Adressage IP
Première partie

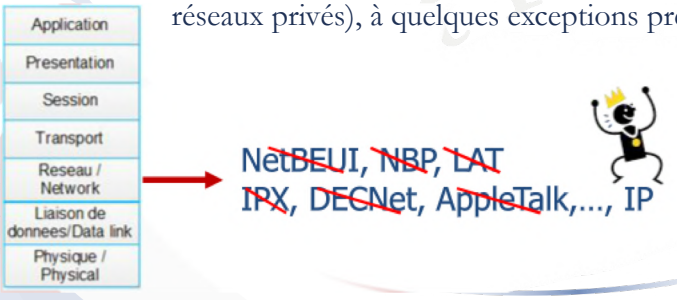
Hainaut Patrick 2016

But de cette présentation

- Les adresses IP sont au cœur de l'étude des réseaux
- Leur compréhension est donc très importante
- Nous allons aborder le sujet de façon progressive, de manière globale pour commencer puis dans le détail
- Dans cette première partie, nous verrons:
  - Pourquoi on utilise des adresses IP
  - Comment on les utilise
  - Comment on organise le réseau autour d'IP
  - Comment se passe une communication sur un réseau IP

Internet protocol

- IP (Internet Protocol) est LE protocole réseau d'Internet
- Le réseau des réseaux a tout balayé sur son passage et tout ce qui se connectait de près ou de loin à un réseau se connecte maintenant en IP (via Internet ou via des réseaux privés), à quelques exceptions près



Internet Protocol

- Internet est formé par des réseaux différents, de technologies différentes, utilisant des protocoles de couche 2 différents (Ethernet, Frame Relay, …)
- Peu importe, car tous ces réseaux transportent des paquets de données, et c'est tout ce qui intéresse IP

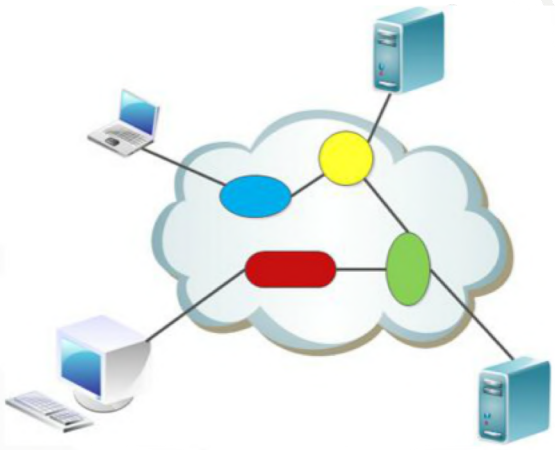
Internet Protocol

- Le fait d'utiliser un système de communication en couches permet de rendre IP indépendant des protocoles de la couche inférieure (couche 2) -> *pour plus d'informations, regardez la présentation sur* ***les modèles de référence***

- Le protocole IP permet donc d'encapsuler les spécificités des différents réseaux physiques pour proposer un service commun aux applications

Internet Protocol

- Vue réelle du réseau des réseaux



Internet Protocol

- Vue applicative du réseau des réseaux

- IP fait apparaitre l'ensemble des réseaux disparates comme un seul et unique réseau

Adresses IP

- Pour pouvoir recevoir du courrier, les habitants d'une ville, ont besoin d'une adresse postale, unique dans cette ville
- De même, pour pouvoir recevoir des paquets de données, les différents hôtes du réseau (ordinateurs) ont besoin d'une adresse les identifiant; l'adresse IP
- Si le réseau est un réseau local (LAN), l'adresse IP attribuée à chaque PC sera, en général, privée et doit être unique sur le réseau
- Si le réseau est Internet, l'adresse IP doit être publique et unique au monde

Structure des adresses IP

- Deux versions de protocole: IPv4 et IPv6
  - En IPv4, les adresses sont codées sur 4 octets (bytes) et représentées sous forme décimale pointée
    Exemple: 212.64.117.67
  - En IPv6, elles sont codées sur 16 octets et représentées sous forme hexadécimale
    Exemple: 1fff:0000:0a88:85a3:0000:0000:ac1f:8001
  - IPv6 a été mis au point car il y a pénurie d'adresses IPv4

Structure des adresses IP

- Ca fait des années qu'on parle d'IPv6, alors, pourquoi autant de temps pour y passer ?
  - Pas de demande des utilisateurs (car pas d'avantages immédiats)
  - Peur des problèmes de compatibilités
  - Surcoûts de transition (surtout en formation)
  - Passage automatique (pour les clients)
- IPv4 étant encore largement employé, le reste de notre propos le concerne
- IPv6 sera abordé dans un cours spécifique

Structure des adresses IP

- Chaque PC reçoit donc une adresse IP constitué de 4 octets pouvant varier de 0 à 255
- On a donc une plage théorique pouvant varier de 0.0.0.0 à 255.255.255.255
- On ne peut pas utiliser la totalité de cette plage mais cela sera vu dans les aspects avancés
- Retenez pour l'instant qu'une adresse classique aura comme valeur comprise entre 1.0.0.0 et 223.255.255.255

