CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Unité Réseaux du CNRS

Outils Réseaux de Windows NT

JRES97 – La Rochelle

17/10/1997

Philippe Leca CNRS/UREC *Philippe.Leca@urec.cnrs.fr*

1. INTRODUCTION

Positionnement de Windows NT sur le marché :

Serveur réseaux : Novell, Lan Manager, Internet

En France : 44% des systèmes d'exploitation réseau pour le 1er semestre 1997.

Windows NT peut-il devenir un serveur de réseau ?

Objectif commercial

Portabilité **: INTEL x86 Cics, ALPHA AXP Risc.**

Extensibilité

Robustesse

Compatibilité

Objectifs attendus :

Un serveur réseau stable, fiable et robuste.

Un vrai " système " d'exploitation.

Une simplification de l'administration système et réseau.

2. ARCHITECTURE SYSTEME

Historique du système : de 1985 à 1997

1985 : Fin de la collaboration IBM / Microsoft autour de OS/2.

1988 : arrivée de Dave Cutler chez Microsoft(ancien architecte de VMS).

1994 : Windows NT 3.5

1995 : Windows NT 3.51

1996 : Windows NT 4.0

1998 (?) : Windows NT 5.0

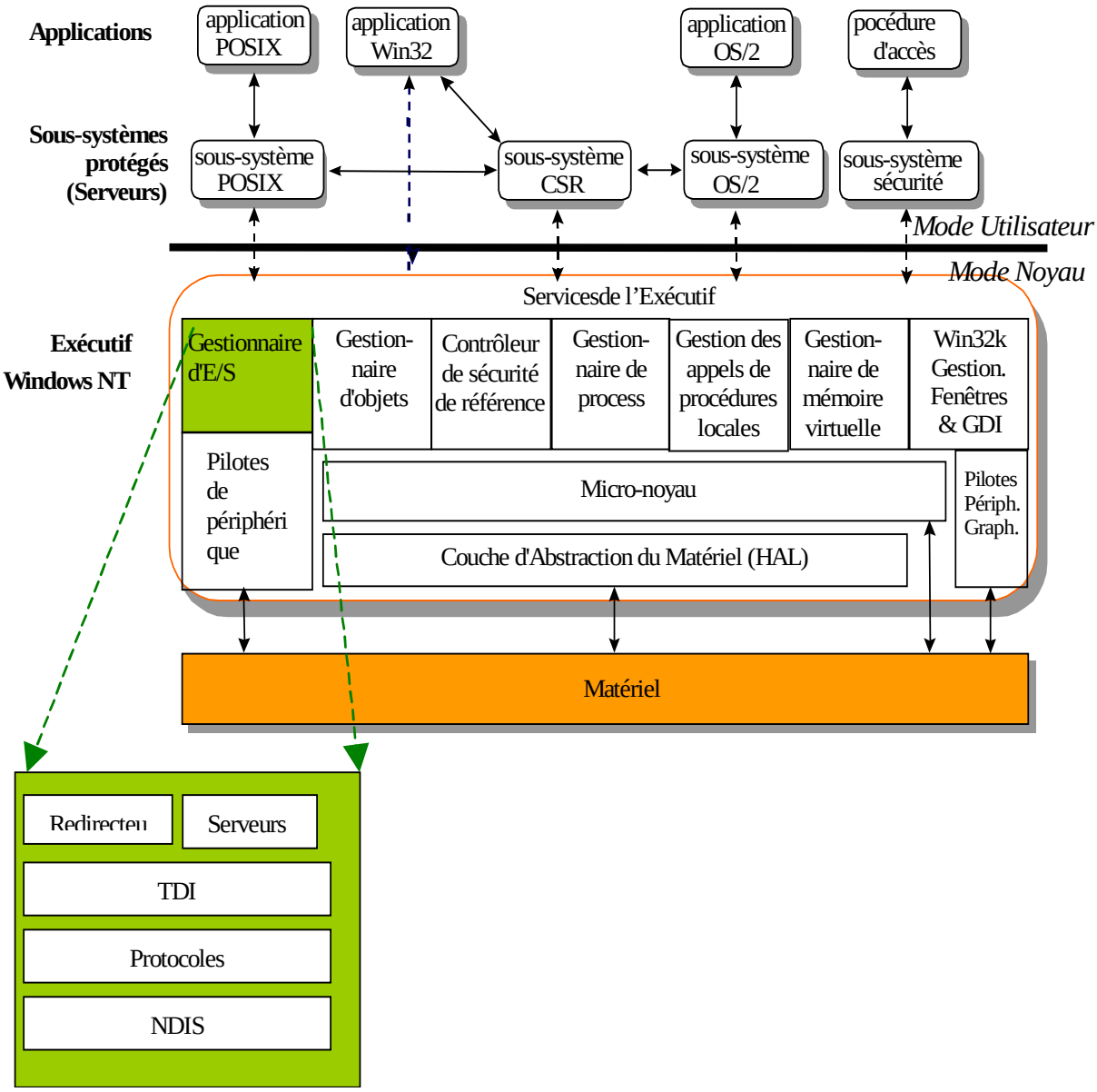
Etat du système : Services Packs et Hotfixs

Caractéristiques

32 Bits

Multitâche préemptif : il est capable d'exécuter plusieurs applications sur une même machine, plusieurs processus. Le noyau du système interrompt les taches les moins prioritaires quand il veut au bout d'un certain temps ou si elles attendent une ressource non disponible.
Multi-threads : chaque processus peut lancer autant de threads (fils d'exécution) qu'il veut.
Multiprocesseurs symétriques : 4 pour NTserver , 2 pour NTWks... à venir 256. Pas de préférences au Niveau du processeur.

Architecture de Windows NT 4.0



Système en couche + client/serveur

Windows NT s'inspire du système MACH :

Un noyau du système d'exploitation fournie des primitives de bas niveau. Des programmes d'applications (appelés SERVEUR) offrent les fonctions complémentaires du système d'exploitation. Pour répondre aux demandes d'évolutions, la base du système reste stable tandis que les serveurs sont modifiés ou créés.

Exécutif de Windows NT

Mode noyau : mode privilégié d'exécution de code dans un microprocesseur, dans lequel toute la mémoire est totalement accessible et toutes les instructions du microprocesseur peuvent être employées.
Permet de garantir que le mauvais fonctionnement d'une application ne mettra pas en

péril le fonctionnement du système dans son ensemble.

Couche d'abstraction du matériel (hal) : partie logicielle commune pour les composants matériels**.** Elle permet d'isoler le système des spécificités matérielle de la plate forme.

Micro noyau : cœur du système (gestion des interruptions, planifications des threads, synchronisation).
Mode Noyaux/Mode utilisateur : les applications (mode utilisateur : accès limité aux données et au matériel à travers des API) sont séparés de l'OS (mode noyaux).

Sous systèmes protégés

Sous systèmes intégraux = serveurs qui exécutent des fonctions du système d'exploitation et qui répondent aux clients.
Ex : sous système de sécurité

Sous systèmes d'environnements **=** serveur en mode utilisateur

chaque serveur est situé dans un processus séparé dont la mémoire est protégée. Comme tous les systèmes ne partagent pas automatiquement la mémoire, ils communiquent entre eux à l'aide de message (LPC).
Fournissent des API spécifiques au système d'exploitation.
Ils permettent l'exécution d'applicatiosn prévus pour d'autres systèmes.
WIN32
POSIX : uniquement avec NTFS si les applications nécessitent des accès aux systèmes de fichiers (ex: ln).
OS2 et autres …
CSR : sous système constitué d'une partie **Console** (accès mode console, arrêt et gestion matériel) et une partie **Fonctions d'environnements divers** (fonctions spécialisées pour les applications 32 bits, ex: création et destruction de processus).

DOS : NTVDM (NT Virtual Dos Machine)
WIN16 : NTVDM 16bits : attention à l'augmentation des ressources CPU avec les applis 16 Bits.

Client/Serveur

les applications utilisateurs sont des clients qui demandent des services aux sous systèmes protégés qui sont des serveurs. Il y a une division du système en processus qui dialoguent avec les clients. Le principe est identique en local ou à travers un réseau.

Multi-utilisateur au sens Windows NT

on accède à des services disponibles et non à un serveur.

Système de fichiers

FAT : compatible DOS
NTFS : support complet de la sécurité WindowsNT, volume étendu, nommage étendus (256 caractères), prise en charge Mac.

Compatibilité

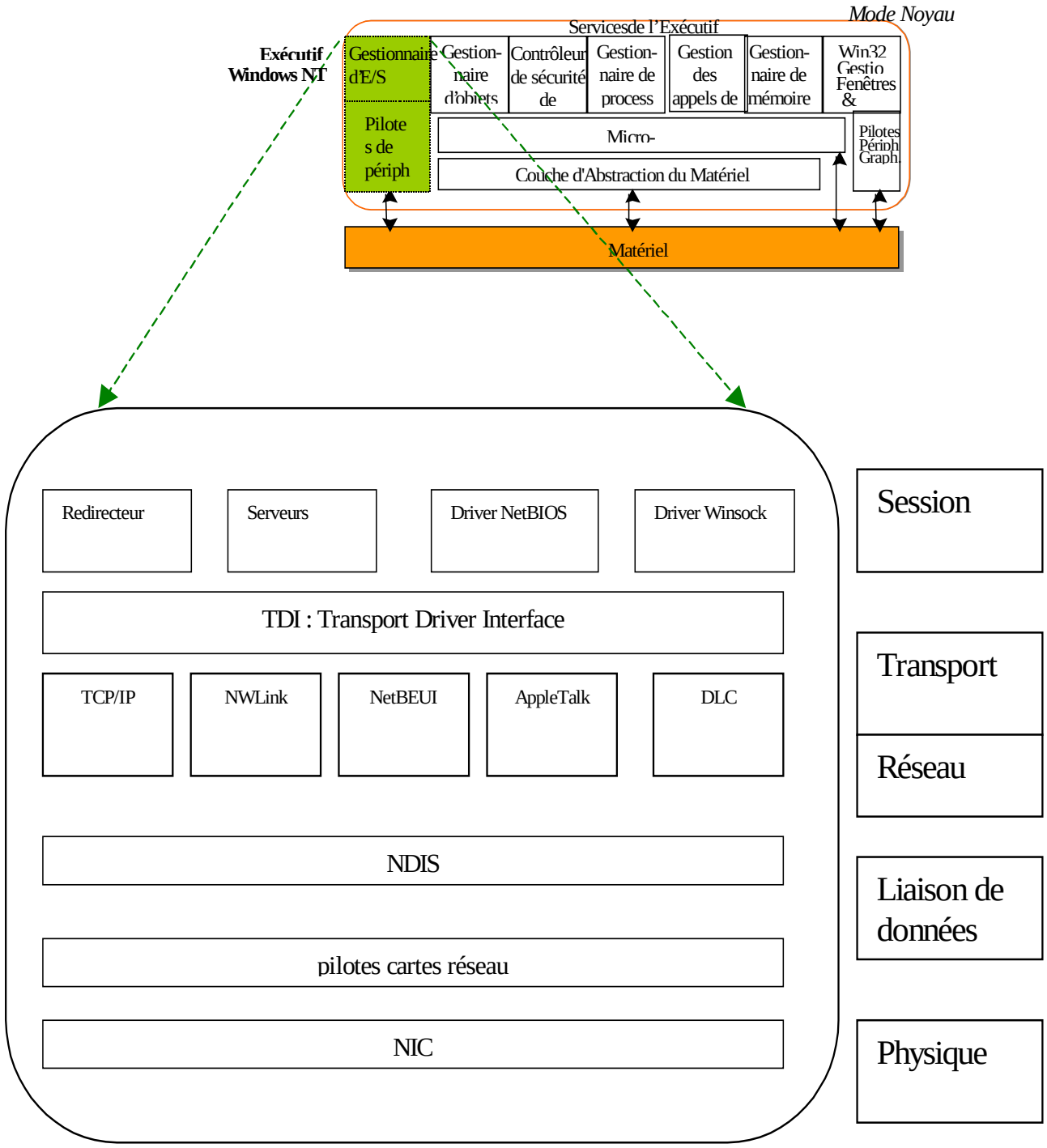
La compatibilité binaire est assurée grâce aux sous systèmes protégés. Windows NT fournit aux applications des environnements autre que son interface d'origine l'API Win32.
Sur Intel : MS-DOS, Win16, OS/2 et LanManager
sur RISC : idem sauf OS/2
le support MS-DOS est limité : les appels directs vers le matériel ne sont pas possibles avec Windows NT.

