LES RESEAUX SUR PC avec le Protocole TCP-IP
ADRESSES MASQUES
CONFIGURATION & PARTAGE DE RESSOURCES

1 * LES PROTOCOLES (rappel)

Un protocole est un ensemble des règles et procédures techniques normalisées permettant l'échange d'informations entre les ordinateurs, on peut le définir plus simplement en disant que c'est une méthode de mise en forme de données expédiées sur le réseau, un langage de communication entre les

2 * LE PROTOCOLE TCPIP

2.1 historique

il date des années 1970, a pour origine une demande du département de la défense des Etats Unis, qui souhaitait disposer d'un protocole robuste et universel.

2.2 avantages

TCP/IP (Transmission Control Protocol/Internet Protocol), le plus utilisé sur les réseaux, c'est le protocole d'Internet. Très riche c'est LE standard des réseaux mais son paramétrage complexe (2500 services de TCP) ainsi que ses règles d'acheminement (le routage) ne sont pas faciles à mettre en place. C'est le seule protocole qui permette de relier des machines totalement différentes entre elles (PC, serveurs UNIX, Macintosh ....) IP est capable de franchir toutes les barrières que constituent des moyens de communication très différents, tels que les routeurs, les modems, les cartes numéris.

le standard TCP/IP est dans le domaine public, personne n'en est propriétaire, quand on l'installe, il n'y a aucun droit de licence à payer. Toute sa description se trouve dans les RFC(les commentaires, Request For Comments)

2.3 Transmisions des données

Les données circulent sur Internet sous forme de datagrammes (on parle aussi de paquets). Les datagrammes 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, ...).

Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit.

Voici ce à quoi ressemble un datagramme:

<table>
<tr><td>Version</td><td>Longueur d'en-tête</td><td>type de service</td><td colspan="2">Longueur totale</td></tr>
<tr><td colspan="3">Identification</td><td>Drapeau</td><td>Décalage fragment</td></tr>
<tr><td colspan="2">Durée de vie</td><td>Protocole</td><td colspan="2">Somme de contrôle en-tête</td></tr>
<tr><td colspan="5">Adresse IP source</td></tr>
<tr><td colspan="5">Adresse IP destination</td></tr>
<tr><td colspan="5">Données</td></tr>
</table>

Voici la signification des différents champs:

Version: il s'agit de la version du protocole IP que l'on utilise Elle est codée sur 4 bits

Longueur d'en-tête: il s'agit du nombre de mots de 32 bits sur lesquels sont répartis l'en-tête

Type de service: il indique la façon de laquelle le datagramme doit être traité

Longueur totale: il indique la taille totale du datagramme en octets. La taille de ce champ étant de 2 octets, la taille totale du datagramme ne peut dépasser 65536 octets. (1500 octets en Ethernet)

identification, drapeaux (flags) et déplacement de fragment permettent la fragmentation desdatagrammes,

Durée de vie: (appelée aussi TTL: *Time To Live*) indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus

Protocole: ce champ permet de savoir de quel protocole est issu le datagramme

Somme de contrôle de l'en-tête (*header checksum*): ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête afin de déterminé si celui-ci n'a pas éteacute; altéré pendant la transmission. Pour ce faire, on considère l'en-tête comme une suite d'entiers, on fait la somme de ces enteirs en complément à 1, puis on complémente le résultat à 1, on obtient alors le total de contrôle. Celui-ci est en fait tel que lorsque l'on fait la somme des champs de l'en-tête (somme de contrôle inclue) donne un nombre avec tous les bits positionnés à 1

Adresse IP Source: Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre

Adresse IP destination: Adresse IP du destinataire du message

ROUTAGE Le routage consiste à assurer l'acheminement d'un datagramme IP à travers un réseau en empruntant le chemin le plus court. Ce rôle est assuré par des machines appelées Routeurs, c'est-à-dire des machines reliées (reliant) au moins deux réseaux.

3 * Les adresses, les classes, les masques

Adresse : nombre de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits),
on les note donc sous la forme xxx.xxx.xxx.xxx où chaque xxx représente un entier de 0 à 255.

Chaque hôte TCP/IP est identifié par une adresse IP logique.

Une adresse IP unique est requise pour chaque hôte et composant du réseau .

