Examen 70-059

Interconnexion en environnements hétérogènes avec Microsoft TCP/IP

ESSENTIEL

Ecole Supérieure d'Informatique de Paris

23, rue de Château Landon
75.010 – Paris -France
http://www.supinfo.com
http://www.laboratoire-microsoft.org

Caractéristiques

Statut	Interne ? Document de travail ☑ Livrable contractuel ?
Réf. Fichier	PC Word97 : G:\Examen 70-059-Essentie1.1l.doc

Mise à jour

Ver	Modification
0.9	version initiale
1.0	Détail DNS, Détail SNMP, Interaction DNS / WINS, précisions diverses.

Liste de diffusion

Organisme	Nom des destinataires	Nombre	Objet de la diffusion
ESI SUPINFO	LABORATOIRE MICROSOFT	1	Pour validation

Niveau de diffusion : Laboratoire
Confidentialité : Confidentiel Laboratoire

Historique du document

Version	Créé le	Par	Vérifié par	Livré le
0.9	12/06/2000	Ali NEDJIMI, JOHANN COLLOT	F. VAN BOXSOM	06/2000
1.0	15/10/2000	Ali NEDJIMI	B.NEDJIMI	10/2000

Préliminaire :

Ce document est une synthèse des notions nécessaires à l'examen Microsoft 70-059.

Chaque chapitre contient une section intitulée "2 questions d'examen" qui sont volontairement en anglais, y compris les réponses.

1.TCP/IP : NOTIONS DE BASE

1.1. Modèle O.S.I. de l'I.S.O

Ce modèle est la première étape vers une normalisation internationale des différents protocoles, il est appelé modèle de référence OSI (Open Systems Interconnection).Ce modèle est divisé en 7 couches bien distinctes :

La couche physique: La couche physique s'occupe de la transmission des bits de façon brute sur un circuit de communication.
La couche liaison de données : Sa fonction principale est de transformer un moyen de transmission en ligne qui parait exempte d'erreurs de transmission à la couche réseau.
La couche réseau : Elle est chargée de transporter les paquets de la source vers la destination tout au long du chemin. Pour atteindre la destination il peut être nécessaire d'effectuer de nombreux sauts de noeud intermédiaire en noeud intermédiaire.
La couche transport : La fonction de base de cette couche est d'accepter des données de la couche session, de les découper, le cas échéant, en unités plus petites, et de s'assurer que tous les morceaux arrivent correctement à destination.
La couche session : La couche session permet à des utilisateurs sur différentes machines d'établir des sessions entre eux. Une session a pour but le transport des données comme la couche transport, mais elle offre également des services avancés, utiles à certaines applications.
La couche présentation : La couche présentation s'occupe de la syntaxe et de la sémantique de l'information transmise.
La couche application : La couche application gère les programmes de l'utilisateur pour lesquels les ordinateurs ont été achetés. Ces programmes utilisent les services de la couche présentation pour leurs besoins de communication.

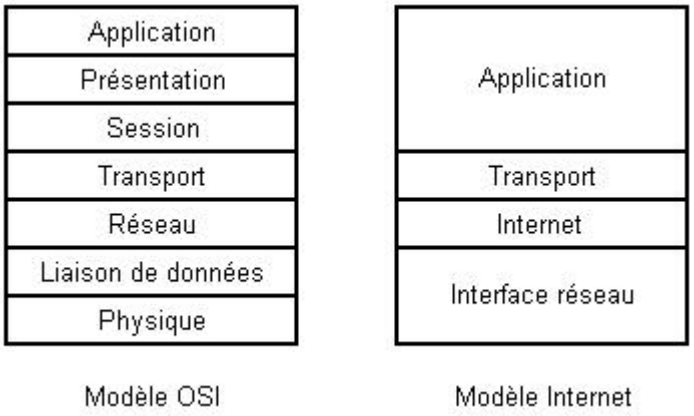
Vous pouvez retenir ce modèle en pensant à l'acronyme **A**LL **P**EOPLE **S**EEMS **T**O **N**EED **D**ATA **P**ROCESSING.

Microsoft adopte le modèle Internet, plus compact :

- **A**pplication
- **T**ransport
- **I**nternet
- **R**éseau

Vous pouvez retenir ce modèle en pensant à l'acronyme **RITA**

Chaque couche du modèle Internet correspond à une ou plusieurs couches du modèle OSI, comme illustré ci-dessous:



1.2. Le protocole TCP (Transmission Control Protocol)

Service de transport en mode connecté au-dessus d'une couche réseau non fiable en commutation par paquets.

Cinq caractéristiques du service TCP

Flot de données : Le récepteur reçoit exactement la séquence d'octets envoyée par le processus source.
Connexion préalable : Avant tout envoi de données, il y a un échange de messages afin de mettre en place la connexion.
Bufferisation : Les données envoyées et reçues sont bufferisées afin d'améliorer la communication.
Flot non structuré : Nécessité d'un format donné afin de comprendre les données.
Connexion Full-Duplex : Communication dans les deux sens. Information de contrôle + données

Format des segments TCP

0	4	10	16	24
Port source			Port destination	
Numéro de séquence				
Numéro d'acquittement				
Taille	Reservé	Code	*Window*	
Checksum			Pointeur urgent	
Options				Bourrage
Données				
...				

- **Numéro de séquence** spécifie le numéro de séquence du premier octet de données.
- **Numéro d'acquittement** spécifie le numéro de séquence du prochain octet attendu.
- **Taille** est la taille de l'entête du segment en nombre de mots de 32 bits.

- ***Window*** donne la taille de la fenêtre de réception. S'il y a perte d'un segment, il n'y a pas de moyen pour, éventuellement, acquitter les segments suivants.
- **Code** détermine le type du segment et son contenu.
- **Pointeur urgent** indique l'offset du caractère urgent dans **données** si le code URG est présent.
- **Options** permet, entre autre, de négocier la taille des segments envoyés, en fonction de la capacité mémoire de la machine réceptrice et éventuellement de la MTU des réseaux traversés.

Checksum est calculée comme pour UDP en ajoutant un pseudo en-tête.

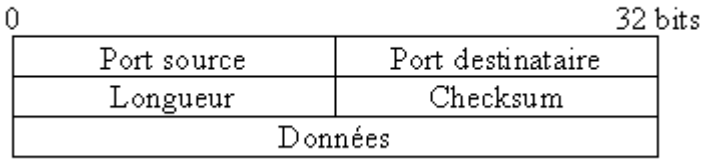
1.3. Le protocole UDP

Le protocole User Datagram Protocol (UDP) est défini dans le but de fournir une communication par paquet unique entre deux processus dans un environnement réseau étendu. Ce protocole suppose l'utilisation du protocole IP comme support de base à la communication.

Ce protocole définit une procédure permettant à une application d'envoyer un message court à une autre application, selon un mécanisme minimaliste. Ce protocole est transactionnel, et ne garantit ni la délivrance du message, ni son éventuelle duplication. Les applications nécessitant une transmission fiabilisée et ordonnée d'un flux de données implémenteront de préférence le protocole TCP (Transmission Control Protocol).

Format :

En-tête UDP



Champs

Le **Port Source** est un champ optionnel. Lorsqu'il est significatif, il indique le numéro de port du processus émetteur, et l'on supposera, en l'absence d'informations complémentaires, que toute réponse devra y être dirigée. S'il n'est pas utilisé, ce champ conservera une valeur 0.

Le **Port Destinataire** a une signification dans le cadre d'adresses Internet particulières.

La **Longueur** compte le nombre d'octets dans le datagramme entier y compris le présent en-tête. (Et par conséquent la longueur minimale mentionnée dans ce champ vaut huit, si le datagramme ne transporte aucune donnée).

Le **Checksum** se calcule en prenant le complément à un de la somme sur 16 bits des compléments à un calculé sur un pseudo en-tête constitué de l'information typique d'un en-tête IP, l'en-tête UDP lui-même, et les données, le tout additionné d'un octet nul éventuel afin que le nombre total d'octets soit pair.

1.4. Le protocole ICMP

Les messages ICMP sont envoyés dans diverses situations: par exemple, lorsqu'un datagramme ne peut pas atteindre sa destination, lorsque le routeur manque de réserve de mémoire pour retransmettre correctement le datagramme, ou lorsque le routeur décide de viser l'hôte destinataire via une route alternative pour optimiser le trafic.

Le protocole Internet n'est pas, dans sa définition, absolument fiable. Le but de ces messages de contrôle est de pouvoir signaler l'apparition d'un cas d'erreur dans l'environnement IP, pas de rendre IP fiable. Aucune garantie que le datagramme soit acheminé ni qu'un message de contrôle soit retourné, ne peut être donnée. Certains datagrammes pourront se perdre dans le réseau sans qu'aucun message de contrôle ne le signale. Les protocoles de niveau supérieur s'appuyant sur une couche IP devront implémenter leurs propres mécanismes de contrôle d'erreur et de retransmission si leur objet nécessite un circuit de communication sécurisé.

Les messages ICMP reportent principalement des erreurs concernant le traitement d'un datagramme dans un module IP.

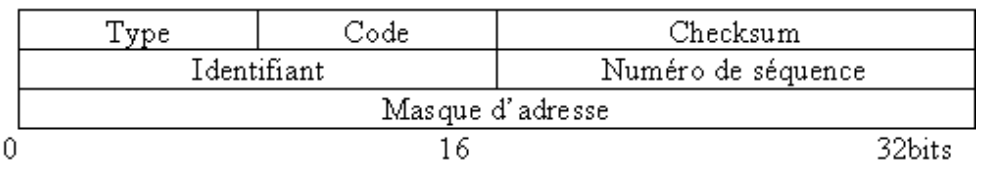
Formats de message :

Les messages ICMP sont émis en utilisant l'en-tête IP de base. Le premier octet de la section de données du datagramme est le champ de type ICMP; Sa valeur détermine le format du reste des données dans le datagramme ICMP.

Résumé des types de Message (champ Type)

0 Réponse Echo
3 Destination non accessible
4 Contrôle de flux
5 Redirection
8 Echo
11 Durée de vie écoulée
12 Erreur de Paramètre
13 Marqueur temporel
14 Réponse à marqueur temporel
15 Demande d'information
16 Réponse à demande d'information

En-tête ICMP



1.5. Fenêtres variables (sliding windows)

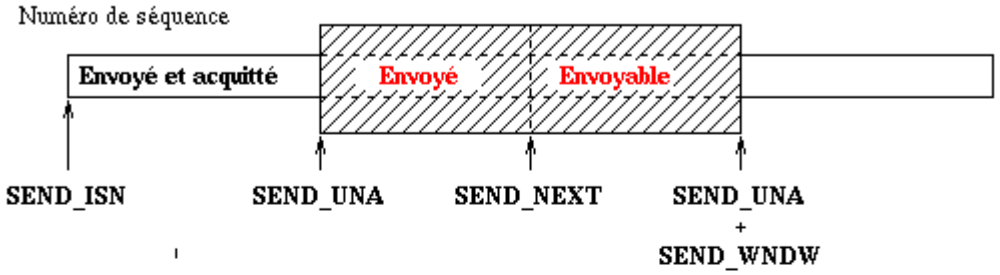
TCP utilise le concept de fenêtres variables pour le transfert des données entre machines. Chaque machine dispose d'une fenêtre d'émission et d'une fenêtre de réception qu'elle utilise comme tampon de données pour rendre la communication qu'elle utilise plus efficace.

Cette technique permet d'acquitter plusieurs paquets en même temps.

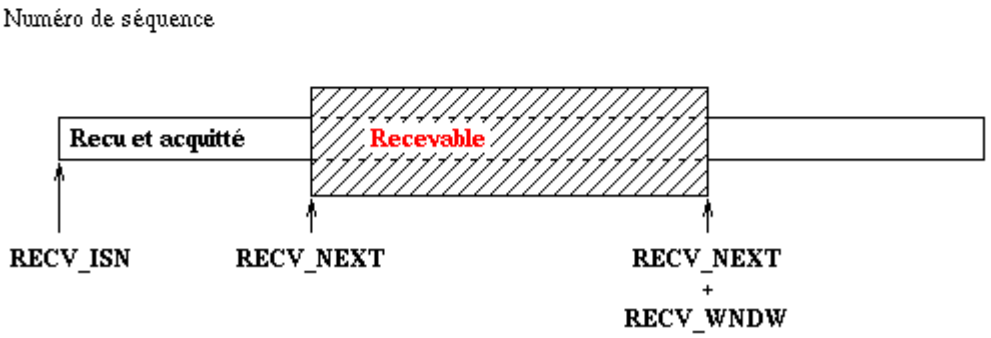
Cette technique nécessite :

- Numéro de séquence : un numéro initial choisi au hasard
- Fenêtre de réception : taille mise à jour à chaque acquittement. Contrôle du flot de données.
- Fenêtre d'émission : taille de la fenêtre de réception. Elle commence au premier envoi non acquitté.

Emission



Réception



L'acquittement d'un paquet allant de A vers B peut être véhiculé par un paquet allant de B vers A. Cette technique est appelée *piggybacking*.

2.Adressage IP

Une adresse IP est un nombre binaire de 32 bits (4 octets) présenté dans le format decimal 10.10.10.10.
La classe du réseau est déterminée par les bits de plus haut rang :

Classe	Préfixe	Numéro de réseau	Numéro d'hôte
A	000.000. 000.000	bits 1-7	bits 8-31
B	100.000. 000.000	bits 2-15	bits 16-31
C	110.000. 000.000	bits 3-24	bits 25-31
D	111.000. 000.000	Multicast	Multicast
E	111.100. 000.000	Réservé	Réservé

Les plages d'adresses pour les différentes classes peuvent être déduites :

Classe	Plage de numéros de réseau	Plage de numéros d'hôte
A	0 à 126	0.0.1 à 255.255.254
B	128.0 à 191.255	0.1 à 255.254
C	192.0.0 à 223.255.255	1 à 254

Une adresse IP fait 32 bits de long et est composée de deux parties: le **numéro de réseau** (l'ID de réseau), et le **numéro d'hôte** (l'ID d'hôte). Par convention, il est exprimé en quatre nombres décimaux séparés par des points, comme par exemple "200.1.2.3". Une adresse valide est dans la plage allant de 0.0.0.0 à 255.255.255.255, soit un total de 4.3 milliards d'adresses.

L'ID réseau 127.x.y.z est une adresse réservée au bouclage local (*loopback*) et à l'auto-diagnostic.
Un ID de réseau ou un ID d'hôte ne peut contenir que des 1 (255).
Si tous les bits sont mis à 1, alors cela est interprété comme une diffusion générale (*broadcast*).
Les adresses dont les bits de haut rang sont à 1110 (224.0.0.0 à 239.255.255.255) en classe D sont utilisées pour le *Multicasting*, ceux à 11110 (240.0.0.0 à 247.255.255.255) en classe E sont réservés pour un usage futur. Tous les bits réservés et adresses réservées réduisent sévèrement le nombre d'adresses IP disponibles (4,3 milliards). La plupart des utilisateurs reliés à l'Internet se verront assignés des adresses de classe C, puisque l'espace devient très limité. C'est la raison principale du développement d'IPv6, qui aura 128 bits d'espace adresse.

2.1. Définir un sous-réseau

Le *subnetting* est une technique qui permet à l'administrateur de diviser un réseau en entités plus petites.

En fait, pour déterminer dans une adresse IP la partie numéro de réseau et celle correspondant au numéro d'hôte, il suffit d'écrire l'adresse IP en binaire et en dessous, le masque de sous-réseau, également en binaire.

Avec un masque de sous-réseau **255.255.255.0**.

On obtient, en binaire :

11000000.10101000.00000010.**00110101** (192.168.2.53)
11111111.11111111.11111111.**00000000** (255.255.255.0)

La partie composée de 1 du masque de sous-réseau correspond au numéro de réseau et celle composée de 0 au numéro d'hôte. Ainsi, dans ce cas, avec un masque de 255.255.255.0, on peut avoir 254 hôtes différents sur le sous-réseau 192.168.2.0.

Soit l'adresse IP **192.168.2.53**

Essayons maintenant avec un masque de sous-réseau **255.255.255.224**.

