16

Administrer son réseau IP

Votre réseau d'entreprise est désormais opérationnel. Il s'étend sur plusieurs sites. Cependant, les problèmes vous guettent. En effet, plus le réseau est important, plus la probabilité qu'une panne survienne à un endroit ou à un autre est importante. C'est statistique.

En outre, plus un réseau est important, plus il est difficile à gérer. Il convient donc d'utiliser des outils qui simplifient sa gestion et diminuent donc le nombre potentiel de pannes.

Dans ce chapitre vous apprendrez :

- à utiliser les outils de base pour le diagnostic réseau ;
- à installer un serveur DHCP qui vous facilitera la vie.

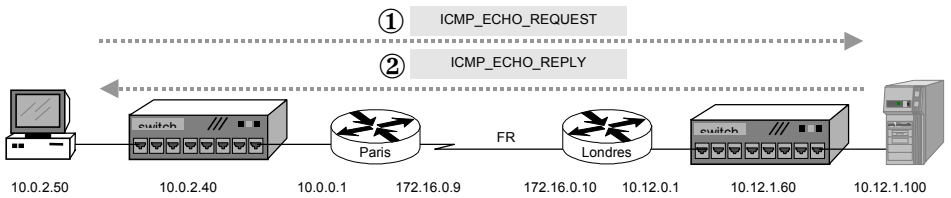
Les utilitaires de base

Le ping

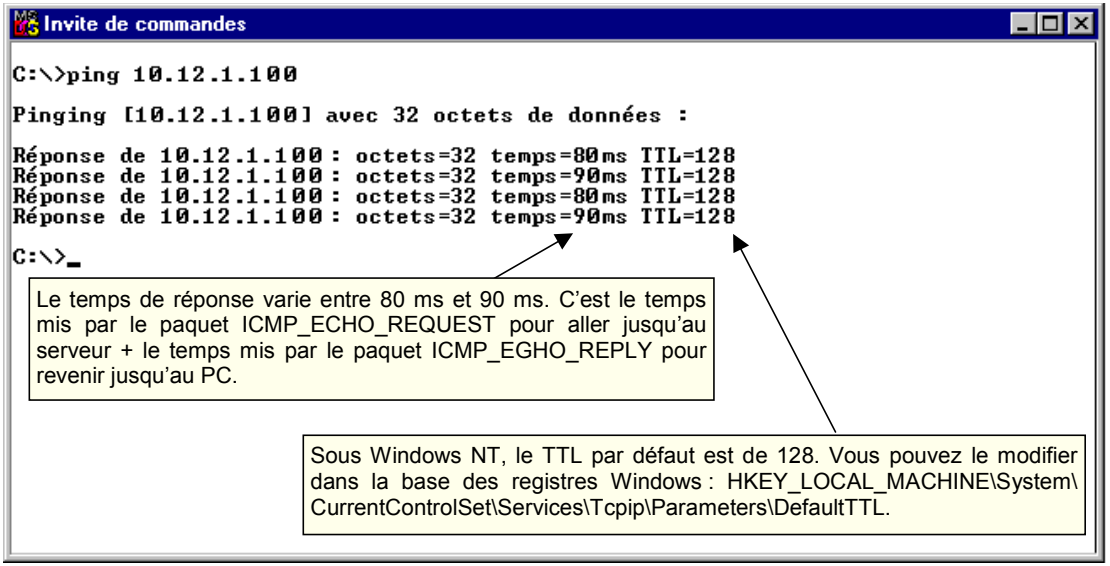
Deux programmes doivent faire partie du « kit de survie » de tout administrateur réseau : ping et Traceroute.

La commande de base est le **ping** (*Packet Internet Groper*, ou *ping-pong*). Ce programme permet de savoir si une station IP est active et, plus généralement, si le réseau fonctionne correctement entre deux points, par exemple, entre votre PC à Paris et le serveur de Londres. Autre fonction intéressante, le programme donne également le temps de réponse mesuré.

Figure 16-1.
Le ping.



La commande ping s'appuie sur le protocole ICMP (*Internet Control Message Protocol*) qui fait partie de la couche IP. Ce protocole est utilisé pour toutes les opérations qui ont trait à la gestion du réseau IP, et ce, de façon transparente pour les utilisateurs.



Le traceroute

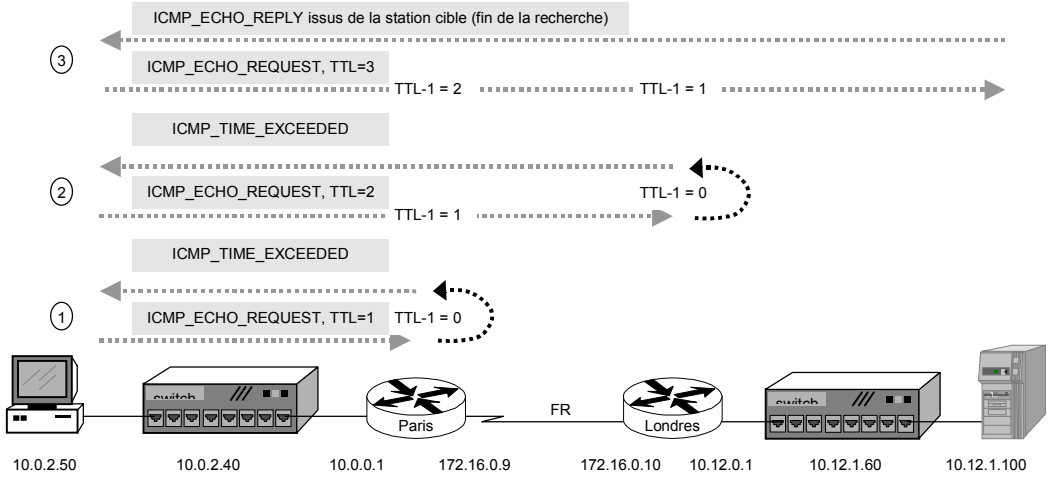
L'autre commande de base est le **traceroute**. Ce programme utilise des mécanismes propres à IP et ICMP pour afficher à l'écran la route empruntée par un paquet IP en plus du temps de réponse. Son principe de fonctionnement est le suivant :

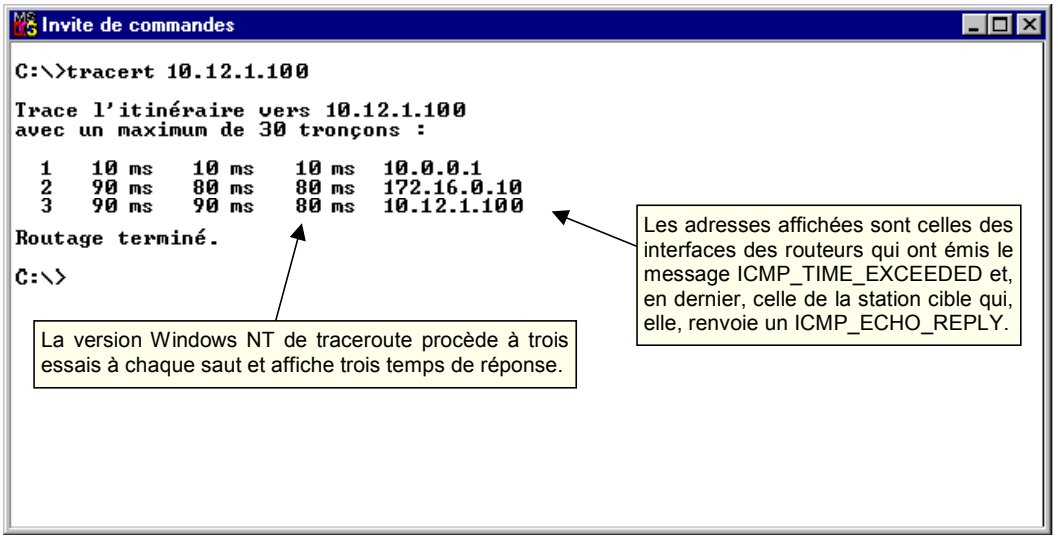
- Le programme envoie un paquet ICMP_echo_request à destination de la machine cible avec un TTL (*Time To Live*) égal à 1.
- Le premier routeur reçoit ce paquet, décrémente le TTL de 1, et constate qu'il est égal à 0. Il détruit le paquet, et renvoie à l'émetteur un message ICMP_Time_exceeded.
- Le programme enregistre l'adresse IP du routeur qui a envoyé de ce message ainsi que le temps écoulé depuis l'émission du paquet ICMP_Echo_request.
- Le programme continue de même en incrémentant le TTL de 1 à chaque paquet ICMP_Echo_request émis. Le paquet ira donc un saut plus loin que le précédent, et le routeur suivant répondra.

Le mécanisme du TTL (*Time To Live*) est expliqué dans l'encart « Le point sur IP v4 «, au chapitre 7.

Certaines implémentations de traceroute utilisent un paquet UDP sur un port quelconque à la place d'un paquet ICMP_Echo_request. La RFC 1393 (statut expérimental) propose, quant à elle, un autre algorithme qui repose sur un message ICMP_Traceroute (type 30). Il est cependant rarement implémenté, aussi bien sur les stations que sur les routeurs.

Figure 16-2.
Le traceroute.



