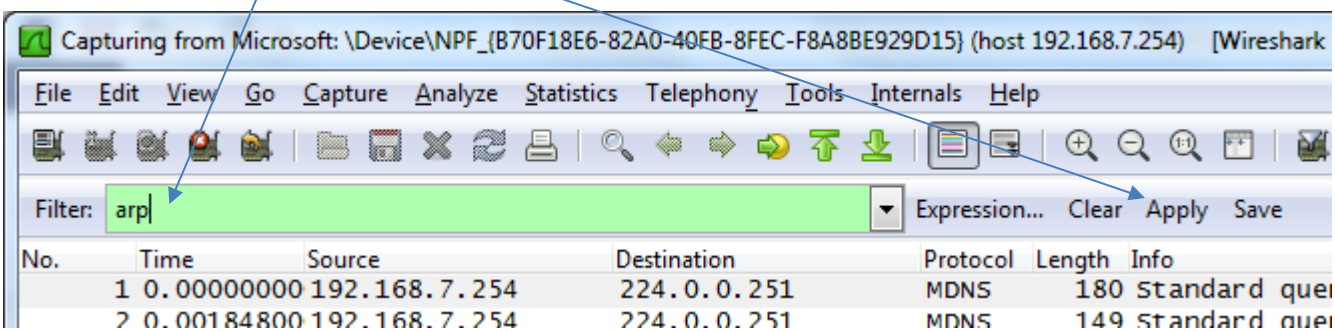


Nous pouvons affiner la recherche de paquets en entrant l'adresse IP de l'équipement avec lequel nous recherchons les communications. Entrer l'adresse IP de l'hôte avec lequel vous allez envoyer des ping (prendre l'adresse IP d'un autre étudiant). Valider, puis cliquer sur Start.

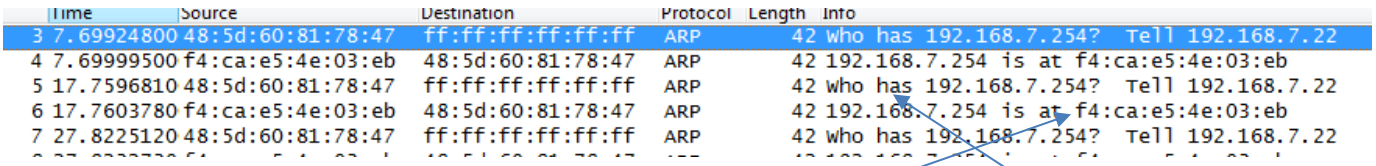
Nous ne récupérons maintenant que les échanges entre l'adresse du PC (192.168.7.22) et l'adresse de l'hôte avec lequel nous voulons dialoguer :



On constate encore beaucoup d'échanges. Affinons de nouveau en travaillant sur le protocole.
Dans Filter, mettre « arp » et cliquer sur Apply.



Nous obtenons alors les requêtes ARP entre les deux hôtes.



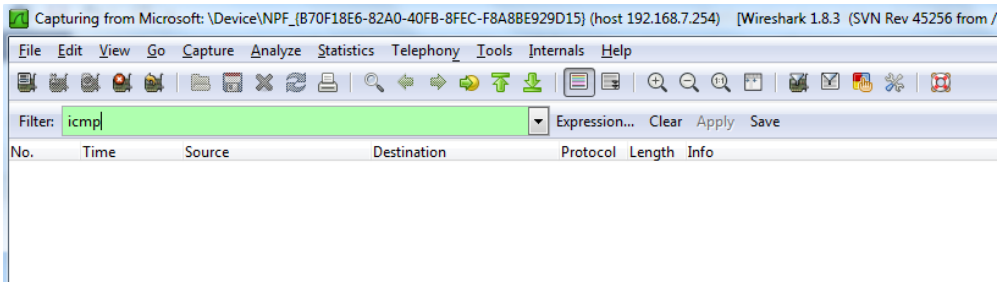
No.	Time	Source	Destination	Protocol	Length	Info
3	7.69924800	48:5d:60:81:78:47	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.7.254? Tell 192.168.7.22
4	7.69999500	f4:ca:e5:4e:03:eb	48:5d:60:81:78:47	ARP	42	192.168.7.254 is at f4:ca:e5:4e:03:eb
5	17.7596810	48:5d:60:81:78:47	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.7.254? Tell 192.168.7.22
6	17.7603780	f4:ca:e5:4e:03:eb	48:5d:60:81:78:47	ARP	42	192.168.7.254 is at f4:ca:e5:4e:03:eb
7	27.8225120	48:5d:60:81:78:47	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.7.254? Tell 192.168.7.22

Ces requêtes correspondent en tout point à ce que nous avons vu lors de la partie simulation sur Packet Tracer. Les requêtes ARP servent à demander à un hôte s'il est toujours présent sur le port de destination (who has). La réponse de l'hôte est le renvoi de son adresse MAC pour confirmer qu'il est toujours connecté et que la communication est possible.
Comme on peut le constater sur la capture, cette requête est récurrente. Le switch ou le routeur met en fait périodiquement sa table ARP (**Address Resolution Protocol)** à jour. Dès qu'un hôte disparait (éteindre un PC par exemple), la table est mise à jour et le transfert des paquets pour cet hôte ne se fera plus.