Chaque adresse IP définit l'**identificateur de réseau et l'identificateur d'hôte**.

L'identificateur de réseau définit les systèmes situés sur le même segment physique.

L'adresse de chaque hôte doit être unique par rapport à l'identificateur réseau.

Chaque adresse comprend en fait deux champs.
·**NetID**, l'adresse logique du **réseau** l'identifiant imposé par l'Internic
·**HostID**, l'adresse logique de **l'équipement** (ordinateur, imprimante, routeur...)

Voici un exemple d'adresse IP selon les formats binaire et décimal.

Format binaire	**Format décimale**
10000011 01101011 00000011 00011000	131 . 107 . 3 . 24

le choix des adresse d'un réseau ne doit pas se faire au hasard il existe 5 classes d'adresses

- Classes réseaux: A, B, C, D, E

adresses pour réseaux **privées** (non routables sur l'Internet):

10.0.0.0 à => 10.255.255.255	**(1 réseau cl. A)**	16 777 214	machines/réseau
172.16.0.0 à => 172.31.255.255	**(15 réseaux cl. B)**	65536	machines/réseau
192.168.0.0 à => 192.168.255.255	**(255 réseaux cl. C)**	255	machines/réseau

Adresse particulières :
loop back (test local de soi-même) : 127.0.0.1
Tous les réseaux doivent avoir une adresse de réseau: où les bits machine sont à 0:
exemple adresse du réseau privé classe A => 10.0.0.0
Tous les réseaux doivent avoir une adresse de diffusion (broadcast): tous les bits machine sont à 1 :
exemple adresse de broadcast du réseau privé classe A => 10.255.255.255

Sous réseaux et Masque

Une adresse IP comporte :
une sous-partie **adresse du réseau** et une sous-partie **adresse de la machine** (**hôte**) dans ce réseau

subdivision de l'adresse IP: parties réseau et hôte	
exemple classe A:	**10.** **20.13.5** **adresse réseau** (netID) **adresse hôte** (hostID)
exemple classe C:	**192.168.20.** **5** **adresse réseau** (netID) **adresse hôte** (hostID)

Si on veut créer des **sous-ensembles fonctionnels** dans un réseau (par exemple pour limiter les communications entre différentes machines, entre machines de salles différentes...) on crée des **sous-réseaux .**
NB: Ceux-ci n'ont pas de relation avec l'organisation physique du cablage, il s'agit de **réseaux logiques**
Pour définir les sous-réseaux, on utilise une partie de l'adresse hôte comme **identificateur de sous-réseau**.

Le nombre de bits réservé pour l'identification du sous-réseau est codé par le **masque de sous-réseau**.
Par définition un masque de sous-réseau est constitué de 4 octets
(notation décimale à points, donc de 0.0.0.0 à 255.255.255.255) que l'on met en correspondance avec l'adresse IP.

Exemple pour un réseau privé de classe A:					
ad. IP des hôtes:	**10**	**25.**	**x.**	**y**	adresse réseau = **10**
masque de sous-réseau:	**255.**	**255.**	**0.**	**0**	**partie de l'adresse hôte utilisée pour définir le sous-réseau**
					adresse de l'hôte dans le sous-réseau

La règle de lecture des masques de sous-réseaux consiste à mettre en correspondance les bits (exprimés en binaire) de l'adresse IP avec le masque de sous-réseau: **tous les bits à 1 du masque de sous-réseau** imposent que les bits correspondants de l'adresse IP soient **identiques pour les hôtes** du sous-réseau.

Exemple pour l'hôte 10.25.96.53 du sous-réseau 10.25.0.0 :				
ad. IP décimale:	10.	**25.**	96.	53
ad. IP binaire:	**00001010**	**00011001**	**01100000**	**00110101**
masque binaire:	**11111111**	**11111111**	**00000000**	**00000000**
masque décimal:	255.	**255.**	0.	0

- Pour les réseaux de classe C (adresse hôte sur un seul octet, par ex 192.168.1-254.**0**) on peut utiliser de la même manière une partie des 8 bits de la partie hôte pour créer des sous-réseaux mais il convient de respecter une méthode rigoureuse pour la définition des sous-réseaux:

Masque binaire (4eme octet)		Masque décimal (4eme octet)	Nombre ss-réseau / nombre d'ordi par réseau
00000000		**0**	pas de sous réseau
1	**0000000**	**128**	**2** ss réseaux de **128** ordis
11	**000000**	**192**	**4** ss réseaux de **64** ordis
111	**00000**	**224**	**8** ss réseaux de **32** ordis
1111	**0000**	**240**	**16** ss réseaux de **16** ordis
11111	**000**	**248**	**32** ss réseaux de **8** ordis
111111	**00**	**252**	**64** ss réseaux de **4** ordis
1111111	**0**	**254**	**128** réseaux de **2** ordi (inutilisable)
11111111		**255**	une seule machine

4 * quelques définitions supplémentaires : Passerelle(Gatway) Proxi Routeur Dhcp

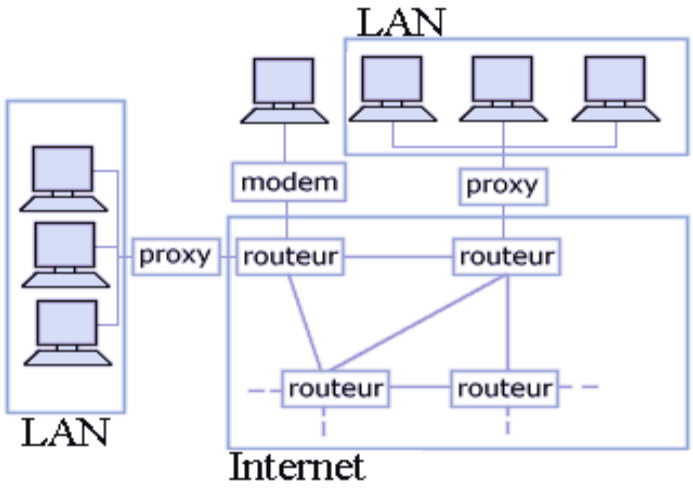
Un routeur est une machine connectée à plusieurs réseaux. Il reçoit des paquets IP en entrée et doit les renvoyer sur une des sorties déterminée par une table de routage.

Soit le destinataire est directement accessible par une des interfaces alors on émet le packet sur cette interface

Soit le destinataire se trouve derrière un routeur alors il faut envoyer le packet vers cette passerelle (gateway)

Les passerelles applicatives (en anglais «gateways») sont des sysèmes matériels et logiciels permettant de faire la liaison entre deux réseaux, servant notamment à faire l'interface entre des protocoles différents.

DHCP est un protocole d'assignation automatique des paramètres des machines connectées à un réseau DHCP



5 * Outils de diagnostic de TCP / IP:

· **Quelques outils en ligne de commande fournis avec Microsoft TCP/IP**

ping: séquence standard de test de la config IP d'un poste= test de TCP/IP: 127.0.0.1 (adr rebouclage),
test de l'interface (ping sur les adresses de la carte réseau),
test de la liaison avec la passerelle (ou le proxy), test d'un hôte sur l'internet.

IPconfig /all (Win NT et Win 9x) ou **winipcfg** (Win 9x exclusivement) => Plus d'info

netstat avec les options possibles:

-a liste les connexions en cours et leur état

-s permet de lister les statistiques des connexions en cours pour **les protocoles TCP, UDP et IP**

-r permet, en plus des statistiques par protocoles, de connaitre le **contenu de la table de routage**

-e permet de lister les statistiques pour le protocole Ethernet

tracert [nom_hôte ou **adresse_IP_hôte]** permet de connaitre la route (succession des routeurs) utilisés par un datagramme IP pour joindre un hôte distant (par ex tracert www.google.com donne le chemin jusqu'à la côte Ouest des USA où sont implantés les serveurs de Google)

6 * La CONFIGURATION sous Windows et le PARTAGE de RESSOURCES

La configuration varie suivant les version de Windows etles droits possédés por Win2000 et winXP
il faut d'abord installer la carte réseaux dans la machine
installer ses DRIVERS si elle n'est pas automatiquement reconnue (disquette fournie)
Puis dans le panneau de configuration choisir réseau /propriété
lier la carte au protocole TCPIP puis paraméter celui-ci
(adresse machine, masque sous réseau adresse passerelle, domaine etc ...)
enfin définir les partage autorisés Répertoires, lecteurs, graveurs imprimantes etc ..

Voir document d'accompagnement des TP