Différence WinNT3.51 et WinNT4.0

Déplacement d'une partie du sous système d'environnement Win 32 en mode noyau.
gain d'espace mémoire et gain de temps d'accès.

3. RESEAU

3.1 Présentation



WinNT est un système acceptant plusieurs protocoles réseaux.

Installation et configuration

START – SETTINGS CONTROL PANEL – NETWORKS

Support API :

API NetBIOS : Network Basic Input Output System
Windows Sockets : Implémentation Windows des API Sockets de Unix.

Transport Protocol Support :

NDIS supporte plusieurs piles de protocoles : il rend les protocoles indépendants de la carte réseaux. Plusieurs protocoles peuvent être liés à la même carte.
TDI : isole les couches hautes (applications) des protocoles de transports. C'est une interface de programmation. elle permet aux redirecteurs et serveurs de communiquer avec les couches transports en restant indépendants.

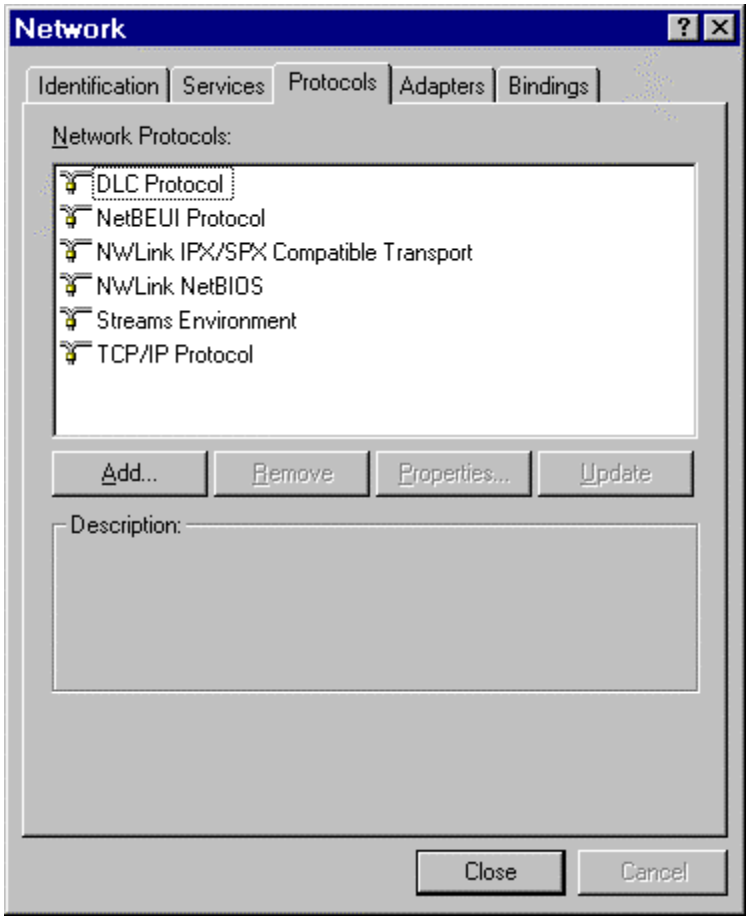
Redirecteur et Serveur : pilote du système de fichiers

Le redirecteur dirige les demandes d'E/S. Il fournit les fonctions nécessaires pour l'accès aux ressources situées sur d'autres machines du réseau en mettant en place le protocole SMB (Server Message Block).
Le serveur traite les demandes provenant des redirecteurs des autres machines.
Déjà présent avec MS-DOS3.X. Permet connexions vers Win3.11, LanManager ...

Composants du traitement distribué :

Canaux nommés (pipe) et *boîtes aux lettres* (liaison inter processus) : protocole de diffusion
Sockets Windows (winsock) : compatible Socket UNIX
appels de procédure distante (rpc) : norme de fait pour le dialogue entre applications sur matériels hétérogène.
NetDDE (network Dynamic Data Exchange) : maintenu pour compatibilité avec les systèmes NetBIOS antérieur (depuis Win2.x).
DCOM (Distributed Component Object Model) : permet de développer des applications modulaires et distribuées (distribution de processus à travers plusieurs ordinateurs).

3.2 PROTOCOLES



NetBEUI : NetBIOS extended user interface

Standard des réseaux Microsoft.
C'est un protocole développé pour exécuter des applications NetBIOS sur un réseau local. Il est "*plug and play*" et non routable

NWLink

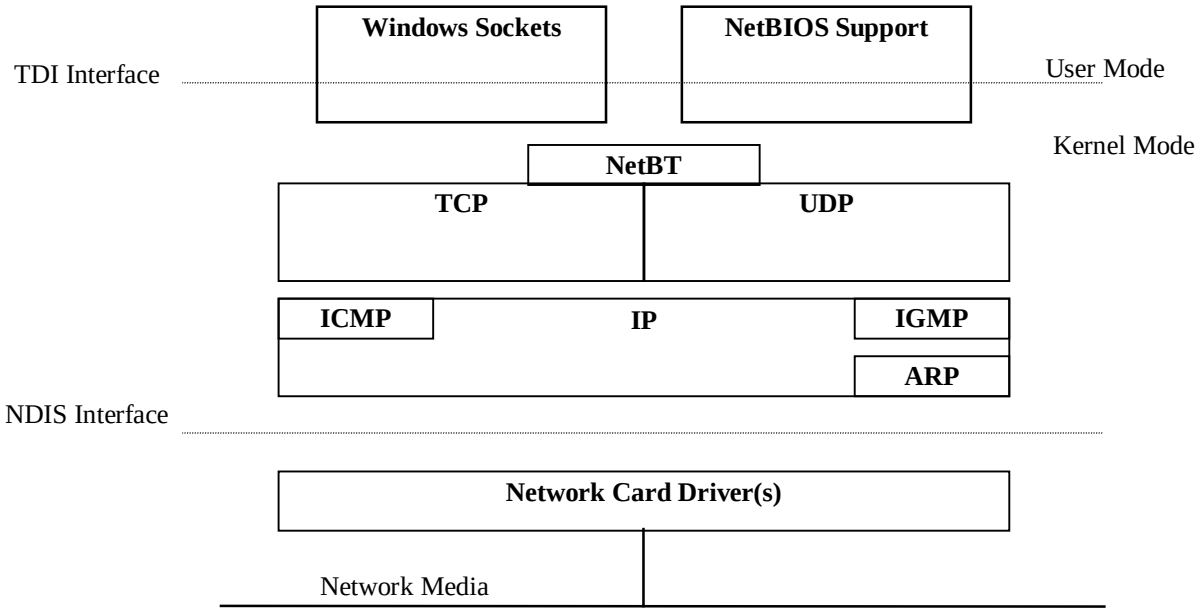
Couche transport compatible avec les protocoles Novell IPX/SPX. Il permet aux clients NetWare d'accéder aux ressources d'un serveur Windows NT. Il peut supporter les applications NetBIOS et Winsock.

TCP/IP

DLC : Data Link Control.

Utilisé pour se connecter aux imprimantes compatibles DLC (imprimantes HP).

3.3 TCP/IP



Nouvelle couche à partir de WinNT 3.5 sur 32 bits.

RFC supportées :

768, 783, 791, 792, 793, 816, 826, 854, 862, 863, 864, 865, 867, 894, 919, 922, 950, 959, 1001, 1002, 1009, 1034, 1035, 1042, 1055, 1112, 1122, 1123, 1134, 1144, 1157, 1179, 1188, 1191, 1201, 1231, 1332, 1334, 1518, 1519, 1533, 1534, 1541, 1542, 1547, 1548, 1549, 1552

DNS : 1034, 1035
Résolution de nom NetBios sur TCP/IP : 1001, 1002

Services disponibles :

Routage
Multicast - IGMP
DHCP client et serveur
WINS : netbios name server
DNS
connexion modem (PPP / SLIP)
Impression lpr-lpd
agent SNMP
Interface Netbios
Interface socket Windows
RPC
Network DDE

NetBIOS sur TCP/IP - NBT

Il autorise les applications écrites avec l'API NetBIOS, à s'exécuter au dessus des couches TCP/IP.
Exemple : NET commande
Tous les réseaux Microsoft ont été bâtis en utilisant le protocole NetBIOS.

Gestion des noms au-dessus de la couche 4
pas de routage
C'est une interface logicielle et une convention de nommage et non un protocole.

Les applicatiosn NetBios (partage de fichiers par exemple) utilise l'API NetBios (via NetBios.dll) puis NetBT

port 137/UDP : Diffusion du service de noms NetBios
port 138/UDP : Session NetBios (exemple : partage de répertoire).
port 139/TCP : Services de Datagram : permet d'envoyer un messaqge à un nom unique ou à un groupe (netsend ...).

Sécurité : pour résoudre les principaux problèmes de sécurités avec Windows NT il est conseillé de bloquer les ports 135, 136, 137, 138 et 139 en TCP et UDP sur votre routeur.

Etude des échanges réseau avec le moniteur réseau

Les captures de paquet ont eu lieu juste après le démarrage de l'ordinateur (WinNT4 SP3). Temps de capture : 5 Minutes.

Cas 1 : protocole installé : TCP/IP uniquement

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
7	3.951	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
8	7.462	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
9	8.208	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
10	8.959	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
11	12.466	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
12	12.467	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
13	12.468	MERCURE	*BROADCAST	NETLOGON	Query for Primary DC
14	13.216	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
15	13.216	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
16	13.967	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
17	13.967	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
18	13.968	MERCURE	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 194.57.137.111
19	13.969	00C04FC8CDD1	MERCURE	ARP_RARP	ARP: Reply, Target IP: 194.57.137.103 Target Hdwr Ad
20	17.475	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
21	17.476	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
22	17.477	MERCURE	*BROADCAST	NETLOGON	Query for Primary DC
23	18.224	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
24	18.224	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
25	18.975	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
26	18.975	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
27	22.111	MERCURE	*BROADCAST	BROWSER	Local Master Announcement [0x0f] MERCURE
28	22.111	MERCURE	*BROADCAST	BROWSER	Local Master Announcement [0x0f] MERCURE
29	52.371	MERCURE	*BROADCAST	BROWSER	Workgroup Announcement [0x0c] UREC
30	112.387	MERCURE	*BROADCAST	BROWSER	Workgroup Announcement [0x0c] UREC
31	0.000	000000000000	000000000000	STATS	Number of Frames Captured = 30

```
+FRAME: Base frame properties
+ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
+IP: ID = 0x7F00; Proto = UDP; Len: 260
+UDP: Src Port: NETBIOS Datagram Service, (138); Dst Port: NETBIOS Datagram Service (138); Length = 2
+NBT: DS: Type = 17 (DIRECT GROUP)
+SMB: C transact, File = \MAILSLOT\NET\NETLOGON
+NETLOGON: Query for Primary DC
```

Trame recherche de contrôleur Primaire de Domaine

Comparaison de trafic :

Lors de l'allumage d'un PDC :

