Activité pratique – Les réseaux

Comment des équipements informatiques peuvent-ils communiquer entre eux ?

La communication au sein de notre monde moderne entre équipements informatiques et électroniques (ordinateur, tablettes, téléphone, imprimante, disque dur multimédia, centrale météo, etc.) est devenue indispensable. Celle-ci se base sur la notion de réseau. Complétement transparent ou presque pour l'utilisateur, les réseaux permettent au travers de protocoles de relier un équipement au reste du monde.

Sans prétendre élucider toutes les questions relatives aux réseaux (d'une complexité élevée), nous allons au travers de cette activité pratique mettre en évidence certains mécanismes simples de communication propres aux réseaux TCP/IP. Les notions d'adresses IP et MAC, de masque de sous-réseaux, de protocoles ARP, ICMP seront abordés. Pour cela nous utiliserons sur un logiciel de simulation de réseaux « professionnel » : *Packet Tracer* conçu par un géant des réseaux, l'entreprise américaine CISCO.

Mais tout d'abord, il faut se faire comprendre …

Pour communiquer nous utilisons différents moyens : l'écrit, la parole, le langage des signes, etc. … Associé au média, le vecteur de communication, il faut en plus pouvoir se comprendre. Il faut donc utiliser un même code, code compréhensible des deux participants. Deux interlocuteurs doivent donc parler une langue commune !

De la même manière de nombreux médias, vecteur d'informations numériques existent ainsi que des protocoles d'échange pour les réseaux informatiques. Deux plus particulièrement, devenus mondiaux et indispensables dans notre monde moderne, se basent sur le protocole appelé **Ethernet** associé au protocole **Internet**. Seuls ceux-ci seront abordés dans cette activité.

<u>Exemple de média utilisé pour Ethernet :</u>

Le câble RJ45

La fibre optique

1. Où il est question de nom …

Pour communiquer avec une autre personne dans une assemblée, il faut pouvoir l'interpeller, lui adresser la parole nominativement.

De la même manière, pour pouvoir échanger entre deux équipements informatiques, il faut pouvoir que l'un d'eux connaisse l'autre pour échanger. La notion de nom dans les réseaux que l'on appelle adresse est donc très importante et son unicité (dans un sous-réseau) doit être garantie.

On appelle adresse IP (Internet Protocol), l'adresse **donnée** à un ordinateur que l'on note souvent par **@IP**.

L'adresse IPv4 (comprendre adresse IP version 4) est codée sur 32 bits, chiffrée par 4 octets écrits souvent sous forme décimale et séparés par un point :

Exemple d'adresse IPv4 : `192 . 168 . 15 . 20`

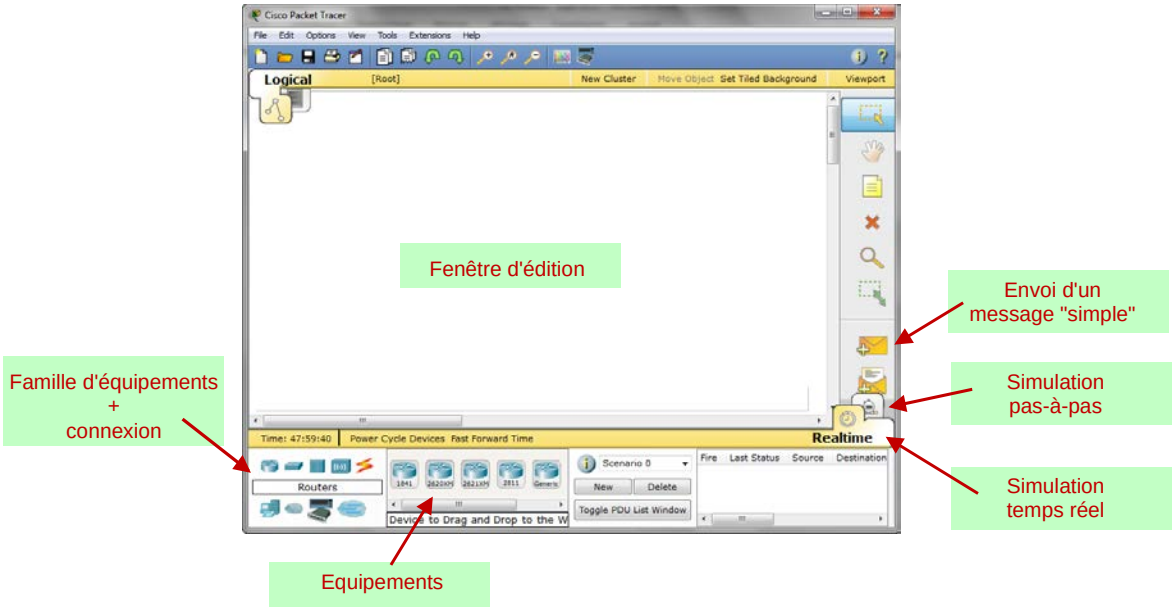
Au vu du nombre croissant et exponentiel du nombre d'équipements se reliant sur le réseau, la version 4 ne suffit plus. L'adresse version 6 IPv6 remplace petit à petit l'IPv4. Cette version permet de coder une adresse sur 128 bits soit 16 octets. Elle n'est plus représentée sous forme décimale mais sous forme hexadécimale séparée par deux points comme l'illustre l'exemple ci-dessous :