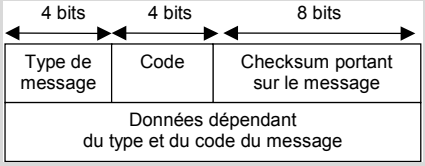


La commande ping sera plutôt utilisée pour savoir si un nœud IP est actif et joignable ainsi que le temps de réponse de bout en bout. Elle offre en outre davantage de possibilités de paramétrage (taille et nombre des paquets, enregistrement de la route, etc.). La commande traceroute permet, quant à elle, de savoir quelle route est empruntée (par exemple, le chemin principal ou celui de backup) et quelles parties du réseau engendrent les temps de réponse les plus longs.

De nombreux utilitaires de ce type sont disponibles sur les sites ftp.lip6.fr, tucows.club-internet.fr et www.winsite.com.

LE POINT SUR ICMP (RFC 792, 950 ET 1256)

ICMP (*Internet Control Message Protocol*) regroupe près de trente types de messages permettant aux nœuds d'un réseau d'échanger des informations de gestion relatives à IP.



Excepté pour les messages Echo des Timestamp, le paquet ICMP contient une copie partielle du paquet original ayant causé l'erreur (en-tête IP + 8 premiers octets des données).

Le tableau de la page suivante recense les types et codes existants à ce jour. Lorsque cela n'est pas précisé, les messages sont générés par les routeurs et les stations IP. Sauf indication contraire, les messages ICMP sont définis dans la RFC 792.

• • •

LE POINT SUR ICMP (RFC 792, 950 ET 1256 – SUITE)

Type	Message	Code et description
3	Destination Unreachable	0 *network unreachable* : le routeur ne connaît pas la route 1 *host unreachable* : le routeur ne peut pas trouver la station 2 *protocol unreachable* : le protocole demandé n'est pas actif. 3 *port unreachable* : aucun programme ne répond sur ce port TCP ou UDP. 4 *fragmentation needed and DF set* : le routeur a reçu un fragment alors que la fragmentation est interdite (bit DF du paquet IP positionné à 1). 5 source route failed
11	Time exceeded	0 Si un routeur reçoit un paquet avec un TTL à 0, il envoie ce message à l'émetteur. 1 Si une station n'obtient pas tous les fragments d'un message dans le temps imparti, elle envoie ce message à l'émetteur.
12	Parameter Problem	0 Des paramètres incorrects ou inconsistants dans l'en-tête du paquet IP ont été détectés (un pointeur indique la position de l'erreur dans l'entête)
4	Source Quench	0 Le routeur, ou la station, est congestionné (ou régule le trafic selon un algorithme propre) et demande à l'émetteur de réduire son flux. Les paquets en excès peuvent être détruits.
5	Redirect	0 *for the Network* : le routeur a détecté une meilleure route et indique à la station quel routeur solliciter 1 *for the Host* : idem pour une station 2 *for the TOS and Network* : idem avec le champ TOS correspondant. 3 *for the TOS and Host* : idem pour une station.
8	Echo request	0 Demande au récepteur de renvoyer un Echo reply (un identifiant et un numéro de séquence identifient le message).
0	Echo reply	0 Réponse à un Echo request. Les données contenues dans le message Echo request doivent être reportées dans ce message.
13	Timestamp	0 Indique le nombre de millisecondes écoulé depuis 00h00 GMT lorsque le message Timestamp a été envoyé. Utilisé pour évaluer le temps de transit.
14	Timestamp reply	0 Indique le nombre de millisecondes écoulé depuis 00h00 GMT lorsque le message Timestamp a été reçu, ainsi que la valeur de ce nombre lorsque la réponse a été envoyée.
15	Information request	0 (obsolète) Permettait aux stations d'obtenir leur adresse IP. Mécanisme remplacé par les protocoles RARP, puis BOOTP et DHCP.
16	Information reply	0 Idem (obsolète).
17	Mask request	0 (RFC 950) Permet à une station d'obtenir le masque IP de son sous-réseau.
18	Mask reply	0 (RFC 950) Réponse du routeur à une demande de masque.

• • •

LE POINT SUR ICMP (RFC 792, 950 ET 1256 – FIN)

Type	Message	Code et description
9	Router Advertisement	0 (RFC 1256) Émis périodiquement par un routeur pour indiquer l'adresse IP de son interface. Permet aux routeurs de découvrir leurs voisins, et aux stations de découvrir leur passerelle par défaut.
10	Router Sollicitation	0 (RFC 1256) Lors de son initialisation, une station peut demander à un routeur de s'annoncer immédiatement. Les routeurs n'envoient, en principe, aucune sollicitation, mais attendent les annonces.

L'IANA recense d'autres messages ICMP, soit expérimentaux, soit pour IPv6.

Observer ce qu'il se passe sur son réseau

Si votre réseau présente un dysfonctionnement et que, malgré toutes vos investigations, vous n'avez pas trouvé d'où provient le problème, il ne vous reste plus qu'à l'ausculter, c'est-à-dire observer les données qui y circulent.

Même lorsque le réseau semble bien fonctionner, il n'est pas inutile d'y jeter un coup d'œil, car bien souvent des erreurs (collision, paquets corrompus, flux non identifié, trafic censé ne pas être présent sur ce segment, etc.) se produisent. Ces erreurs ne sont alors pas perceptibles, mais peuvent le devenir sous certains conditions, par exemple lorsque la charge réseau augmente. Une **maintenance préventive** permet donc d'éviter le pire.

L'**analyseur réseau** est l'outil tout indiqué pour ce type de situation. Il permet :

- de capturer toutes les trames qui circulent sur un segment Ethernet ;
- d'analyser le contenu de toutes les couches réseau, de la trame aux données applicatives en passant par le paquet IP ;
- de déterminer si des erreurs se produisent (collision, erreur de transmission, etc.) et en quelle proportion ;
- de connaître les temps de réponse précis (au millième de seconde près).

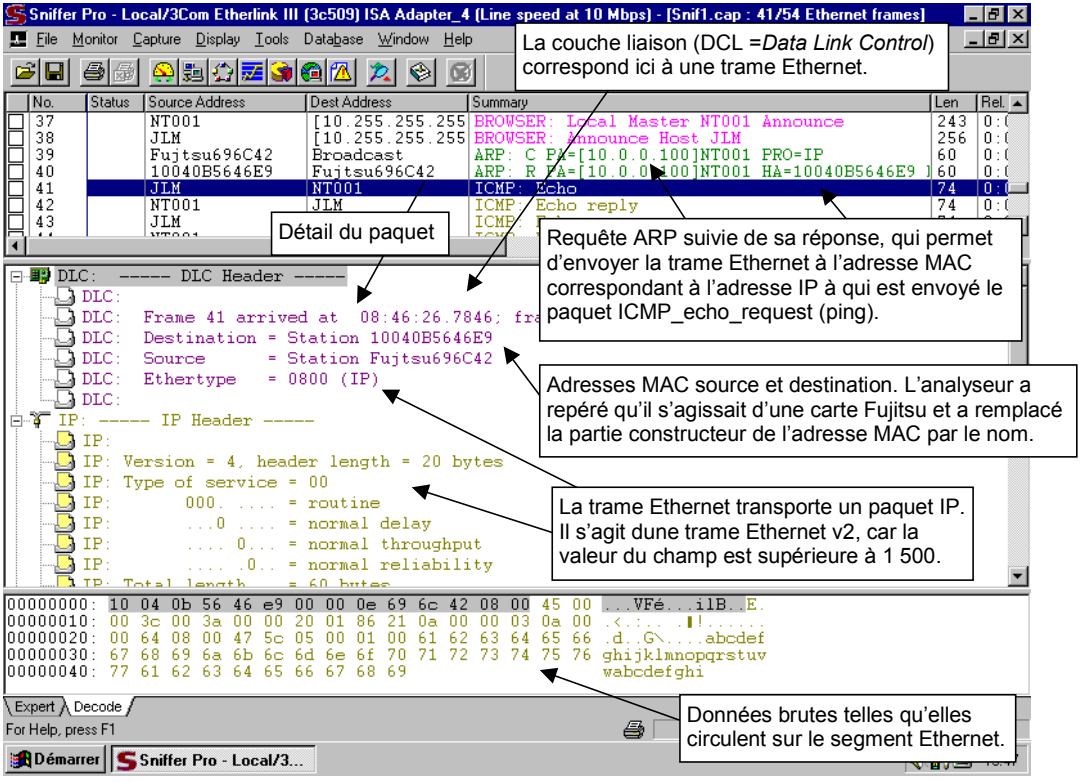
En positionnant des filtres, il est possible de suivre précisément les échanges entre deux stations, soit à partir de leurs adresses MAC, soit à partir de leurs adresses IP.

COMMENT UN ANALYSEUR RÉSEAU FONCTIONNE-T-IL ?

Un analyseur réseau est un logiciel capable de décoder idéalement tous les protocoles existants, du niveau 2 au niveau session. Il fonctionne de concert avec une carte réseau, de préférence haut de gamme, capable de capturer toutes les trames, même à pleine charge.

Le coût d'un tel produit dépend donc du nombre de protocoles reconnus et de la carte d'acquisition : Ethernet, Token-Ring ou ATM pour les LAN, et série synchrone pour les liaisons WAN en Frame Relay, ATM, etc.

La carte réseau doit fonctionner en mode **promiscus**. Dans un mode de fonctionnement normal, une carte ne prend en compte que les trames multicast et de broadcast, ainsi que celles dont l'adresse de destination MAC correspond à celle qui est programmée dans sa mémoire (PROM, Flash, etc.). En mode promiscus, la carte prend en compte toutes les trames. Toutes les cartes réseau ne supportent pas le mode promiscus.