Structure des adresses IP

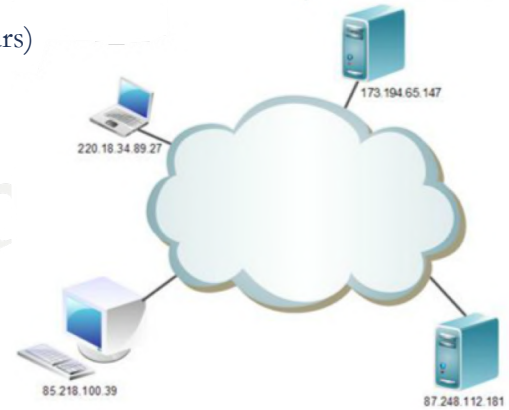
- Exemple: 212.68.195.18

  1er octet 2ème octet 3ème octet 4ème octet

- Chaque octet pouvant varier entre 0 et 255, les adresses suivantes seront valides: 10.0.0.1, 192.192.192.192, 172.18.15.255, 10.20.30.40
- Les adresses suivantes ne sont pas valides: 192.0.257.1, 10.0.0.260 et aussi 0.10.20.30, 255.0.0.1 (voir dia précédente)

Adresses IP privées et publiques

- Les adresses IP publiques sont uniques au monde et permettent donc d'adresser des ordinateurs qui sont directement connectés à Internet
(PC clients ou serveurs)



Adresses IP privées et publiques

- Votre fournisseur d'accès Internet (FAI) vous procure une adresse publique quand vous vous connectez au modem
- Cette adresse est généralement dynamique, c'est-à-dire qu'elle peut varier dans le temps

Adresses IP privées et publiques

- Un serveur présent sur Internet, comme un serveur Web, aura lui, généralement, une adresse publique statique, qui ne varie pas dans le temps
- De cette façon, on pourra toujours le contacter facilement

Adresses IP privées et publiques

- L'emploi des adresses publiques est réglementé et payant
- On doit obligatoirement passer par un agent (le FAI, dans votre cas) pour en obtenir une ou plusieurs
- Par conséquent, si on a un réseau local de 9 PC, on ne va pas attribuer une adresse publique à chacun d'eux, cela reviendrait trop cher
- L'organisme gérant l'attribution des adresses IP (IANA à l'époque, ICANN maintenant) a donc défini des plages d'adresses privées, qui sont libres d'utilisation et gratuites

Adresses IP privées et publiques

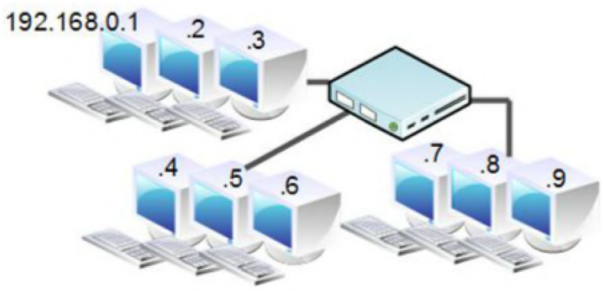
- Les plages d'adresses privées les plus communément employées sont:
  10.0.0.0 à 10.255.255.255
  172.16.0.0 à 172.31.255.255
  192.168.0.0 à 192.168.255.255

- Veillez à connaître par cœur ces plages de façon à pouvoir adresser les ordinateurs d'un réseau local correctement

- Ces adresses sont réservées pour les réseaux locaux, elles ne peuvent pas se retrouver sur Internet, donc elle ne seront jamais attribuées par un modem (sauf si votre FAI place ses abonnés dans un réseau local qui lui sera connecté à Internet) …

Adresses IP privées et publiques

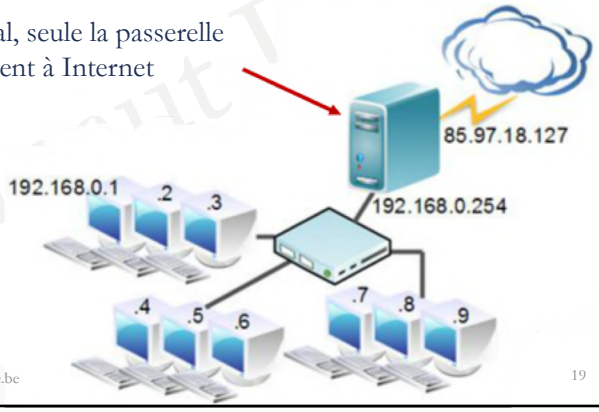
- Nos 9 PC sont reliés entre eux par un commutateur (switch) et possèdent tous une adresse IP différente