Exemple d'adresse IPv6 : `2A01:0E35:2421:4BE0:CDBC:C04E:A7AB:ECF3`

Pendant cette activité de découverte sur les réseaux informatiques, nous utiliserons uniquement la version 4 d'adressage : **IPv4**.

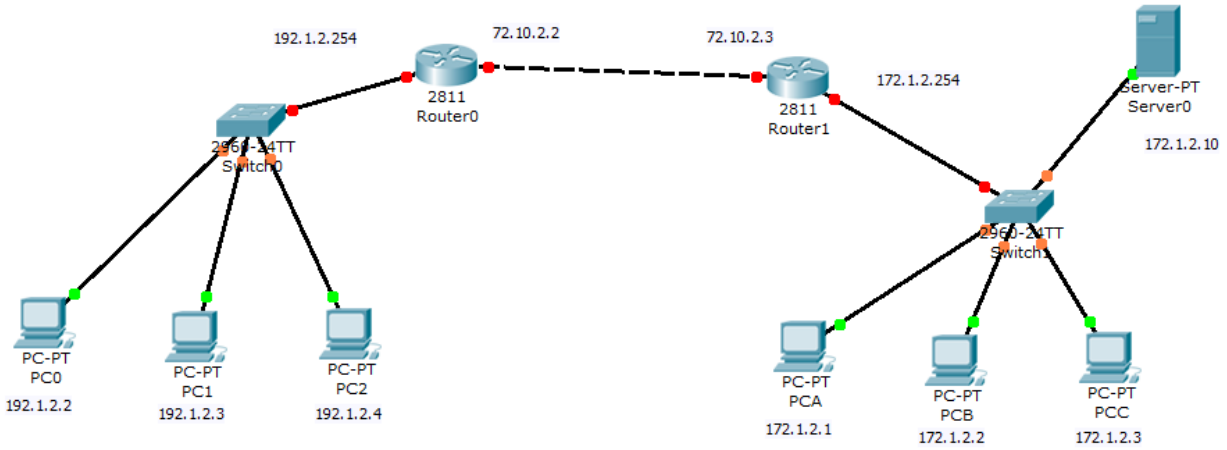
Lancer le programme « Packet Tracer ». Ce logiciel permet de concevoir, de configurer et de simuler des réseaux informatiques. Puissant, il est utilisé par des écoles d'informatique pour certifier des stages réseaux.

La fenêtre de *Packet Tracer* se présente ainsi :