L'analyseur réseau peut également être utilisé comme outil d'analyse pour :

- mesurer la volumétrie générée par une application entre un client et un serveur ;
- évaluer la part de responsabilité du réseau, du serveur et du client dans le temps de réponse global entre un client et un serveur ;
- surveiller la charge du réseau pendant 24 heures ou sur une semaine ;
- déterminer quelles stations génèrent le plus de trafic ;
- déterminer la répartition du trafic par protocole, par adresse IP, etc.

Enfin, l'analyseur réseau offre souvent des fonctions évoluées, telles que :

- une minuterie (*triger*) qui permet de déclencher et d'arrêter la capture sur réception d'une trame particulière (adresse, données, etc.) ;
- un générateur de trafic pour vérifier le comportement du réseau et des applications à pleine charge (par exemple si trop d'erreurs surviennent à partir d'une certaine charge, le câblage est sans doute en cause) ;
- la possibilité de rejouer un échange de trames préalablement capturées.

Piloter son réseau

Si votre réseau prend de l'ampleur — le nombre des équipements (routeurs, concentrateurs, commutateurs, etc.) augmente, et ces derniers sont répartis sur différents sites —, il devient de plus en plus nécessaire de centraliser la gestion des équipements.

Pour ce faire, la famille des protocoles TCP/IP propose le protocole SNMP (*Simple Network Management Protocol*) qui permet l'échange d'information entre **une station d'administration** (le client) et des **agents** (les serveurs) implantés dans chaque équipement. On parle alors d'**agent SNMP** ; celui-ci se présente sous forme d'un petit programme qui répond aux requêtes SNMP émises par la station d'administration.

Quelle station d'administration ?

Une station d'administration, ou **plate-forme d'administration**, est constituée d'un ordinateur sous Windows NT/2000 ou sous Unix, ainsi que d'un logiciel, tel qu'OpenView de Hewlett-Packard, Tivoli d'IBM, Unicenter de Computer Associates, Spectrum de Cabletron, etc.

Ces logiciels haut de gamme (environ 100 000 francs) sont en fait des boîtes à outils sur lesquelles s'installent des **modules dédiés** à chaque constructeur (CiscoView pour les équipements Cisco, Optivity pour ceux de Bay Networks, etc.). Ces modules peuvent, par ailleurs, fonctionner de manière autonome.

L'intérêt d'une telle plate-forme est de fédérer la gestion d'un parc d'équipements hétérogène autour d'une gestion centralisée des alarmes et d'une carte réseau sur laquelle s'affichent les équipements découverts dynamiquement.

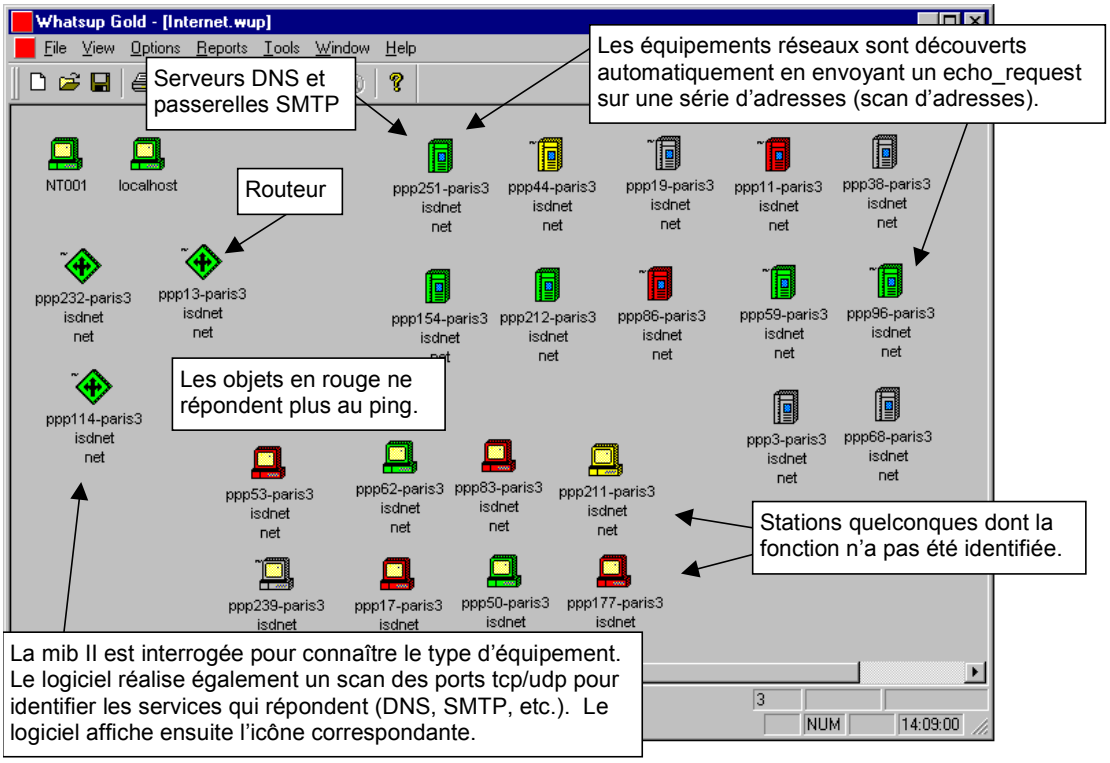
En fait, les plates-formes d'administration nécessitent un paramétrage très important dont le coût peut être plus élevé que celui du matériel et du logiciel réunis. Elles sont pour cela réservées aux grands réseaux, notamment chez les opérateurs.

Pour un réseau de plus petite taille, il est préférable d'utiliser les modules des constructeurs en mode autonome : si vous disposez d'un parc d'équipements homogène, nul besoin d'investir dans une « usine à gaz ». L'intérêt est de pouvoir visualiser graphiquement les équipements et de cliquer sur les cartes et ports que vous voulez configurer.

Certains administrateurs de grands réseaux se dispensent même de ce type de logiciel, préférant utiliser Telnet, TFTP et les fichiers de configuration en mode texte, le ping et le traceroute étant utilisés pour les dépannages quotidiens.

Pour quelle utilisation ?

Si vous désirez néanmoins visualiser et surveiller votre réseau de manière graphique, vous pouvez toujours utiliser des petits logiciels, tels que *Whatsup*. Le principe est identique à celui des plates-formes, mais avec un peu moins de fonctionnalités.



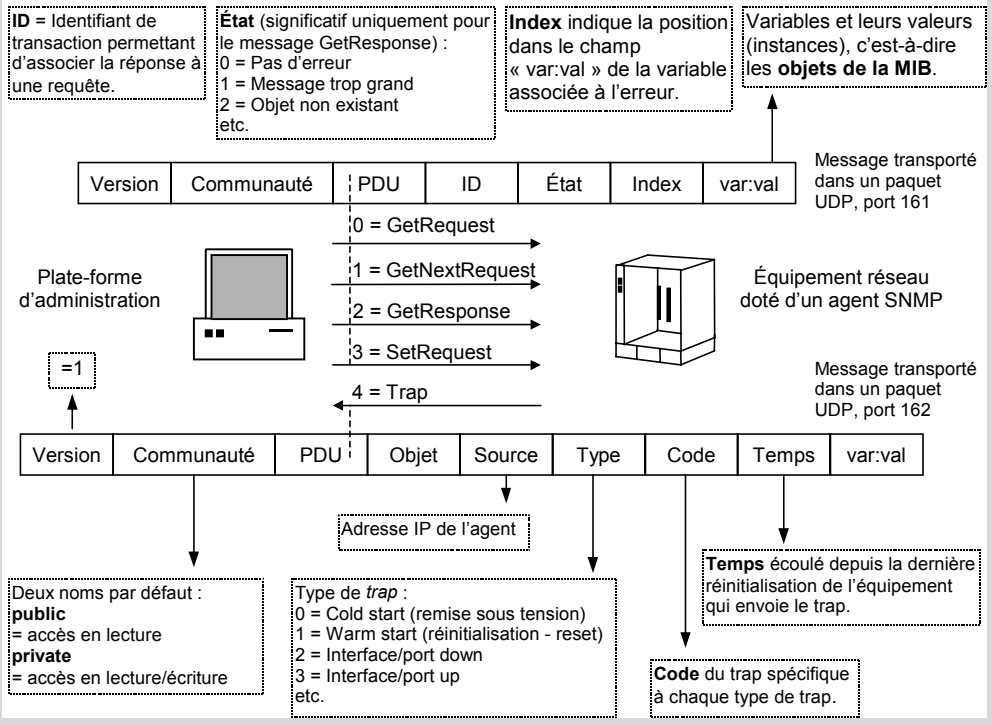
Cette carte a été obtenue en scannant les adresses IP d'un fournisseur d'accès à l'Internet (ISP). Le logiciel a ainsi trouvé des routeurs, des serveurs DNS, des passerelles de messagerie SMTP, ainsi qu'un certain nombre de stations non identifiées.

La première tâche est d'agencer les icônes qui apparaissent dans le désordre. L'administrateur peut ensuite dessiner un réseau et positionner les objets dessus, de manière à faire correspondre la carte à la réalité.