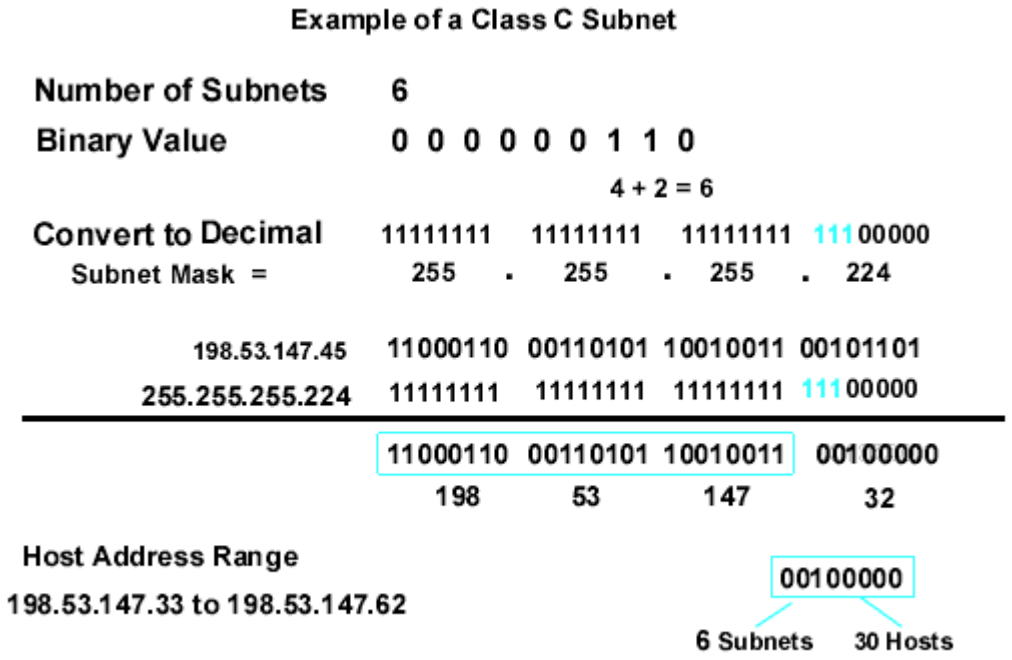
On obtient, en binaire :

11000000.10101000.00000010.001**10101** (192.168.2.53)
11111111.11111111.11111111.111**00000** (255.255.255.224)

La partie numéro de réseau devient donc 192.168.2.32 et le numéro d'hôte est 21. Ainsi, avec le masque 255.255.255.224, on peut diviser le réseau 192.168.2.0 en 8 sous-réseaux différents. Les numéros d'hôte dans ce cas ne peuvent aller que de 1 à 31, la machine d'adresse IP 192.168.2.65 ne fera donc pas partie du même réseau.

2.2. Comment calculer le masque de sous-réseau ?

1.Déterminer le nombre de segments requis dans le réseau et le convertir en binaire.
2.Compter le nombre de bits requis pour représenter le nombre de segments en binaire.
3.Convertir le nombre requis de bits en décimal, au niveau des bits de poids fort(gauche à droite).



Bits	Bits du masque	Subnets	Masque	Hôtes par sr Classe A	Hôtes par sr Classe B	Hôtes par sr Classe C
11000000	2	2	192	4,194,301	16,382	62
11100000	3	6	224	2,097,150	8190	30
11110000	4	14	240	1,048,574	4,094	14
11111000	5	30	248	524,286	2,046	6
11111100	6	62	252	262,142	1,022	2
11111110	7	126	254	131,070	510	0
11111111	8	254	255	65,534	254	0

2.3. Adressage privé

Les adresses IP suivantes ne sont pas routables sur Internet.

Classe A: 10.x.y.z
Classe B: 172.16.x.y - 172.32.x.y
Classe C: 192.168.x.y

2.4. Exercice corrigé :

L'adresse réseau qui vous a été attribuée est 149.3.0.0. Vous voulez mettre en place un réseau de 46 sous-réseaux, et vous n'espérez pas disposer de plus de 1 000 hôtes par sous-réseau.

1) Convertissez en binaire le nombre de sous-réseaux requis plus 1.
   L'équivalent binaire du nombre décimal 47 est 101111.

2) Notez le nombre de bits nécessaires à l'expression de ce nombre en binaire.
   Il faut 6 bits.

3) Ecrivez un nombre binaire de 8 bits, qui contienne des 1 dans les chiffres les plus significatifs et des 0 dans les chiffres les moins significatifs. Le nombre de 1 correspond à la valeur trouvée à l'étape 5 et le nombre de 0 permet d'en faire un nombre à 8 bits.
   Le masque de sous-réseau de cet octet est 11111100

4) Convertissez le nombre en décimal.
   L'équivalent décimal de 11111100 est 252

5) Avec ce résultat définissez la masque de sous réseau personnalisé pour ce réseau.
   Le masque de sous-réseau résultant pour un réseau de classe B est 255.255.252.0.

6) Pour determiner le nombre d'hôtes par sous réseau, elevez 2 à la puissance du nombre de bits restants pour les ID d'hôtes et ôtez 2 pour déterminer le nombre total d'hôtes par sous-réseau permis par ce masque de sous-réseau .

   11111111.11111111.111111**00**.00000000 soit 10 bits restants.

   Le nombre d'hôte par sous-réseau est donc 1022 (2^10 – 2).

2.5. 2 QUESTIONS D'EXAMEN

Claudette's company has been assigned the network address 145.3.0.0. Currently, she oversees 50 subnets on her network, which will grow to 56 subnets over the next year. Subnets on the network will require up to 800 hosts each. Which subnet mask should Claudette assign to the network?
a. 255.255.192.0.
b. 255.255.224.0.
c. 255.255.252.0.
d. 255.255.254.0.

Réponse: c
In order to determine which subnet mask to apply, you must first determine the class of the IP address. In binary, the leftmost octet (the w octet) of a class A address must begin with 0. This creates the address range 00000001 through 01111110. No address can be all zeros or ones. In decimal, this range translates to 1 through 126, i.e., 1.x.y.z through 126.x.y.z. A class B address must begin with 10, filling the range 10000000 through 10111111 (128.x.y.z through 191.x.y.z). A class C address must begin with 110, leaving the range 11000000 through 11011111 (192.x.y.z through 223.x.y.z). Therefore, the network address

145.3.0.0 is a class B address. The network address class determines which octets are used to define the number of subnets created.

Mrs. Spectra is troubleshooting a Windows NT Server computer on a TCP/IP network. The server is on a subnet with the network ID 139.168.0.0. The default gateway address is 139.168.2.1. Users on a remote subnet cannot access the server. Mrs. Spectra runs the command IPCONFIG /ALL on the server and receives the following output:

Windows NT IP Configuration:
Host Name. . . . . : MYCOMP
DNS Servers. . . . . :
Node Type. . . . . : hybrid
NetBIOS Scope ID . . . . . :
IP Routing Enabled . . . . . : No
WINS Proxy Enable. . . . . : No
NetBIOS Resolution Uses DNS. . . . : No
Ethernet Adapter . . . . . : ELNK31
Description. . . . . : ELNK3 Ethernet adapter
Physical Address . . . . . : 00-AA-00-51-29-45
DHCP Enabled . . . . . : No
IP Address . . . . . : 139.168.2.223
Subnet Mask. . . . . : 255.255.240.0
Default Gateway. . . . . : 139.168.2.1
Primary WINS Server. . . . . : 139.168.2.46

What is the most likely cause of the server's problem?
a. DHCP is not enabled.
b. The NetBIOS scope ID is incorrect.
c. The primary WINS server is incorrect.
d. The subnet mask is incorrect.

Réponse: d
A network ID beginning with 139 indicates a class B IP address. For a class B address, the default subnet mask 255.255.0.0 indicates that the network is not configured for subnetting. Subnet masking always begins in the first (leftmost) host octet. For a class A address, the subnet mask will begin in the second octet; for a class B address, in the third octet; for a class C address, in the fourth octet. Therefore, to subnet a class B address would require the subnet mask 255.255.192.0 to create two subnets, 255.255.224.0 to create six subnets, 255.255.240.0 to create 14 subnets, 255.255.248.0 to create 30 subnets, 255.255.252.0 to create 62 subnets, 255.255.254.0 to create 126 subnets, 255.255.255.0 to create 254 subnets, and so on. When applying subnets, it is important to remember that each subnet mask subtracts the first block and last block of subnets it creates.
In other words, the subnet mask 192 creates four blocks of 64 within the first host octet: 1 through 63, 64 through 127, 128 through 191, and 192 through 255. However, only the blocks 64 through 127 and 128 through 191 contain legal addresses. The blocks 1 through 63 and 192 through 255 are illegal. For this reason, we can surmise that in the above case the correct subnet mask for the class B subnet 139.168.0.0 must be either 255.255.254.0 or 255.255.255.0. Otherwise, the IP addresses 139.168.2.x listed by IPCONFIG /ALL would be illegal.

3.Utilitaires en ligne de commande.

Arp

Arp.exe est utilisé pour résoudre une adresse IP en adresse matérielle (MAC).Le cache local arp est vérifié en premier avant de lancer un broadcast ARP.

-a : voir le contenu de cache arp local
-g : idem que -a (son utilité est incertaine)
-s : ajouter une entrée Arp statique
-d : supprimer une entrée

Ipconfig

Il est disponible sous Windows NT (et Win98) . Il montre la configuration de la pile IP de l'ordinateur.

C:\ipconfig ✍

```
Configuration IP Windows NT:

Ethernet adapter 3C589XL:

IP Address ...................:192.168.100.10
Subnet Mask ..................:255.255.255.0
Default Gateway...............:198.168.100.1
```

/all : Affiche des informations supplémentaires, nom d'hôte, DNS et WINS.
/release : Si DHCP est activé, l'on abandonne le bail avec ce switch
/renew : Renouvellement du bail si DHCP est activé.

Netstat

Il affiche les statistiques des protocoles et l'état des **connexions TCP/IP**.
Affiche les statistiques du protocole et les connexions réseau TCP/IP en cours.

C:\netstat ✍

```
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalle]

 -a         Affiche toutes les connexions et les ports en écoute.
 -e         Affiche les statistiques Ethernet. Cette option peut être
            combiné avec l'option -s.
 -n         Affiche les adresses et numéros de port en format numérique.
 -p proto   Affiche les connexions du protocole spécifié par proto ; proto
            peut être TCP ou UDP. Utilisé avec l'option -s pour afficher
            les statistiques par protocole, proto peut être TCP, UDP ou IP.
 -r         Affiche la table de routage.
 -S         Affiche les statistiques par protocole. Par défaut, les
            statistiques sont affichées pour TCP, UDP et IP ; l'option -p
            peut être utilisée pour spécifier un seul de ces protocoles.
```

Nbtstat

Affiche les statistiques du protocole et l'état des connexions TCP/IP utilisant **NBT(NetBIOS sur TCP/IP).**

```
C:\nbtstat ✍

NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-s] [S] [interval] ]

-a : adapter status  : affiche les entrées d'une machine distante (via son nom)
-A : Adapter status  : affiche les entrées d'une machine distante (via son @ IP)
-c : cache : affiche le cache en incluant les adresses IP
-n : names : affiche les noms NetBIOS locaux
-r : resolved : affiche des statistiques de résolution via diffusion et WINS
-R : purge et recharge le cache des noms NetBIOS
-S : liste des sessions actives avec les @ IP destination
-s : liste les sessions en convertissant les @IP destination en noms d'hôtes.
```

✍ **Remarque : Netstat fonctionne pour les connexions TCP/IP, et Nbtstat pour les connexions NETBIOS.**

Connectivité

nslookup	Il permet de tracer les requêtes DNS du début à la fin. En cas de doute concernant une résolution DNS, il faut utiliser nslookup.
Ping	Ping permet de faire des tests de configuration et de connectivité.
Tracert	Montre la route qu'un paquet va prendre d'un réseau à un autre.
Winipcfg	La version graphique de ipconfig pour Windows 95/98.

3.1. QUESTIONS D'EXAMEN

Henrietta administers a small Windows-based network that uses LMHOSTS files for computer name resolution. A user complains that he cannot connect to a remote server using Windows NT Explorer. She examines the user's LMHOSTS file and discovers that the remote server's IP address has been entered incorrectly. After correcting the entry, what should Henrietta do?

a. rename the LMHOSTS file
b. run nbtstat -r
c. run nbtstat -R
d. run netstat -r
e. run netstat -R

Réponse: c

After correcting an LMHOSTS file, it is necessary to purge the computer of its cached NetBIOS names. The nbtstat -R command then reloads the name cache, including all of the LMHOSTS file's #PRE entries. The nbtstat -r command lists the name resolution statistics for Windows networking. The netstat -r command displays the routing table's contents.

Which commands can you use to see the routing tables of a Windows NT Server computer?
a. arp
b. nbtstat
c. netstat
d. route

Réponse: cd
Either the NETSTAT -r command or the ROUTE PRINT command will display the routing table of a Windows NT computer. Both commands display the network address, the netmask, the gateway address, the interface and the metric. In addition, the NETSTAT -r command will also display the protocol, the local address, the foreign address and the state of active connections.

4.Routage

✍Multihoming (multirésident) : Un ordinateur multirésident (multihomed) contient au moins deux cartes d'interface connectées à au moins deux sous-réseaux. [il "réside" sur plus d'un sous-réseau].

✍Un routeur fonctionne au niveau de la couche réseau.

✍La couche IP utilise une table de routage pour savoir où envoyer les paquets.

Il existe deux types de routage : statique et dynamique

✍Une passerelle (gateway) est une machine où sont envoyés les paquets qui ne sont pas concernés par une route particulière. La passerelle est censée connaître les chemins qui mènent à la destination souhaitée.

✍ Lors de la configuration via DHCP, si une passerelle est spécifiée, elle outrepasse le paramètrage automatique. Tous les paramètres sont écrasés **sauf** la passerelle.

4.1. Routage Statique

Un routeur statique n'échange pas d'informations de routage avec les autres routeurs, il utilise seulement une table de routage prédéfinie.

L'utilitaire Route : il permet de configurer les routes statiques .

Route add *[network]* mask *[netmask] [gateway]*	Ajoute une route.
Route -p add *[network]* mask *[netmask] [gateway]*	Ajoute une route persisente.
Route delete *[network] [gateway]*	Supprime une route.
Route change *[network] [gateway]*	Modifie une route.
Route print	Affiche les tables de routage.
Route -f	Efface toutes les routes.

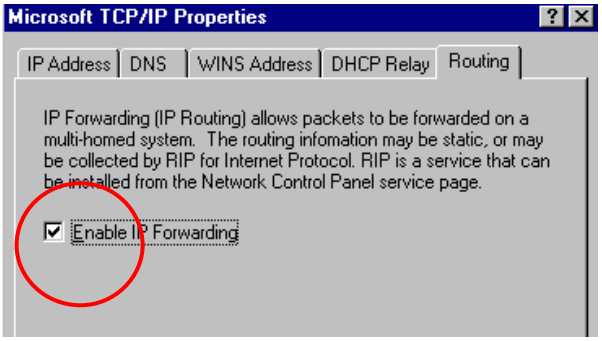
✍ *Exemple :*

Je suis en 205.16.9.10 et pour atteindre le sous-réseau 208.23.25.0 je dois utiliser la passerelle 205.16.9.1 :

```
Route -p -add 208.23.25.0 mask 255.255.255.0 205.16.9.1
```

Comment utiliser NT comme routeur ?

1.Installer au moins deux cartes réseaux et les connecter physiquement au réseau distant.
2.Donner une adresse IP valide à chaque carte.
3.Activer le routage IP (*IP Forwarding*) dans l'onglet Routage



4.2. Routage Dynamique

Les routeurs peuvent découvrir les informations des autres réseaux automatiquement s'ils utilisent un protocole de routage dynamique comme Routing Internet Protocol (RIP) ou Open Shortest Path First (OSPF) .

Windows NT ne supporte que le routage RIP en tant que routage dynamique.

4.2.1. RIP

Tous les messages RIP sont envoyés à travers le port UDP 520.
Les routeurs RIP s'échangent les Network ID's des réseaux qu'ils peuvent atteindre.
RIP utilise un champ compteur de saut, ou métrique, dans sa table de routage pour déterminer la distance vers un ID de réseau.
Le nombre de saut maximum est de 15 pour RIP. Les réseaux avec des sauts de 16 ou plus sont considérés inaccessibles. Si des entrées multiples vers un hôte sont saisies dans la table de routage, un routeur RIP va toujours utiliser la route avec le moins de sauts comme route par défaut.