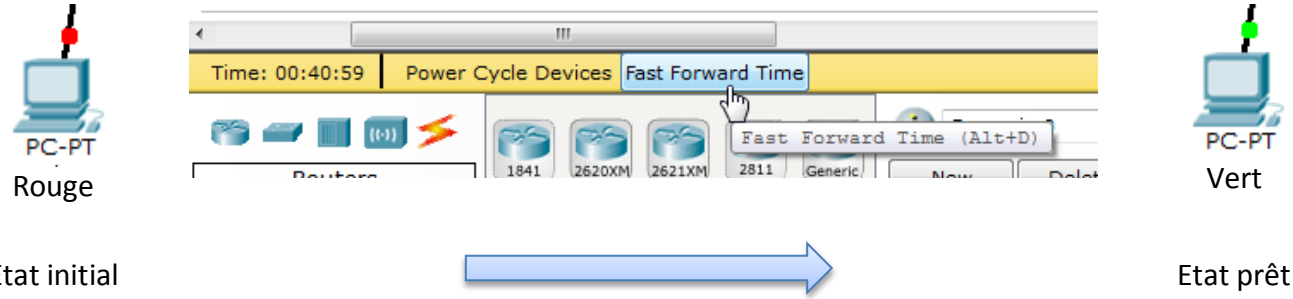


Activité pratique – Les réseaux

Ouvrir le fichier « *Exemple.pkt* » (aller dans menu File/Open) et vous obtenez un exemple de réseau faisant intervenir un certain nombre d'équipements des stations (les ordinateurs), des switchs, des routeurs et un serveur :



Pour la suite, il faudra se rappeler que tant que les indicateurs de connexion sont rouges, le réseau se configure comme dans la réalité. Et comme dans la réalité, cela peut prendre du temps. Pour accélérer cette étape (qui peut être relativement longue), cliquer sur « *Fast Forward Time* » en bas de la fenêtre (cf. ci-dessous).



Etat initial → Etat prêt

Le **réseau est prêt** à fonctionner dès que tous les indicateurs passent au **vert**.

Activité 1-1 : Echange entre 2 ordinateurs

Vous allez maintenant analyser le plus simple des réseaux qui soit dans le cadre du protocole TCP/IP, un réseau composé uniquement de deux ordinateurs.

Ouvrir le fichier « Activite1-1.pdf » et suivez les instructions. Les réponses sont à reporter sur le document réponse papier.

Activité 1-2 Echange entre 2 ordinateurs ou plus

Pour connecter un ensemble d'ordinateur sur un réseau local (appelé **LAN : local Aera Network**), il faut utiliser un équipement supplémentaire qui permet d'interconnecter les ordinateurs entre eux. Le **HUB** (disparu depuis) et le **SWITCH** (qui a remplacé le HUB) jouent ce rôle. On ne peut pas avec le protocole Ethernet comme dans certain réseau (bus de terrain I2C par exemple), connecter directement en dérivation deux câbles du réseau. Le mot anglais « Switch » signifie littéralement en français « Commuter ». C'est le rôle du Switch, d'aiguiller les messages au bon destinataire.

Ouvrir le fichier « Activite1-2.pdf » et suivre les instructions. Les réponses sont à reporter sur le document réponse papier.

2. Où il est question de mieux gérer le réseau…

Internet est le réseau des réseaux (dans la famille des WAN : Wide Aera Network), c'est-à-dire qu'il interconnecte des réseaux entre eux-composés d'un ensemble d'équipements informatiques qui peuvent accéder à Internet. En considérant que seule l'adresse IP d'une station existe, il faudrait que celle-ci pour qu'elle puisse communiquer dans le monde entier, retenir un nombre extravagants d'adresses des stations hôtes. Pour éviter cela, le réseau a été segmenté en sous-réseaux. Donc en plus de l'adresse IP, un masque de sous-réseau a été associé sur chacune des stations. Cela amène à la notion de classe de réseau (classe A, B, C, D et E), notion qui sera abordée en cours.

Le masque de sous-réseau compatible IPv4 est composé comme l'adresse IP, de 32 bits représenté sous forme de 4 octets en décimal.

Exemple de masque de sous réseaux : `255 . 255 . 255 . 128`

Par ce masque et une opération basique : un ET logique, on distingue l'adresse de réseau de l'adresse du sous-réseau auquel appartient la station en question.

En prenant l'exemple suivant :

@IP :	192	.	168	.	15	.	20
Masque	255	.	255	.	255	.	0
Résultat du ET logique	192	.	168	.	15	.	0

Le résultat du ET logique donne l'adresse du réseau, ici donc `192.168.15.0`, le complément fournit la plage d'adresse des stations appartenant à ce réseau, ici de `0` à `255`. Ce réseau accepte donc en théorie 256 stations maximums (2^8). En pratique il y'en a moins (deux en moins) car certaines adresses sont réservées.