Avec TCP/IP : 88 paquets de 12,7 Ko en 60 s

Avec NWLink : 116 paquets de 15,9 Ko en 70 s

lors de l'allumage d'un client Win95

Avec TCP/IP : 66 paquets de 9,6 Ko en 35.2 s

Avec NWLink : 85 paquets de 11,3 Ko en 29.5 s

Lors de la connexion d'un utilisateur

Avec TCP/IP : 39 paquets de 6,5 Ko en 2,5 s

avec NWLink : 35 paquets de 6,5 Ko en 2,5 s

Cas 2 : avec les protocoles NWLink et TCP/IP installés :

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
62	20.682	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
63	22.193	MERCURE	*BROADCAST	NBT	NS: Release req. for MERCURE+++++++++
64	22.193	MERCURE	*BROADCAST	NBIPX	Delete Name MERCURE+++++++++
65	22.935	MERCURE	*BROADCAST	NBT	NS: Release req. for MERCURE+++++++++
66	23.187	MERCURE	*BROADCAST	SAP	General Svc Resp [MERCURE!!!!!!!... - Unknown Servic
67	23.686	MERCURE	*BROADCAST	NBT	NS: Release req. for MERCURE+++++++++
68	24.188	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
69	24.189	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
70	24.190	MERCURE	*BROADCAST	NETLOGON	Query for Primary DC
71	24.191	MERCURE	*BROADCAST	NETLOGON	Query for Primary DC
72	24.938	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
73	24.938	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
74	25.689	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
75	25.690	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
76	54.208	MERCURE	*BROADCAST	BROWSER	Workgroup Announcement [0x0c] UREC
77	54.211	MERCURE	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 194.57.137.111
78	54.211	00C04FC8CDD1	MERCURE	ARP_RARP	ARP: Reply, Target IP: 194.57.137.103 Target Hdwr Adc
79	67.489	MERCURE	*BROADCAST	BROWSER	Workgroup Announcement [0x0c] UREC
80	83.202	MERCURE	*BROADCAST	SAP	General Svc Resp [MERCURE!!!!!!!... - Unknown Servic
81	114.223	MERCURE	*BROADCAST	BROWSER	Workgroup Announcement [0x0c] UREC
82	127.504	MERCURE	*BROADCAST	BROWSER	Workgroup Announcement [0x0c] UREC
83	143.218	MERCURE	*BROADCAST	SAP	General Svc Resp [MERCURE!!!!!!!... - Unknown Servic
84	203.232	MERCURE	*BROADCAST	SAP	General Svc Resp [MERCURE!!!!!!!... - Unknown Servic
85	263.248	MERCURE	*BROADCAST	SAP	General Svc Resp [MERCURE!!!!!!!... - Unknown Servic
86	0.000	000000000000	000000000000	STATS	Number of Frames Captured = 85

```
+FRAME: Base frame properties
+ETHERNET: 802.3 Length = 232
+LLC: UI DSAP=0xE0 SSAP=0xE0 C
+IPX: NetBIOS Packet - 0.00C04FC90B1D.455 -> 0.FFFFFFFFFFFF.455 - 0 Hops
+NBIPX: Directed Datagram
+SMB: C transact, File = \MAILSLOT\NET\NETLOGON
+NETLOGON: Query for Primary DC
```

Différence :
2 trames NET LOGON car une fois avec NWLink et une fois avec TCP/IP
Nombre de paquets : 30 dans le premier cas, 85 dans le deuxième.

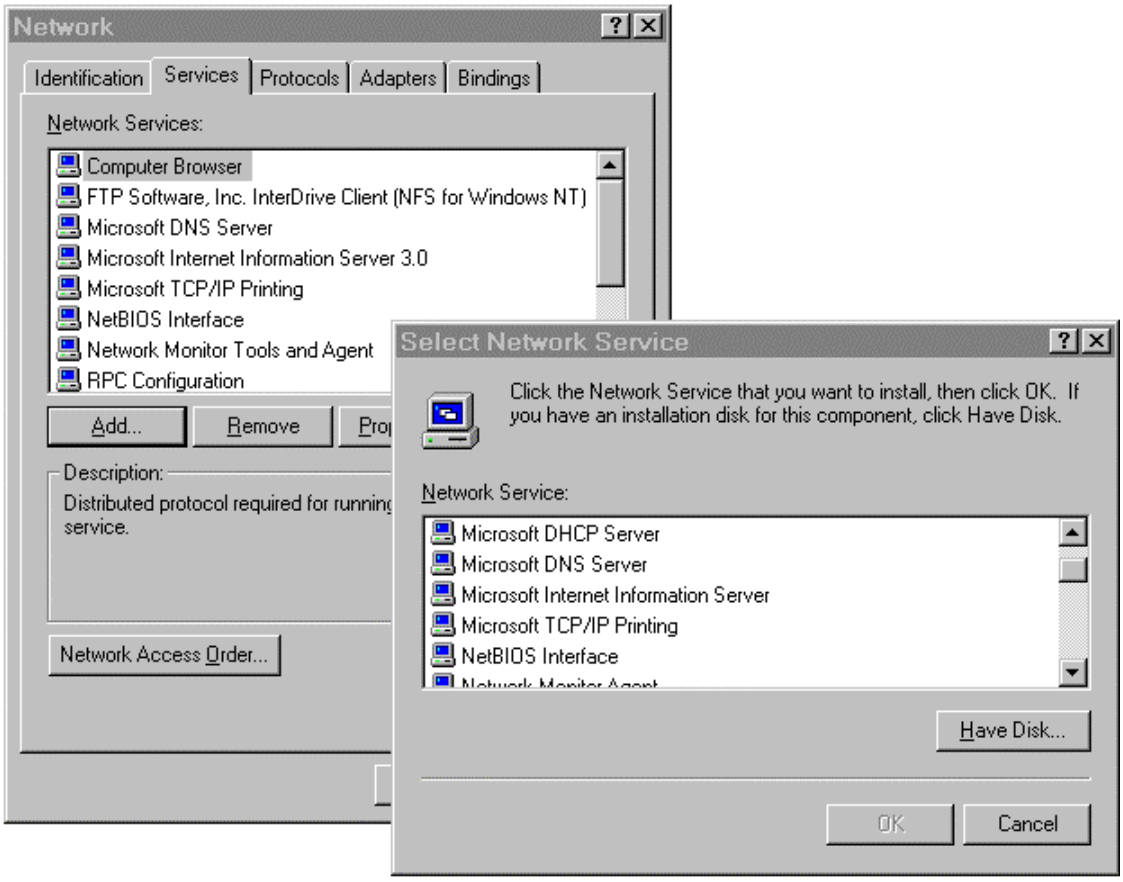
Remarque : requête ARP : mise à jour du cache toutes les 10 minutes.

Cas 3 : avec le protocole NetBEUI

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
35	17.373	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
36	17.373	MERCURE	*NETBIOS Mult	NETLOGON	Query for Primary DC
37	17.375	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
38	17.375	MERCURE	*NETBIOS Mult	NETLOGON	Query for Primary DC
39	17.378	MERCURE	*BROADCAST	NETLOGON	Query for Primary DC
40	17.379	MERCURE	*NETBIOS Mult	NETLOGON	Query for Primary DC
41	18.123	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
42	18.123	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
43	18.874	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
44	18.874	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
45	22.391	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
46	22.391	MERCURE	*NETBIOS Mult	NETLOGON	Query for Primary DC
47	22.394	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
48	22.394	MERCURE	*NETBIOS Mult	NETLOGON	Query for Primary DC
49	22.398	MERCURE	*BROADCAST	NETLOGON	Query for Primary DC
50	22.399	MERCURE	*NETBIOS Mult	NETLOGON	Query for Primary DC
51	23.141	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
52	23.141	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
53	23.892	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1B>
54	23.892	MERCURE	*BROADCAST	NBT	NS: Query req. for UREC <1C>
55	54.344	MERCURE	*BROADCAST	BROWSER	Workgroup Announcement [0x0c] UREC
56	57.358	MERCURE	*NETBIOS Mult	BROWSER	Workgroup Announcement [0x0c] UREC
57	114.332	MERCURE	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 194.57.137.111
58	114.332	00C04FC8CDD1	MERCURE	ARP_RARP	ARP: Reply, Target IP: 194.57.137.103 Target Hdwr Ad
59	114.359	MERCURE	*BROADCAST	BROWSER	Workgroup Announcement [0x0c] UREC

```
+FRAME: Base frame properties
+ETHERNET: 802.3 Length = 211
+LLC: UI DSAP=0xF0 SSAP=0xF0 C
+NETBIOS: Datagram (0x08), MERCURE        <00> -> UREC           <00>
+SMB: C transact, File = \MAILSLOT\NET\NETLOGON
+NETLOGON: Query for Primary DC
```

4. SERVICES



Types de services :

Les services réseaux MS-NET (WINS, Domaine, partages de ressources)

Les services réseaux Internet (DNS, Messagerie, WWW, FTP).

Le choix des protocoles et des services se fera en fonction du type de réseau souhaité.

La liste des services et les ports associés

http://www.urec.cnrs.fr/wnt/doc/port1.txt (de 0 à 1023)

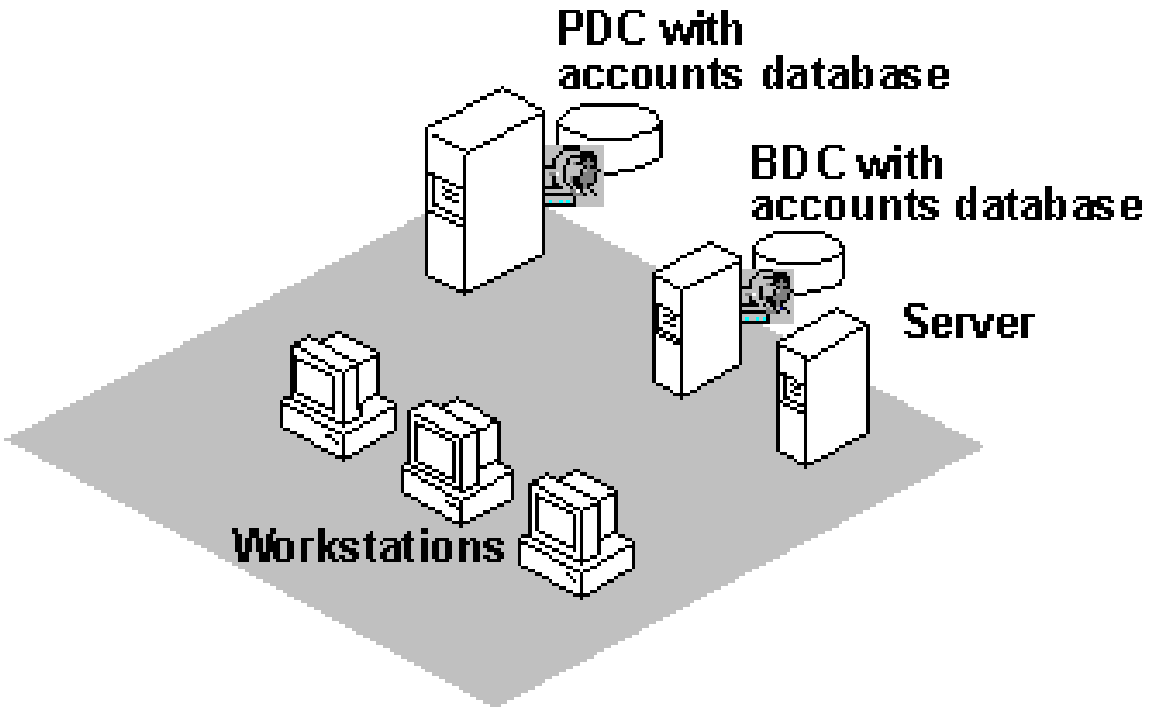
http://www.urec.cnrs.fr/wnt/doc/port2.txt (1023 et suivant).