Inconvénients

✍RIP est un protocole de routage à vecteur de distance donc chaque routeur contient une table du réseau et des routes pour tous les hôtes connus. Les tables de routage peuvent devenir importantes. La taille maximale d'un paquet RIP est de 512 octets, donc les tables de routages importantes doivent être envoyées en paquets multiples, ceci peut représenter une masse importante de traffic réseau.

✍Les routeurs RIP annoncent le contenu de leurs tables toutes les 30 secondes via un broadcast de niveau MAC sur tous les réseaux attachés.

✍Le problème du routage par vecteur de distance est la convergence lente.
Lorsqu'un changement est fait, il doit être propagé à chaque routeur.Cette propagation impose à chaque table de routage concernée d'être recalculée.
Ainsi, lorsqu'un routeur ne fonctionne plus , il peut se passer plusieurs minutes avant que l'information (routeur HS) ne se soit propagée à travers tout le réseau.

4.2.2. ROUTEUR SILENT RIP

Il reçoit toutes les broadcast des autres routeurs RIP. Cependant, il n'effectue pas de diffusion.
Son utilité est de permettre de voir les réseaux que les autres routeurs ont découvert.

4.3. 2 QUESTIONS D'EXAMEN

Noriko has five multihomed Windows NT Server computers functioning as routers on her network. She wants to configure the routing tables on these servers with the least amount of administrative effort possible. How should Noriko proceed?

a. by installing DHCP Relay Agent
b. by installing RIP for IP
c. by running netstat.exe
d. by running route.exe

Réponse: b
The Multi-Protocol Router (MPR) for Windows NT 4.0 contains the Routing Information Protocol (RIP) for TCP/IP, RIP for IPX and the Boot Protocol (BOOTP) Relay Agent for DHCP. Once installed, you only need to enable IP Routing on the Advanced TCP/IP tab. Typing ROUTE PRINT at the command prompt displays the current routing table. You stop and start the RIP for IP service using Control Panel.

Henrietta has been tasked with setting up a small network with three subnets as shown in the Exhibit. (Imaginer le schéma ...) She plans to connect the subnets with two multihomed gateways. The subnet mask on the network is 255.255.255.0.
Which routing entries should Sue make to ensure that every host on the network can communicate with every other host on the network?
a. on Router1: ROUTE ADD 173.52.100.0 MASK 255.255.255.0 173.52.75.1
b. on Router2: ROUTE ADD 173.52.45.0 MASK 255.255.255.0 173.52.75.1
c. on Router1: ROUTE ADD 173.52.100.0 MASK 255.255.255.0 173.52.75.2
d. on Router2: ROUTE ADD 173.52.45.0 MASK 255.255.255.0 173.52.75.2

Réponse: bc

The syntax for ROUTE ADD is ROUTE ADD [destination net ID] MASK [netmask] [gateway address]. Even though the subnet mask is the same for the entire network, it must be added whenever subnet masking is used. Both correct choices list the network ID of the remote subnet that the local subnet needs to reach, the mask (if necessary), and the gateway address to the remote subnet. This gateway address is always the near side of a router that can either forward IP diagrams to the destination subnet by itself or knows how to reach it via other routers.

5. DHCP

✍ Dynamic Host Configuration Protocol (DHCP) est utilisé pour assigner automatiquement des paramètres TCP/IP aux clients.

✍Les adresses IP viennent d'un pool défini dans la base de données du serveur DHCP et qui se nomme une Etendue (**Scope)**.

✍Le serveur attribue l'adresse IP pour une période de temps appelée un Bail (**Lease)**.

✍Il faut configurer le client pour qu'il ne soit pas en IP fixe mais en DHCP :

5.1. Processus de Configuration DHCP : 4 phases

1.Demande de bail : **REQUEST**

Le client initialise une pile IP limitée et a été configuré pour recevoir automatiquement une adresse IP à partir d'un serveur DHCP sur le réseau.
Le client demande ce bail via un broadcast.L'adresse IP du serveur DHCP lui est inconnue et le client n'a pas encore recu d'IP , il utilises donc 0.0.0.0 comme adresse source et 255.255.255.255 comme adresse destination.
Cette requête est envoyée en tant que message **DHCPDISCOVER**, qui contient l'adresse MAC du client et le nom d'ordinateur.

2.Offre de bail : **OFFER**

Le serveur DHCP envoit un message de broadcast au client sous la forme d'un message **DHCPOFFER.** Le client prendra le premier bail qu'il reçoit, s'il y'a plusieurs DHCP sur le réseau, les autres sont ignorés.

3.Choix du bail : **SELECTION**

Après que le client ait reçu une offre, il broadcast à tous les serveurs DHCP qu'il a accepté un bail. Le broadcast se fait sous la forme d'un message **DHCPREQUEST** et inclut l'identifiant du serveur (son adresse IP) dont l'offre a été acceptée. Tous les autres serveurs DHCP retirent leur offre.

4.Acquitement : **ACK**

Le serveur DHCP broadcast un ACK au client sous la forme d'un message **DHCPACK**, qui contient un bail d'adresse IP valide. Après avoir reçu le ACK, le client initialise sa pile IP complètement et stocke les paramètres dans la base de registre.

Vous pouvez vous rappeler ces 4 phases en pensant à l'acronyme ROSA (**R**equest - **O**ffer - **S**election - **A**CK). Distinguez bien la phase des types de messages (l'acronyme pour les messages serait alors DORA).

5.2. Renouvellement de bail DHCP

Première tentative de renouvellement : à **50 %**

- Tous les clients DHCP tentent de renouveler leur bail quand **50 %** du temps de bail a expiré. Le client envoit un message DHCPREQUEST au serveur à partir duquel il a obtenu son bail.
- Si le serveur DHCP est disponible, alors le bail est renouvelé et un message DHCPACK est renvoyé avec tous les paramètres mis à jour.
- Si le client ne reçoit pas un DHCPACK, il continue à utiliser le bail car 50% sont encore disponibles.

2. Seconde Tentative : à **87,5 %**

- Si le client n'a pas pu renouveler le bail à 50% de la durée de vie, il contacte, à 87.5 % de celle ci, n'importe quel serveur DHCP sur le réseau.

3. Expiration du bail

- Après l'expiration du bail, le client annule le bail et tente de le renouveler de la même façon qu'il l'a initialisé à l'origine et le processus complet recommence. Si le client ne peut pas obtenir de bail, la pile IP ne peut plus fonctionner.

5.3. Serveurs DHCP Multiples & Agent de Relais DHCP

Le rôle de l'agent de relais DHCP est faire suivre les messages de diffusion DHCP entre les clients et les serveurs DHCP au travers des routeurs IP.

Si un réseau comprend plus d'un sous-réseau, il est habituellement conseillé d'avoir un serveur DHCP par sous-réseau.Cependant, grâce à l'agent de relais DHCP ou à des routeurs qui peuvent faire suivre les diffusions BOOTP, les demandes d'adresses DHCP peuvent être gérées par un seul serveur.

Un serveur DHCP possède une étendue d'adresses IP configurée pour chaque sous-réseau auquel il envoie des offres DHCP. Si le serveur DHCP reçoit une demande DHCP relayée provenant d'un sous-réseau distant, il offre un bail d'adresse IP à partir de l'étendue qui correspond au sous-réseau.

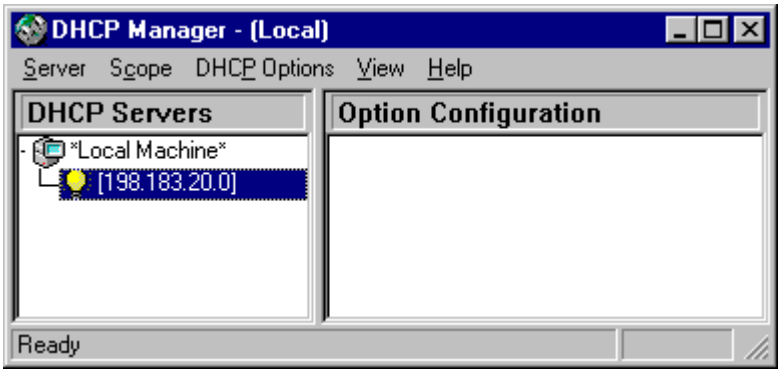
Pour vous assurer qu'un client DHCP peut recevoir un bail d'adresse IP même quand un serveur ne fonctionne pas, vous devrez configurer l'étendue d'un sous-réseau donné sur plus d'un serveur DHCP.Ainsi, si un client DHCP ne peut obtenir de bail du serveur DHCP local, l'agent de relais DHCP passe la requête au serveur DHCP d'un réseau distant qui peut offrir le bail au client.

Exemple : un réseau possède deux sous-réseaux avec chacun un DHCP , reliés par un routeur compatible RFC 1542. Microsoft conseille que chaque serveur contienne environ 75 % des IP disponibles sur le sous-réseau sur lequel il est installé et 25% des adresses IP disponibles du sous-réseau distant.

Si la plage des adresses IP disponibles va de 120.50.7.10 à 120.50.7.110 sur le sous - réseau A , et de 120.50.8.10 à 120.50.8.110 sur le sous-réseau B, la configuration des étendues pourrait être la suivante :

Sous-Réseau	Serveur DHCP A	Serveur DHCP B
A	De 120.50.7.10 à 120.50.7.84	De 120.50.7.85 à 120.50.7.110
B	De 120.50.8.10 à 120.50.8.34	De 120.50.8.35 à 120.50.8.110

5.4. Gestionnaire DHCP



Ecran du Gestionnaire DHCP

5.4.1. OPTIONS DE L'ETENDUE DHCP

DHCP peut,en plus de fournir une adresse IP, donner des paramètres réseaux aux clients DHCP.
Ces paramètres peuvent être les @ des serveurs DNS ou WINS.

5.4.2. PORTEE DES OPTIONS

Les options possèdent une portée :

Globale - Les options Globales sont disponibles pour tous les clients DHCP et sont utilisées sur tous les sous-réseaux qui nécessitent la même configuration.
Etendue - Les options sont disponibles pour les clients d'une étendue spécifique.
Les options d'étendue prennent le pas sur les options Globales.
Client - Les options Clients sont utilisées pour un client spécifique. Elles outrepassent les Options Globales et d'Etendue.

Options DHCP pour Microsoft TCP/IP

Code	Nom	Description
1	**Masque sous-réseaux**	Masque de sous-réseau des clients
3	**Routeur**	Adresse IP routeurs
6	**Serveur DNS**	Adresse IP des serveurs DNS
15	**Domain**	Spécifie le nom de domaine à utiliser lors de la résolution

44	**WINS/NBNS**	Spécifie une liste des adresses IP pour les serveurs de noms NetBIOS.
46	**WINS/NBT**	Type de nœud : 0x1=b-node 0x2=p-node 0x4=m-node 0x8=h-node
47	**NETBIOS ID**	Chaine d'étendue NetBIOS à utiliser

5.5. Maintenance du serveur DHCP

✍ Utiliser Ipconfig pour libérer ou renouveler le bail (*ipconfig /release* et *ipconfig /renew*)

5.5.1. Sauvegarder la base DHCP

La base de données DHCP est sauvegardée toutes les 60 minutes, ce paramètre peut être changé dans le registre :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Parame
ter              Flag: BackupInterval (Minutes)
```

Les fichiers de DHCP sont dans \systemroot\system32\DHCP
Les fichiers de sauvegarde sont dans \systemroot\system32\DHCP\backup\jet

✍ **Fichiers de DHCP**

✍ DHCP.MDB - base de donnée DHCP
✍ DHCP.TMP - Fichier temporaire transactionnel.
✍ JET.LOG - Enregistre les transactions
✍ SYSTEM.MDB - structure DHCP (?)

5.5.2. Restaurer une base de donnees DHCP

✍ Arrêter le service, mettre la clé de registre Restore à 1 et redémarrer le service

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Parame
ters\Restore
```

✍ Autre possibilité : copier les fichiers manuellement (service arrêté).

5.6. 2 QUESTIONS D'EXAMEN

Paco moves a Windows NT Workstation computer originally configured as a DHCP client from one subnet to another on a DHCP network. He discovers that the workstation cannot connect to the local Windows NT Server computer. What is the most likely cause of the problem?
a. The workstation's default gateway address has been manually set.
b. The workstation's default gateway address is set as a local-level option on the DHCP server.

c. The workstation's IP address has been manually set.
d. The workstation's IP address is set as a scope-level option on the DHCP server.

Réponse: c
A client-level option such as an IP address is only available in DHCP Manager to reserved DHCP clients. However, this does not prevent someone from manually setting the IP address or default gateway address in the IP configuration of the client machine. Wherever set, client-level options will override those set at the scope and global levels. If the computer had been able to connect to another host on the local subnet, then its default gateway address would have been a possible cause of the problem.

You administer a network of 850 client computers on seven subnets. You use DHCP to assign IP addresses to all client computers. You install two DNS servers on the network. Now you want to specify the IP addresses of both DNS servers on each client computer across all seven subnets. How do you configure the DHCP option?

a. as a client option
b. as a global option
c. as a scope option
d. as an Internet option

Réponse: b
The DHCP Options dialog box allows you to configure several TCP/IP settings at the global level, the scope level, and the client level. Client options override scope options; scope options override global options. The level at which an option is set depends on the nature of the option. For example, when configuring DHCP to work with WINS, the 44 WINS Servers option will normally be set at the scope level since DHCP clients will most likely register with the WINS server within their scope or subnet. The 46 Node Type option, on the other hand, should be set at the global level, since different broadcast nodes might cause servers to ignore client datagrams. In the example, since you want every DHCP-enabled client to receive the IP addresses of both DNS servers, you should set the DNS Servers option (006) as a global option.

6. NetBIOS sur TCP/IP

6.1. Nom NetBIOS

Un nom NetBIOS est une adresse de 16 octets unique utilisée pour identifier une ressource NetBIOS sur le réseau. Il s'agit soit d'un nom unique (exclusif), soit d'un nom de groupe (non exclusif). Les noms uniques sont généralement utilisés pour l'envoi de communications réseau à un processus spécifique présent sur un autre ordinateur. Les noms de groupe sont utilisés pour envoyer des informations à plusieurs ordinateurs simultanément.

Le service Serveur d'un ordinateur Windows NT constitue un exemple de processus utilisant un nom NetBIOS. Lorsque votre ordinateur démarre, le service Serveur enregistre un nom NetBIOS unique reposant sur celui de l'ordinateur. Le nom exact utilisé par le service Serveur est le nom de l'ordinateur composé de 15 caractères, plus un 16ème caractère, le 20 hexadécimal. D'autres services de réseau utilisent également le nom de l'ordinateur pour construire leurs noms NetBIOS. Le 16ème caractère a donc pour seul but d'identifier spécifiquement chaque service, tel que le redirecteur, le serveur ou la messagerie.

Lorsque vous tentez de vous connecter à un ordinateur Microsoft Windows NT Server à l'aide de la commande **net use**, le nom NetBIOS du service Serveur est recherché au moyen d'une demande de *recherche de nom*. Le processus serveur correspondant est trouvé, et la communication est établie.

Les noms NetBIOS sont toujours des chaines de 16 octets. Les noms d'ordinateur peuvent faire au maximum 15 caractères, le dernier est réservé à un suffixe qui est le code du service demandé. Le tableau ci dessous présente quelques codes associés aux services.

Nom NetBIOS	Service
Nom ordinateur [00h]	Station de Travail
Nom ordinateur [03h]	Messagerie (en écoute pour les messages envoyés à l'ordinateur)
Nom ordinateur [20h]	Serveur (Partage vos ressources sur le réseau)
Nom utilisateur [03h]	Messagerie (en écoute pour les messages envoyés au nom de login)
Nom de domaine [1Dh]	Explorateur Maître
Nom de domaine [1Bh]	Explorateur Maître de Domaine

6.2. Les 3 fonctions de NetBIOS sur TCP/IP

3 fonctions principales :

- gestion des noms (point clé de l'utilisation de Netbios sur TCP/IP car ce dernier utilise l'adresse IP alors que Netbios utilise des noms d'ordinateurs)
- **gestion de session**
- transfert de données

Les 3 fonctions principales de la **gestion des noms** sont : Inscription, requête, libération des noms.