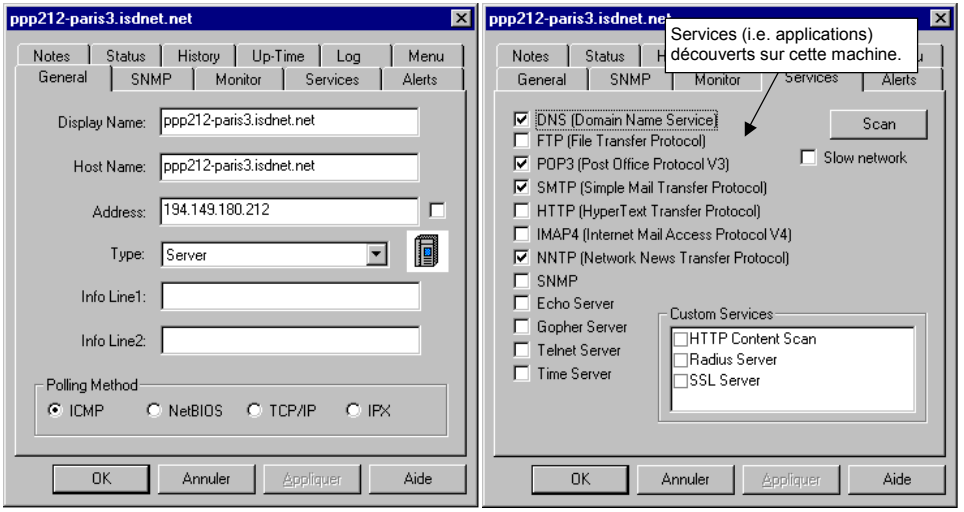
En sélectionnant une icône, il est alors possible d'opérer plusieurs actions sur l'équipement : ajouter des informations complémentaires, interroger son agent SNMP, surveiller des paramètres de cet agent, positionner des seuils d'alerte, etc.

LE POINT SUR SNMP V1 (RFC 1157, 2571, 2572)

Le protocole SNMP (*Simple Network Management Protocol*) est utilisé pour piloter tous les équipements du réseau (routeurs, commutateurs, concentrateurs, serveurs, etc.) à partir d'une **station d'administration**.
Il est ainsi possible de **configurer** à distance les équipements (activation d'une interface, ajout d'une adresse IP, etc.) et de récupérer les paramètres actifs. Inversement, un équipement peut envoyer une alarme à la station d'administration *via* un **trap SNMP**.



Presque tous les équipements réseau intègrent un **agent SNMP**. Ce logiciel réalise l'interface entre les **requêtes SNMP** et la base de donnée **MIB** (*Management Information Base*) qui regroupe tous les paramètres de l'équipement.



Le problème de ce type de logiciel est qu'il faut sans cesse le mettre à jour, car le réseau ne cesse d'évoluer. L'autre problème tient à la gestion des alertes : le logiciel doit être très précisément paramétré pour ne générer que des alarmes réelles. Ces deux activités peuvent prendre beaucoup de temps à l'administrateur.

```
RFC1213-MIB DEFINITIONS ::= BEGIN
IMPORTS
       mgmt, NetworkAddress, IpAddress, Counter, Gauge, TimeTicks
FROM RFC1155-SMI
OBJECT-TYPE
FROM RFC-1212;
```

Importe ces groupes de la MIB SMI et tous les objets de la MIB-I.

Cette MIB définit le groupe MIB-II situé sous le groupe Management.

```
mib-2  OBJECT IDENTIFIER ::= { mgmt 1 }
       DisplayString : := OCTET STRING
       PhysAddress ::= OCTET STRING
-- groups in MIB-II
       system OBJECT IDENTIFIER ::= { mib-2 1 }
       interfaces    OBJECT IDENTIFIER ::= { mib-2 2 }
       at     OBJECT IDENTIFIER ::= { mib-2 3 }
       ip     OBJECT IDENTIFIER ::= { mib-2 4 }
       icmp   OBJECT IDENTIFIER ::= { mib-2 5 }
       tcp    OBJECT IDENTIFIER ::= { mib-2 6 }
       udp    OBJECT IDENTIFIER ::= { mib-2 7 }
       egp    OBJECT IDENTIFIER ::= { mib-2 8 }
       -- cmot       OBJECT IDENTIFIER ::= { mib-2 9 }
```

Définition de l'objet **system**, identifiant n° 1 dans le groupe **mib-2**

Noms et identifiants dans la MIB 2.

```
       transmission OBJECT IDENTIFIER ::= { mib-2 10}
       snmp   OBJECT IDENTIFIER ::= { mib-2 11 }

-- the System group
sysDescr OBJECT-TYPE
       SYNTAX  DisplayString (SIZE (0..255))
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
       "Par ex. : Cisco 761 Software Version c760-i…"
::= { system 1 }

sysObjectID OBJECT-TYPE
       SYNTAX  OBJECT IDENTIFIER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
       "Par Ex. : Cisco2503"
::= { system 2 }
.....................................

ifNumber OBJECT-TYPE
       SYNTAX  INTEGER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION "Nombre d'interfaces, par exemple, 3"
::= { interfaces 1 }
.....................................
END
```

Description de l'objet **sysDescr**, identifiant n° 1 dans le groupe **system**.

Description de l'objet **sysObjectID**, identifiant n° 2 dans le groupe **system**.

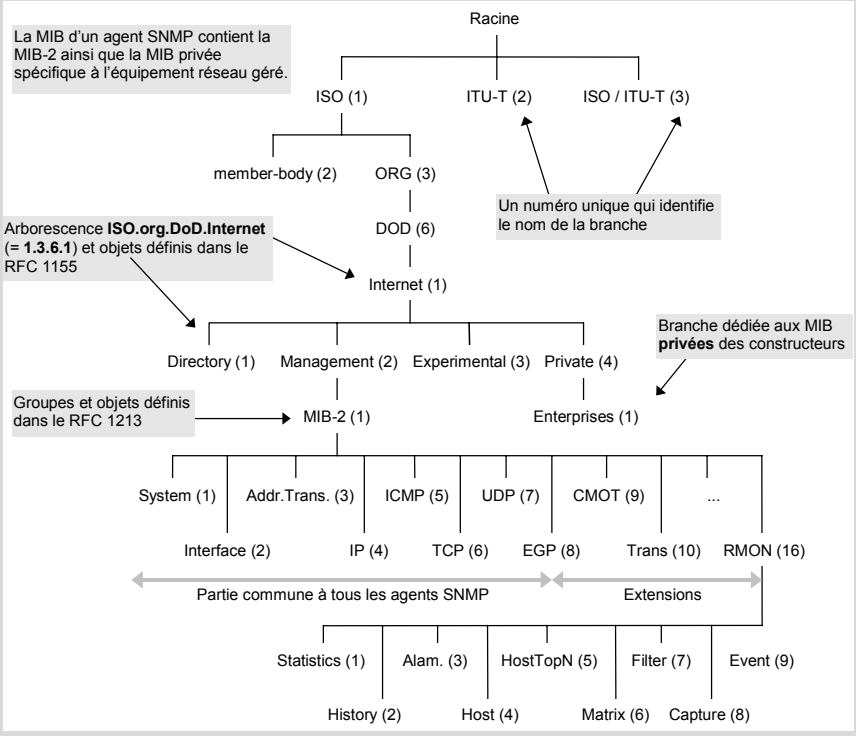
Description de l'objet **ifNumber**, identifiant n° 1 dans le groupe **interfaces**.

Pour que la station d'administration puisse interroger la MIB, il faut en premier lieu la **compiler** à partir du fichier en syntaxe ASN.1. Le fichier texte est alors intégré sous une autre forme (binaire généralement) dans le gestionnaire de MIB du logiciel d'administration.

Le moyen le plus simple de visualiser la MIB d'un équipement réseau est d'utiliser le module dédié, propre à chaque constructeur. La manipulation des variables est alors transparente, puisque le module affiche graphiquement l'équipement, par exemple, un commutateur. Il suffit alors de cliquer sur un port et de sélectionner les options qui vous sont proposées: activation/désactivation, vitesse (10, 100 ou *autosense*), nombre d'octets émis et reçus, etc.). Par ailleurs, l'interface graphique affiche les éléments dans différentes couleurs en fonction des alarmes (*trap*) qui lui sont remontées.

LE POINT SUR LA MIB (RFC 1212, 1213, 1155 ET 2863)

Les agents SNMP interagissent avec la **MIB** (*Management Information Base*) qui contient tous les paramètres de l'équipement réseau. Cette base de données se présente sous forme d'arborescence, normalisée ISO, dans laquelle une branche est réservée à l'Internet. Chaque objet de l'arborescence est identifié par un numéro.

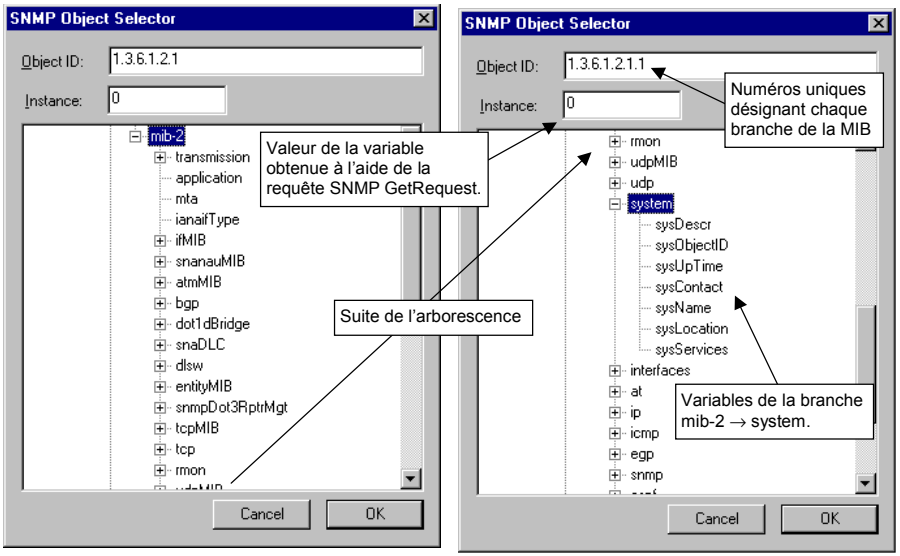


La structure de cette base de données est décrite dans la syntaxe **ASN.1** (*Abstract Syntax Notation 1*) normalisée ISO 8824. Un fichier MIB comporte deux parties (RFC 1212), la première décrivant les types et groupes d'objets (macro **Definitions**), la seconde décrivant les objets (série de macro **Object-Type**).