4.1 Domaines et Groupes de travail

Modèle de domaine :

Un domaine est une unité d'administration : si on a plusieurs serveurs dans le domaine, on déclare un compte par domaine et non par serveurs.
Base distribuée de compte : netlogon
La notion de domaine est indépendante des réseaux physiques et/ou des réseaux IP (au sens numéro IP).

Pour des raisons de sécurités, 1 serveur de domaine ne peut pas changer : réinstallation obligatoire.



Un serveur WinNT4 peut avoir 3 rôles

PDC : primary domain controler
BDC : Backup Domain Controler
SERVER : pas de copie de la base.

Installer un PDC crée automatiquement le domaine associé.
Le premier serveur WinNT installé dans un domaine est obligatoirement PDC.

Groupe de travail : (3.X et 95 ont uniquement des groupes de travail) : Chaque machine garde son mécanisme de sécurité. Les comptes sont uniquement locaux.

Rôle du contrôleur principal : PDC

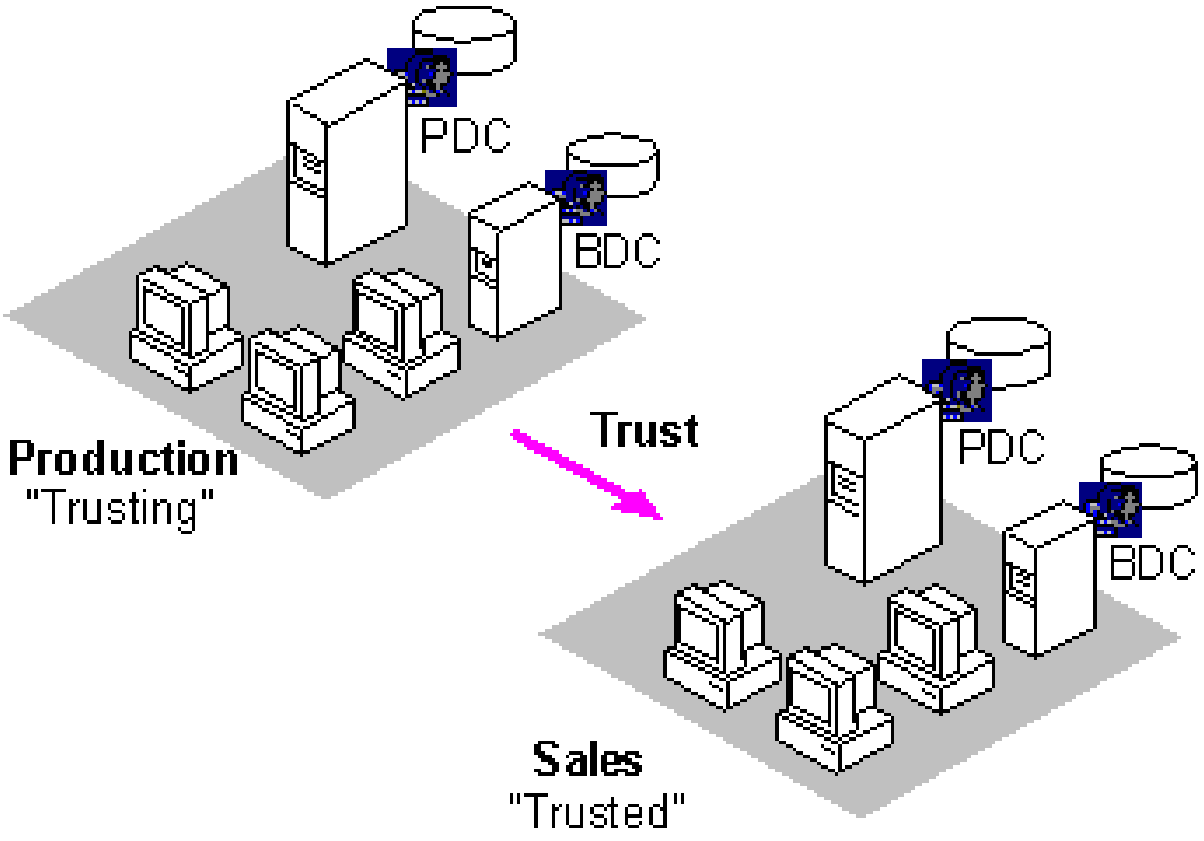
Présence impérative d'un ordinateur avec WinNT4.0 pour avoir un domaine.
Il contient l'original de la base de données des utilisateurs et des groupes du domaine. Toutes les modifications de la base doivent être faites sur cette exemplaire.

Rôle du contrôleur secondaire : BDC
Il contient une copie de la base des utilisateurs et des groupes du domaine. La duplication se fait automatiquement sur tous les BDC. Il peut traiter les demandes d'ouverture de session.
Il a donc un rôle actif permanent dans le domaine.
En cas de panne du primaire, il le remplace dans toutes ses fonctions.

Rôle du NT4Server et du NT4Wks, ni PDC, ni BDC
Il ne possède pas de copie de la base.
Il autorise des comptes d'administrateurs et d'utilisateurs locaux différents du domaine.
NT4WKS favorise le travail local alors que NT4Server favorise le travail en réseau.

Relation entre groupe de travail et domaine :
Un NT4 peut accéder sans problème aux ressources partagées d'un Windows 3.11 WFW.
Les Windows 3.11 WFW sont organisés en groupe de travail et ils peuvent parcourir le réseau par le biais des groupes de travail ou des domaines (pour y accéder l'utilisateur devra être déclaré dans le domaine).

Relation d'approbation



Autoriser les utilisateurs de SALES à accéder aux ressources de PRODUCTION.

Ajout d'un groupe global du « trusted domain »dans un groupe local du « trusting domain ».

Synchronisation du PDC et du_ BDC :

Pour éviter les incohérences de bases.
Effectuée par le service « NetLogon » (Directory service Synchronisation)

3 bases à synchroniser :

SAM Account Database : utilisateurs et groupes et stations du domaine.
SAM Built-in Database : utilisateurs par défaut
LSA DataBase : mot de passe et stratégie

Quand ?

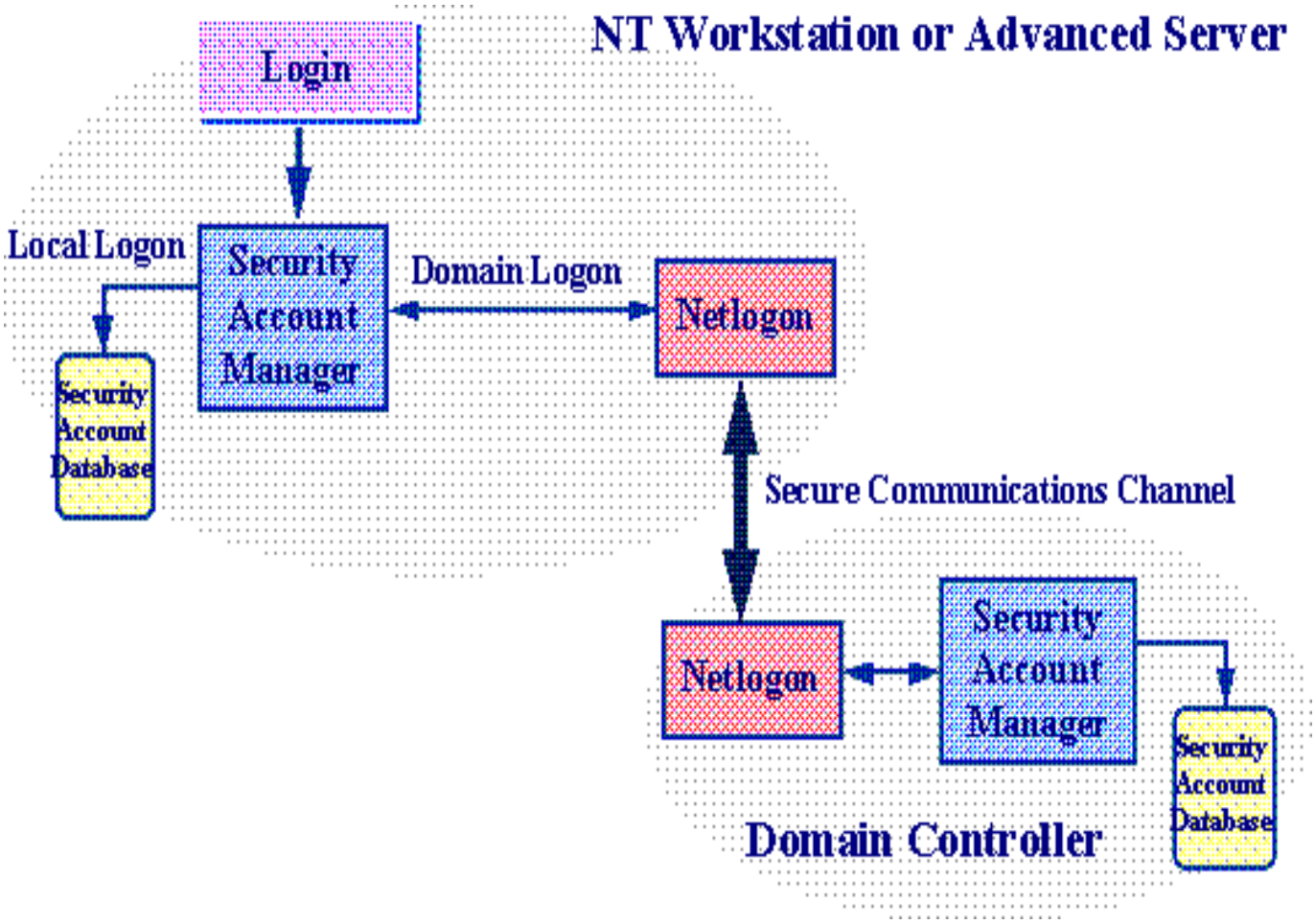
Démarrage du BDC
forcé par l'administrateur
forcé par le PDC en fonction des registres.

Par défaut, le PDC regarde sa base toutes les 5 Minutes. S'il y a eu une modification, il envoie un message à tous les BDC qui ne sont pas à jours. Ce paramètre peut être modifié en passant par le *NetLogon services* du *Server Manager.*

4.2 Accès aux ressources

Mécanismes de connexion : NetLogon

Lors de l'ouverture d'une session sur un ordinateur WinNT4, l'utilisateur doit entrer son nom et son mot de passe. Un des contrôleurs vérifie la correspondance avec la base de données des utilisateurs puis la session est ouverte : téléchargement des informations de session relative à l'utilisateur concerné (représentation du bureau, répertoire de base …).



SAM : Security Account Manager
SAM Accounts database
SAM Built-in database

Base contenant les mots de passes et stratégies.

LSA (local Security Authority): appelé lors du début de la session. Il s'assure que l'utilisateur à la permission d'accéder au système. Il crée les jetons d'accès.

Mécanismes de sécurité :

Droits d'accès : sur les ressources de la station ou du serveur. L'administrateur met en place des ACL (Access Control List) sur les ressources. Le système de sécurité vérifie le droit d'accès à une ressource en comparant la requête de l'utilisateur et les ACL .

Droits des utilisateurs et groupes : à la connexion, l'utilisateur est vérifié à travers le système de sécurité (en local ou sur le PDC). Un jeton d'accès (SID, Groupe ID, user right) est utilisé pour « vérifier » l'utilisateur lors de tous les accès aux ressources. WinNT compare le jeton d'accès de l'utilisateur avec le decripteur de sécurité de l'objet à accéder.
L'utilisateur se connecte en local, au domaine ou à un « trust domaine ».

Compte utilisateur
Un compte utilisateur est unique. Il est représenté par un SID (Security Ident) qui est un numéro.
Attention à la suppression d'un compte.