7. Méthodes de résolution des noms

7.1. Cache des noms NetBios

C'est une zone mémoire qui conserve la correspondance entre un nom NetBios et une adresse IP.
Ce cache est vérifié en premier quelle que soit la méthode de résolution utilisée.
Il conserve les entrées pendant 10 minutes (600 s) sauf les entrées préchargées.
Les noms peuvent être chargés de façon permanente dans le cache via le tag #PRE définit dans le fichier LMHOSTS.

A un instant t, il contient donc les entrées préchargées ainsi que les noms résolus durant les 10 dernières minutes.

Il existe cependant une subtilité : les entrées ne restent dans le cache 10 minutes que si elles ont été accédées durant les 2 premières minutes après leur entrée.

✍ **nbtstat -c** montre les entrées du cache.

7.2. Diffusion

Si le nom ne peut pas être trouvé dans le cache, la machine tente de le retrouver par une diffusion sur le réseau local.

NetBios utilise UDP (sur le port 137) pour envoyer une requête de nom à tous les ordinateurs du réseau.

✍Problème : augmentation du traffic & utilisation du temps processeur.

7.3. Fichier LMHOSTS

✍ Le fichier se trouve dans %winroot%\system32\drivers\etc

✍ Il faut le renommer de LMHOSTS.SAM (SAM comme SAMPLE, LM comme Lan Manager) en LMHOSTS.

Le fichier LMHOSTS établit la correspondance entre les noms NetBios et les adresses IP.

Il comporte des balises :

- ✍ #PRE : les entrées sont préchargées et leur durée de vie est mise à -1 (statique)
- ✍ #DOM:[nom_domaine] : indique que l'ordinateur est DC ainsi que le domaine qu'il contrôle.
- ✍ #INCLUDE: Indique l'emplacement d'un fichier LMHOSTS central. (Chemin UNC)
- ✍ #BEGIN_ALTERNATE : s'utilise conjointement avec la balise #INCLUDE. Elle marque le début d'une liste d'autres emplacements du fichier LMHOSTS central, au cas où la première entrée ne serait pas disponible.
  #END_ALTERNATE : Termine la liste.
- ✍ #MH : Multihomed : des ordinateurs multirésidents peuvent apparaître plus d'une fois dans la liste : cette balise indique à la machine que, dans ce cas, elle ne doit pas ignorer les autres entrées de la liste.

Exemple : fichier LMHOSTS.SAM (win98)

```
------------------------------------------------------------------
# 102.54.94.97     rhino         #PRE #DOM:networking  #net group's DC
# 102.54.94.102    appname                               # app server
# 102.54.94.123    popular            #PRE             #source server
------------------------------------------------------------------
```

✍ **Remarques :**

- Mettre les entrées les plus utilisées en tête et faire en sorte que le fichier ne soit pas trop volumineux car son parcours est linéaire.
- Mettre les entrées en #PRE en fin de fichier car elles sont déjà préchargées dans le cache des noms NetBIOS.
- Nbtstat -R : recharge le cache NetBios à partir du fichier LMHOSTS.

7.4. Serveur de noms NetBios (WINS)

NetBios Name Service (NBNS) , NT le met en œuvre sous la forme d'un serveur WINS.

- WINS réduit le traffic lié aux diffusions,
- réduit la surcharge administrative de maintenance,
- facilite l'activité d'un domaine sur un réseau étendu,
- fournit des services d'exploration au travers de plusieurs sous-réseaux.

7.5. Fichiers Hosts

Le fichier se trouve dans %winroot%\system32\drivers\etc

Il est avant tout associé à la résolution des noms d'hôtes. Windows NT l'utilise cependant si toutes les autres méthodes de résolution ont échoué.

Il est semblable au fichier LMHOSTS mais est plus simple :

- Il ne comporte pas de balises
- Il est possible d'associer plus d'un nom d'hôte en les saisissant tous sur la même ligne en les séparant par un espace.

Exemple :

```
192.168.100.1      www.fireball.com  #serveur
192.168.100.2 maverick missile
 127.0.0.1   localhost
```

Les commentaires sont toujours en fin et marqués par #.

7.6. Ordre de résolution

Les **types de nœuds NetBios** établissent l'ordre de résolution. Un type de nœud est simplement la méthode que l'hôte va employer pour résoudre un nom.

Le nœud par défaut est b-node (Broadcast) à moins qu'une adresse de serveur WINS ne soit définie, auquel cas, le défaut est h-node (Hybride).

7.6.1. TYPES DE NŒUDS

- Diffusion générale (b-node, broadcast)
- Point à point (p-node, peer to peer)
- Mixte (m-node, utilise b-node puis p-node)

- Hybride (h-node, utilise p-node puis b-node)

B-node

La méthode la plus simple consiste à demander à tout le monde si le nom est le sien.
Elle doit être faite au travers d'une diffusion à laquelle tous les hôtes du réseau répondent.
Les requêtes de nom NetBios en diffusion peuvent occuper une quantité importante de la bande passante sur le réseau, en utilisant du temps processeur sur chaque machine.
Windows NT fait 3 tentatives pour résoudre le nom en utilisant une diffusion, avec une attente de 7.5 secondes chaque fois.

Une machine en B-node passe par les étapes suivantes pour résoudre un nom

- 1.Vérification de son cache NetBios
- 2.Diffusion d'une requête de nom NetBios
- 3.Vérification du fichier LMHOSTS (uniquement pour le m-node MS)
- 4.Vérification d'un fichier HOSTS
- 5.Vérification sur un serveur DNS

P-Node

Une machine en P-node

Demande le nom NetBios à la machine centrale .
3 tentatives espacées de 15 secondes.

Ordre de résolution :

- 1.Vérification de son cache NetBios
- 2.Demande à un serveur de noms NetBIOS (NBNS)
- 3. Vérification d'un fichier HOSTS
- 4.Vérification sur un serveur DNS

M-Node

Une machine en M-node

Une machine en m-node essaie toutes les méthodes de résolution. Ce type de résolution est, avec h-node, une concaténation de p-node et de b-node.

La seule différence est l'ordre:

- 1.Vérification de son cache NetBios
- 2.Diffusion d'une requête de nom NetBios
- 3.Vérification du fichier LMHOSTS (uniquement pour le m-node MS)
- 4.Demande à un serveur de noms NetBIOS (NBNS)
- 5. Vérification d'un fichier HOSTS
- 6.Vérification sur un serveur DNS

H-Node

Une machine en H-node

C'est aussi une concaténation de p-node et b-node.
Il commence par consulter le serveur de noms.

- 1.Vérification de son cache NetBios

- 2.Demande à un serveur de noms NetBIOS (NBNS)
- 3.Diffusion d'une requête de nom NetBios
- 4.Vérification du fichier LMHOSTS (uniquement pour le m-node MS)
- 5. Vérification d'un fichier HOSTS
- 6.Vérification sur un serveur DNS

✍Pour déterminer le type de nœud : ipconfig /all

✍Pour définir un autre type de nœud, il faut modifier la clé :

```
HELY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters
NodeType :

1 = B-node  2 = P-node  3 = M-node  4 = H-node
```

Dans le cas d'un client DHCP, on peut utiliser DHCP pour faire la configuration automatique.

7.7. 2 QUESTIONS D'EXAMEN

Jan administers a TCP/IP network that is comprised of multiple domains. The network is divided into six subnets. Jan wants every Windows-based computer to be able to browse every domain. Which entries must Jan include in the LMHOSTS file on each Windows-based computer?

a. one entry for a BDC in each remote domain; one entry for a BDC in the local domain
b. one entry for a BDC in each remote domain; one entry for each domain controller in the local domain
c. one entry for the PDC in each remote domain; one entry for a BDC in the local domain
d.one entry for the PDC in each remote domain; one entry for each domain controller in the local domain

Réponse: d

How many entries you make in an LMHOSTS file depends largely on the size and stability of your network. However, the file should contain an entry for each domain controller on the local domain and the PDC of every remote domain. Upon this baseline, you can continue to add more remote domain BDCs as warranted. Regardless of which domain controllers you enter in an LMHOSTS file, they should all be flagged with the #PRE and #DOM keywords so that they will be loaded into cache on each host as domain controllers.

Which of the following entries in a HOSTS file residing on a Windows NT Server computer will fail to connect to the UNIX server CorpServer?
a. 68.112.45.98 #CorpServer #corporate server
b. 68.112.45.98 CorpSrvr #corporate server
c. 68.112.45.98 CORPSERVER #corporate server
d. 68.112.45 CorpServer #corporate server

Réponse: abd
Like an LMHOSTS file, a HOSTS file that resides on a computer running Windows NT Server 4.0 is not case-sensitive. Also, remember that a HOSTS file does NOT recognize #PRE, #DOM, #INCLUDE, #BEGIN_ALTERNATE and #END_ALTERNATE as keywords. Everything that begins with a pound sign (#) is taken as a comment and is ignored. IP addresses listed in a HOSTS file must contain four octets to be valid.

8.Mise en œuvre de WINS

✍WINS offre les services d'inscription, de renouvellement, de libération et de résolution des noms NetBIOS en adresses IP .

✍Il est mis en œuvre en tant qu'extension des RFC 1001 et 1002.

✍Il gère une base de données dynamique des liens entre noms NetBios et adresses TCP/IP où chaque inscription dispose d'une de durée de vie.

✍WINS élimine le besoin de broadcast pour résoudre les noms d'ordinateurs en adresses IP.
Un serveur WINS peut être configuré à la fois avec WINS et DNS pour résoudre des noms NetBios et des noms d'hôtes pour les clients Microsoft.
WINS est une base de données dynamique, donc la résolution est toujours à jour et n'a pas besoin d'être modifiée manuellement comme pour le fichier LMHOSTS.

8.1. Processus de résolution WINS

8.1.1. Enregistrement de Nom

Lorsqu'un client WINS s'initialise, il enregistre son nom NetBIOS en envoyant une inscription de nom (nom ordinateur + adresse IP) au serveur WINS. Si tout se passe bien, le serveur renvoie au client un message d'inscription réussie.

Nom dupliqué
Si le nom NetBIOS est déjà enregistré, le serveur WINS envoit une demande (challenge) au propriétaire actuel du nom. Cette requête est envoyée 3 fois à 500 ms d'intervalle. Si le propriétaire répond, le serveur WINS renvoit une réponse négative au client qui essaie d'enregistrer le nom. Dans le cas contraire, le nom est enregistré.

Serveur WINS non disponible
Un client WINS fait 3 tentatives pour enregistrer son nom via le serveur WINS primaire. Si cela n'aboutit pas, alors le client essaie avec le serveur WINS secondaire. Si cela ne fonctionne pas, le client enregistre son nom via une diffusion générale.

8.1.2. Renouvellement de Nom

Une fois un nom inscrit, une durée de vie lui est attribuée, à l'expiration de laquelle le nom sera retiré de la base de donnée.
Pour continuer à utiliser le même nom NetBIOS, un client doit renouveler son bail avant qu'il n'expire.
Un client WINS va contacter le serveur WINS pour un renouvellement quand 1/8 de la durée de vie s'est écoulée.
S'il ne reçoit pas de réponse, le client fait une tentative toutes les 2 minutes, jusqu'à ce qu'il soit arrivé à la moitié de la durée de vie.Il tente alors de renouveler son inscription à partir du serveur WINS secondaire, de la même manière qu'avec le serveur WINS primaire .

8.1.3. LIBERATION

Un client WINS envoie une demande de libération de nom au serveur WINS lorsqu'il est arrêté normalement. Ce message est une requête de suppression de l'adresse IP et du nom NetBios de la base de donnée du serveur WINS.

8.1.4. RESOLUTION DE NOM

Les clients WINS envoient des requêtes de résolution de nom au serveur :

1. Cache local des noms NetBIOS
2. Une requête de noms est envoyée au serveur WINS primaire
   si ce dernier est indisponible, la requête est expédiée deux fois avant de passer au WINS secondaire
3. Diffusion etc … (voir parties précédentes).

✍ **Remarques :**

Un serveur WINS peut effectuer en moyenne 1500 requêtes d'inscription par minute ; il peut résoudre 4500 noms par minute.

Microsoft conseille 1 serveur WINS pour 10000 machines

8.2. Le Proxy WINS

Les proxy WINS permettent aux clients non-WINS de résoudre des noms NetBIOS sur le réseau.
Le proxy WINS (=agent proxy) **DOIT** être un client WINS et donc ne peut pas être un serveur WINS.
Il peut être mis en place sur Windows NT, Windows 95/98 et WFW.

Au maximum 2 agents proxy par sous-réseau.