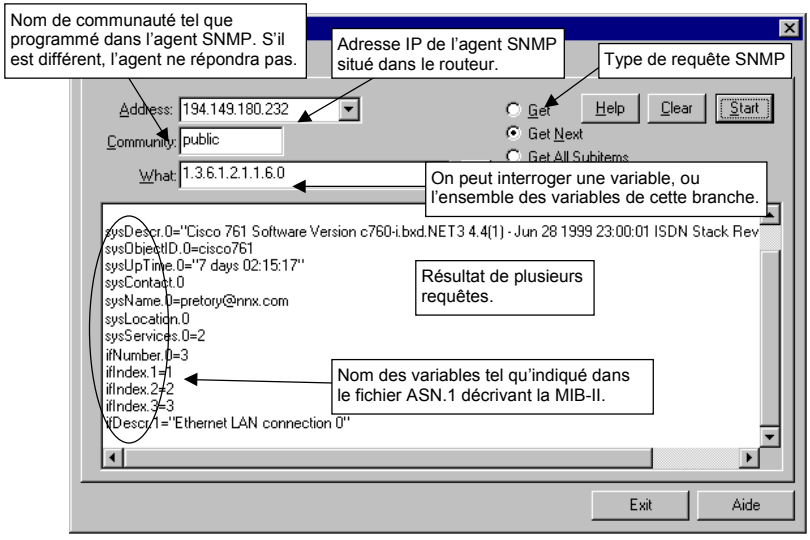
La macro Definitions contient deux **clauses** :
Import : importe des définitions d'autres fichiers MIB.
Object Identifier : définit un nouveau groupe (nom + identifiant).

La macro Object-Type contient trois clauses obligatoires, qui prennent les valeurs suivantes :
Syntax = integer | object identifier | octet string | networkaddress | ipaddress.
Access = read-only | read-write | write-only | not-accessible.
Status = mandatory | optional | obsolete | deprecated.
Et quatre autres facultatives, qui prennent les valeurs suivantes :
Description = " texte décrivant l'objet ".
Reference = référence à un autre objet.
Index = noms d'objets dans un objet structuré, par exemple, " ifIndex " pour l'objet *ifEntry* qui contient une liste d'interfaces.
Defval = valeur par défaut de l'objet, par exemple, " sysDescr " pour une syntaxe *Object Identifier*, ou " 1 " pour une syntaxe *Integer*.

La seconde solution est de parcourir la MIB à l'aide d'un ***browser* de MIB**. Cet outil permet de visualiser l'arborescence et d'interroger ou de modifier chaque variable.

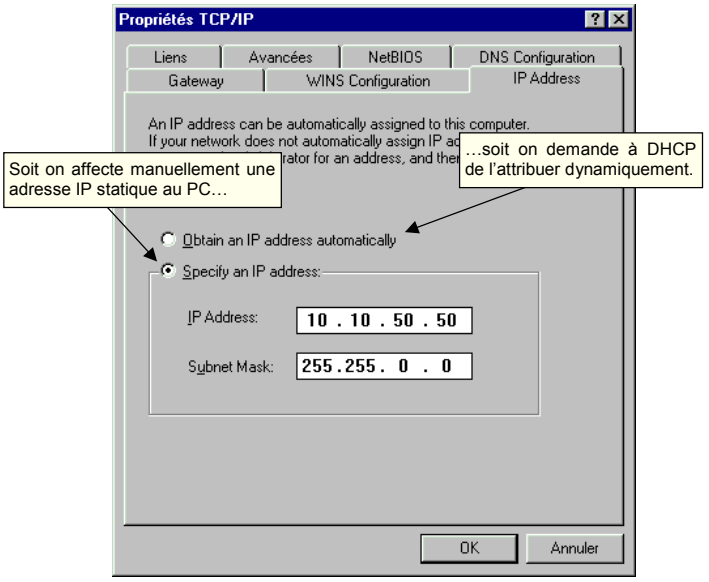


Grâce au browser de MIB, il est possible d'interroger une variable en particulier, puis de programmer des actions automatiques, comme une interrogation périodique du débit entrant et sortant d'une interface, de manière à suivre l'évolution de la charge d'un lien. Avec une série de valeurs, il sera par la suite possible de produire un graphique.



Configurer automatiquement ses PC

La configuration des PC peut s'avérer fastidieuse et être source d'erreurs : adresses dupliquées, masques incorrects, etc. Le protocole **DHCP** (*Dynamic Host Configuration Protocol*) permet d'automatiser ces tâches à l'aide d'un serveur qui héberge les configurations. La plupart des piles IP, dont celle de Microsoft, intègrent un client DHCP. L'unique configuration nécessaire sur les PC consiste à indiquer l'option " Obtenir l'adresse IP par un serveur DHCP " lors de la configuration de la carte réseau.



Par défaut, le PC envoie sa requête à tous les serveurs DHCP et sélectionne généralement le premier qui répond. Il est cependant possible de choisir le serveur DHCP en modifiant la clé de registre " HKEY_local_machine\System\CurrentControlSet\Services\VxD\DHCP\DhcpInfo00\DhcpIPAddress ".

Il s'agit de la même configuration que nous avons réalisée au premier chapitre lorsque nous nous sommes connectés à l'Internet. En effet, les fournisseurs d'accès Internet (les ISP) utilisent systématiquement un serveur DHCP pour attribuer les adresses IP aux PC qui se connectent à leur réseau *via* un modem. Il s'agit généralement d'une adresse publique prise dans le plan d'adressage affecté officiellement à l'opérateur par le NIC (*Network Information Center*).

Quelle utilisation de DHCP ?

Que vous disposiez de 10 ou 10 000 postes de travail, DHCP sera tout aussi simple à configurer et, dans tous les cas, il vous facilitera la vie.

Ce protocole permet, avant tout, d'affecter une adresse IP à une station pendant une durée limitée. À chaque initialisation — et lorsque la période de validité est expirée —, le PC demande une nouvelle adresse. Cela procure plusieurs avantages :

- Il n'y a plus de risque d'erreur lié à une configuration manuelle.
- Lorsqu'un PC est déplacé et qu'il change de réseau IP, il n'est plus nécessaire de modifier son adresse IP.
- En considérant que tous les PC ne se connectent pas en même temps, on peut utiliser un pool de 253 adresses (une classe C) pour connecter 500 PC, par exemple. Un ratio de un pour quinze est généralement utilisé par les ISP. Cela permet de pallier la pénurie d'adresses publiques.

On peut également affecter l'adresse de façon permanente, mais on perd alors tous les avantages énumérés précédemment.

Plus intéressant, l'utilisation de DHCP peut être étendue à la configuration de tous les paramètres réseau du PC (liés à la famille TCP/IP ou à d'autres protocoles), tels que le routeur par défaut, le masque IP ou encore le TTL par défaut. Cela procure de nouveaux avantages pour l'administrateur réseau :

- Tous les équipements réseau disposent des mêmes paramètres, ce qui assure une meilleure stabilité de fonctionnement de l'ensemble.
- Tout changement de configuration réseau est automatisé. Des opérations complexes, telles que la migration vers un nouveau plan d'adressage ou l'application d'un paramètre TCP permettant d'optimiser le réseau, sont rendues extrêmement simples et rapides.

Les matériels réseau (routeurs, agents SNMP, etc.) ainsi que les serveurs doivent disposer d'adresses fixes, car ils doivent être connus de tous. Ils peuvent faire appel à DHCP pour obtenir une adresse permanente que vous aurez préalablement réservée ou pour obtenir des paramètres de configuration IP.

LES OPTIONS DHCP (RFC 2132)

La RFC 2132 précise les principales options qui peuvent être affectées par un serveur DHCP. Parmi les plus importantes, on trouve (les numéros d'options sont indiqués entre parenthèses) :

- le masque de l'adresse IP (004) ;
- l'adresse IP des serveur DNS et le nom du domaine DNS dans lequel est situé la station (006 et 015) ;
- le nom de la station ;
- l'adresse IP des serveurs WINS et le type de nœud Netbios (044 et 046) ;
- des paramètres IP, TCP et ARP tels que le MTU (026), le TTL (023), la durée du cache ARP (035), etc. ;
- des routes statiques par défaut ainsi que l'adresse du routeur par défaut (033 et 003) ;
- les serveurs de messagerie SMTP et POP (069 et 070) ;
- divers serveurs par défaut tels que web (072), News (071), NTP (042), etc. ;
- des paramètres relatifs à DHCP (durée de validité de l'adresse, etc.) ;
- les types de messages DHCP (DISCOVER, REQUEST, RELEASE, etc.).