On pourra alors découper l'adresse IP en deux : l'adresse réseau que l'on appelle **NetID**, et l'adresse hôte que l'on appelle **HostID**. Dans l'exemple : NetID = `192.168.15.0` et HostId=`20`. L'adresse où le HostID est égal `0` correspond au réseau lui-même. Elle ne peut pas être utilisée pour nommer une machine. De même l'adresse de l'HostId où tous les bits sont à `1` correspond à une adresse bien particulière : l'adresse de broadcasting. Elle est aussi réservée.

Pour effectuer le ET logique, il faut convertir le nombre décimal en binaire et appliquer bit à bit le ET, comme l'illustre l'exemple ci-dessous entre deux nombres quelconques 249 ET 224 :

$(249)_{10}$ =	1	1	1	1	1	0	0	1
$(224)_{10}$ =	1	1	1	0	0	0	0	0
Résultat du ET (224)	1	1	1	0	0	0	0	0

Par exemple la station A a cette adresse et ce masque :

@IP Station A :	192	.	168	.	100	.	249
Masque de la station A:	255	.	255	.	255	.	224
Résultat du ET logique	192	.	168	.	100	.	224

La station A appartient au réseau `192.168.100.224` (le *NetId*). Ce réseau comporte (2^5 -2) stations au maximum soit 30, sur la plage `224` exclu à `255` exclu.

Pour calculer le *HostId* de la station, le principe est le même que celui du calcul du *NetID* sauf qu'il faut prendre le complément du masque avant d'effectuer le ET logique avec l'adresse IP :

@IP Station A :	192	.	168	.	100	.	249
Complément du Masque de la station A:	0	.	0	.	0	.	31
Résultat du ET logique	0	.	0	.	0	.	25

L'adresse de la station A est donc `25` (le *HostId*).

Pour noter un masque et une adresse IP de manière plus synthétique, on utilise cette notation : « `@IP / n` » où n est le nombre de bit masqué (à 1). Cela implique (et c'est très souvent le cas) que les bits masqués se suivent en partant de la gauche, sans 0 intercalé. Cette écriture provient de la répartition des adresses mis en place par le CIDR (*Classless InterDomain Routing*).

Avec l'exemple précédent pour décrire la configuration de la station A, on peut écrire :

Station A : `192.168.100.224 / 27`

Pourquoi `27` ? Rappelons-nous, le masque de sous réseau de la station A est le suivant :

En décimal	255	255	255	224
En binaire	1111 1111	1111 1111	1111 1111	1110 0000

➔ Soit **27** bits consécutifs à 1.

? Comment savoir alors si une station B appartient ou non au réseau d'une station A ? Il suffit d'effectuer le ET logique de l'adresse de la station B avec le masque de la station A. SI l'adresse obtenue du réseau est identique à celle de la station A, alors la station B appartient au même réseau que la station A.

En reprenant l'exemple précédent pour la station A et en prenant pour B :

@IP Station **B** :	192	.	168	.	100	.	150
Masque de la station **A** :	255	.	255	.	255	.	224
Résultat du ET logique	192	.	168	.	100	.	128

Le résultat obtenu est différent. La station A appartient au réseau `192.168.100.224` et non pas au réseau `192.168.100.128`.

Activité 2-1 : Notion de masque de sous-réseaux

Pour s'en convaincre, ouvrir le document « Activité 2-1.pdf ». Vérifier que les adresses sont bien celles définies précédemment, puis tester une communication entre les deux stations A et B.

Configurer la station C (adresse IP et masque) pour qu'elle appartienne au même réseau que la station A.

Activité 2-2 : Configurer les stations d'un réseau

Ouvrir le document « Activité 2-2.pdf » et suivre les consignes. Ne pas oublier de répondre aux questions sur le document réponse.

Activité 2-3 : Maitrise des masques de sous-réseaux ?

Cette activité est à faire si vous avez le temps.
Demandez à votre professeur !