- Ils ont tous une adresse IP commençant par 192.168.0

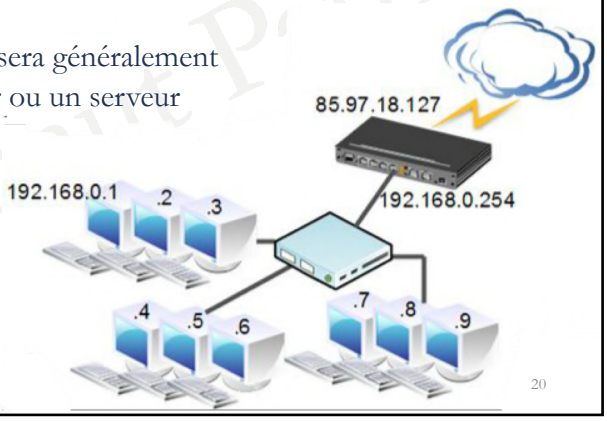
Passerelle (Gateway)

- Pourtant, notre réseau doit pouvoir être connecté à Internet et nos 9 PC doivent pouvoir surfer sur le net, non ?
- Oui, et pour cela, nous allons ajouter un élément à notre réseau; la passerelle
- Dans un réseau local, seule la passerelle se connecte réellement à Internet



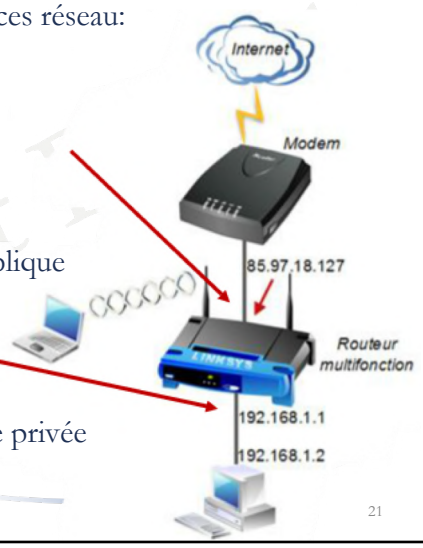
Passerelle (Gateway)

- Grâce au mécanisme de NAT (vu plus loin), nos 9 PC pourront cependant surfer simultanément sur Internet en passant tous par la passerelle pour sortir du réseau local
- Le rôle de passerelle sera généralement assuré par un routeur ou un serveur



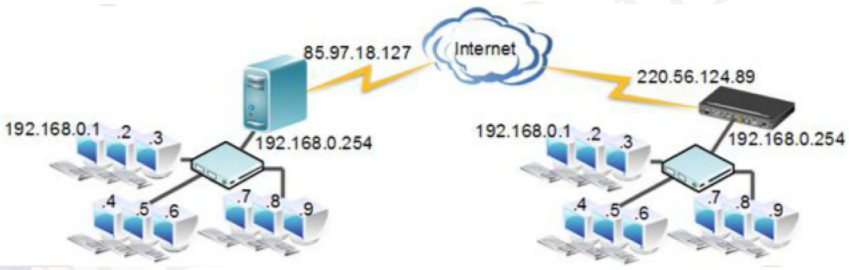
Passerelle (Gateway)

- La passerelle possède deux interfaces réseau:
  - La première, interface WAN, connectée à Internet (via un modem par exemple) et recevant dynamiquement (en général) une adresse IP publique
  - La deuxième, interface LAN, connectée au réseau local, configurée avec une IP statique privée



Adresses IP privées et publiques

- Tous les réseaux locaux du monde, reliés par Internet, peuvent employer les mêmes adresses privées sans risque de conflit, puisque seules leurs adresses publiques (différentes) sont en contact



- Attention, ce schéma n'est pas complet et sera complété par les notions vues par la suite ☺

Masque de sous-réseau

- Nos PC seront regroupés en réseaux locaux (LAN), ce qui leur permettra de s'envoyer des données et de partager des ressources
- Pour déterminer si les PC font partie du même réseau ou pas, on doit encore ajouter un élément; le masque de sous-réseau
- Le masque (en première approche) permet de fixer un, deux ou trois octets de l'adresse IP des nœuds réseau (ordinateur, routeur, …)

Masque de sous-réseau

- Si un octet du masque est à 255, l'octet correspondant au niveau de l'adresse est fixé, et tous les PC du réseau ont une adresse avec la même valeur pour cet octet

Exemples: 192.168.100.1 -> le premier octet est fixé
255. 0 . 0 .0

192.168.100.1 -> les 2 premiers octets sont fixés
255.255. 0 .0

192.168.100.1 -> les 3 premiers octets sont fixés
255.255.255.0

Masque de sous-réseau

- Soit les adresses suivantes:

  10.0.0.1
  10.0.2.1
  10.0.0.10
  10.0.2.254
  10.0.0.15

- Quelles sont les adresses faisant parties d'un même réseau ?