D'autres RFC peuvent décrire des options spécifiques (par exemple la RFC 2244 pour des paramètres Novell). La liste exhaustive des options officiellement reconnues est disponible sur http://www.iana.org.

Certains concentrateurs ou commutateurs peuvent télécharger leur système d'exploitation (un fichier exécutable appelé image de boot) ou un fichier de configuration en utilisant le sous-ensemble **BOOTP** également pris en charge par le serveur DHCP.

Avant de commencer, vous pourrez prendre en compte les recommandations suivantes :

- Installez au moins un serveur par site pour des questions de performance et de charge sur les liaisons WAN.
- Pour des questions de sécurité (surtout lorsque le nombre de PC est important), il est préférable de configurer deux serveurs par site, chacun gérant un pool d'adresses.
- La durée de validité des paramètres doit être limitée dans le temps dans le cas où les stations ne sont jamais éteintes (ce qui est le cas des serveurs, par exemple). Une durée de 12 ou 24 heures permet de couvrir une journée de travail et de diffuser de nouveaux paramètres assez rapidement. Pour les serveurs et équipements réseau, une durée plus longue peut être définie, mais l'application d'un nouveau paramètre prendra plus de temps. Vous pourrez de toute façon modifier la durée à tout moment.

Enfin, toutes les piles IP ne prennent pas l'ensemble des options possibles en charge. Il convient donc de vérifier que celle que vous utilisez accepte les options que vous voulez distribuer *via* DHCP.

Comment configurer un serveur DHCP ?

Pour installer le serveur sous Windows NT, il faut se rendre dans la configuration des services IP : " Démarrer→ Paramètres→ Panneau de Configuration→ Réseau→Services→Ajouter ".

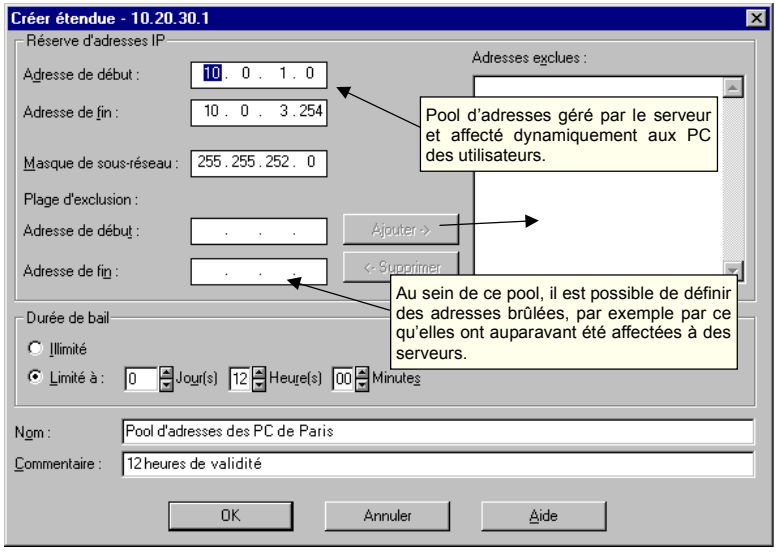
Pour configurer le serveur DHCP, cliquez sur " Démarrer→Programmes→Outils d'administration→ Gestionnaire DHCP ". Nous prenons l'exemple de Windows NT, mais le principe est le même sous Unix.

Définir les pools d'adresses

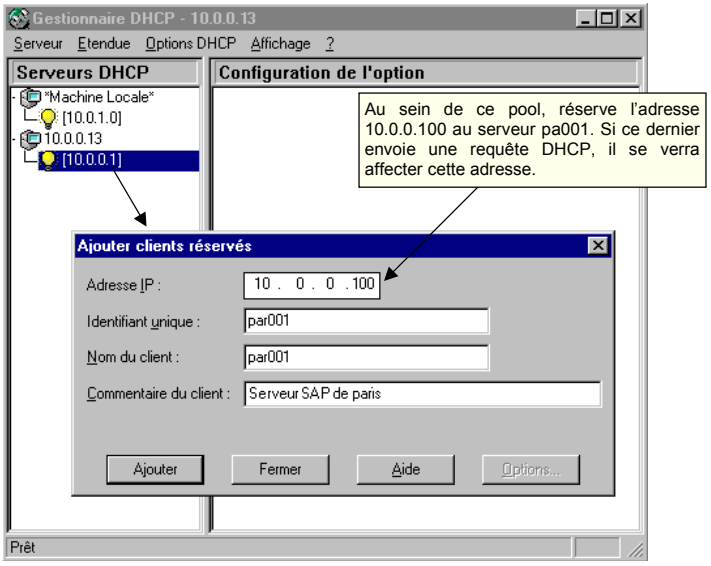
La première étape consiste à définir des pools d'adresses dans lesquels le serveur va piocher pour les affecter aux stations qui en feront la demande. Conformément à notre plan d'adressage, nous avons découpé notre espace d'adressage en trois parties.

Plage d'adresses	Affectation
De 0.1 à 0.64	Équipements réseau (routeurs, hubs, switches, etc.). Les adresses seront fixes, et seules les options seront distribuées (éventuellement des images de boot). Cela implique de référencer tous les équipements concernés (noms et adresses MAC notamment). Durée de validité des options = 1 semaine.
De 0.65 à 0.255	Serveurs NT, Unix, etc. Les adresses seront fixes, et seules les options seront distribuées. Les options peuvent être communes à tous les serveurs. Durée de validité des options = 1 semaine.
De 1.0 à 3.254	Postes de travail (PC, etc.). Adresses et options affectées dynamiquement. Durée de validité = 12 heures.

Rappelons qu'il est souvent souhaitable de limiter le découpage à deux tranches, une pour les équipements réseau et serveur, et une pour les postes de travail. Les deux premières parties peuvent donc être fusionnées.
À Paris, le serveur DHCP prendra ainsi en charge la plage d'adresses allant de 10.0.0.1 à 10.0.3.254, découpée en deux pools (appelés *scope* ou *étendue* chez Microsoft). Le *scope* dédié aux stations commencera à 10.0.1.0. En cas de saturation de la première tranche, il sera toujours possible de modifier la plage d'adresses affectée à ce *scope*.



La configuration du pool d'adresses pour les équipements réseau et les serveurs nécessite, en plus, de réserver les adresses *via* le menu " Etendue→Ajouter adresse réservée ". Avec les clients Windows, le seul moyen d'identifier les stations est d'utiliser l'adresse MAC de la carte réseau. La norme prévoit cependant que l'identifiant puisse être une chaîne de caractères quelconque, le nom de l'utilisateur ou du PC, par exemple.

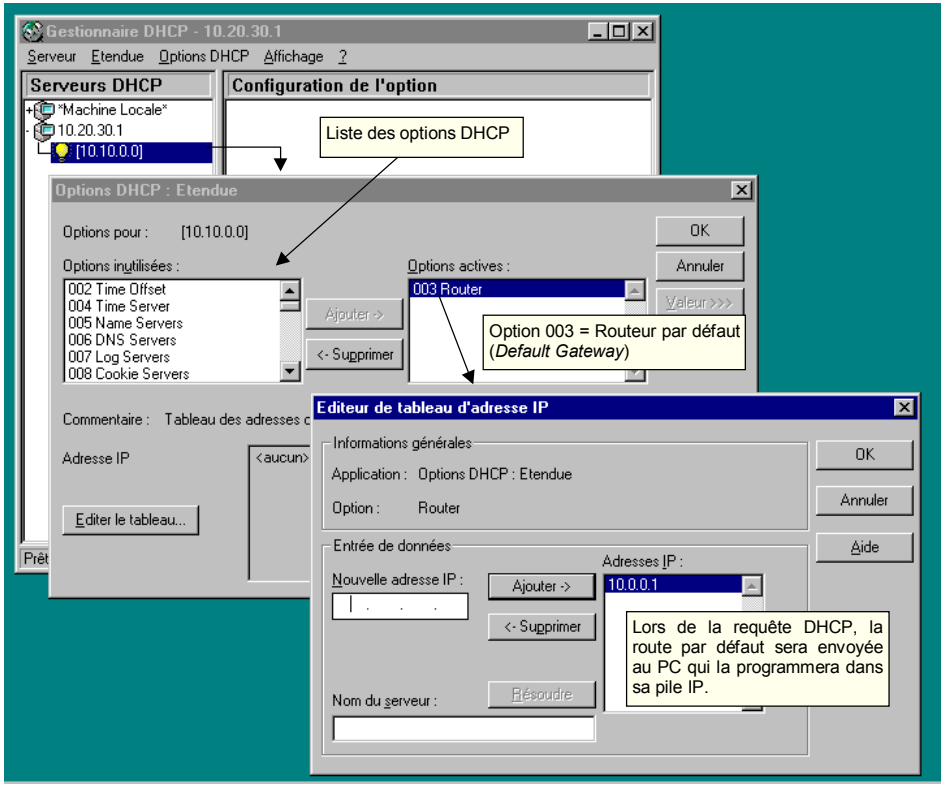


Cette opération peut être fastidieuse, car il faut relever les adresses MAC de tous les équipements concernés (qui sont cependant en nombre moins élevé que les PC). De plus, lorsqu'une carte réseau est changée, il faut mettre à jour la base de données DHCP (c'est une opération en principe peu fréquente, mais il faut y penser le jour où cela arrive).

Si vous ne voulez pas utiliser DHCP pour cette classe d'équipements, il suffit de ne pas ajouter de pool d'adresse. La plan d'adressage facilite votre choix.