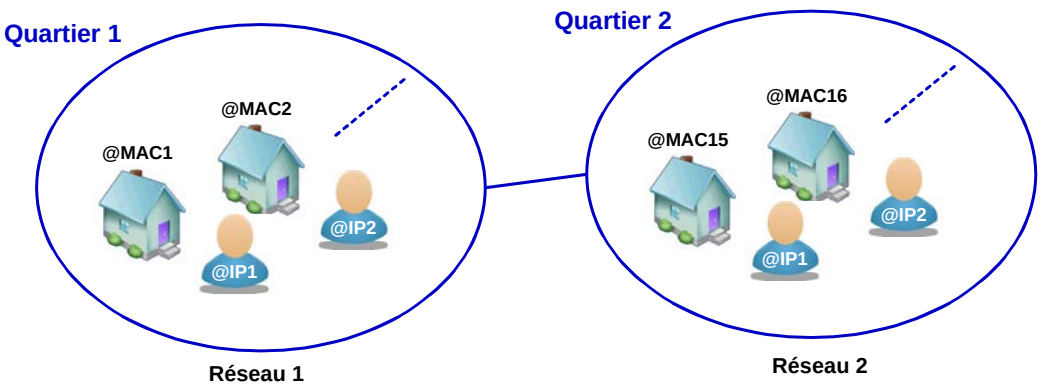
Dans cette activité vous allez mettre à l'épreuve votre compréhension des masques de sous-réseau.

Ouvrir le document « Activité 2-3.pdf » et suivre les consignes. Ne pas oublier de répondre aux questions sur le document réponse.

3. Où il est question de matériel …

L'adresse logique IP ne suffit pas, il faut pouvoir identifier une station de manière sure et rapidement. C'est pour cela que toute carte réseau possède une adresse MAC (*Media Access Control*) que l'on note souvent par **@MAC**. Cette adresse, on ne la choisit pas, elle est définie physiquement par le constructeur de la carte et elle unique dans le monde.

Par analogie, on peut dire que l'adresse MAC serait l'adresse d'une maison. Quant à l'habitant de cette maison, son nom serait l'adresse IP. Avec le protocole TCP/IP, on ne peut pas avoir des habitants ayant de même nom dans un même quartier (le réseau) et bien évidemment deux maisons ayant la même adresse. Par contre il est possible d'avoir des habitants ayant le même nom (@IP) dans des quartiers différents (réseau), leur lieu d'habitation de fait étant située à des adresses différentes (@MAC).

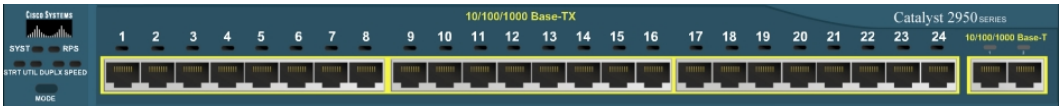


Pourquoi alors ne pas se contenter seulement de l'adresse MAC ? Tout simplement pour pouvoir sortir du réseau local auquel appartient la station et faciliter la gestion des réseaux. De plus, le traitement du message est plus rapide au niveau de l'adresse MAC (ce n'est pas le même niveau dans la couche du protocole) qu'au niveau de l'adresse IP.

Dans une trame réseau Ethernet, on retrouve ces deux adresses : l'adresse MAC et l'adresse IP.

Activité 3-1 : Notion d'adresse MAC et de ports physiques

Chaque station par liaison filaire cuivrée est reliée à un port physique du Switch. Selon le modèle, un switch possède 3, 4, … jusqu'à 24 ports.



Exemple de switch ayant 24 ports de connexion
(donc 24 stations peuvent y être connectées)

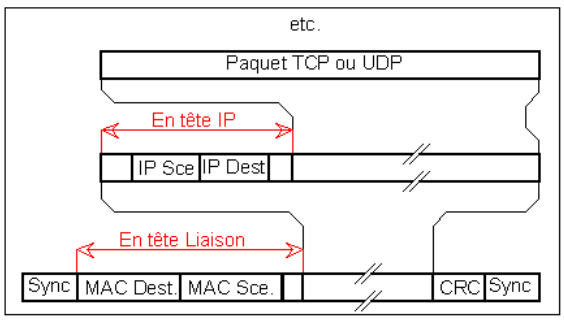
Il faut se rappeler qu'un réseau type TCP/IP est toujours en perpétuel changement. L'architecture ne reste jamais longtemps figée : ajout d'une imprimante réseau, suppression d'un ordinateur, remplacement d'un équipement, ordinateur portable qui se connecte …. Les protocoles mis en œuvre justement se chargent de prendre en compte facilement et de façon quasi transparente ces changements vis-à-vis de l'utilisateur final.