Masque de sous-réseau

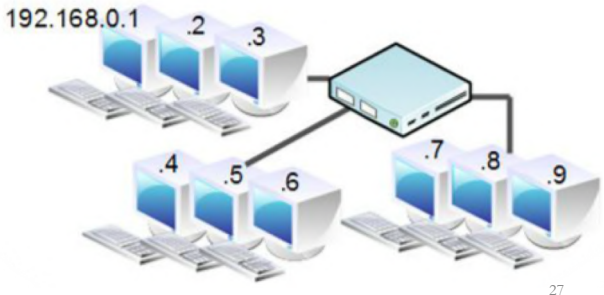
- Ca dépendra du masque employé:

10.0.0.1	10.0.0.1
10.0.2.1	10.0.2.1
10.0.0.10	10.0.0.10
10.0.2.254	10.0.2.254
10.0.0.15	10.0.0.15
255.0.0.0	255.255.255.0
-> un seul réseau car tous les PC ont la même valeur pour l'octet fixé	-> deux réseaux car deux combinaisons différentes pour les octets fixés

Masque de sous-réseau

- Dans notre réseau exemple, tous les PC ont une adresse commençant par 192.168.0 (on n'a noté que le dernier byte pour une question de visibilité)
- Le masque associé pourra être 255.255.255.0
- en pratique, l'adresse IP est toujours associé à un masque de sous-réseau

- Attention, ce schéma n'est pas complet et sera complété par les notions suivantes ☺



Masque de sous-réseau

- Pour un gain de place et de visibilité, on note souvent le masque de sous-réseau sous forme du nombre de bits à 1
- Un bit est une valeur binaire élémentaire qui peut prendre comme valeur 0 ou 1
- Un octet ou byte est égal à 8 bits et 8 bits à 1 = 255 en décimal tandis que 8 bits à 0 = 0 en décimal
- 255.0.0.0 sera donc représenté par /8
  255.255.0.0 par /16 (2x 8 bits à 1)
  255.255.255.0 par /24 (3x 8 bits à 1)
- Un masque de sous-réseau est toujours une suite continue de bits à 1 (tous des 1 puis tous des 0)

Plage IP

- Avec une adresse IP et son masque de sous-réseau associé, on peut déterminer la plage IP dont elle fait partie

  Exemple: 10.0.1.34/24 -> on fixe les 3 premiers octets

  Le dernier octet peut varier: - sa valeur minimum sera 0
  - sa valeur maximum sera 255

  La plage IP sera donc: 10.0.1.0 à 10.0.1.255

  on a 256 adresses IP disponibles dans cette plage (et pas 255 ! car on commence à compter à 0 et pas à 1)

Adresse de réseau (network address)

- Dans l'exemple précédent, nous avons un réseau de 256 adresses IP
- Pour mentionner ce réseau dans un routeur, si on veut tenir compte de ces 256 adresses, il faudrait introduire 256 lignes dans la table de routage -> pas pratique du tout
- Il faut donc une adresse qui représente et qui résume le réseau -> c'est l'adresse réseau
- Ce sera toujours la première adresse de la plage IP, et elle ne peut être attribuée à une machine

Adresse de diffusion (broadcast address)

- Il arrive parfois que l'on doive envoyer un paquet de données à tous les PC du réseau
- Si notre réseau comporte 200 PC, on devrait envoyer 200 fois le même paquet de données successivement -> pas pratique du tout
- Il faut donc une adresse particulière qui permette d'envoyer automatiquement le paquet de données à tous les hôtes du réseau -> c'est l'adresse de diffusion
- Ce sera toujours la dernière adresse de la plage IP, et elle ne peut être attribuée à une machine

Plage utile

- Donc dans notre réseau 10.0.1.0/24 qui comporte 256 adresses différentes, on doit enlever deux adresses (la première et la dernière), ce qui nous laisse 254 adresses IP pour identifier les hôtes réseau
- La plage utile sera toujours égale au nombre d'adresses de la plage IP -2

Exercices

- Pour les adresses suivantes, donnez la plage IP, l'adresse de réseau, l'adresse de diffusion, l'adresse du premier et du dernier PC

192.168.12.0/24

172.17.18.25/16

10.30.50.45/24

223.15.18.64/24

10.200.110.90/8

10.0.0.0/8

10.0.0.0/24

Résolution de quelques exercices

- 192.168.12.0/24
  Plage IP: 192.168.12.0 à 192.168.12.255
  Adr. de réseau: 192.168.12.0
  Adr. de diffusion: 192.168.12.255
  Adr. du 1er PC: 192.168.12.1
  Adr. du dernier PC: 192.168.12.254

- 172.17.18.25/16
  Plage IP: 172.17.0.0 à 172.17.255.255
  Adr. de réseau: 172.17.0.0
  Adr. de diffusion: 172.17.255.255
  Adr. du 1er PC: 172.17.0.1
  Adr. du dernier PC: 172.17.255.254

Résolution de quelques exercices

- 10.0.0.0/8 Plage IP: 10.0.0.0 à 10.255.255.255
  Adr. de réseau: 10.0.0.0
  Adr. de diffusion: 10.255.255.255
  Adr. du 1er PC: 10.0.0.1
  Adr. du dernier PC: 10.255.255.254

- 10.0.0.0/24 Plage IP: 10.0.0.0 à 10.0.0.255
  Adr. de réseau: 10.0.0.0
  Adr. de diffusion: 10.0.0.255
  Adr. du 1er PC: 10.0.0.1
  Adr. du dernier PC: 10.0.0.254