Pour transformer une machine NT or 95/98 en tant que Proxy WINS, il faut modifier la clé suivante dans le registre :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netbt\Parameters
EnableProxy = 1
```

Scénario :

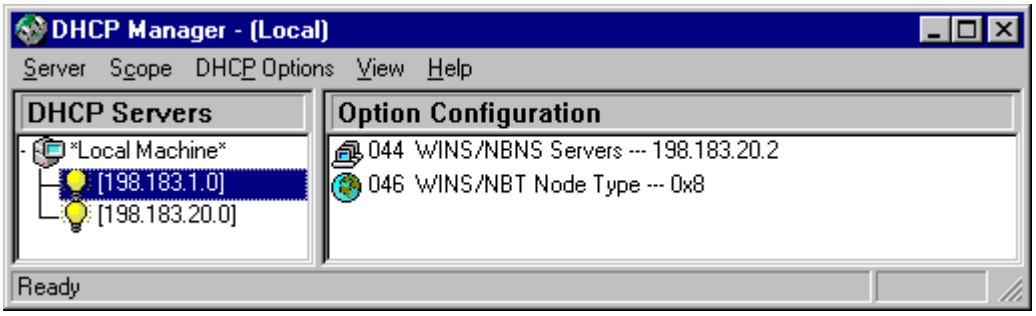
Un client non-WINS émet une diffusion générale pour résoudre un nom.
L'agent proxy à l'écoute reçoit le message : il vérifie dans son cache de noms NetBIOS s'il dispose d'une entrée relative au nom.
S'il ne l'a pas, il ajoute au cache une entrée pour ce nom, avec l'indication "en attente"
Il envoit au serveur WINS une requête pour ce nom. Dès réception, il ajoute l'entrée et supprime l'indicateur "en attente". **L'agent proxy ne renvoit pas la réponse au client non-WINS qui a effectué la requête.** Lorsque le client non-WINS émettra une nouvelle requête, l'agent proxy lui répondra.
L'agent proxy redirige également les requêtes d'inscription vers le serveur WINS.

8.3. Intégrer WINS à DHCP

Dans une étendue DHCP, il faut configurer :

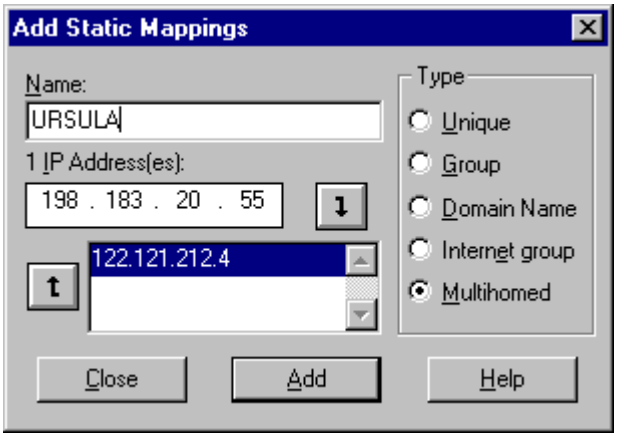
44 WINS/NBNS Server : Cette option spécifie le serveur WINS que le client va utiliser.

46 WINS/NBT Node Type : Cette option spécifie le mode de résolution que le client WINS va employer. Ce paramètre devrait être mis au niveau global, étant donné que les clients WINS vont employer le type de nœud Hybride (H-Node).



8.4. Configurer des mappings WINS statiques.

Il n'est pas toujours possible ou souhaitable de rendre tous les ordinateurs du réseau clients WINS, ces entrées n'apparaitront alors pas dans la base WINS.
Ces entrées peuvent être définies en tant que mappings statiques dans la base WINS.
Les noms d'hôtes Unix peuvent être ajoutés dans la base WINS, pourvu que le nom d'hôte soit en concordance avec les 15 caractères du nom NetBIOS.



(Menu WINS Manager puis Mappings puis Static Mappings)

Unique : Un nom unique dans la base WINS, il correspondra à une adresse IP unique.
Groups : Les groupes sont des cibles de messages de diffusion et ne sont pas associés avec des adresses IP
Domain Name : Un groupe associé avec l'adresse IP d'un PDC et de 24 BDC pour un total de 25. Ceci est utilisé pour faciliter l'activité sur un domaine.
Internet Group : Un groupe défini par l'utilisateur qui peut include différentes ressources telles que des imprimantes.
Multihomed (Multirésident) : Un nom unique peut être associé jusqu'à 25 adresses, correspondantes aux adresses IP d'un ordinateur multirésident.

8.5. 2 QUESTIONS D'EXAMEN

Mr. Krueger manages a TCP/IP network of both Windows-based and UNIX computers with three subnets, SubnetA, SubnetB and SubnetC, connected by a single router. After installing a WINS server on SubnetA, he configures each Windows-based computer on his network to register its NetBIOS/domain name with WINS. However, he soon discovers that the UNIX computers on SubnetB and SubnetC are not able to use the WINS server for name resolution. What can Mr. Krueger do to correct the problem?
a. install a second router
b. on SubnetB and SubnetC, install BOOTP Relay Agents
c. on SubnetB and SubnetC, install WINS proxies
d. on the WINS server, install DHCP
e. on the WINS server, reserve the names of the clients on SubnetB and SubnetC

Réponse: c
Normally, on a routed network you should place a WINS server on each Internetwork. The servers would then replicate the WINS database amongst themselves. Where such a solution is not feasible, you can use WINS proxies. A WINS proxy assists a WINS server in name resolution. When non-WINS-enabled computers use b-node broadcasts for name queries, the WINS proxy listens for the broadcast and tries to resolve the query using its cache. If the WINS proxy cannot solve the query directly, then it forwards the query across the router to the WINS server for resolution. When the WINS server responds to the remote query, the WINS proxy not only forwards the data to the requesting host, it also caches the response for future reference. You create a WINS proxy by setting the computer's registry parameter, EnableProxy, to 1 in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Netbt\Parameters key.

Kilroy uses DHCP to assign IP addresses to all client computers on his network. Kilroy sets up the DHCP server to assign the IP address of the WINS server to all client computers. What else should Kilroy do in order to allow client computers to use WINS?
a. In DHCP Manager, specify the NetBIOS resolution mode.
b. On each client computer, enter the IP address of at least one DNS server.
c. On each client computer, enter the IP address of the PDC.
d. On each client computer, specify a NetBIOS Scope ID.

Réponse: a
In order to work with WINS, DHCP clients must be assigned the 44 WINS/NBNS Servers and the 46 WINS/NBT Node Type options. DHCP option 44 WINS/NBNS Servers specifies the WINS server(s) that the computers will try to use. Usually this is set at the scope level. DHCP option 46 WINS/NBT Node Type specifies the address resolution mode the WINS client will use. This is set at the global level. DNS for Windows Resolution can be enabled on the WINS Address tab of the Microsoft TCP/IP Properties page, but is not required for DHCP/WINS interoperability. A DHCP/WINS client does not need to be configured with the PDC address. The NetBIOS Scope ID isolates a group of computers on the network so that they can communicate only with other computers configured with the same NetBIOS Scope ID. It is to be used with extreme caution since it can wreak havoc on logon services and other resources.

9.Administrer un environnement WINS

9.1. La base de données WINS

Les fichiers utilisés sont :

- WINS.MDB : la base de données des baux.

- WINSTMP.MDB : fichier temporaire, supprimé lors de l'arrêt (sauf en cas de crash)
- J50.log : journal des transactions
- J50.chk : fichier de vérification

Compacter la base WINS

Il est possible de compresser cette base à l'aide de l'utilitaire JetPack mais il faut arrêter le service WINS.

Syntaxe : `Jetpack WINS.MDB temp.MDB`

Sauvegarde de la base WINS : ne pas oublier les informations du registre

Restaurer une base WINS corrompue :

- Arrêter et redémarrer le service serveur WINS pour restaurer automatiquement,
- Dans le gestionnaire WINS, sélectionner Mappings, puis Restore Local Database,
- Remplacer manuellement la base,
- Dans une fenêtre DOS, taper NET STOP WINS,
- Puis CD \<systemroot>\system32\wins,
- DELETE JET*.LOG, WINSTMP.MDB, and SYSTEM.MDB
- Copy SYSTEM.MDB à partir du CD-ROM de NT Serveur ainsi que la version sauvegardée du fichier WINS.MDB vers le dossier C:\<systemroot>\system32\wins.
- NET START WINS, puis exit

Nettoyer la base de données

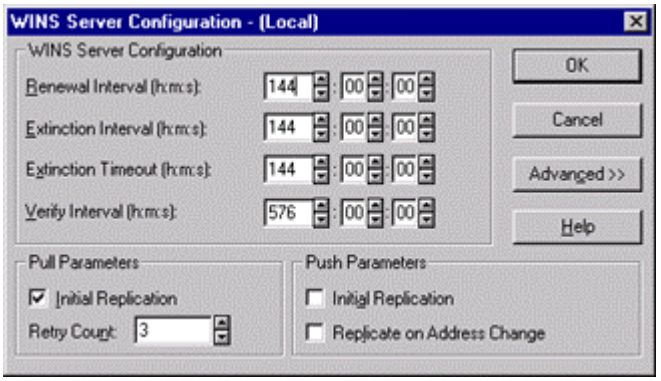
Il existe 3 états pour les noms NetBIOS: active, released (-), and extinct (+, comme une croix).
Si le nom n'est pas renouvelé, il est marqué comme relaché dans la base.
Les entrées Relachées restent dans la base jusqu'à ce que l'intervalle d'extinction soit atteint.
Les entrées éteintes sont conservées dans la base jusqu'à ce que le délai (timeout) d'extinction soit lui aussi atteint. Elles sont alors retirées de la base.

Vous êtes perdus ?

De Actif jusqu'à ce que l'intervalle de renouvellement expire, l'on passe à Relaché
De Relaché jusqu'à ce l'intervalle d'extinction soit atteint on passe à Eteint
Eteint tant que le Timeout d'extinction n'est pas atteint, l'entrée est ensuite retirée de la base.

Intervalles et délais

L'intervalle de renouvellement : c'est le temps nécessaire pour qu'une entrée passe d'active à Relachée. L'intervalle par défaut est de 6 jours (144h)
L'intervalle d'extinction : c'est le temps nécessaire pour passer de relachée à éteinte. L'intervalle par défaut est de 6 jours (144h).
Délai d'extinction : c'est le temps nécessaire pour passer d'éteinte à supprimée.

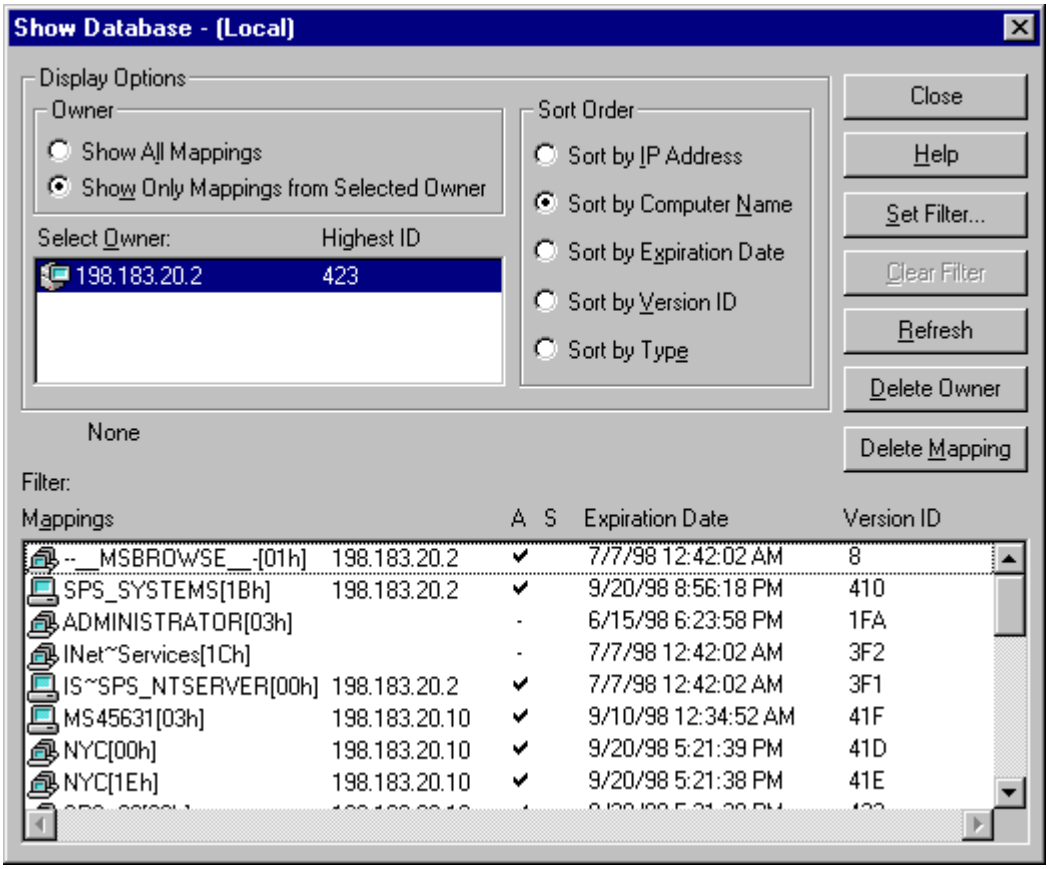


Contenu de la base WINS

L'image ci-dessous montre le contenu de la base de donnée WINS. A la fin de chaque nom NetBIOS, vous pouvez voir les codes de noms NetBios entre crochets [ ] et les adresses IP correspondantes aux machines.
Ces codes de ressources représentent les ressources ou services qui sont disponibles sur ce nom.
Les colonnes A et S sont des marques qui indiquent comment l'enregistrement s'est effectué.

A - indique un enregistrement actif (automatique, dynamique) effectué lors du démarrage de l'ordinateur
S- indique un enregistrement statique que l'administrateur a manuellement entré.

La quatrième colonne indique quand l'enregistrement va expirer.
Le client rafraîchit automatiquement un enregistrement durant le prochain démarrage.
Dans la dernière se trouve une valeur hexadécimale représentant l'enregistrement de réplication. Ceci détermine quel serveur WINS possède l'enregistrement client WINS le plus a jour.



9.2. La Duplication WINS

Types de partenaires

La duplication consiste à copier la base de données WINS d'un serveur vers un autre ainsi que les mappages statiques.

Il existe deux types de partenaires : PUSH (poussés) et PULL (tirés)

Un serveur WINS doit être au moins un partenaire poussé (PUSH) afin d'envoyer ses entrées tandis que l'autre sera un tiré (cela n'exclue pas 2 partenaires PULL-PULL , cf présentation).

Si les deux serveurs sont tirés et poussés, les entrées de chaque serveur se retrouvent sur les deux serveurs.

Poussé (Push) ou Tiré (Pull) ?

Il est plus intéressant d'utiliser un serveur tiré (Pull) a travers une connexion lente car il est possible de configurer ce type de partenaire afin qu'ils ne se dupliquent qu'à certains moments.

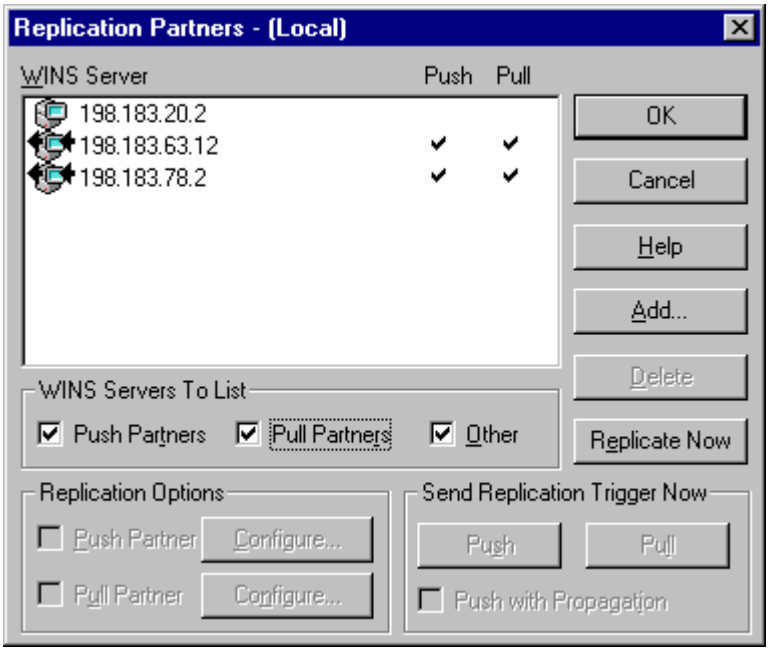
Sur des liaisons plus rapides, utiliser des partenaires poussés, qui se dupliquent après avoir modifié la base.

Si l'on désire deux bases identiques, chacun doit être configuré comme PUSH/PULL.

Il est possible de configurer un partenaire de duplication afin de lancer la duplication selon plusieurs techniques :

- Duplication au démarrage TIRE (PULL) ou POUSSE (PUSH)
- A des intervalles de duplication, par exemple : toutes les 24 heures : TIRES (PULL)
- Lorsqu'un partenaire poussé atteint un certain nombre de modifications dans la base de donnée.
  Quand ce seuil est atteint, il informe ses partenaires tirés qu'il y'a des modifications.
- Imposer manuellement la duplication depuis le gestionnaire WINS.

WINS peut automatiquement se dupliquer avec d'autres serveurs WINS si le réseau supporte le multicast.
Par défaut, toutes les 40 minutes, chaque serveur WINS envoie un message de diffusion restreinte à l'adresse 224.0.1.24 (possible de le désactiver dans le registre).



9.3. 2 QUESTIONS D'EXAMEN

Donna's company is headquartered in Miami with a second office in Chicago. Both offices use TCP/IP as the networking protocol. The Miami office has ten Windows NT Server computers and 1,000 Windows NT Workstation computer clients. The Chicago office has two Windows NT Server computers and 225 Windows NT Workstation computer clients. The WINS server in Miami is called MIA; the WINS server in Chicago is called CHI. Donna wants to set up WINS database replication between the two WINS servers.
Required result:
She must replicate the Miami WINS server database to the Chicago WINS server.
Optional desired results:
1) She wants to replicate the Chicago WINS server data on the Miami WINS server.
2) She wants to be sure that the Miami WINS database is replicated to Chicago at least once a day.
Proposed solution:
Configure Miami to push its WINS database update information to Chicago once every 50,000 updates.
Configure Chicago to pull Miami's WINS database update information once every 24 hours.

Which results does the proposed solution produce?
a. The proposed solution produces the required result and both of the optional desired results.
b. The proposed solution produces the required result and one of the optional desired results.

c. The proposed solution produces the required result and none of the optional desired results.
d. The proposed solution does not produce the required result.

Réponse: B. No where in the proposed solution does Chicago's database get replicated with Miami. Miami pushes its changes to Chicago every 50,000 updates and Chicago PULLS Miami's database every 24 hours.

Joey's Windows NT Workstation computer resides on a WINS-enabled network. In which order will Joey's computer perform name resolution if his computer is configured to use an LMHOSTS file?
a. local cache, broadcasting, LMHOSTS file, WINS server
b. local cache, WINS server, broadcasting, LMHOSTS file
c. WINS server, local cache, broadcasting, LMHOSTS file
d. WINS server, local cache, LMHOSTS file, broadcasting

Réponse: b
Hosts always check their cache first for name resolution before employing other options. In h-node mode (which first employs p-node, then b-node), the host next polls the WINS server. If the WINS server fails, the host broadcasts on the local subnet for name resolution. Finally, should broadcasting fail, the LMHOSTS file is examined.

10. DNS (Domain Naming Server)

Le système de nom de domaine (DNS) est un système de gestion de base de données (SGBD) client-serveur distribué et hiérarchisé. DNS fonctionne au niveau de la couche application et utilise UDP et TCP en tant que protocoles sous-jacents.
Le rôle de la base de données DNS consiste à **traduire les noms d'ordinateurs en adresses IP**. Dans DNS, les clients sont appelés solveurs (resolvers) ; ils adressent leur requête à des serveurs de noms (name servers).

✍TLD = Top Level Domains (com, edu , org ...)

✍FQDN = Fully Qualified Domain Name = Nom d'hôte + Nom de domaine
Le nom de domaine peut être une combinaison de lettres de A à Z, de numériques 0 à 9, le trait d'union (-).

10.1. Requêtes Récursives , Itératives et Inverses

Récursive
Quand un serveur DNS effectue une requête récursive pour le client, le serveur "reste" avec cette requête jusqu'à ce qu'elle soit résolue. Le serveur est ainsi forcé à répondre soit par un message d'hôte non trouvé, soit par l'adresse IP du nom de domaine transmis.

Itérative
Une requête itérative demande au serveur de renvoyer la meilleure information dont il dispose en local, à travers de ses fichiers de zone internes ou aux travers des informations stockées dans le cache. Si le serveur de noms ne dispose pas d'informations aptes à résoudre la requête il peut renvoyer au client l'endroit où il peut trouver la réponse.

Requête Inverse
Dans une requête inverse, le client fournit une adresse IP et demande au serveur DNS le FQDN correpondant.

10.2. Fichiers de zone

La base de données DNS est stockée dans des fichiers appelés zones. Il est possible et même préférable, de décomposer la base de données DNS en un certain nombre de zones.

10.3. Types de Serveurs DNS

10.3.1. SERVEUR PRIMAIRE, SECONDAIRE ET MAITRE

Un serveur de noms primaire est un serveur qui dispose de la copie principale du fichier de zone. Les modifications apportées à une zone, comme l'ajout d'un domaine ou d'un hôte, se font sur le serveur DNS primaire.
Un serveur DNS secondaire possède une copie en lecture seule des fichiers de zone qui proviennent des autres serveurs. Si des modifications doivent être faites, cela doit se passer sur la copie originale du fichier de zone. Les modifications seront alors propagées aux serveurs secondaires via la réplication des fichiers de zone. Le mécanisme de copie des fichiers de zone d'un serveur à l'autre s'appelle le transfert de zone.
Le serveur auquel s'adresse un serveur secondaire pour recevoir un transfert de zone s'appelle le serveur de noms maître. L'adresse IP du serveur de noms maître est configurée sur le serveur secondaire.

10.3.2. CACHE-SEUL

Ce sont des DNS dont le travail consiste à effectuer des requêtes, mettre en cache les réponses et retourner le résultat.
Un Serveur Cache-seul (Caching Only) permet d'alleger le traffic DNS, il ne participe pas aux transferts de zones.

10.3.3. FICHIERS DE LA BASE DE DONNEE DNS

Les fichiers de BIND peuvent être utilisés pour configurer le serveur DNS Microsoft. Bind est le format le plus utilisé pour les serveurs DNS sur Internet.

Il y'a 4 fichiers essentiels :

- Fichier de base de données
- Fichier de reverse lookup (résolution inverse)
- Fichier de cache
- Fichier de boot

L'édition manuelle de ces fichiers nécessite que le service DNS soit arrêté puis relancé.
Les fichiers se trouvent dans - %WINROOT%\SYSTEM32\DNS

domain.dns

Le fichier de base de donnée (domain.dns) stocke les enregistrements pour le domaine.
Pour la zone "lordcomp.com", le fichier de zone sera appelé lordcomp.com.dns. C'est ce fichier qui sera répliqué entre les serveurs de noms primaires et secondaires.

Au sein du fichier domain.dns il y'a plusieurs types d'enregistrements définis dans DNS.
La RFC 1034 définit ces enregistrements en détail.

Boot

Le fichier boot est le fichier principal de configuration.Il contient la localisation de tous les fichiers nécessaires pour DNS

Cache.dns

Pour l'essentiel, le fichier de cache est identique sur tous les serveurs de noms, et doit être présent. Ce fichier contient le nom et l'adresse des serveurs de noms qui gèrent le domaine racine.

Recherche inversée

- 127.0.0.dns
  Ce fichier contient les entrées inverses pour l'adresse de bouclage 127.

- [netid-inversé].in-addr.arpa.dns
  Le fichier de résolution inverse permet au DNS de renvoyer le nom correspondant à une IP. Le fichier de recherche inverse mappe les adresses IP sur les noms d'hôte. Par exemple, si votre réseau est affecté de l'adresse réseau de classe C 192.138.154.0, ce fichier sera nommé 154.138.192.IN-ADDR.ARPA.

10.4. Les types d'enregistrements DNS

Enregistrement SOA

Dans tout fichier de base de données, le premier enregistrement doit être l'enregistrement de début d'autorité (SOA, *Start Of Authority*). Il définit les paramètres généraux pour la zone DNS. L'enregistrement ci-dessous est un exemple d'enregistrement SOA :