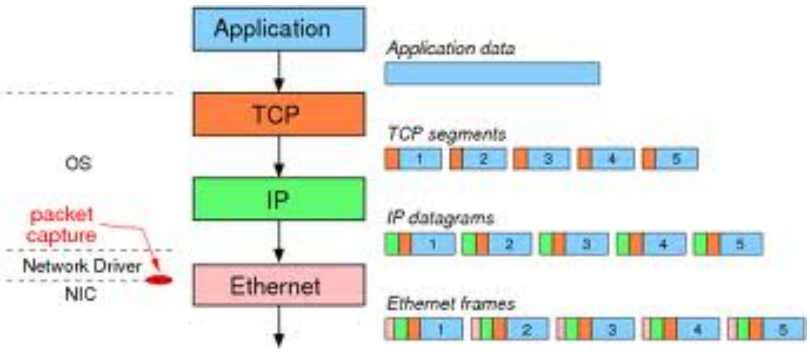
Le Switch en l'occurrence doit s'adapter sans pour autant ralentir les communications. Un mécanisme dans cet objectif a été mis en place, c'est la table dite d'adressage MAC. Elle est remplie au fur et à mesure des échanges. Contrairement au HUB (et c'est la raison pour laquelle il n'existe plus), le switch utilise donc les adresses MAC pour aiguiller correctement les messages au destinataire. Il lie une adresse MAC d'un équipement avec chacun de ses ports physiques de connexion.

Ouvrir le document « Activité 3-1.pdf ». Dans cette activité, vous allez apprendre à connaître l'adresse MAC des deux ordinateurs ainsi que les ports physiques du switch auxquels ils sont connectés.

Activité 3-2 : Datagramme Ethernet

Dans un Datagramme Ethernet, l'adresse IP (dans la couche IP) ainsi que l'adresse MAC (lorsqu'elle est connue) sont toujours renseignées aussi bien pour le destinataire du message que pour l'émetteur de celui-ci.





Ouvrir le document « Activité 3-2.pdf ». Repérez les adresses MAC et IP dans un datagramme Ethernet.

Nous verrons dans le chapitre suivant comment l'adresse MAC du destinataire est directement remplie (dès que possible) par l'hôte source du message.

4. Où il est question de se faire connaître et de connaître les autres …

Une station doit au sein d'un sous-réseau se faire connaître. En effet dans un datagramme Ethernet, il faut connaître les adresses MAC du destinataire et de la source ainsi que leur adresse IP. Or à priori, l'adresse MAC du destinataire n'est pas connue. C'est le rôle du **protocole ARP**.

Pour un **switch** cela va consister à établir pour chacun de ses ports de connexion, de faire la relation avec l'adresse MAC de la station auquel ce port est connecté. Cela a été vu lors du chapitre précédent.

Pour une **station**, elle va associer une adresse IP destinataire à son adresse MAC dès qu'elle l'a connaît. Ceci va permettre de gagner en efficacité pour l'aiguillage des informations. Les adresses MAC pour chaque équipement terminal sont stockées dans une table que l'on appelle **table ARP**.

Si l'on reprend notre analogie d'adresse postale et de courrier, une table ARP vide serait un facteur nouvellement nommé qui découvre son quartier de distribution du courrier. Une table ARP remplie, serait alors un facteur expérimenté ayant une connaissance précise de sa tournée.

Activité 4-1 : Découverte du Protocole ARP

Lorsque le destinataire d'un message n'est pas connu par la source autrement que par son adresse IP, une requête ARP est d'abord envoyée à l'ensemble des équipements du sous-réseau. C'est que nous allons découvrir dans cette activité.

Ouvrir le document « Activité 4-1.pdf ». Faire attention au cheminement et au type des messages. Reporter au fur et à mesure vos réponses dans le document réponse.