Résumé IP

- Une adresse IP se compose de 4 octets et utilise la représentation décimale pointée (pour IPv4 du moins)
- Elle se décompose en une partie réseau (partie fixée) et une partie hôte (variant d'un PC à l'autre)
- Le masque de sous-réseau permet de différencier la partie réseau de la partie hôte
- Pour chaque réseau, une adresse de réseau et une adresse de diffusion sont définies, elles ne peuvent **jamais** être attribuées à une interface réseau quelle quel soit (PC, routeur, passerelle, …)

Remarques

- Une plage d'adresse est également prévue pour l'auto-configuration IP des PC clients DHCP qui n'obtiennent pas d'adresses (plage de 169.254.0.0 à 169.254.255.255)

  -> les PC ayant ce type d'adresse IP peuvent communiquer entre eux mais ne peuvent pas sortir du réseau local et ne peuvent donc pas accéder à Internet

- C'est une adresse APIPA (Automatic Private Internet Protocol Addressing) créée par un protocole zeroconf

Remarques

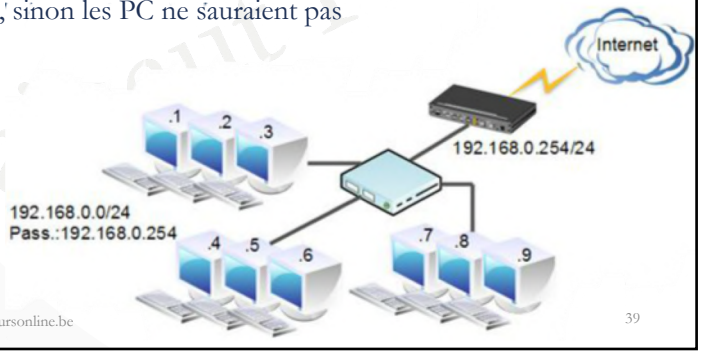
- Chaque hôte possède une adresse de bouclage interne (localhost) qui commence par 127 (traditionnellement 127.0.0.1) et qui permet de faire tourner les services réseaux même sans interface réseau

- Ca permet d'éviter un crash de la pile TCP/IP

- Elle reste interne au PC, donc pas de conflit (tous les PC ont la même sans que cela pose problème)

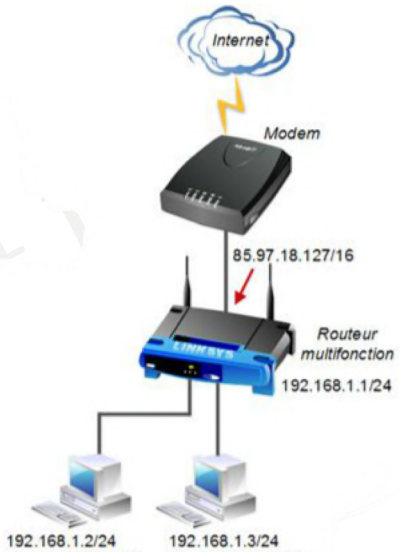
Schéma réseau

- Dans notre schéma complété, on trouve le masque de sous-réseau, l'adresse de réseau (qui n'est attribuée à aucune machine ! mais représente le réseau) et l'adresse passerelle éventuelle
- L'adresse de passerelle est toujours une adresse du réseau local, sinon les PC ne sauraient pas la contacter



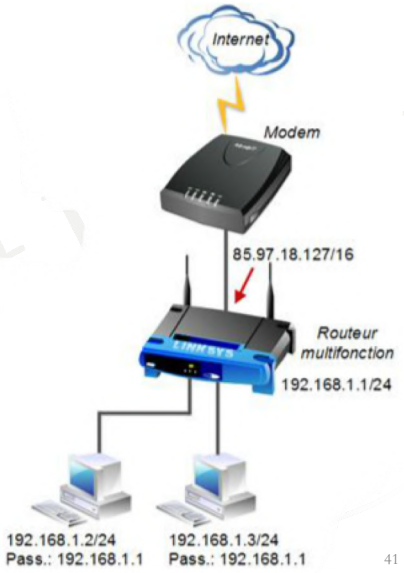
Communication sur un réseau

- Nos PC clients, pour pouvoir communiquer sur le réseau local, doivent posséder une adresse IP et un masque de sous-réseau
- Pour accéder au réseau étendu (WAN), ils ont besoin d'une adresse de passerelle qui leur permettra de sortir du réseau local
- L'adresse de passerelle est toujours une adresse de la même plage IP que les PC du réseau local



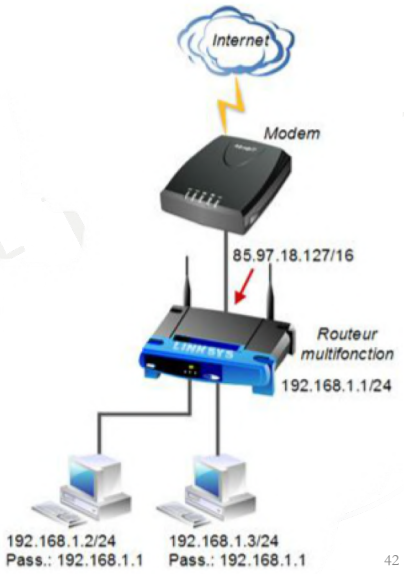
Communication sur un réseau

- Ne pas confondre l'adresse de passerelle et l'adresse de réseau (celle-ci représente le réseau et ne peut être attribuée à aucune interface d'aucun équipement …) !
- La passerelle est généralement constituée par un routeur ou un serveur (qui possède alors deux cartes réseaux, une reliée au LAN et l'autre au WAN)