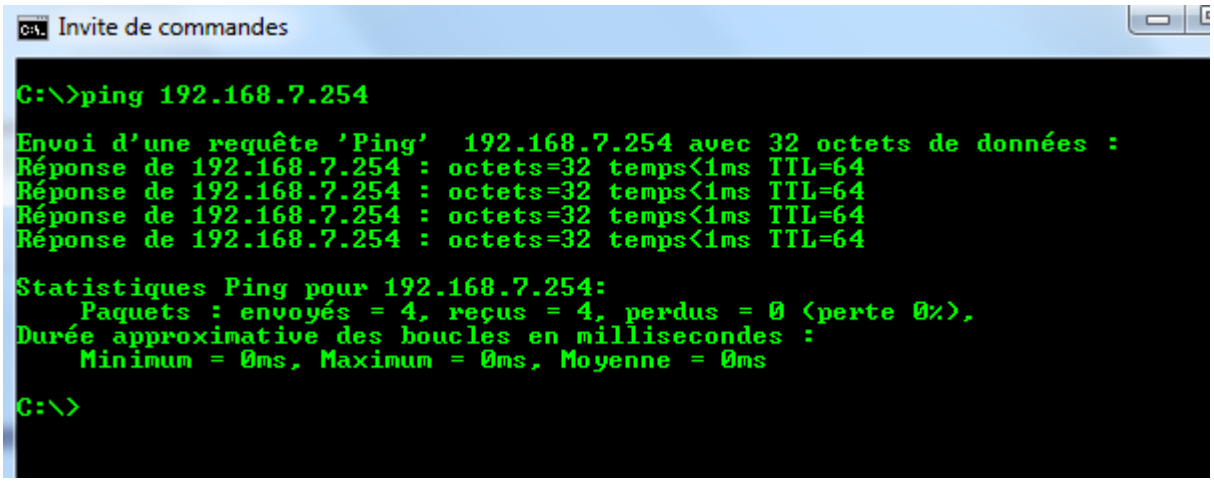
Nous allons maintenant visualiser les échanges lors d'une demande de ping. Le ping, correspond au protocole ICMP (**Internet Control Message Protocol)**. Modifier le filtre en enlevant ARP et en le remplaçant par ICMP.

Q42 : Que constatez-vous ?

Réponse : La zone de capture est vide, aucun échange ne se fait entre les deux adresses entrées.

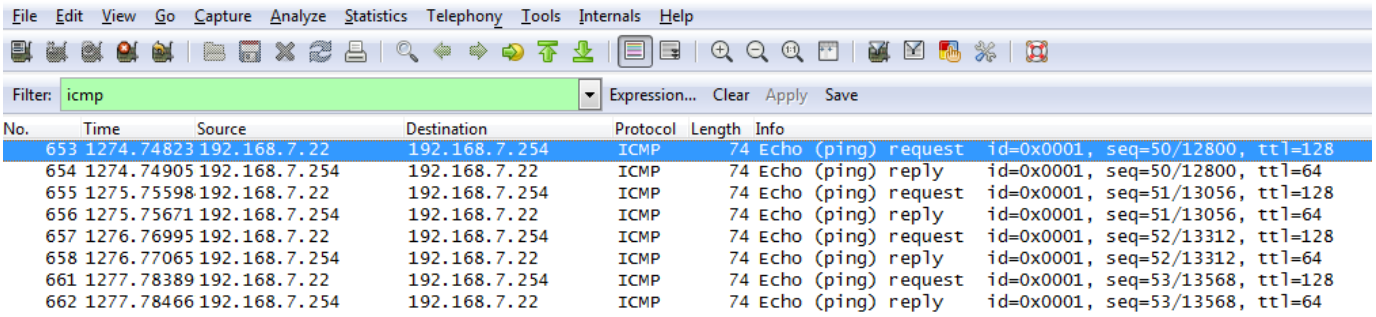


Faire un ping entre les deux hôtes. Exemple :

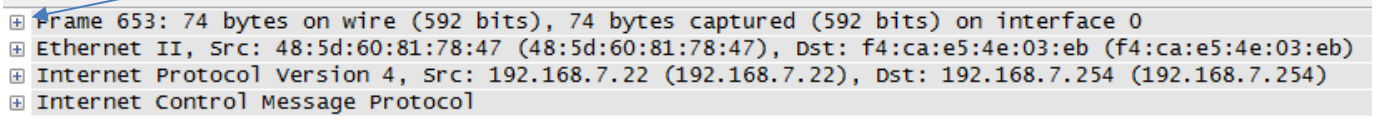


Q43 : Retourner sur Wireshark, que constatez-vous ?

Réponse : Nous retrouvons tous les échanges présents dans la capture ci-dessous.