Activité 4-2 : Le Protocole ARP plus en détail…

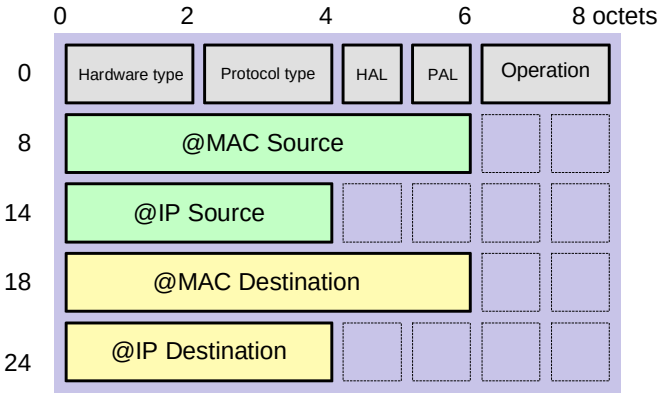
Le **protocole ARP** (*Adress Resolution Protocol*) permet d'associer à chaque adresse IP d'un réseau, l'adresse MAC de l'équipement. Le résultat de l'association est sauvegardé dans une table ARP au niveau de l'équipement et elle est continuellement remise à jour.

Lorsqu'un équipement veut communiquer avec un autre équipement qu'il ne connaît pas (sauf son adresse IP bien entendu), le protocole agit de la manière suivante :

- Il envoie une requête Ethernet de type ARP à tout le monde → cela s'appelle en jargon informatique un **broadcast**.

- Tous les équipements du sous-réseau reçoivent le message. Mais seul le concerné répond en retournant son adresse MAC et en profite pour compléter sa table ARP avec les adresses MAC et IP de l'équipement source.
- L'équipement source peut alors compléter son datagramme avec l'adresse MAC du destinataire et en profite pour compléter lui aussi sa table ARP.

Le **datagramme ARP** est composé de la manière suivante :



Longueur du datagramme : 28 octets

Hardware Type : format d'entête ARP selon le type de matériel (=1 pour Ethernet)

Protocol type : type de protocole (=0x008 pour IP)

HAL : Hardware Address Length (=6 pour Ethernet)

PAL : Protocol Address Length (=4 pour IPv4, =16 pour IPv6)

Operation : type d'opération effectuée (=1 pour une requête ARP, =2 pour une réponse).

Cette activité appliquée à un réseau simple, permet d'illustrer les mécanismes mis en œuvre pour qu'une station inconnue des autres se fasse connaître au sein de son réseau.

Ouvrir le document « Activité 4-2.pdf ». Respecter scrupuleusement les étapes de l'activité. Reporter au fur et à mesure vos réponses dans le document réponse.

5. Ou il est question de communiquer avec d'autres réseaux

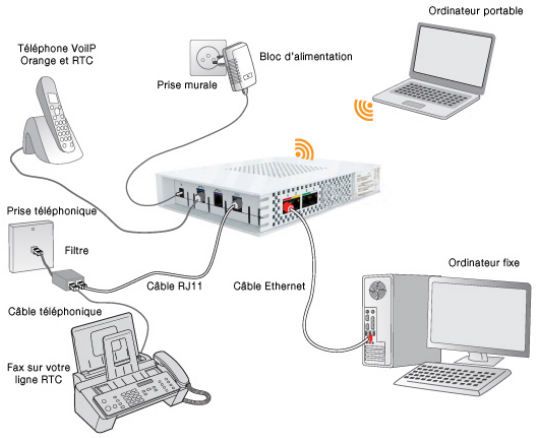
Pour pouvoir communiquer entre deux réseaux ou plus, un autre équipement est nécessaire : le routeur. Il va permettre au travers d'une table de routage de faire transiter les informations (les paquets) d'un réseau à un autre.

Un exemple de routeur que l'on retrouve dans presque tous les foyers sont les fameuses « Box » (freebox, livebox, etc…). Elles permettent de créer un réseau familial (switch intégré, wifi et CPL) et de connecter ce réseau à celui de l'Internet via une ligne ADSL.