```
@ IN SOA nameserver1.microsoft.com. glennwo.microsoft.com. (
1       ; serial number
10800       ; refresh [3 hours]
3600        ; retry [1 hour]
604800  ; expire [7 days]
86400 ) ; time to live [1 day]
```

Le gestionnaire DNS Microsoft nous permet de faire des modifications via l'interface graphique.

Enregistrement NS

Un enregistrement de serveur de nom (NS, *Name Server*) permet de répertorier un autre serveur de nom. Un fichier de base de données peut contenir plusieurs enregistrements de serveur de noms. La ligne suivante est un exemple d'enregistrement de ce type :

```
@ IN NS nameserver2.microsoft.com
```

Enregistrement A

Un enregistrement d'hôte (A) associe de manière statique un nom d'hôte à l'adresse IP correspondante. Les enregistrements d'hôtes constituent l'essentiel du fichier de base de données. Ils permettent de répertorier tous les hôtes situés au sein de la zone. Les lignes suivantes sont des exemples d'enregistrements d'hôtes :

```
rhino       IN A 157.55.200.143
localhost   IN A 127.0.0.1
```

Enregistrement CNAME

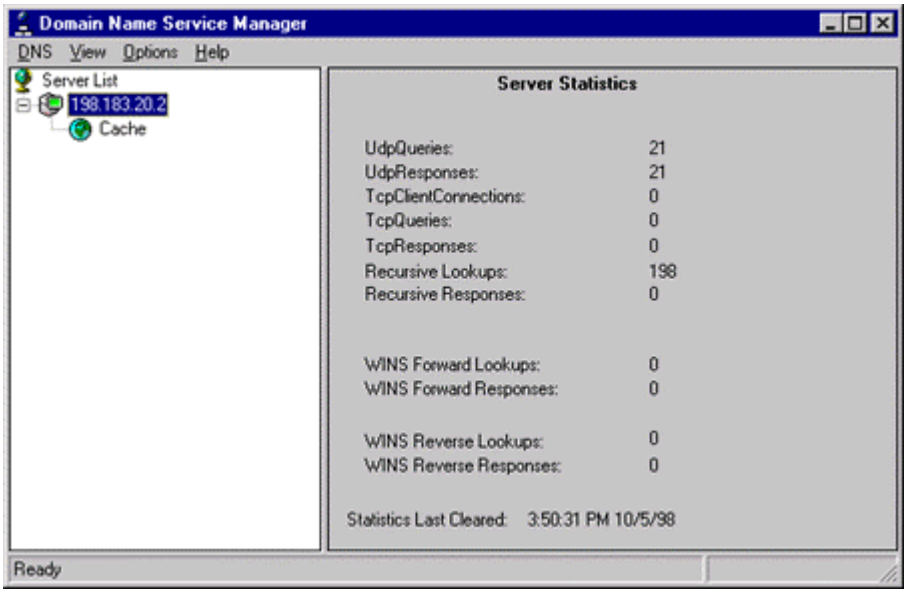
Un enregistrement CNAME (*Canonical Name*) permet d'associer plusieurs noms d'hôte à une même adresse IP. L'utilisation de cet enregistrement est parfois appelée *aliasing*. Les lignes suivantes constituent un exemple d'enregistrement CNAME :