Secure communication Channel : utilisé pour communiquer avec le service Netlogon vers une station distante. La connexion sécurisée est établit entre deux ordinateurs certifiées.

Notion de groupe local et global :

Local : (Local à la base où il est défini) utilisé en local sur la station ou dans le domaine. Contient des utilisateurs et des groupes globaux. Par défaut : administrators, users, guest, replicator, backup
Global : non restreint à la base ou il est défini. Un groupe global peut être membre de tous les groupes locaux. Il contient uniquement des utilisateurs du domaine. Les groupes globaux sont définis sur le PDC.
Stratégie : les groupes globaux contienent un ensemble d'utilisateurs, les groupes locaux un ensemble de droits d'accès à des ressources et des groupes globaux.

Accès à une ressource partagée : NET USE

Résolution par défaut du nom par un Broadcast
Envoi du triplet {nom de login, domain, mot de passe }
Si l'utilisateur est déclaré dans la base : connexion
Si le mot de passe est incorrect : demande de mot de passe

Sinon,
si le compte Guess est activé : connexion avec les droits de Guess,
sinon : accès refusé

Profils utilisateurs

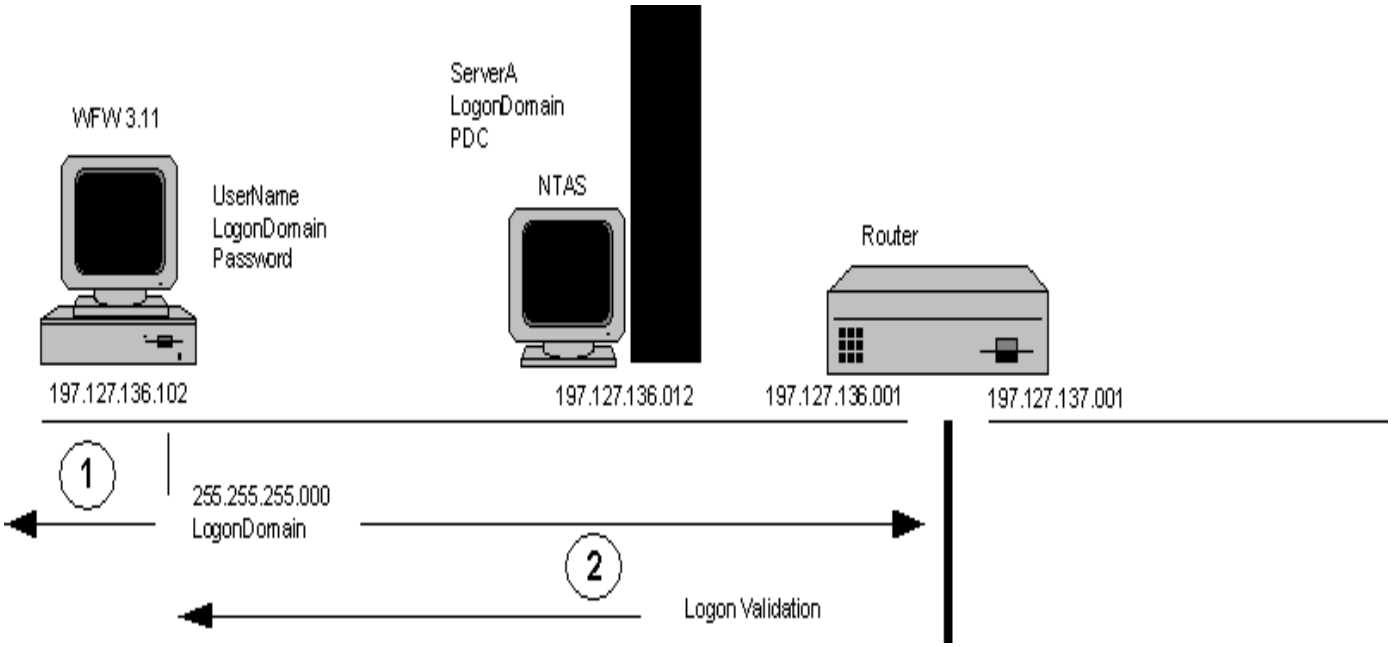
Fichiers qui contiennent les environnements du bureau.
Profil local : propre à la station de connexion
profil serveur (Server based profile) : partage d'un profil par un groupe. Le même profil sur toutes les stations du domaine. Attention aux différences de matériel et de logiciels sur les stations.
On y retrouve toutes les spécificité de l'utilisateur dans le réseau MS comme les programmes accessibles, imprimantes, connexion réseau ...
On peut restreindre l'accès de l'utilisateur. Il y a deux types de profiles, l'un modifiable par l'utilisateur (fichiers ayant comme extension .USR) et l'autre non (fichiers ayant comme extension .MAN). = profils errants.
Profil par défaut : utilisé la première fois si il n'y a pas de profil serveur.
Profil Système par défaut : contient couleur et fond d'écran quand personne n'est connecté sur la station.

Mise en place de profils :

1/ créer le profil avec Profil Editor
2/ assigner le profil aux utilisateurs ou aux groupes globaux (user Manager for Domains).

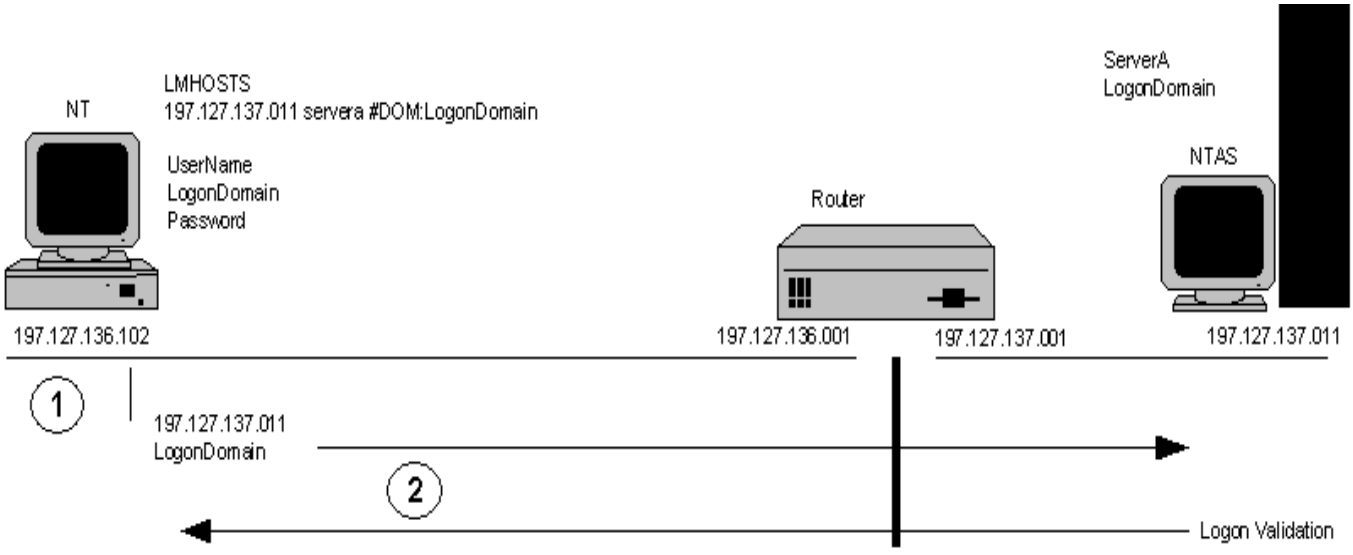
Attention : par défaut tout le monde sur le réseau à un accès total à un répertoire nouvellement partagé.

Connexion vers un PDC sur le même segment



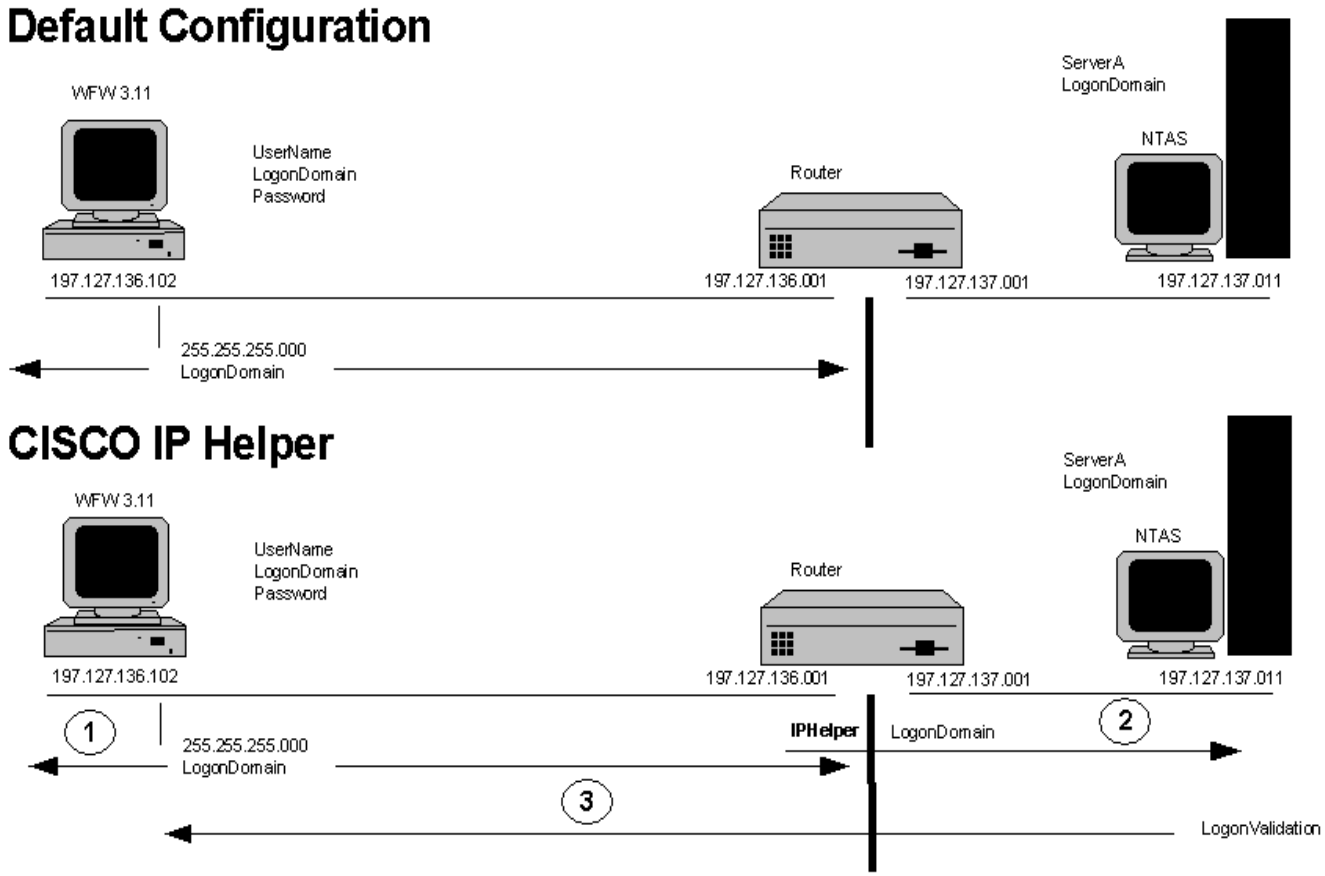
Connexion vers un PDC sur un segment différent