Définir les options à distribuer

Les options peuvent être définies à trois niveaux : soit globalement pour tous les pools d'adresses, soit pour chaque pool (*scope*), soit encore individuellement pour chaque client.
Les options communes à tous les nœuds du réseau — par exemple le TTL par défaut ou l'adresse d'un serveur NTP servant de référence à la mise à l'heure des horloges — peuvent être définies globalement dans le menu " Option DHCP → Global ".



Si vous voulez affecter comme passerelle par défaut l'adresse IP de la station elle-même (voir chapitre 8), il faut ajouter et positionner à " 1 " la clé de registre suivante au niveau du pool " HKEY_local_machine\System\ CurrentControlSet\ Services\ DHCPServer\ Subnets\ a.b.c.d\ SwitchedNetworkFlag ", où a.b.c.d est l'adresse IP du pool.

LE POINT SUR DHCP (RFC 2131)

DHCP (*Dynamic Host Configuration Protocol*) permet à une station d'obtenir l'intégralité de ses paramètres IP (plus de 65 options recensées ˆ ce jour), ce qui épargne à l'administrateur de devoir configurer manuellement chaque poste de travail. DHCP est une extension du protocole **BOOTP** ; il utilise le même format de paquet.

8 bits	8 bits	8 bits	8 bits
1 = Requête 2 = Réponse	Type d'adresse physique (1=MAC Eth)	Longueur de l'adresse physique	Saut incrémenté de 1 par les routeurs
XID : numéro identifiant de manière unique la transaction. La réponse du serveur doit contenir le même XID que la demande du client			
Nombre de secondes depuis que le client a initialisé sa demande	B	Indicateurs (non utilisés) B = bit de Broadcast	
ciaddr - Adresse IP du client si celui-ci la connaît Il peut la connaître s'il demande une prolongation de l'affectation de l'adresse.			
yiaddr - Adresse IP affectée par le serveur			
siaddr - Dans son message DHCP_OFFERT, le serveur DHCP indique ici son adresse IP que le client devra indiquer en retour dans son message DHCP_REQUEST			
giaddr - Adresse IP du routeur ayant relayé le message DHCP. Si cette adresse est non nulle, le serveur sait que la requête a traversé au moins un routeur.			
chaddr - Adresse physique du client (16 octets) Dans le cas d'Ethernet, il s'agit de l'adresse MAC			
sname - Nom optionnel du serveur (64 octets maximum terminés par un 0)			
file - Nom optionnel du fichier à télécharger (128 octets maximum terminés par un 0)			
Options - Liste des paramètres supplémentaires affectés au client (les options son listées dans le RFC 2132) ainsi que le type de message DHCP (DISCOVER, REQUEST, etc.).			

Si la pile IP (et notamment le module ARP) peut fonctionner sans adresse IP, le **bit de broadcast** peut être mis à 0 dans les requêtes DHCP, ce qui permet au serveur de renvoyer ses réponses dans des trames unicast (à l'adresse MAC indiquée par le client dans le champ *chaddr*). Dans le cas contraire, le bit de broadcast est positionné à 1 par le client, et le serveur répond dans des trames de broadcast MAC (FF:FF:FF:FF:FF:FF).

Cependant, si le champ ***giaddr*** est non nul, cela veut dire que la requête a transité par un routeur. Le serveur envoie alors le paquet DHCP à cette adresse IP (et donc à l'adresse MAC du routeur *via* ARP). Le port UDP de destination est alors 67 (celui du serveur) — au lieu de 68 qui désigne le client —, ce qui permet au routeur d'identifier les paquets DHCP à traiter (voir plus loin).

Si le client possède déjà une adresse IP (champ *ciaddr* non nul), il peut demander des paramètres de configuration complémentaires (les **options DHCP**) en envoyant le message DHCP_INFORM. Le serveur envoie alors sa réponse à l'adresse IP indiquée (donc dans une trame MAC unicast).

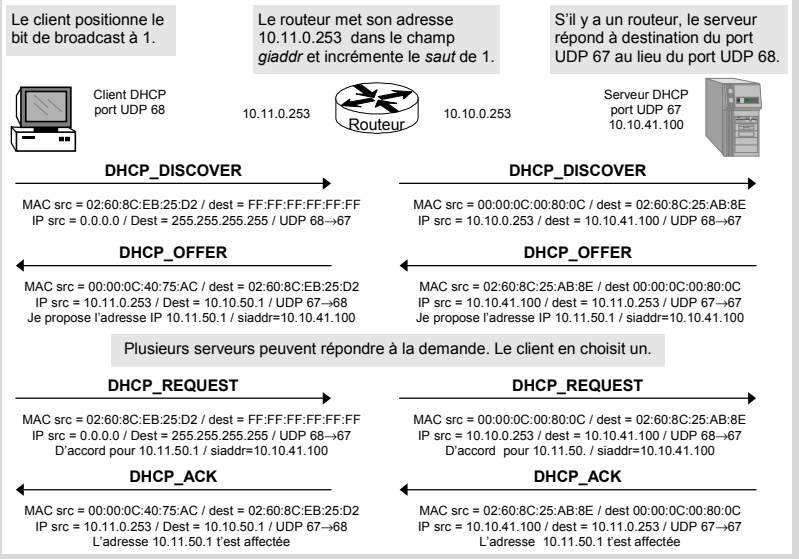
• • •

LE POINT SUR DHCP (SUITE)

Un client effectue sa requête en deux temps :

- Tout d'abord, il recherche un serveur DHCP, et attend les offres du ou des serveurs.
- Ensuite, il confirme sa demande auprès du serveur qu'il a choisi, et attend une réponse lui confirmant que l'adresse IP a bien été réservée.

Les options sont également négociées au cours de cet échange : le client indique celles déjà configurées dans sa pile IP, et les serveurs lui proposent les leurs.



Le client envoie toujours ses requêtes dans des trames de **broadcast MAC** pour plusieurs raisons :

- La requête initiale (DHCP_DISCOVER) permet de découvrir plusieurs serveurs (un serveur principal et un serveur de secours).
- Lors de la requête de confirmation (DHCP_REQUEST), la plupart des piles IP ne peuvent activer le module ARP sans adresse IP.
- Le client ne sait pas si le serveur est situé sur le même réseau ou s'il est séparé par un routeur. Dans ce dernier cas, si la trame est destinée à l'adresse MAC du serveur, elle ne traversera pas le routeur, sauf s'il fonctionne en mode proxy ARP (voir chapitre 8), ce que la station ne peut présupposer.

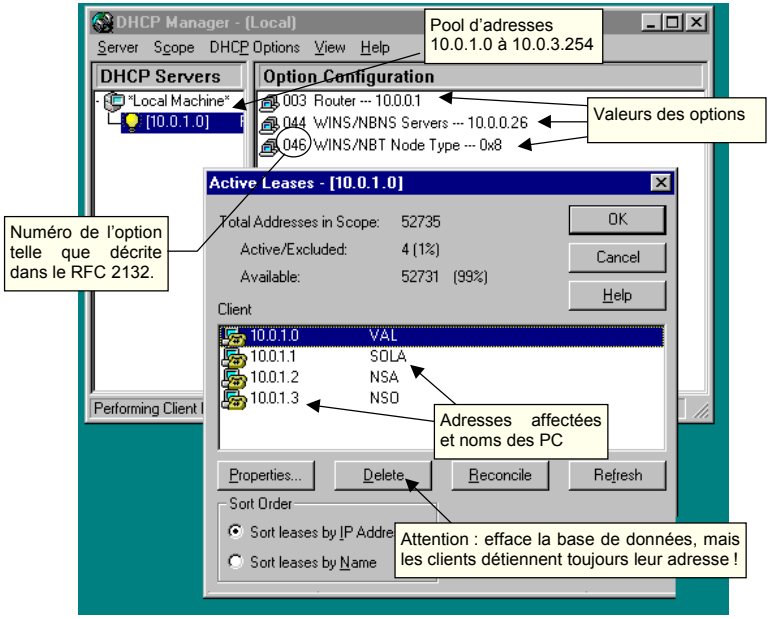
Configuré en relais DHCP/BOOTP, le routeur convertit les broadcast MAC/IP en adresses unicast à destination du serveur DHCP ou BOOTP.

À l'approche de l'expiration de la période de validité, le client demande à renouveler son bail auprès du serveur (DHCP_REQUEST) en indiquant son adresse IP dans le champ *ciaddr*. Le serveur peut alors proposer la même adresse, une nouvelle, ou encore accepter celle demandée par le client.

En principe, c'est au client qu'il incombe de vérifier que l'adresse allouée par le serveur n'est pas utilisée par une autre station (le serveur peut, en effet, être situé de l'autre côté d'un routeur). Le client génère à cet effet une requête ARP sur l'adresse qui vient de lui être allouée.

La même option peut être définie à plusieurs niveaux, mais les options individuelles ont priorité sur les options d'un pool, qui elles-mêmes ont priorité sur les options globales.

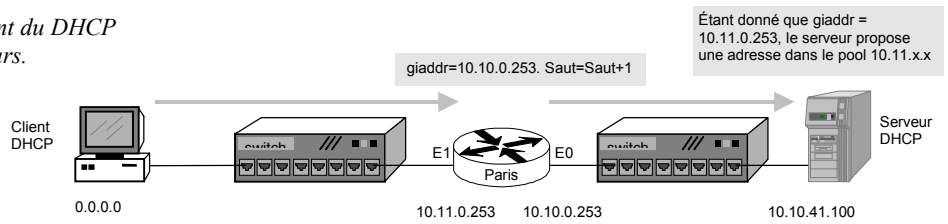
L'exemple suivant montre les options définies pour un pool, ainsi que les adresses déjà affectées à des clients.