```
FileServer1 CNAME rhino
www     CNAME rhino
ftp     CNAME rhino
```

10.5. Mise en place de DNS

- Installer le service DNS en l'ajoutant sous services dans Réseau et redémarrer la machine.
- Lancer le gestionnaire DNS et ajouter le DNS dans la liste de gestion.

Le serveur DNS fonctionne alors comme un serveur cache-seul.
Le fichier de cache contient les adresses des serveurs root sur Internet. Il peut résoudre les requêtes qui lui sont envoyées.



10.6. Interactions DNS & WINS

Le serveur DNS repose sur une base de données statique contenant des mappages nom vers adresse. Cette base de données doit être mise à jour manuellement. Le service WINS permet aux machines d'enregistrer dynamiquement leurs mappages nom vers adresse, ce qui simplifie les tâches d'administration. Le serveur DNS met en œuvre un modèle hiérarchisé qui autorise la répartition des tâches d'administration et de duplication de la base de données sur différentes zones. À l'inverse, WINS s'appuie sur un espace de noms « à plat ». Chaque serveur WINS doit tenir à jour une base de données complète, par le biais de la duplication.

10.6.1. ENREGISTREMENT WINS

Pour intégrer le serveur DNS et le service WINS, un nouvel enregistrement est défini au sein du fichier de base de données DNS. Un serveur DNS Microsoft ne peut comporter qu'un seul enregistrement WINS. Il est stocké au niveau du domaine racine de la zone lors de son enregistrement dans le fichier de base de données. Si un mappage nom vers adresse ne peut être trouvé dans le fichier de base de données, le serveur DNS interroge la base de données WINS. Ce mécanisme peut, par exemple, se dérouler de la façon suivante :

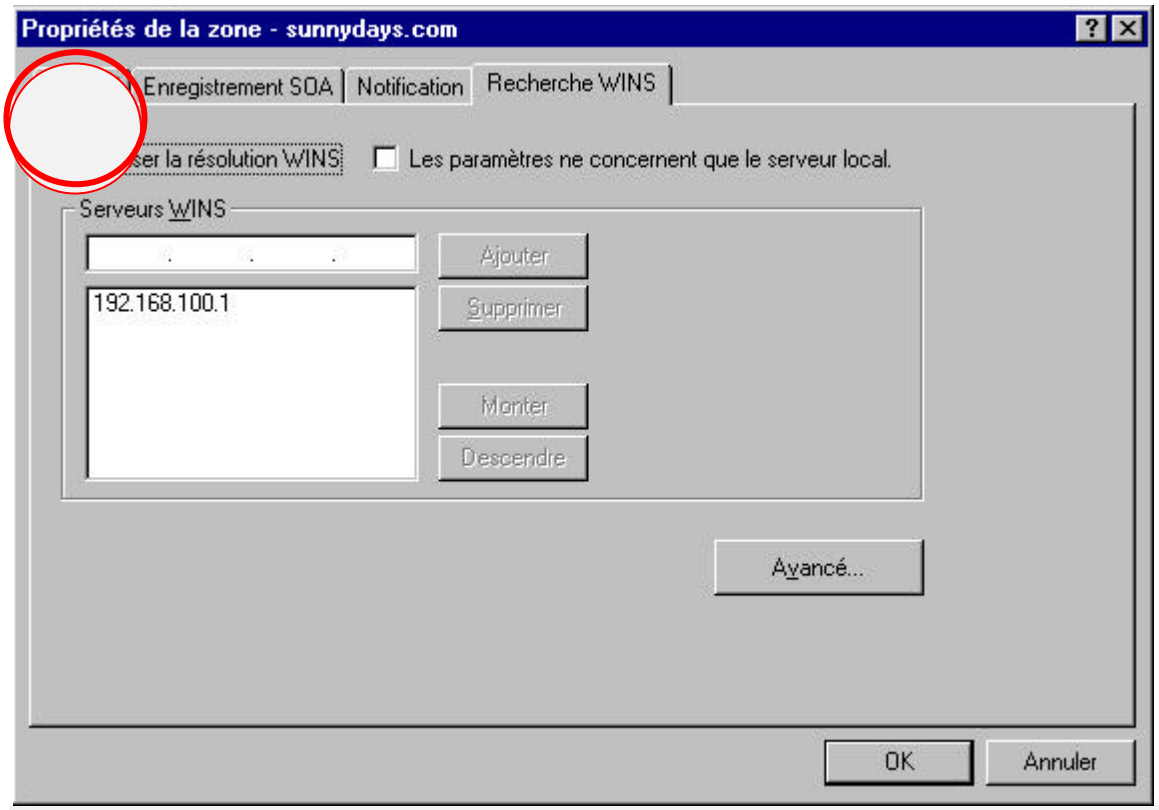
1. Un client contacte son serveur DNS et demande l'adresse IP d'un autre hôte.

   Le serveur DNS parcourt sa base de données et ne trouve pas d'enregistrement d'adresse pour l'hôte considéré.
2. Puisque le fichier de base de données contient un enregistrement WINS, le serveur DNS va convertir la partie « hôte » du nom en un nom NetBIOS, et envoyer au serveur WINS une requête portant sur ce nom NetBIOS.
3. Si le serveur WINS est en mesure de résoudre ce nom, il renvoie l'adresse IP au serveur DNS.

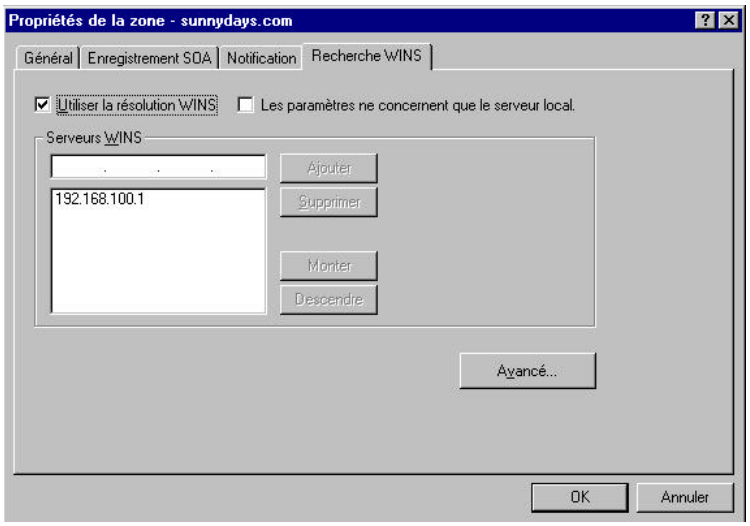
   À son tour, le serveur DNS renvoie cette adresse IP au client.

10.6.2. ACTIVATION DE LA RECHERCHE WINS

La recherche WINS est activée à partir du Gestionnaire DNS. Pour ce faire, cliquez avec le bouton droit de la souris sur la zone désirée, puis cliquez sur **Propriétés**dans le menu contextuel. Cliquez sur l'onglet **Recherche WINS**, activez la case à cocher **Utiliser la résolution WINS**, et entrez l'adresse IP des serveurs WINS que vous voulez spécifier.



Remarque :
Il est possible de demander aux clients d'utiliser un serveur DNS pour effectuer la résolution de noms. Il s'agit de la seconde interaction DNS/WINS possible.



10.7. 2 QUESTIONS D'EXAMEN

Which file does a DNS root server use to connect to the Internet?
a. cache.dns
b. domain.dns
c. HOSTS
d. place.dom
e. reverse-netid.in-addr.arpa.dns

Réponse: a
The cache.dns file holds the IP addresses of the nine domain name servers that provide root-level name resolution in the United States. Located in the \<systemroot>\System32\DNS directory, the cache.dns file is automatically installed on a Microsoft DNS server. If you do not plan to use your Microsoft DNS server to connect to the Internet, then the cache.dns file should be deleted and replaced with a file containing the NS and A records used by your intranet root name servers.

You want to minimize the number of static records on your network's DNS server. How can you make the non-Microsoft TCP/IP clients use WINS to resolve the hostname portion of each Fully Qualified Domain Name (FQDN)?
a. Enable the WINS server to resolve Fully Qualified Domain Names.
b. Enable the DNS server to use the WINS server for name resolution.
c. Under name resolution on the client computer, list DNS first, then WINS.
d. Under name resolution on the client computer, list WINS first, then DNS.

Réponse: b
You can closely integrate Microsoft DNS and WINS servers to reduce the number of static records on the DNS server. This can be accomplished by checking the Use WINS Resolution box on the WINS Lookup tab of the Zone Properties page of the DNS server and by adding the IP address(es) of the appropriate WINS server(s). Working in tandem, the DNS server can resolve the FQDN down to the hostname, which it then passes on to the WINS server. Assuming the hostname is the same as the NetBIOS name, WINS resolves the NetBIOS name to its IP address and returns the address to the DNS server.

11. Services d'Exploration

Pour partager de manière efficace des ressources au sein du réseau, les utilisateurs doivent être en mesure de déterminer quelles sont les ressources disponibles. Le service Explorateur d'ordinateurs de Windows NT assure l'affichage de la liste des ressources disponibles à un moment donné.

Le service Explorateur d'ordinateurs est une série distribuée de listes de ressources réseau disponibles. Ces listes sont distribuées à des ordinateurs désignés spécifiquement, et qui assurent des services d'exploration pour le compte des clients de l'exploration.
Dans la mesure où seuls certains ordinateurs sont désignés en tant qu'*explorateurs*, il n'est pas nécessaire que les autres machines tiennent à jour une liste de toutes les ressources partagées sur le réseau. En affectant le rôle d'explorateur à des ordinateurs spécifiques, le service Explorateur permet de diminuer le volume de trafic réseau nécessaire à la construction et à la maintenance de la liste de toutes les ressources partagées sur le réseau.

Les services d'exploration de Windows NT peuvent être abordés sous l'angle de trois processus fondamentaux :

- Collecte des informations d'exploration
- Distribution des informations d'exploration
- Traitement des requêtes émanant des clients de l'exploration.

11.1. Construction de la liste d'exploration

Explorateur maître (master browser) : Quand un client démarre, il diffuse son nom sur le réseau. L'explorateur maître collecte et tient à jour la liste maîtresse des ressources disponibles dans son domaine ou groupe de travail ainsi que la liste des noms des autres domaines et groupes de travail.
Il distribue la liste aux explorateurs secondaires.
Des machines sous Windows NT Server, Workstation, Windows 95/98 et WFW peuvent agir en tant qu'explorateur maître

Explorateur maître de Domaine : il remplit le rôle d'explorateur maître pour son domaine. De plus, il coordonne et synchronise la liste d'exploration provenant de tous les autres explorateurs maîtres pour les domaines qui résident sur des réseaux distants.

11.2. Distribution de la liste d'exploration

Explorateur secondaire : Il obtient sa liste d'exploration de l'explorateur maître, et transmet cette liste aux clients qui en font la requête.

Toutes les 15 minutes, l'explorateur secondaire contacte l'explorateur maître et télécharge la liste d'exploration.

Lorsqu'un client tente d'accéder à une ressource dans un domaine ou un groupe de travail, l'explorateur maître va faire suivre une liste de 3 explorateurs secondaires (maximum) où le client peut obtenir la liste d'exploration.
Le client, après avoir reçu la liste des explorateurs secondaires, va demander à l'un des explorateurs la liste des ressources réseau.

Explorateur potentiel : Un ordinateur qui pourrait être si nécessaire, un explorateur maître, secondaire ou maître de domaine, mais qui ne l'est pas pour l'instant et ne détient pas de liste d'exploration.

Le dernier état d'un ordinateur est **Non-explorateur** : il ne tient pas de liste, il a été configuré pour ne pas participer aux mécanismes d'exploration.

11.3. 2 QUESTIONS D'EXAMEN

You manage a single domain of Windows-based computers. The Windows-based computers run TCP/IP as their only network protocol. The network has four subnets: SubnetA, SubnetB, SubnetC and SubnetD. Users on SubnetC complain that they cannot browse servers and resources on SubnetB. However, they can browse local servers and resources on their own subnet. To examine the problem, you run Windows NT Explorer on a Windows NT Workstation computer on SubnetC and successfully map to a network drive on SubnetB. What is the cause of the problem?

a. The default gateway address on SubnetB is incorrect.

b. The DNS server is not available.
c. The primary domain controller is not available.
d. The router is not functioning.
e. The WINS server is not available.

Réponse: c
In a Windows environment, it is easy to confuse browsing with name resolution. However, browsing only concerns itself with maintaining hostname databases, not hostname-to-IP-address resolution. Differences between the two functions can clearly be seen when subnet-crossing problems occur. In this situation, the ability to successfully map to a remote network drive using Windows NT Explorer eliminates name resolution as a possible cause of the problem. That you can successfully connect to another subnet eliminates both the router and the default gateway address as possible causes. Browsing across subnets depends upon the Domain Master Browser, which is always the primary domain controller (PDC). The PDC, in its role as Domain Master Browser, collects from each subnet's Master Browser the browse list for that subnet. The Domain Master Browser then merges these browse lists to form a single browse list for the entire domain. Local browsers depend on this list when browsing outside the subnet. Therefore, if the PDC fails, cross-subnet browsing fails.

Ralph's TCP/IP network is comprised of three subnets. SubnetA contains a primary domain controller (PDC). SubnetB and SubnetC each have a backup domain controller (BDC). Each domain controller is the master browser of its subnet. WINS is not enabled on the network. Ralph wants to ensure that each BDC can communicate with the PDC. What should Ralph do?
a. Create a fourth subnet. Move all domain controllers to the new subnet.
b. On each BDC, change the BDC directive to 0x1b in the registry.
c. On each BDC, create an LMHOSTS file with an entry for the PDC.
d. On the PDC, create an LMHOSTS file with an entry for each of the BDCs.

Réponse: c
By default, a domain controller on a subnet is also its master browser. When a Windows NT computer discovers it is a master browser, it checks its LMHOSTS file for any #DOM entries. The #DOM tag signifies a domain controller. The master browser then queries all #DOM entries to find out which entry is for the primary domain controller. Only the PDC responds. The local master browser sends its browse list to the PDC which merges the list into a browse list for the entire domain. This compiled list is then sent to the BDC. Updates to the list are made every 12 to 15 minutes

12. CONNECTIVITE

Microsoft TCP/IP permet à Windows NT de se connecter à de nombreux hôtes TCP/IP étrangers, et d'opérer conjointement avec eux.

12.1. UTILITAIRES TCP/IP

Trivial File Transfer Protocol (TFTP)
FTP utilise TCP, et TFTP utilise UDP.
Il n'y a pas de processus d'authentificaton, les utilisateurs ont accès à la ressource via un fichier rhosts.

Telnet
Fournit une émulation de terminal pour VT100, VT52 et TTY. Ne supporte pas TN3270.

Remote Shell (RSH)
Permet de lancer des commandes sur un démon RSH à partir d'un hôte distant. Ne supporte pas l'authentification d'utilisateurs

Remote Copy (RCP)
Copie des fichiers entre un hôte Windows NT et un serveur Unix . Permissions via .rhosts

Remote Execute (REXEC)
Lance des commandes sur un serveur distant faisant tourner le démon REXEC.
Plus sécurisé que RSH. Demande un mot de passe pour chaque commande.

RSH , RCP et TFTP ne requièrent pas de mots de passe lors de la connexion.

12.2. IMPRESSION TCP/IP

NT peut fonctionner avec un démon LPD (Line Printer Daemon).
Pour partager des imprimantes comme sous Unix, NT doit fonctionner comme un démon LPD.
Il faut installer les services d'impression TCP/IP.

LPR et LPQ sont des applications clientes qui communiquent avec LPD sur le serveur d'impression. Ces trois applications assurent les fonctions suivantes :

- LPD s'exécute en tant que service sur l'ordinateur Windows NT (LPDSVC) et permet à tout ordinateur configuré avec TCP/IP et LPR d'envoyer des travaux d'impression à l'ordinateur Windows NT.
- LPR constitue l'application d'impression cliente et permet au client Windows NT d'imprimer sur n'importe quel hôte exécutant LPD.

LPQ peut être utilisé pour interroger l'imprimante une fois que les travaux d'impression ont été soumis.

LPR- Soumet un travail à l'imprimante réseau
LPR -S *Nomordinateur* -P *queue_d'impression* FICHIER
1 2 3

LPR = **L**ine **P**rinter **REQUEST**

LPQ-Affiche l'état de la queue d'impression
LPQ -S *Nomordinateur* -P *queue_d'impression*
1 2

LPQ = **L**ine **P**rinter **QUERY**

Il faut connaître LPR et LPQ ainsi que leurs paramètres. LPR envoie le travail d'impression à l'imprimante LPD, LPQ permet de voir la queue d'impression. Les arguments sont sensibles à la casse.

Pour que Windows NT accepte les travaux d'impression émanant de clients LPR, le service Serveur d'impression Microsoft TCP/IP (LPDSVC) doit être installé et en cours d'exécution. Dans l'onglet **Services** de la boîte de dialogue **Réseau** (accessible à partir du Panneau de configuration), installez le service Impression Microsoft TCP/IP.

12.3. 2 QUESTIONS D'EXAMEN

You connect a print device to the Windows NT Server computer COWARDS. You want this print device to be available to every UNIX computer on the network. How do you do this?
a. by implementing the Microsoft TCP/IP Printing service on the server
b. by implementing the LPR utility on the server
c. by implementing a share name for the printer
d. by giving an IP address to the printer

Réponse: ac
Printing in a TCP/IP environment requires a Line Printer Daemon (LPD), which is installed with the Microsoft TCP/IP Printing service. This service can be installed on any Windows NT computer on the network. To configure the TCP/IP Printing service, you need either the DNS name or the IP address of the print server on which the LPD is installed. You also need the name of the printer (not its IP address) as it is known to the LPD print server. As with any other network printer, an LPD printer must be shared on the network.

You configure a UNIX computer as an LPD server. Users on a Windows NT Workstation computer want to send documents to a print device connected to the UNIX LPD server. How must they send their documents to this print device?
a. by installing the TCP/IP Printing service on each workstation
b. by mapping a logical printer port to the UNC name for the printer
c. by using the LPR utility
d. by using the LPQ utility

Réponse: c