Communication sur un réseau

- Si PC1 communique avec PC2, PC1 s'adresse directement à PC2 car le système sait (grâce au masque) qu'ils sont dans le même réseau
- Si le client doit communiquer avec une adresse en dehors de sa plage IP (ici, de 192.168.1.1 à 192.168.1.254), il envoie le paquet IP à la passerelle (qui se débrouille avec …)

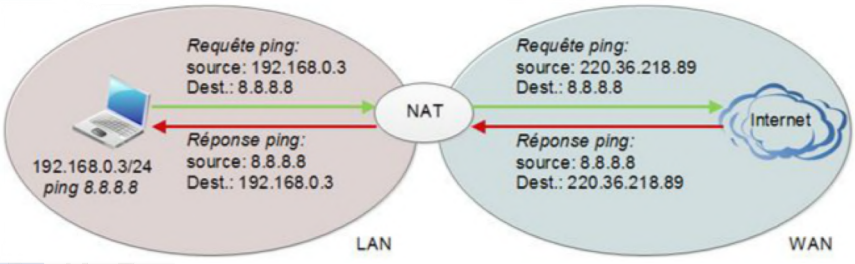


NAT

- Pour accéder à Internet, deux problèmes se posent:
  - Un problème au niveau IP
  - Un autre au niveau des noms de domaines
- Au niveau IP, lorsque le client d'adresse 192.168.1.2 veut faire une requête sur Internet, la requête est bloquée par le premier routeur qu'elle rencontre, parce que l'adresse employée est une adresse privée qui n'a pas sa place sur Internet
- Pour que cela puisse fonctionner, il faut que le mécanisme de NAT (Network Address Translation) soit activé (ce qui est le cas dans la plupart des modem-routeurs ou routeurs sans fils)

NAT

- Le mécanisme du NAT va échanger l'adresse privée du client par l'adresse publique du routeur, pour pouvoir effectuer la requête sur Internet



NAT

- Une fois la réponse à la requête reçue d'Internet, l'échange se fait dans l'autre sens et la réponse est renvoyée sur le réseau local
- Le routeur tenant à jour une table NAT, qui renseigne sur qui a demandé quoi, plusieurs clients peuvent effectuer simultanément des requêtes sur Internet sans qu'il y ait de problèmes. Chaque client récupère les paquets de données qui lui sont dus

DNS

- Notre système permettra, par exemple, de communiquer (via la passerelle) avec un serveur Skynet d'adresse 195.238.2.21
- Par contre, pour surfer sur le web, il manque encore un élément au PC client: l'adresse du serveur DNS (Domain Name System) qui permettra de réaliser la résolution de nom
- Si on veut par exemple accéder à www.google.be, il faut connaître l'adresse IP correspondant à ce nom de domaine, car les machines n'utilisent que les adresses pour communiquer entre elles, pas les noms
- Le DNS contient des tables de correspondance IP - Nom

DNS

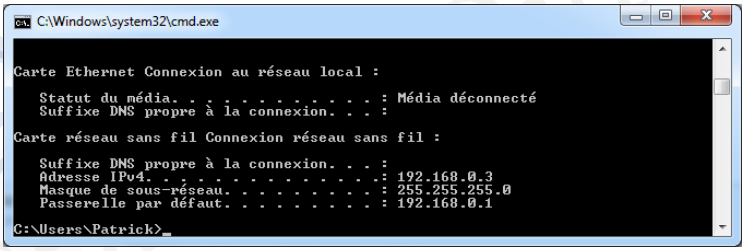
- L'adresse du serveur DNS est généralement donnée par le FAI
- Elle n'est pas liée au réseau local
- On peut changer de serveur DNS et prendre par exemple, celui de Google dont l'adresse est 8.8.8.8
- Le système DNS est en fait un système hiérarchique, utilisant plusieurs serveurs DNS, interrogés à tour de rôle (voir présentation sur Internet)

Relever les paramètres IP

- Sous Windows:
  - Dans une invite de commande (tapez **cmd** dans la zone Rechercher), tapez **ipconfig** pour obtenir l'adresse IP, le masque et la passerelle éventuelle (mais nécessaire pour sortir du LAN)
  - Pour avoir l'ensemble des paramètres, tapez **ipconfig /all** (vous verrez entre-autre l'adresse du serveur DNS)
  - Pour accéder à l'invite de commande, tapez **cmd** et validez, dans la zone de recherche (Windows 7) ou dans Exécuter (Windows XP)
- Sous Linux:
  - Dans une console, tapez, **ifconfig**