BDC local
Utilisation du fichier LMHOST sur la station locale

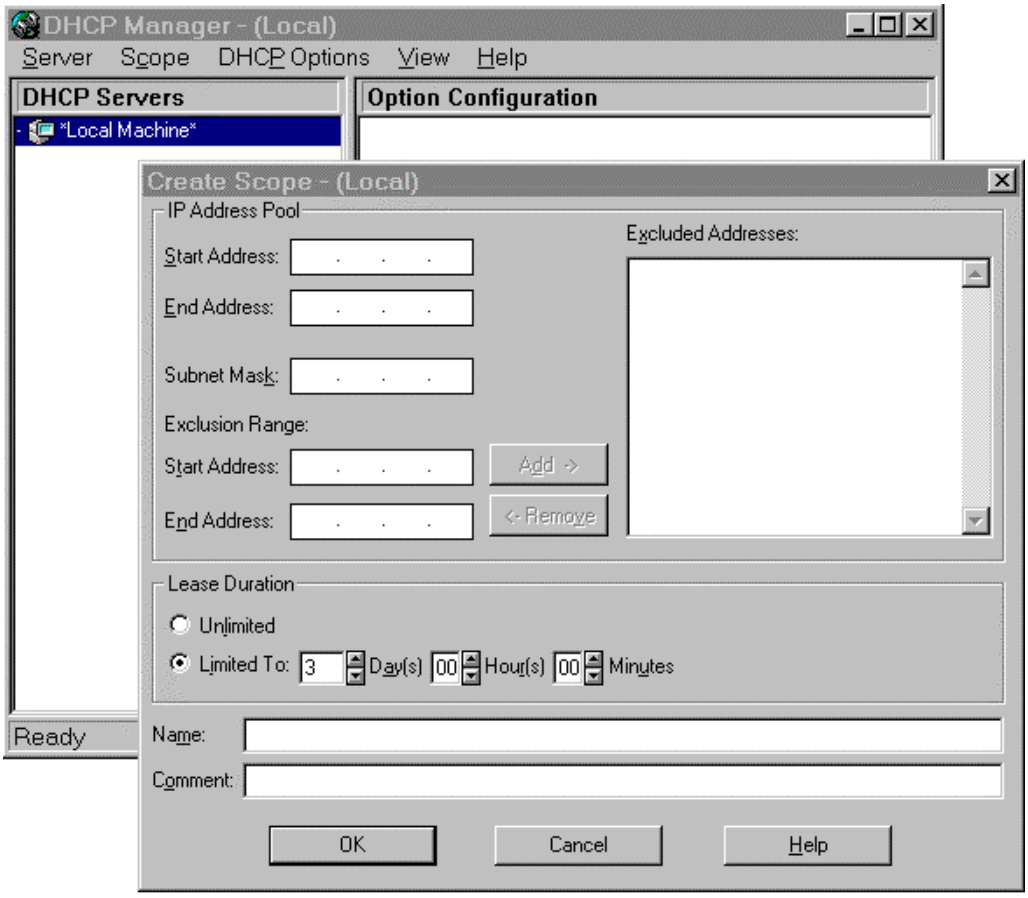


Relations d'approbations : 1 PDC sur le segment1 reçoit la requête et la renvoie vers le segment2

Cisco IP HELPER



4.3 DHCP



Centralisation de la configuration des machines du réseau TCP/IP.

RFC 1533/1534, 1541 et 1542

Paramètres disponibles pour les clients

l'adresse IP,
le masque de sous-réseau,
la passerelle par défaut,
l'adresse du serveur de noms (netbios/Wins ou DNS)
Le type de nœud NetBIOS
le nom de domaine Internet

Mécanisme de bail : temps fixes ou illimités pour l'attribution des adresses.

La recherche d'un serveur DHCP : broadcast. 1 serveur par segment (ou relais DHCP).

Option globale : fournie à l'ensemble des clients DHCP. Exemple : nom de domaine

Option étendue : ne concerne que le réseau local. Exemple : passerelle par défaut

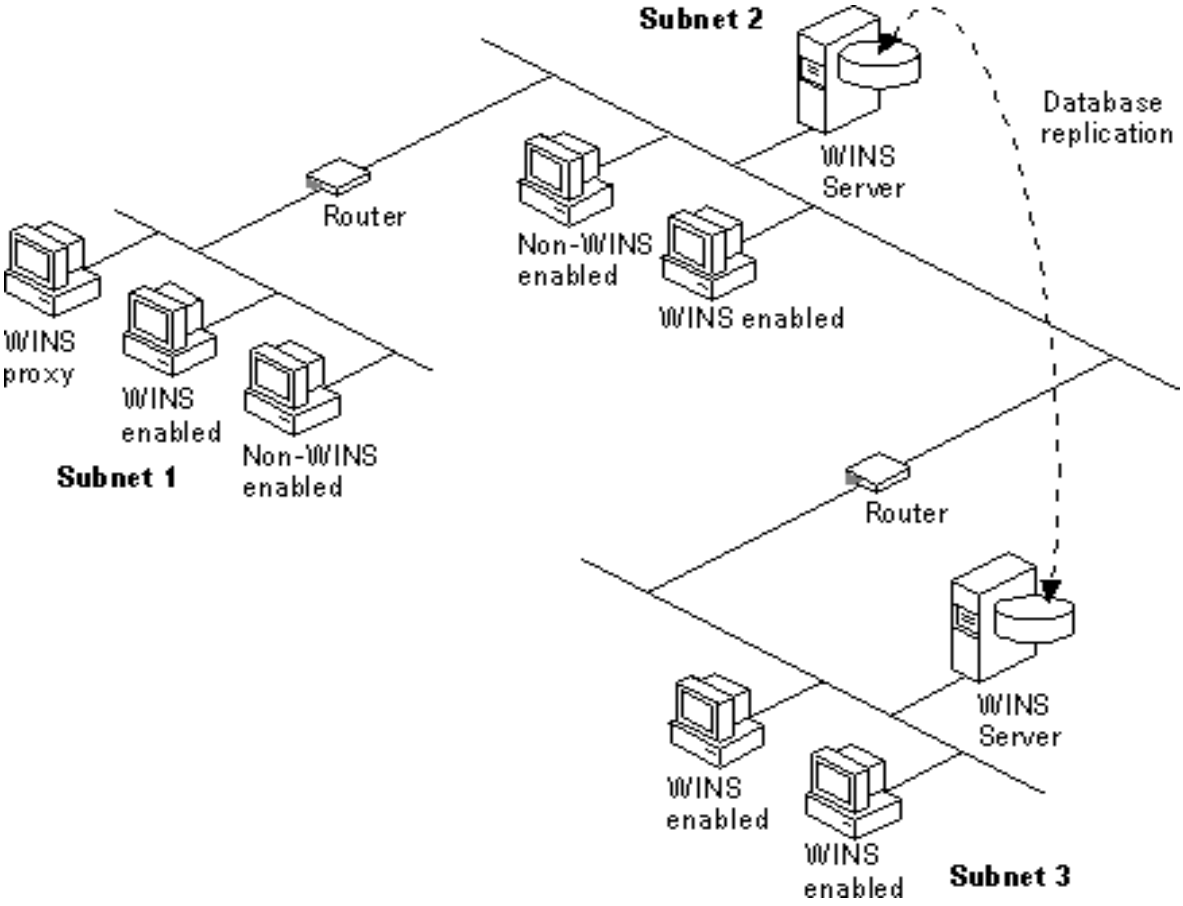
agent relais DHCP

4.4 WINS

Objectifs

Serveur de Noms NetBios
Conserver la flexibilité des noms Netbios pour TCP/IP
spécifier un nom plutôt qu'une adresse
minimiser les diffusions réseau : pas de broadcast régulier pour obtenir les adresses.

WINSD : base de données contenant les liaisons entre les noms logiques utilisés par NetBIOS et les adresses IP. C'est un protocole Client/Serveur
La mise à jour du serveur WINS est dynamique. Chaque nouvelle machine s'annonce auprès du serveur au démarrage



Seule une machine avec Windows NT server peut être serveur Wins.

Méthode recherche d'un serveur de noms NetBios

B-node : broadcast pour enregistrement et résolution (le routeur doit « *forwarder* » les ports 137 et 138)
B-node modifié par Microsoft : consultation du cache LMHOSTS, Broadcast, consultation du fichier LMHOSTS
P-node : utilisation d'un NBNS
M-node (Mixed node) :

A l'enregistrement :

1/ B-node

Si 1/ est bon, alors P-node, si c'est bon, l'initialisation est bonne

Sinon, l'initialisation de TCP/IP ne s'effectue pas.

Pour la résolution :

B-node. Si c'est bon, arrêt de la résolution, sinon, P-node.

H-node (non RFC mais sous forme de draft) : B-node puis P-node uniquement si échec de B-node. On peut configurer cette méthode pour utiliser le fichier MHOSTS après P-node et avant B-node

Méthode utilisée par WINS

Pour l'enregistrement : H-node

Pour la résolution :

1/ regarde si le nom est local
2/ consulte le cache de NBNS (valide 10 minutes)
3/ interrogation de WINS
4/ Broadcast
5/ LMHOSTS
6/ HOST et DNS

En utilisant DHCP, on peut configurer les clients pour qu'ils utilisent la méthode M-Node : inversion étape 3 et 4

Enregistrement :

Si le nom est libre, la réponse du serveur est positive avec un TTL indiquant au client quand il devra se réenregistrer.
Sinon, le serveur vérifie que le client déjà annoncé existe toujours.
Si oui, l'enregistrement est refusé.

Rafraîchissement

Tous les 1/8 du TTL, le client essaie de se rafraîchir.

Libération

A l'extinction, le client prévient le serveur.

Réplication de bases : PUSH et PULL

Les enregistrements du premier seront connus chez le deuxième et vice versa.

Wins Proxy Agent :

permet aux stations non WINS de résoudre es noms. Le proxy écoute les broadcast d'enregistrement et de résolutions des clients non Wins puis il les transmet au serveur.(Il transmet les requêtes d'enregistrement juste pour vérifier que le nom est libre et non pour les enregistrer).
Le proxy agent doit être un client WINS.

Contenu de la base WINS

Nom ordinateur [service] : network Monitor, netdde, Messager Service
Nom de domaine[1Ch] pour retrouver PDC et BDC
Nom de domaine[7Dh] pour retrouver Master Browser
Username