Toujours avec la même analogie, le routeur pourrait être comparé au bureau central de tri de la poste. Tous les courriers arrivent au bureau et sont ensuite dispatchés par tournée. Ce ne sera pas toujours le cas avec les messages TCP/IP …

ex : un routeur Wifi

Exemple ci-contre, la live box et ses connexions :



Activité 5-1 : Connecter deux réseaux entre eux

Deux réseaux ont par définition des *NetId* différents. Relier ces deux réseaux via à Switch est possible mais cela ne servira pas à grand-chose car les stations des deux réseaux ne vont pas pouvoir communiquer ensemble. Pour s'en convaincre, vous allez faire l'activité suivante :

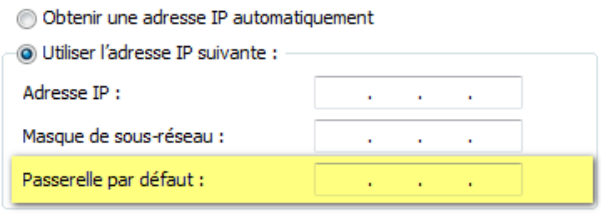
Ouvrir le document « Activité 5-1a.pdf ». Effectuer la simulation et répondre aux questions dans le document réponse.

Comme il a été dit en préambule, le routeur sert via sa table de routage à connecter deux réseaux différents.

Mais comment le message est acheminé au routeur ?

C'est le rôle de la **passerelle** (ou Gateway). Lorsqu'une station veut envoyer un message, elle détermine dans un premier temps si le destinataire appartient à son réseau (rôle du masque) ou non. Si tel est le cas, alors elle envoie directement le message au destinataire. Si ce n'est pas le cas, elle va envoyer le message via la passerelle. Pour cela elle doit connaître son adresse IP. La passerelle alors prend en charge le message et se débrouille pour le faire parvenir au destinataire.

Sous Windows 7 par exemple, il faut renseigner le champ « Passerelle par défaut » :



Un routeur est mis à la place du switch. Ouvrir le document « Activité 5-1b.pdf ». Effectuer la simulation et répondre aux questions dans le document réponse.

Activité 5-2: Cheminement des messages via les routeurs

Dans cette activité vous allez découvrir comment les routeurs font pour acheminer correctement le message d'un réseau à un autre.

Ouvrir le document « Activité 5-2.pdf ». Effectuer la simulation et répondre aux questions dans le document réponse.

Lexique

ARP	Address Resolution Protocol	Protocole de résolution d'adresse permettant d'associer à une adresse IP d'une station distante, une adresse MAC.
CIDR	Classless Inter Domain Routing	L'adressage par classe (A, B, C etc…) a été abandonné au profit d'adressage CIDR.
Datagramme	Datagram	Les datagrammes (ou paquets de données) sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP de destination).
DHCP	Dynamic Host Configuration Protocol	protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau.
DNS	Domain Name System	Service permettant de traduire un nom de domaine (www.rouen.fr) en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.
FTP	File Transfer Protocol	Protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP.
HTML	Hypertext Markup Language	Langage sous forme textuelle permettant d'écrire des pages web.
HTTP	HyperText Transfer Protocol	Protocole de communication client-serveur développé pour le World Wide Web (www).
ICMP	Internet Control Message Protocol	Ce protocole est utilisé pour véhiculer des messages de contrôle et d'erreur. Il permet par exemple de vérifier si un hôte est accessible ou pas (commande PING).
IP	Internet Protocol	Le protocole IP élabore et transporte des datagrammes IP (les paquets de données), sans toutefois en assurer la « livraison ».
LAN	Local Area Network	Textuellement réseau local. Réseau informatique interne.
MAC	Media Access Control	identifiant physique stocké dans une carte réseau ou une interface réseau et utilisé pour attribuer mondialement une adresse unique.
Pare-Feu	FireWall	logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés sur ce réseau informatique.
Passerelle	Gateway	Dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet.
Proxy	Proxy	Programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet en vue de surveiller ou de faciliter les échanges.
TCP	Transmission Control Protocol	Ce protocole de contrôle de transmissions est un protocole de transport fiable, en mode connecté contrairement au protocole UDP.
UDP	User Datagram Protocol	Le rôle de ce protocole est de permettre la transmission de données de manière très simple sans mécanisme de contrôle contrairement au protocole TCP.
WAN	Wide Area Network	Textuellement réseau étendu. Réseau informatique couvrant une grande zone géographique, le plus connu étant Internet.

Source : Wikipédia ou CommentCaMarche.net pour la plupart des définitions