Relever les paramètres IP

- L'ordinateur peut comporter plusieurs cartes, relevez les paramètres de la carte connectée à Internet



Relever les paramètres IP

- Remarque: rappelez-vous que l'adresse de passerelle relevé dans la figure précédente correspond à l'adresse du routeur (ou du serveur) qui fait le lien avec un autre réseau (généralement Internet)
- En tapant cette adresse dans un navigateur, généralement vous accédez à l'interface d'administration du routeur, ce qui vous permettra de vérifier les paramètres et la présence de la connexion à Internet
- Dans le cas d'un serveur, vous pourrez généralement vous connecter via une console ssh (avec putty par exemple) -> voir Manip10

Renouveler les paramètres IP

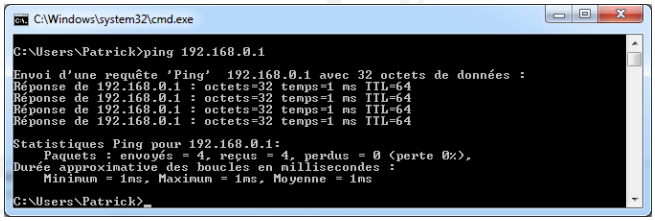
- Sous Windows, pour libérer l'adresse IP, on tape **ipconfig /release** (accessible uniquement si l'invite de commande est exécutée en tant qu'administrateur -> Tous les programmes
  -> Accessoires -> bouton droit sur Invite de commande
  -> Exécuter en tant qu'administrateur)
- Pour la renouveler (en demander une autre au serveur DHCP), on tape **ipconfig /renew**
- Remarque: le serveur DHCP réattribue par défaut, la même adresse IP (si il en avait attribué une …)

Renouveler les paramètres IP

- Sous linux, ça dépend de la distribution …
- Sous CentOS, on tapera **dhclient eth0** (si eth0 est la carte réseau connectée au net)
- Sous Ubuntu, un **service network restart** relira le contenu du fichier **/etc/network/interfaces**

Vérifier la présence d'un hôte

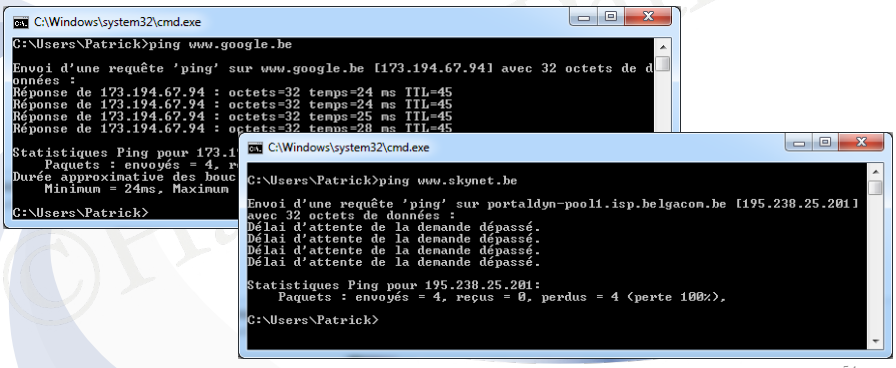
- On envoie un écho radar pour vérifier la présence de l'hôte
- Sous Windows ou sous Linux, tapez la commande **ping** suivi de l'adresse IP à vérifier
  - Exemple: ping 192.168.1.1



- C'est une commande ICMP (protocole de messages/erreurs du protocole IP) qui envoie un echo radar (un "echo request" et qui attend un "echo reply")

Vérifier la présence d'un hôte

- Remarque: certains serveurs bloquent le trafic ICMP et le **ping** ne fonctionne pas même si le serveur est présent sur Internet
  - Exemple: ping www.skynet.be

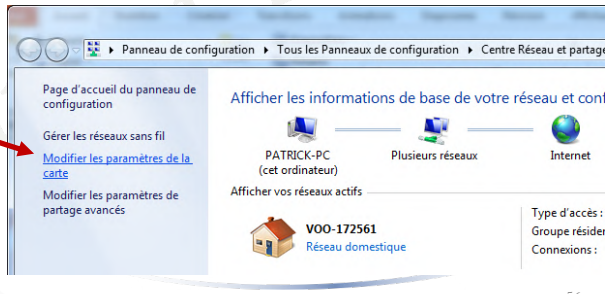


Manipulations

- Soit un PC avec une carte réseau configurée avec les paramètres automatiques
- Vérifiez, avec **ipconfig** (ou **ifconfig** sous linux), que vous avez bien une adresse de passerelle
- Faites un **ping** du 8.8.8.8 (serveur DNS de Google)
- Par **ipconfig /all** (ou **cat /etc/resolv.conf** sous linux), vérifiez l'adresse du serveur DNS
- Faites un **ping** de www.google.be et relevez l'adresse IP correspondante