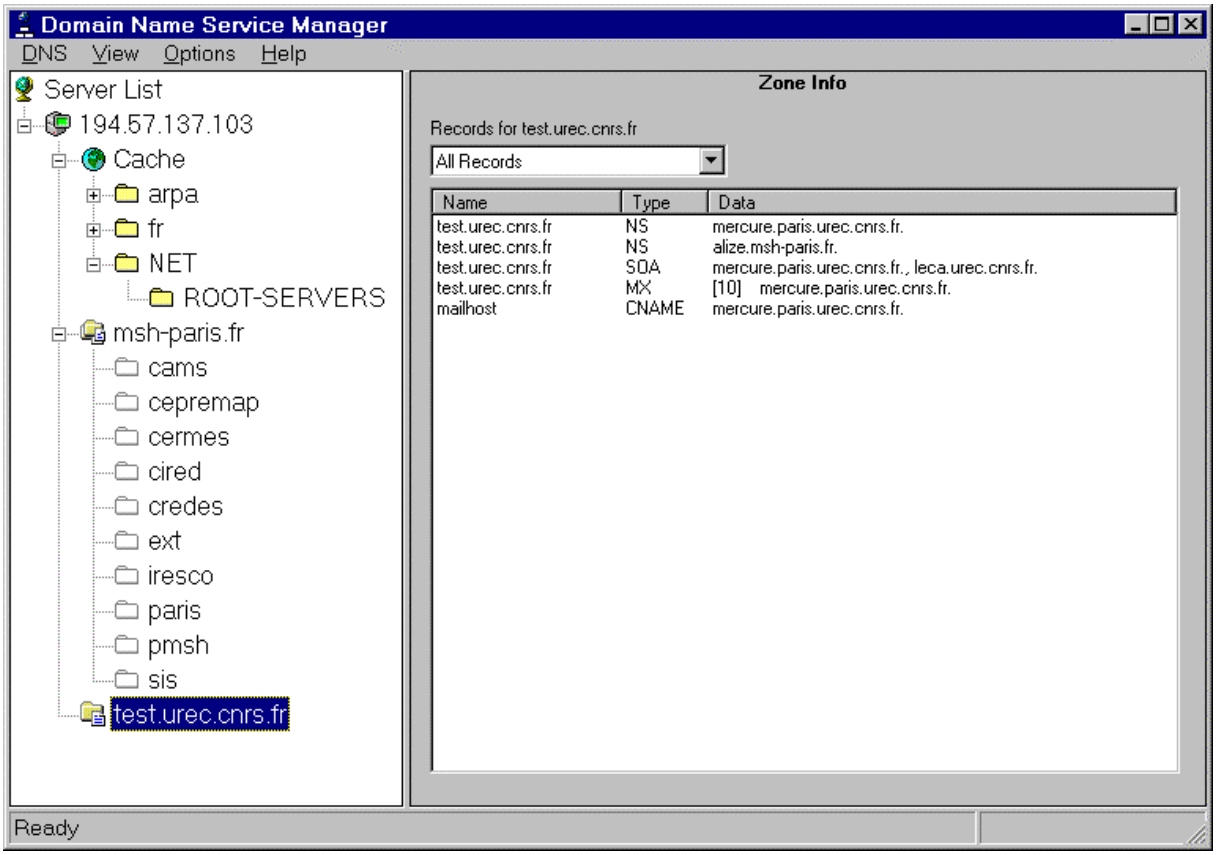
Configuration

TTL pour se re-déclarer : par défaut 40 Minutes.
Temps d'extinction quand un client ne répond plus

Mappage Statique : important pour les serveurs.

Fichiers de la base WINS : JET.LOG, SYSTEM.MDB, WINS.MDB, WINSTMP.MDB
Pour la sauvegarde, penser aussi à sauvegarder la partie registres.

4.5 DNS



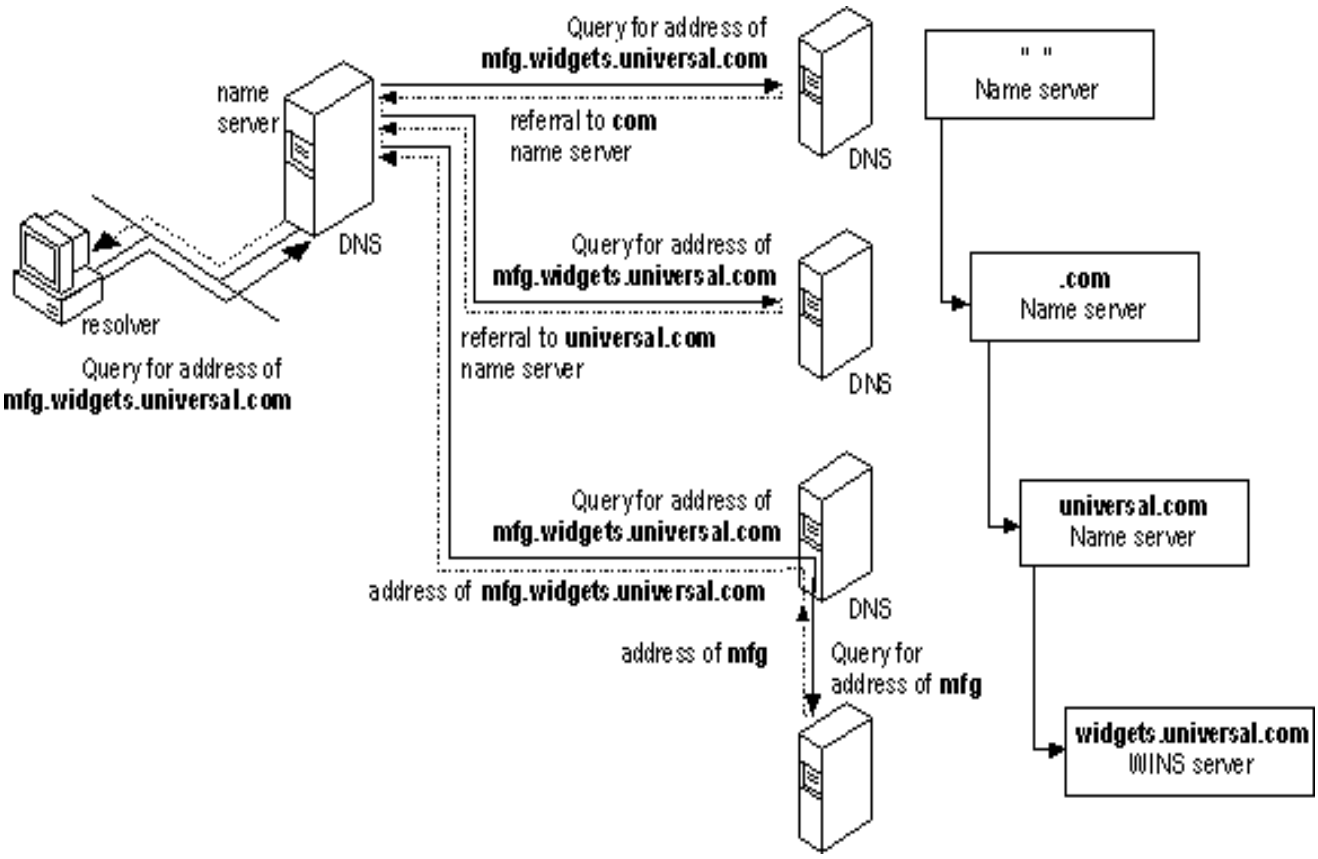
Il est déconseillé d'utiliser le service DNS fournit avec IIS :

Problèmes au bout d'un certain nombre de requêtes par seconde,
mauvais secondaire,
extension vers Wins ne fonctionne pas

On peut utiliser d'autres produits (portage de BIND sur NT) mais on perd la facilité de configuration.

Intégration du service WINS et du service de nom de domaine :

Le serveur DNS demande au service WINS de convertir un nom d'hôte en adresse IP. L'intégration du serveur WINS pour la résolution du DNS permet de ne pas rentrer dans le DNS les clients WINS (choix : utiliser la résolution WINS dans la configuration du serveur DNS de NT) .



Remarques :

Attribut WINS.
Par défaut le nom DNS est le même que le nom NetBIOS. On peut le modifier (dans la config DNS de la machine).

4.6 Impressions

Serveur d'imprimantes réseaux ou locales

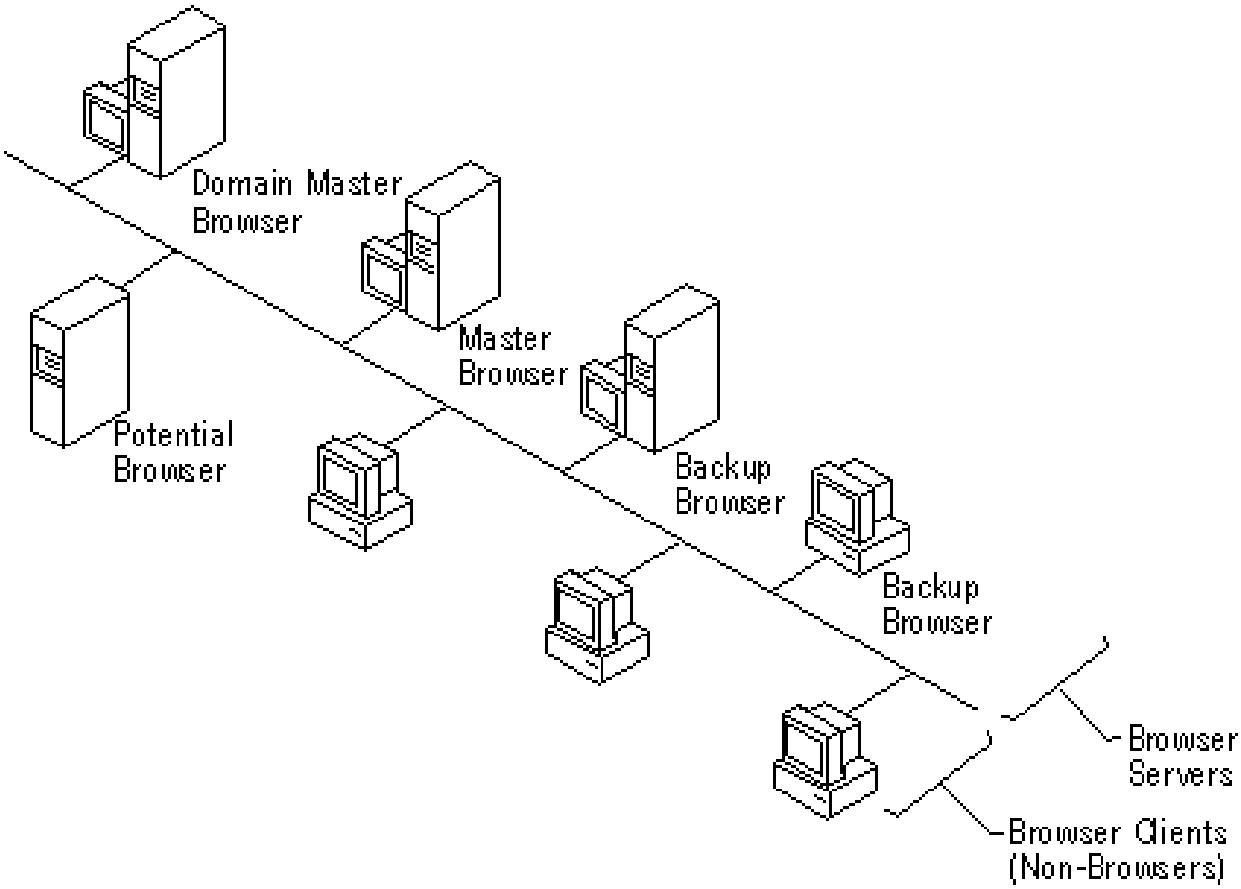
Client imprimantes distantes ou locales

Protocole LPD (Unix Berkeley)

Protocole DLC : imprimante HP

Pour imprimer sur une imprimante distante via le protocole LPR/LPD, il faut installer le service " Microsoft TCP/IP Printing " en passant par " Control Panel – Networks – Services "

4.7 Explorateur réseau – Voisinage réseau :



Services Explorateur d'ordinateurs

Maintient d'une liste des ressources disponible pour le domaine.
Un explorateur maître par domaine. Automatiquement, il choisit les explorateurs de sauvegardes.
Le choix de l'explorateur maître se fait automatiquement en fonction d'un poids définit sur l'OS par élection.

Si un *Master Browser* s'arrête, les autres ordinateurs élisent un nouveau *Master Browser* (élection lancée par le premier ordinateur qui se rend compte de l'arrêt).
Les autres sont des *Backup Browse*r qui interrogent toutes les **15 minutes** le maître pour mettre la base à jour .

Quand un nouveau serveur arrive, il s'annonce au *Master Browser* par Broadcast

Types d'explorateurs

Explorateur Maître – Master browser : maintient la liste sur son sous-réseau.
Explorateur Maître de Domaine – Domain Master Browser : maintient la liste de tout le domaine.
Explorateur Maître préféré – Preferred master Browser
Explorateur de Sauvegarde – Backup Browser
Explorateur potentiel – Potential Browser
Non Explorateur – Non Browser

Trafic

Lors de la mise en marche d'une station Non browser :

1/ annonce au Master Browser : 1 fois par Minute pendant 5 Minutes.