When configured with the LPR utility, both Windows NT computers and UNIX computers can send documents to an LPD server. During setup, the LPR client only needs to know the IP address of the LPD print server and the printer name as entered on the LPD print server (not its share name). The LPQ utility returns the status of the print queue on the LPD server.

13. Simple Network Management Protocol (SNMP)

Le protocole SNMP (*Simple Network Management Protocol*) fait partie de la suite de protocoles TCP/IP. À l'origine, il a été développé au sein de la communauté Internet pour observer et dépanner les routeurs et les ponts.

Par le biais du service SNMP Microsoft, un ordinateur Windows NT peut communiquer ses informations d'état à un système de gestion SNMP situé sur un réseau TCP/IP.
Le service SNMP envoie des informations d'état à un hôte (ou plusieurs) lorsque celui-ci les demande, ou si un événement significatif se produit — par exemple, si l'hôte ne dispose plus suffisamment d'espace disque.

13.1. Système de gestion SNMP

La principale fonction d'un système de gestion consiste à demander des informations à un agent. Ce système peut être mis en œuvre sur n'importe quel ordinateur exécutant le logiciel de gestion SNMP. Un système de gestion peut lancer les opérations **get**, **get-next** et **set**.

- L'opération get est une requête portant sur une valeur spécifique, telle que la quantité d'espace disque disponible.
- L'opération get-next est une requête portant sur la valeur « suivante » (next). Cette opération est utilisée pour parcourir l'ensemble d'une table conceptuelle d'objets.
- L'opération set permet de modifier une valeur. Elle est rarement réalisée, dans la mesure où la plupart des valeurs n'autorisent qu'un accès en lecture seule, et ne peuvent donc pas être redéfinies.

Remarque :

GET: demande la valeur d'un objet spécifique dans la MIB de l'agent.

GET-NEXT: demande la prochaine valeur d'un objet spécifique dans la MIB de l'agent

SET: utilisé pour changer la valeur d'un objet dans la MIB de l'agent., SI CET OBJET EST EN LECTURE ECRITURE. La plupart des MIB sont en lecture seule.

13.2. Agent SNMP

La principale fonction d'un agent consiste à réaliser les opérations **get**, **get-next** et **set** demandées par un système de gestion. Le rôle d'agent peut être joué par n'importe quel ordinateur exécutant le logiciel d'agent SNMP. Il s'agit, généralement, d'un serveur ou d'un routeur. Le service SNMP Microsoft est un logiciel d'agent SNMP. La seule opération que peut lancer un agent est l'interruption (opération **trap**).
L'opération **trap** alerte les systèmes de gestion lorsqu'il se produit un événement significatif, tel que la violation d'un mot de passe.

Remarque

Avec Windows NT, il y'a un service SNMP qui est un Agent. Il n'y a pas de Gestionnaire SNMP.

13.2.1. BASE MIB

Les informations qu'un système de gestion peut demander à un agent sont contenues dans une base d'informations de gestion (MIB, *Management Information Base*). Une MIB est un ensemble d'objets de gestion. Ces objets recouvrent des informations de types divers se rapportant à un périphérique réseau, telles que le nombre de sessions ouvertes sur un hôte, ou la version du système d'exploitation réseau qu'il exécute. Les systèmes de gestion et les agents SNMP interprètent les objets MIB de la même manière.

Le service SNMP prend en charge les bases d'informations de gestion suivantes : Internet MIB II, LAN Manager MIB II, DHCP MIB et WINS MIB.

Definitions SNMP

Communauté : un groupe fonctionnel d'agents SNMP. Les noms de communauté sont sensibles à la casse. Les hôtes appartiennent généralement à une communauté appelée 'public'.

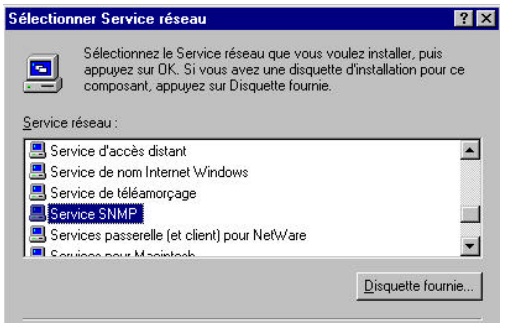
Trap: un message non demandé à un gestionnaire SNMP, il est envoyé comme un évenement extraordinaire, tel qu'une erreur de mot de passe.

Management Information Base (MIB): une base de données hiérarchique d'objets et de valeurs qui réside sur l'agent SNMP.

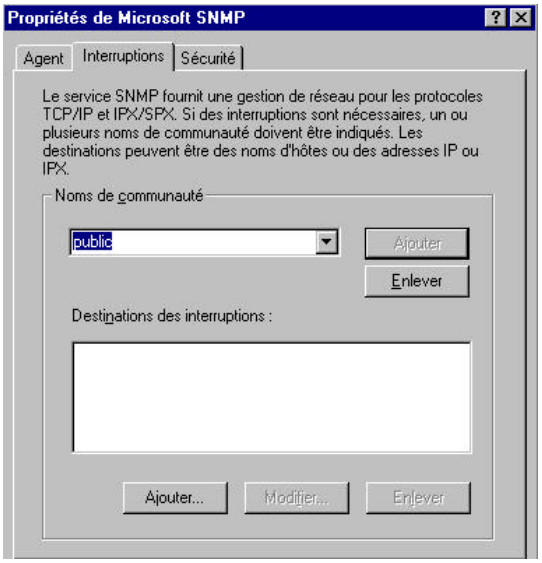
L'installation du service SNMP met en place et active les compteurs de performances TCP/IP. Persuadez-vous en, c'est au moins une question à l'examen.

13.3. Installation et sécurisation de SNMP

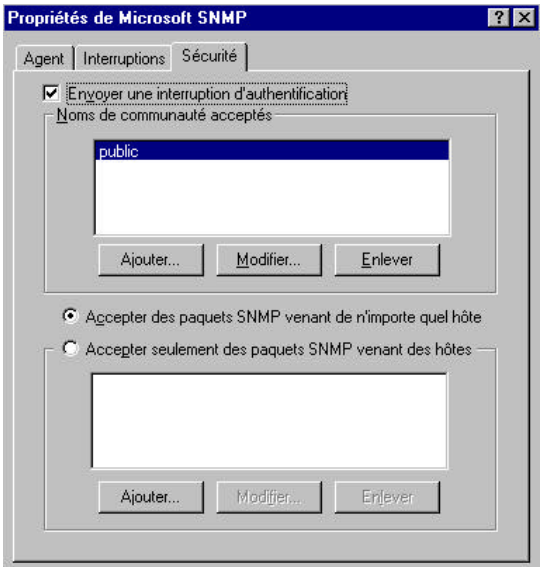
Pour installer et configurer l'agent SNMP, vous devez être connecté avec les privilèges Administrateurs.



Vous pouvez spécifier jusqu'à 5 noms de communautés dans la configuration du service SNMP pour recevoir les traps (interruptions) des agents SNMP.



Pour une plus grande sécurité, sélectionnez Send Authentication Traps (Envoyer des interruptions d'authentification) pour un nom de communauté différent de 'public', spécifiez une destination (trap destination), puis configurez la Sécurité pour n'accepter que des paquets SNMP provenant d'hôtes spécifiques.



Pour configurer une interruption (trap), sélectionnez le nom de communauté qui doit recevoir l'interruption. Une boite de dialogue Trap Destination for <community>" (Destination des interruptions) apparaît. Dans la boite IP Host/Address or IPX Address, taper le nom d'hôte DNS, l'adresse IP ou IPX et cliquer sur Add.

13.4. 2 QUESTIONS D'EXAMEN

Adele wants the SNMP service on her Windows NT Server computer to send trap messages to an SNMP trap destination. Which of the following must be supplied?
a. the SNMP management station's community
b. the SNMP management station's IP address
c. the SNMP management station's scope ID
d. the SNMP management station's subnet mask

Réponse: ab
An SNMP trap destination is an SNMP management station or console that is set to receive trap messages from trap agents. Trap messages can contain a notification of an agent's startup, shutdown, or password violation. SNMP-enabled computers are grouped into administrative units called communities. Although an SNMP-enabled computer can belong to more than one community, it cannot communicate with a community of which it is not a member. Therefore, when designating the SNMP trap destination on the Traps tab of the SNMP Properties page, you must specify the community to which the SNMP trap destination belongs. You must also specify the SNMP trap destination by either its hostname, IP address or IPX address. Trap messages can be sent to more than one SNMP trap destination.

Henrietta installs the SNMP service on a Windows NT Server computer. She wants to prevent any unauthorized SNMP management consoles from managing this server. What should Henrietta do?
a. Assign a password to the SNMP community name.
b. Designate the server to be a trap destination.
c. Enable CHAP encryption on the MIB file packets.
d. Enable the Only Accept SNMP Packets From These Hosts option on the server.

Réponse: d
In SNMP, the community name that the SNMP management console shares with its SNMP hosts functions as a kind of password. For any interaction to occur between SNMP hosts, they must all belong to the same community. However, the community name cannot be protected with a password. A second level of security is provided with the Only Accept SNMP Packets From These Hosts option on the Security tab of the Microsoft SNMP Properties page on the server. Here you can enter specific host IP or IPX addresses (in this example, that of the SNMP management console) from which SNMP packets will be accepted. All other packets will be rejected. Because SNMP management programs must initiate data gathering operations with an SNMP packet, enabling the Only Accept SNMP Packets From These Hosts option will preclude access by unauthorized SNMP management consoles.

14. Service d'accès Distant

RAS (Remote Access Service) permet essentiellement aux utilisateurs de se connecter au réseau et d'agir comme s'ils y étaient directement reliés. RAS possède deux composants : le serveur et le client.

RAS supporte les protocoles SLIP et PPP

14.1. SLIP

Développé pour autoriser des connexions TCP/IP à distance. SLIP est un protocole extrêmement rudimentaire qui souffre d'une absence de standardisation stricte.

Slip ne supporte que le protocole TCP/IP alors que PPP accepte non seulement TPC/IP mais aussi d'autres protocoles tels que NetBEUI, IPX , AppleTalk et DECNet.
De plus, PPP peut gérer plusieurs protocoles sur la même ligne.

SLIP nécessite l'emploi d'adresses IP statiques. C'est la raison pour laquelle il n'accepte pas le protocole DHCP.
Comme SLIP ne supporte pas l'adressage dynamique par DHCP, les connexions SLIP ne peuvent également pas assigner de serveurs de noms WINS ou DNS.

14.2. PPP

Avec **PPP**, RAS peut supporter NetBEUI, NWLink et TCP/IP sur la ligne de communication.
PPP a été défini par l'IETF pour supplanter SLIP en fournissant les fonctionnalités supplémentaires suivantes :

- Sécurité par ouverture de session avec mot de passe
- Support simultané pour plusieurs protocoles sur la même liaison
- Adressage IP dynamique
- Contrôle d'erreurs avancé

PPP possède deux extensions importantes : le protocole Mutlilink ou MP (Multilink Protocol) et le protocole PPTP (Point to Point Tunneling Protocol).
PPTP facilite les connexions sécurisées à travers Internet.

Remarques
Le Multilink : agrégation de liens.
Rappel (Dial Back) sur Multilink : pas de rappel (Dial Back) sur Multilink.

14.3. 2 QUESTIONS D'EXAMEN

A number of employees at your company have Windows NT Workstation installed on their laptop computers. They need to dial up over the Internet to access client/server applications on your network's Windows NT Server computer. You need to provide adequately encrypted security for these connections and prevent unauthorized users from accessing the server. How can you best do this?

a. by enabling IP address filtering on the server
b. by implementing Point-to-Point Tunneling Protocol (PPTP)
c. by setting up FTP with user-level security
d. by setting up RAS with SSL security

Réponse: b
The "tunneling" aspect of PPTP refers to its ability to piggy-back one protocol upon another. For example, NetBEUI or IPX packets can be encapsulated in PPP packets and transported over TCP/IP. When establishing a PPTP connection, the RAS client and server negotiate a 40-bit session key for RSA RC4 bulk data encryption. PPTP also employs Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP) encryption. Because FTP transmits usernames and passwords unencrypted, it should never be used where security is an issue.
Although Microsoft's Internet Information Server allows you to grant or deny server access by IP address, this security measure offers little protection from users of Internet Service Providers (ISPs) that randomly assign IP addresses from an assigned pool to their users.

Henry sets up a RAS server that connects to an Internet Service Provider (ISP) over an ISDN line. How should the default gateway address be configured so that Windows 95 users on the local network can access the Internet through the RAS server?
a.The default gateway address on the RAS server must specify the IP address of the ISP router's interface to the Internet.
b.The default gateway address on the RAS server must specify the IP address of the ISP router's interface to the local network.
c.The default gateway address on each Windows 95 computer must specify the IP address of the ISP router's interface to the local network.
d.The default gateway address on each Windows 95 computer must specify the IP address of the RAS server's network interface to the local network.

Réponse: d
Host computers that cannot resolve IP addresses locally route messages to their default gateways. Since all traffic bound for the Internet is not local by definition, it is necessary for each host computer on the local network to be configured with the IP address of the RAS server. This IP address functions as each host computer's default gateway address to the Internet. The RAS server is not configured with a default gateway. Its default gateway address is provided by the ISP.

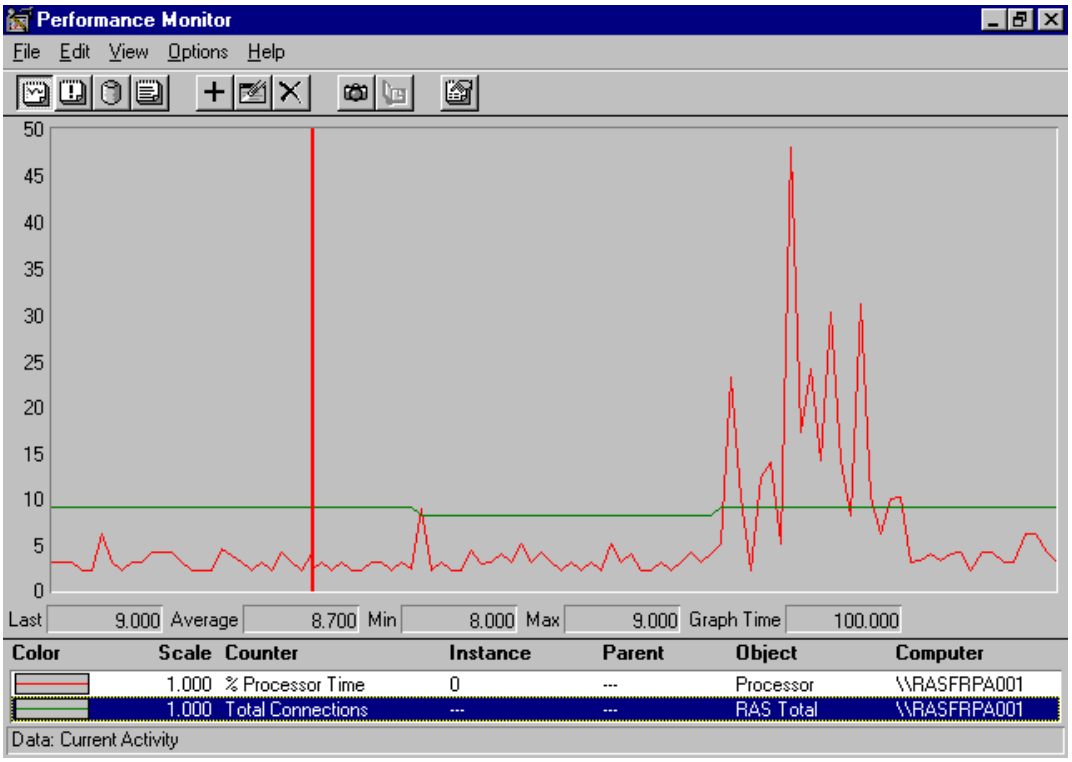
14.4. Anayseur de performances et moniteur réseau

14.4.1. ANALYSEUR DE PERFORMANCES

L'outil de mesure de performances de Windows NT le plus efficace est l'analyseur de performances, installé par défaut dans le groupe de programmes Outils d'administration. C'est un outil essentiel de surveillance du système, permettant de l'analyser et d'améliorer ses performances.

L'analyseur peut être configuré pour enregistrer une variété de mesures statistiques (appelées compteurs) pour une variété de systèmes matériels et de composants logiciels (appelés objets). Chaque objet possède son propre ensemble de compteurs.

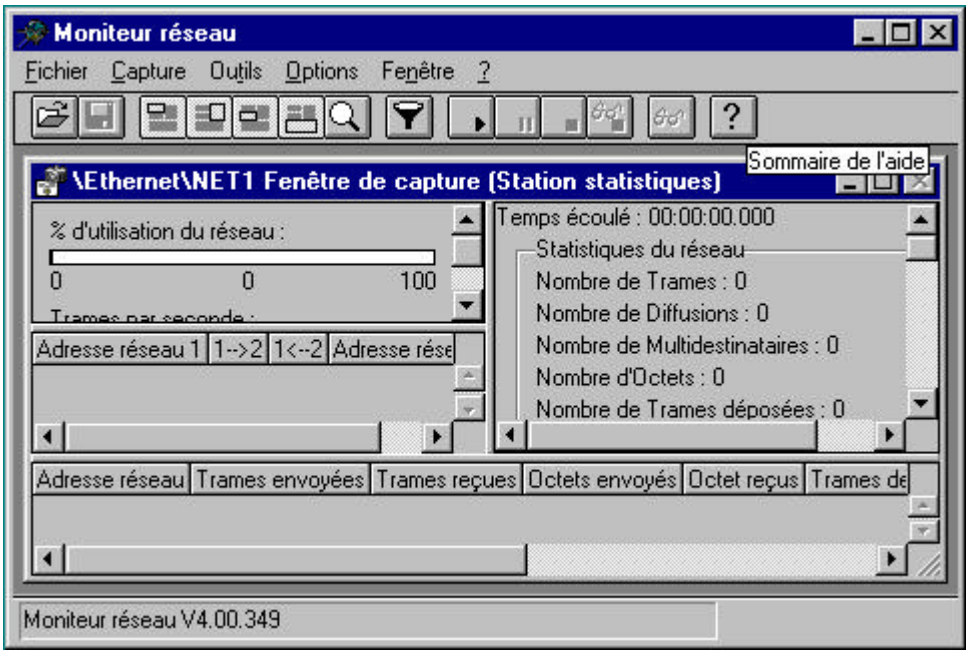
Le graphe ci dessous présente en rouge le compteur Processor Time de l'objet processeur, et en vert le compteur Total Connections de l'objet RAS Total :



Exemple de Graphe de surveillance avec l'anayseur de performances

14.4.2. MONITEUR RESEAU

Le Moniteur Réseau, fourni avec Windows NT, est un outil d'analyse de l'activité du réseau. Il permet de capturer le traffic émis ou reçu sur l'ordinateur local. Des filtres de capture peuvent être définis afin de ne conserver que certaines trames spécifiques. Quand une capture a été obtenue et filtrée, le moniteur réseau interprète les données binaires afin de les afficher "en clair", pour qu'elles soient exploitables par l'administrateur.

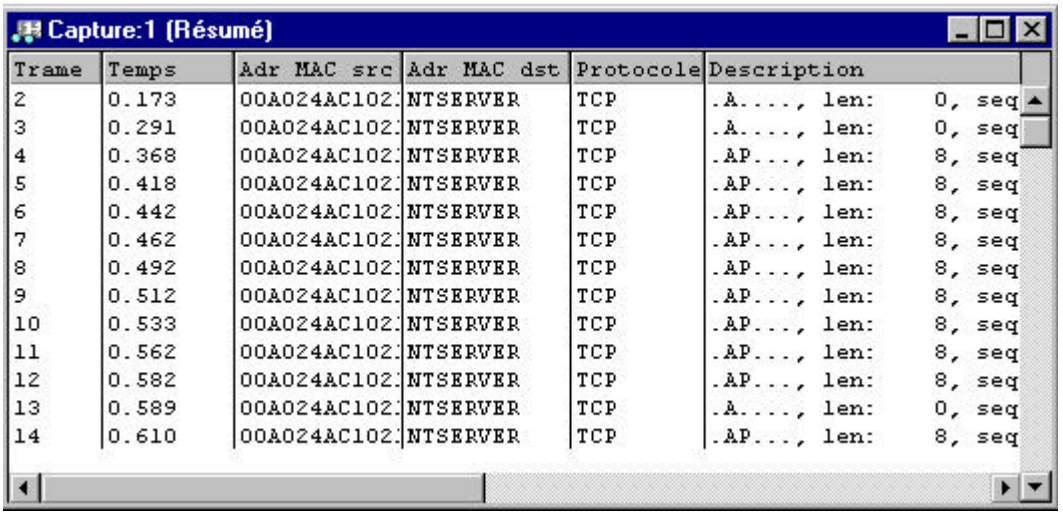


Ecran Principal Moniteur Réseau

La fenêtre du moniteur réseau est divisée en quatres sections:

- une section graphique qui montre l'activité du réseau (pourcentage d'utilisation du réseeau, trames et octets par seconde…)
- une section réferencant les statistiques d'echange d'informations pour l'ensemble des sessions ouvertes
- une autre section présentant les statistiques globales donnant des informations sur l'ensemble de l'activité du réseau
- un panneau qui indique des informations spécifiques à l'activité d'une station de travail sur le réseau.
-

Notons que le moniteur réseau fourni avec Windows NT peut surveiller le traffic entrant et sortant uniquement sur le systeme sur lequel ilest installé. La version fournie par SMS (Systems management Server) peut surveiller tout le traffic réseau



Trame	Temps	Adr MAC src	Adr MAC dst	Protocole	Description
2	0.173	00A024AC102:	NTSERVER	TCP	.A...., len: 0, seq
3	0.291	00A024AC102:	NTSERVER	TCP	.A...., len: 0, seq
4	0.368	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
5	0.418	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
6	0.442	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
7	0.462	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
8	0.492	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
9	0.512	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
10	0.533	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
11	0.562	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
12	0.582	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq
13	0.589	00A024AC102:	NTSERVER	TCP	.A...., len: 0, seq
14	0.610	00A024AC102:	NTSERVER	TCP	.AP..., len: 8, seq

Détail d'une capture