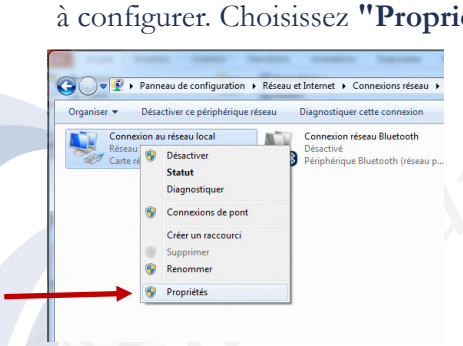
Manipulations

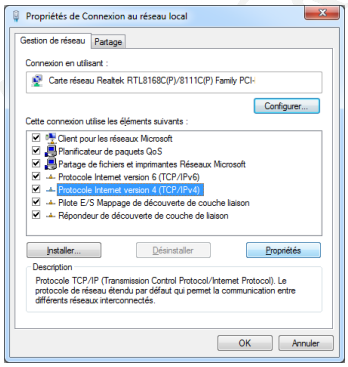
- Notez les paramètres attribués automatiquement à votre PC (adresse IP, masque, passerelle, adresse du serveur DNS)
- Passez en configuration manuelle via le **Centre réseau et partage** (Windows 7), **"Modifier les paramètres de la carte"**



Manipulations

- Cliquez avec le bouton droit de la souris sur l'interface réseau à configurer. Choisissez **"Propriétés"**

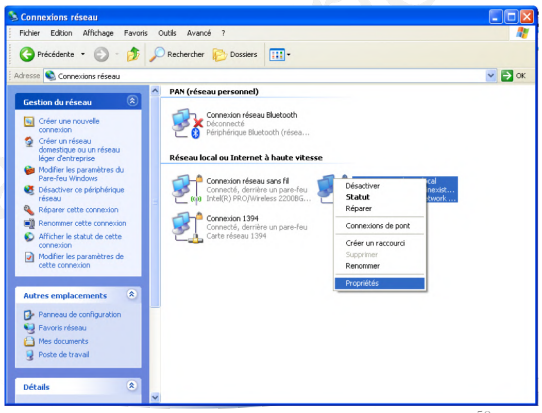




- Choisissez **"Protocole Internet version 4 (TCP/IPv4)"**, puis **"Propriétés"**

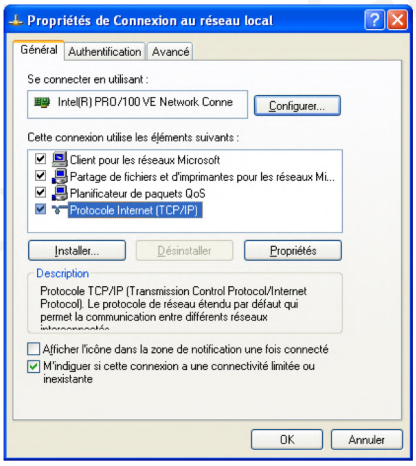
Manipulations

- Sous Windows XP, dans le panneau de configuration, choisissez **"Connexions réseau"** et cliquez avec le bouton droit de la souris sur la carte réseau connectée à Internet et choisissez **"Propriétés"**



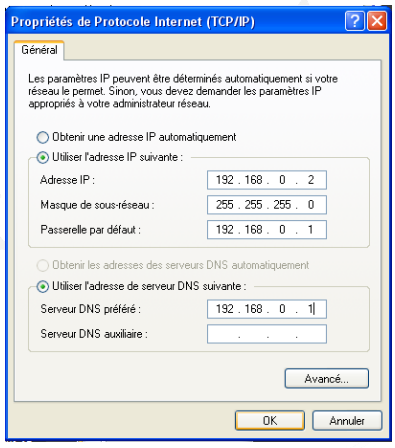
Manipulations

- Choisissez **"Protocole Internet (TCP/IP)"**, puis **"Propriétés"**



Manipulations

- Que ce soit sous Windows 7 ou XP notez les paramètres relevés dans les différents champs à votre disposition et validez (vous devez valider les deux fenêtres sinon les nouveaux paramètres ne sont pas actifs)



- Vérifiez que vous avez tjs accès à Internet et que vous savez résoudre les noms de domaine

Manipulations

- Enlevez le serveur DNS et retestez le **ping** vers Google et vers l'adresse 8.8.8.8
- Ouvrez un navigateur, dans la barre d'adresse, tapez www.google.be puis l'adresse IP que vous avez relevé précédemment, lors du **ping** de www.google.be
- Enlevez la passerelle et retestez le **ping** vers 8.8.8.8 puis le **ping** vers l'adresse de passerelle
- Tirez, à chaque fois, les conclusions qui s'imposent

Conclusions des manipulations

- Des manipulations précédentes, déterminez le rôle:
  - de l'adresse IP
  - du masque de sous-réseau
  - de la passerelle
  - du serveur DNS
- Les outils **ipconfig** et **ping** sont les outils les plus simples et les plus précieux pour dépanner les réseaux, maîtrisez-les et utilisez-les autant que possible !

Conclusion

- Vous savez maintenant ce que sont les adresses IP et les paramètres associés
- Vous pouvez vérifier les paramètres reçus dynamiquement, tester la présence d'hôtes (entre autre la passerelle) et configurer des paramètres IP statiques
- Merci de votre attention