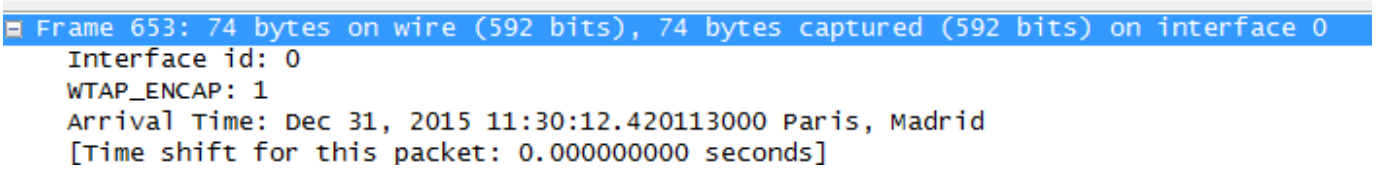


Q44 : Cliquer sur les différentes trames visualisées et expliquer ce que vous voyez. Parler des adresses IP et MAC, des types d'information et de séquence. Analyser le contenu des trames en développant les zones inférieures :

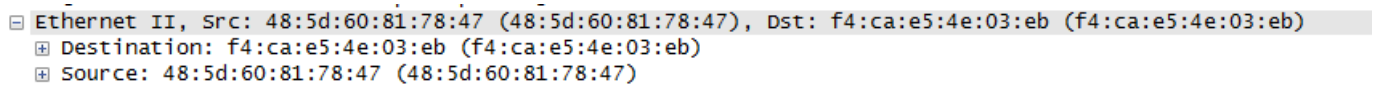


Réponse :
1er ligne : On voit la requête apparaître. La source est bien mon PC (192.168.7.22) et la destination correspond bien au 192.168.7.254. Le protocole est bien ICMP (internet control message protocol) et la demande est de type écho (une simple demande d'information). Issu de mon PC la demande est une requête (ping request), du 192.168.7.254, la réponse est une réplique (ping reply).
On constate qu'il y a bien 4 demandes du 192.168.7.22, comme l'indique le ping sur les commandes Prompt et 4 réponses.
Les numéros de séquences se suivent, seq=50 (réponse à seq=50), jusqu'à seq=53, on retrouve bien les 4 séquences de la demande.

Dans Frame, on trouve plusieurs informations, la taille du message, l'interface concernée (Fa0/0), la date et l'heure de l'envoi, le fuseau horaire :



Dans Ethernet II, on retrouve cette fois les adresses MAC des deux périphériques.



Dans Internet protocol, on trouve la version du protocole, les adresses IP, la longueur des données avec vérification (Checksum) et le TTL (Time To Live = durée de vie du paquet) qui est de 128. Ce qui veut dire que ce paquet pouvait traverser 128 équipements au total, au-delà, la trame aurait été rejetée.

```
Internet Protocol Version 4, Src: 192.168.7.22 (192.168.7.22), Dst: 192.168.7.254 (192.168.7.254)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 60
    Identification: 0x6a91 (27281)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x3fcb [correct]
    Source: 192.168.7.22 (192.168.7.22)
    Destination: 192.168.7.254 (192.168.7.254)
```

Dans ICMP, on trouve le type de la demande, le numéro de séquence (ici 50) et le numéro du dernier bit envoyé (12800). La réponse en reply doit faire apparaître ce numéro, pour que la requête suivante puisse envoyer le paquet suivant, sinon il y a réémission de ce paquet.

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d29 [correct]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 50 (0x0032)
    Sequence number (LE): 12800 (0x3200)
    [Response In: 654]
  ⊟ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
      [Length: 32]
```

Quand on clique sur Data, on obtient le contenu du message envoyé, ici l'alphabet …

```
Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    [Length: 32]

0010  00 3c 6a 91 00 00 80 01  3f cb c0 a8 07 16 c0 a8   .<j..... ?.......
0020  07 fe 08 00 4d 29 00 01  00 32 61 62 63 64 65 66   ....M).. .2abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

6 – Tracer votre réseau

En vous aidant de l'exercice effectué sous Packet Tracer, tracer en utilisant la commande « **tracert** » les équipements suivants :

- PC Etudiant 2
- PC Etudiant 3
- PC professeur (demander l'adresse IP au professeur)
- Serveur Loritz, en traçant l'adresse « www.loritz.fr »

Q45 : En analysant les réponses obtenues, établir le schéma du réseau de votre salle de classe en utilisant le logiciel Packet Tracer. Configurer tous les équipements, comme précédemment avec les adresses réseau qui correspondent à votre salle de classe.

Réponse : Ramasser le fichier PT et le noter.

Q46 : Télécharger et installer le logiciel "Advanced IP scanner" (ou ipscan) qui permet de tracer un réseau.

https://www.advanced-ip-scanner.com/fr/

Comparer vos résultats à celui du logiciel, en identifiant et expliquant les écarts éventuels.

Réponse : Montrer le résultat du logiciel et expliquer les écarts éventuels aux étudiants. Sous Windows 7 vous avez également la possibilité d'afficher l'arborescence de votre réseau s'il est identifié comme "Bureau" ou "Public". Pour cela, ouvrir le centre de réseau et partage et cliquer sur "Afficher l'intégralité du réseau".