Configurer les routeurs

Si les stations sont situées sur un réseau IP autre que le serveur DHCP, les requêtes DHCP doivent transiter par un routeur. Or, ce type d'équipement ne transmet jamais les trames de broadcast MAC, car il est justement conçu pour délimiter les domaines de broadcast (voir l'encart « Le point sur Ethernet » au chapitre 6). Il faut donc configurer explicitement les routeurs afin de pouvoir relayer les requêtes DHCP.

Figure 16-3.
Fonctionnement du DHCP avec les routeurs.



```
interface ethernet 1
ip helper-address 10.10.41.100
ip helper-address adresses ip d'autres serveurs DHCP
```

Avec la commande précédente, les trames de broadcast MAC dont le port UDP est égal à 67 seront transmises dans une trame unicast (*via* la résolution ARP) à destination du serveur DHCP ou BOOTP et, en retour, vers le client.

LE POINT SUR BOOTP (RFC 951 ET 1542)

BOOTP (*Bootstrap Protocol*) permet à un équipement réseau d'obtenir son adresse IP ainsi que le nom d'un fichier à télécharger *via* **TFTP** (*Trivial File Transfer Protocol*). Il peut s'agir d'un **fichier de configuration** ou d'un **exécutable** (appelé image de boot), tel qu'un système d'exploitation ou un micro-code. Ce protocole ne permet pas d'affecter dynamiquement les adresses, et nécessite donc de connaître les adresses MAC ou d'affecter un nom aux équipements qui émettent des requêtes.

DHCP a repris exactement les mêmes spécifications que BOOTP en étendant ses possibilités. Un serveur DHCP prend en charge les requêtes BOOTP (compatibilité ascendante), alors que l'inverse n'est pas possible.

Des équipements réseau qui ne disposent pas de mémoire flash, tels que des concentrateurs, des commutateurs ou des serveurs d'accès distants, utilisent BOOTP pour télécharger leur code exécutable.

Pour la petite histoire, la RFC 1542, relative aux extensions de BOOTP (l'équivalent des options DHCP), discute de l'utilité du bit de broadcast en rappelant le paradigme de la poule et de l'œuf : une station ne peut pas fonctionner sans adresse IP ; cependant, elle envoie et reçoit des paquets IP qui doivent justement lui permettre d'obtenir cette adresse IP ; mais elle ne peut pas traiter ces paquets puisqu'elle ne dispose pas d'adresse IP, etc.

Installer plusieurs serveurs

Si plusieurs serveurs sont utilisés (en partage de charge et en redondance), le pool d'adresses doit être découpé afin d'éviter les doubles affectations. La répartition peut se faire à parts égales, comme suit :

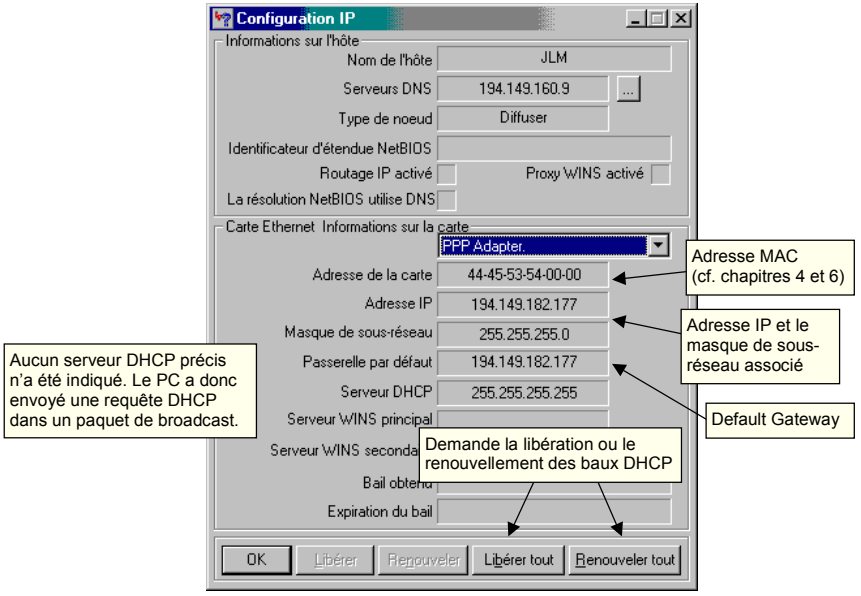
- le premier serveur affecte les adresses comprises entre 10.0.1.0 et 10.0.2.127 ;
- le second serveur affecte les adresses comprises entre 10.0.2.128 et 10.0.3.254.

Les adresses affectées de manière fixe doivent être réservées de manière identique sur chaque serveur.

Le serveur de Microsoft ne permet pas de mettre en place un réel partage de charge avec une redondance complète. Pour cela, d'autres serveurs DHCP plus perfectionnés existent sur le marché.

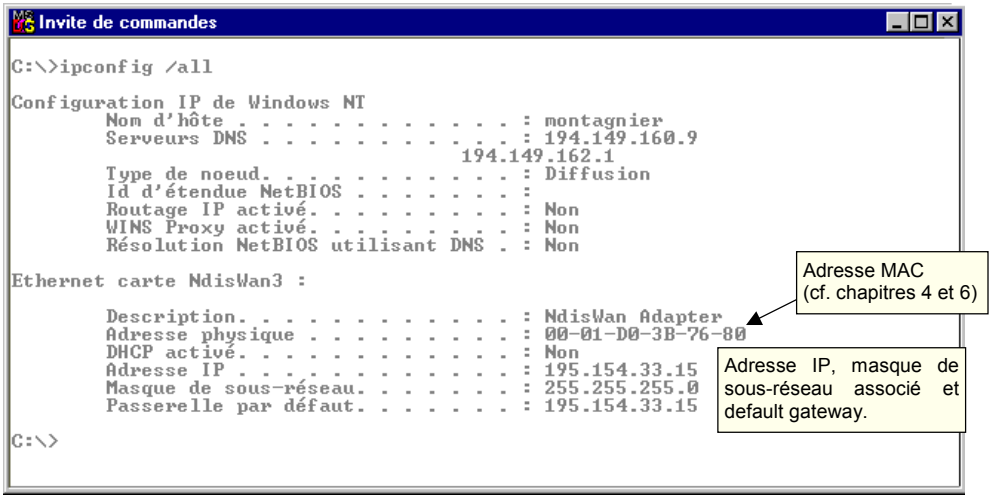
Vérifier la configuration de son PC

Plusieurs utilitaires permettent de vérifier le paramétrage TCP/IP de son PC. Sous Windows 9.x et Me, il s'agit de la commande **winipcfg**.

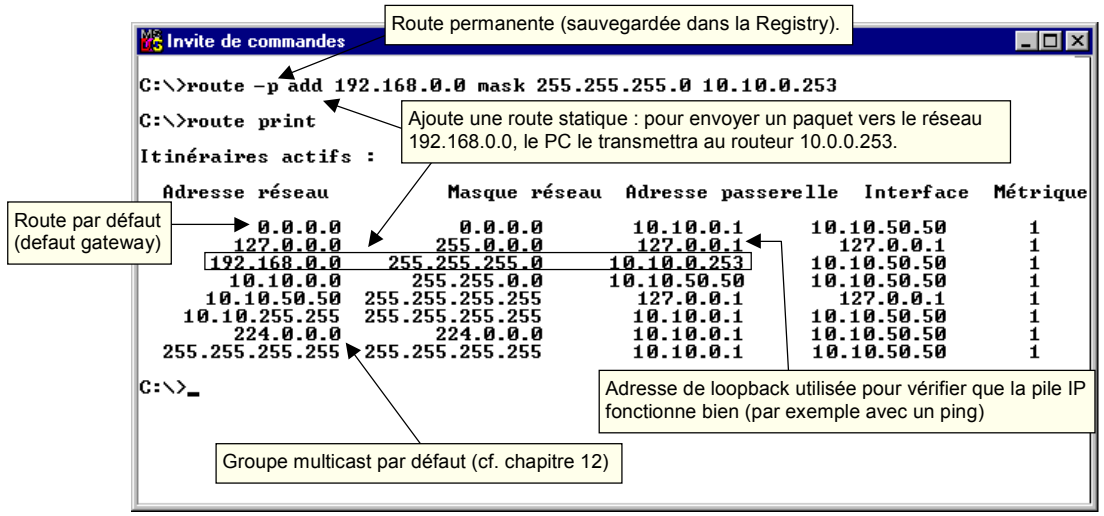


Sous Windows NT, la commande équivalente est **ipconfig** :

- **ipconfig /all** affiche tous les paramètres réseau.
- **ipconfig /release** envoie un message DHCP_RELEASE au serveur pour libérer l'adresse IP.
- **ipconfig /renew** envoie un DHCP_REQUEST pour demander le prolongement de la validité de l'adresse IP, ou un DHCP_DISCOVER si la station ne possède pas d'adresse.



Sous les deux environnements, la commande **route** permet de visualiser la table de routage de la pile IP.



Enfin, la commande **Netstat** permet de vérifier le bon fonctionnement de la couche TCP/IP. Elle permet, par exemple, de visualiser les connexions actives.