Lors de la mise en marche d'une station Browser

1/ Recherche du Master Browser : Annoucement request
2/ réponse par le Master : Local Browser Annoucement
3/ si c'est un Master Browser, il force les stations à se réannoncer

Elections :

Si aucun Master Browser n'est trouvé ou si la nouvelle station peut devenir Master Browser ou si un PDC s'allume:
Envoi d'un paquet « election »
Envoi d'un broadcast indiquant les critères
Si une station à des critères supérieurs, elle envoie un broadcast avec ses critères
Délai entre les stations pour répondre (NT server répondra plus vite).

Toutes les 12 minutes, les stations se réannoncent au master Browser.
Si le Master Browser ne reçoit plus de confirmation au bout de 3x12 mn, la ressource est supprimée de sa liste. S'il y a des Explorateurs de sauvegarde, on rajoute 15 minutes pour qu'elle soit supprimée.

A travers des sous-réseaux :

Le Local Master Browser demande le nom du Domain Master Browser au serveur WINS
Le serveur Wins renvoie le nom du PDC
Le Master domain envoie un paquet au PDC pour s'annoncer
puis il récupère la liste des ressources du domaine que connaît le Domain Master Browser
Le domain master Browser récupère ensuite des Local Master Browser la liste des ressources du sous-réseaux toutes les 15 minutes.

Remarques :

Si une ressource n'apparaît par dans le voisinage réseau, cela ne veut pas dire forcément qu'elle est indisponible (on peut y accéder par *net view\\serveur ou net use\\serveur\ressource*)

Il y a un Explorateur maître par *PROTOCOLES*

En général, il est conseillé de configurer une station (si possible le PDC) pour être Master Browser et de configurer les autres pour ne pas l'être afin d'éviter les suites d'élection.

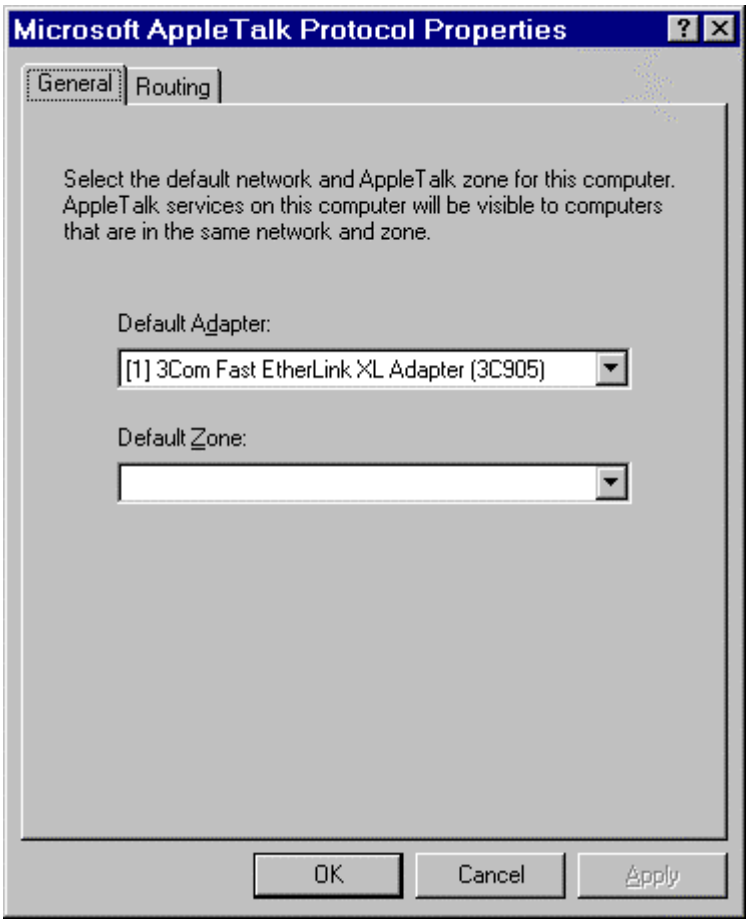
Sur WindowsNT :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\browser\Parameters

Sur Windows95 :

Control Panel - Network Application – Print and File sharing –

Sur Windows3.11 for Workgroups :
Rajouter MaintainserverList dans le SYSTEM.INI – section [Network]

4.8 Services pour Macintosh



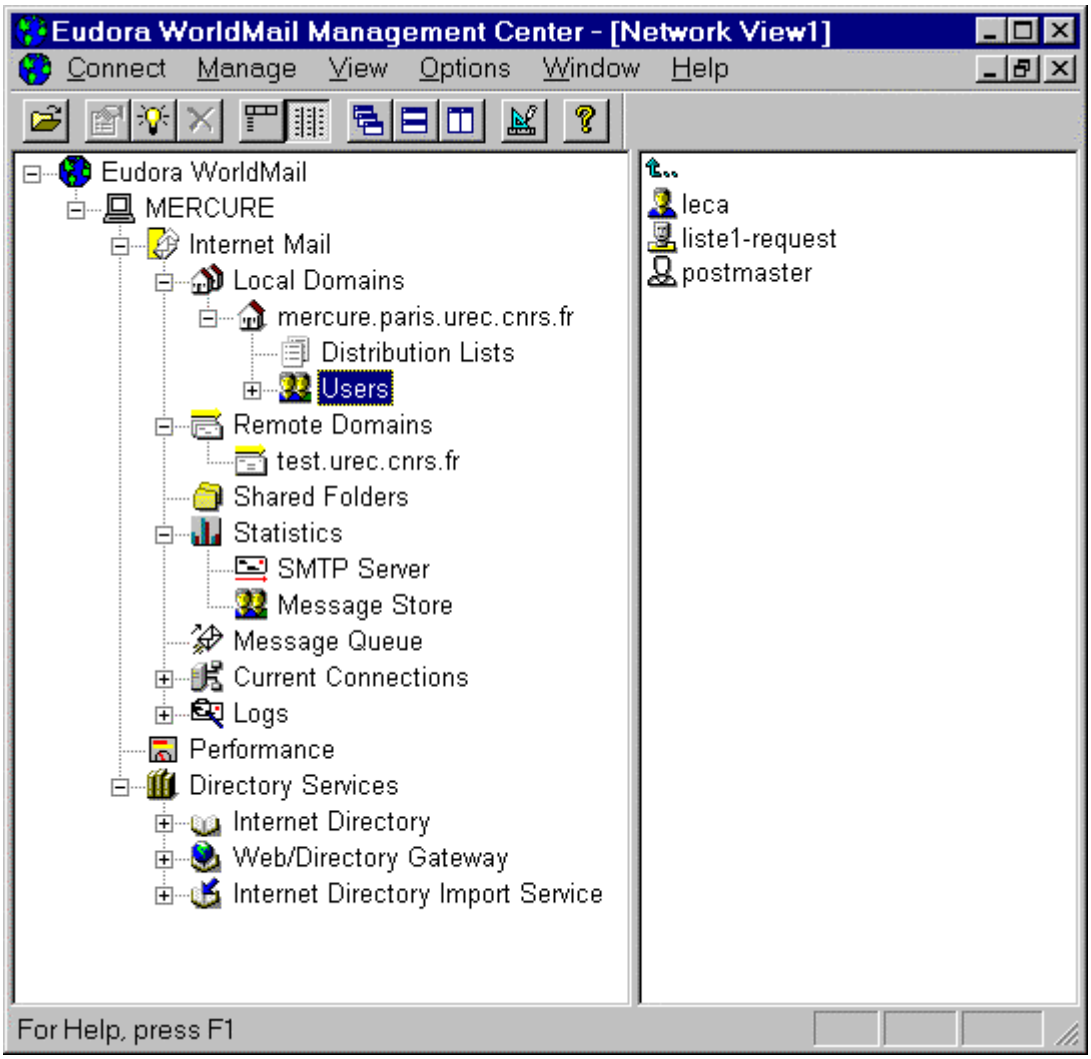
Mise en place du protocole AppleTalk

Partage de fichiers
partage d'imprimantes
administration simplifiée
prise en charge du routage AppleTalk

Prérequis : avoir un système de fichier NTFS et un système MacOS > 6.07

Installation : installer le service « *Services for Macintosh* » en passant par Control Panel – Networks – Services

4.9 MESSAGERIE

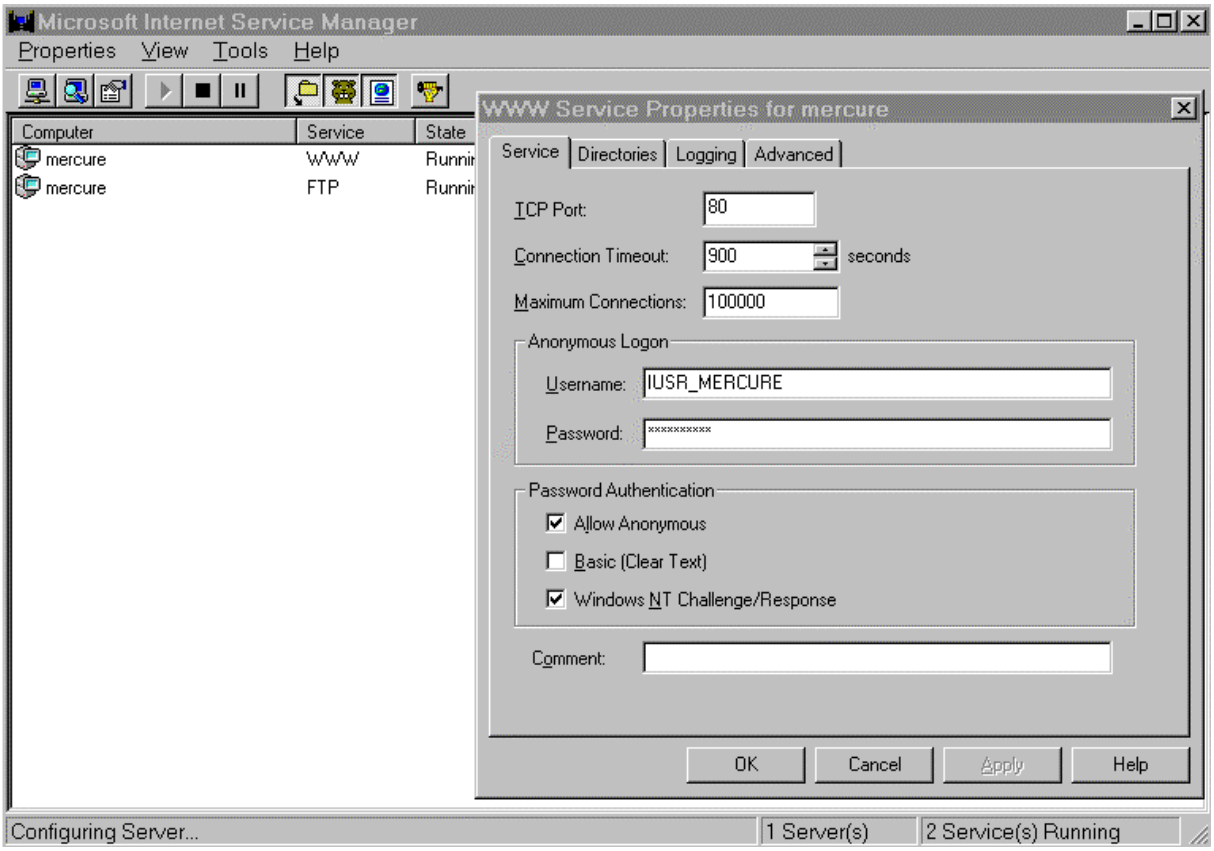


Messagerie SMTP

NTMail

Eudora WorldMail

4.10 Internet Information Server : WWW, FTP et GOPHER



Il existe un portage de Apache sur NT .
FTP : War-Ftp permet de gérer la reprise sur erreur + une gestion indépendante des comptes utilisateurs (ils ne sont plus obligés d'être dans le domaine).

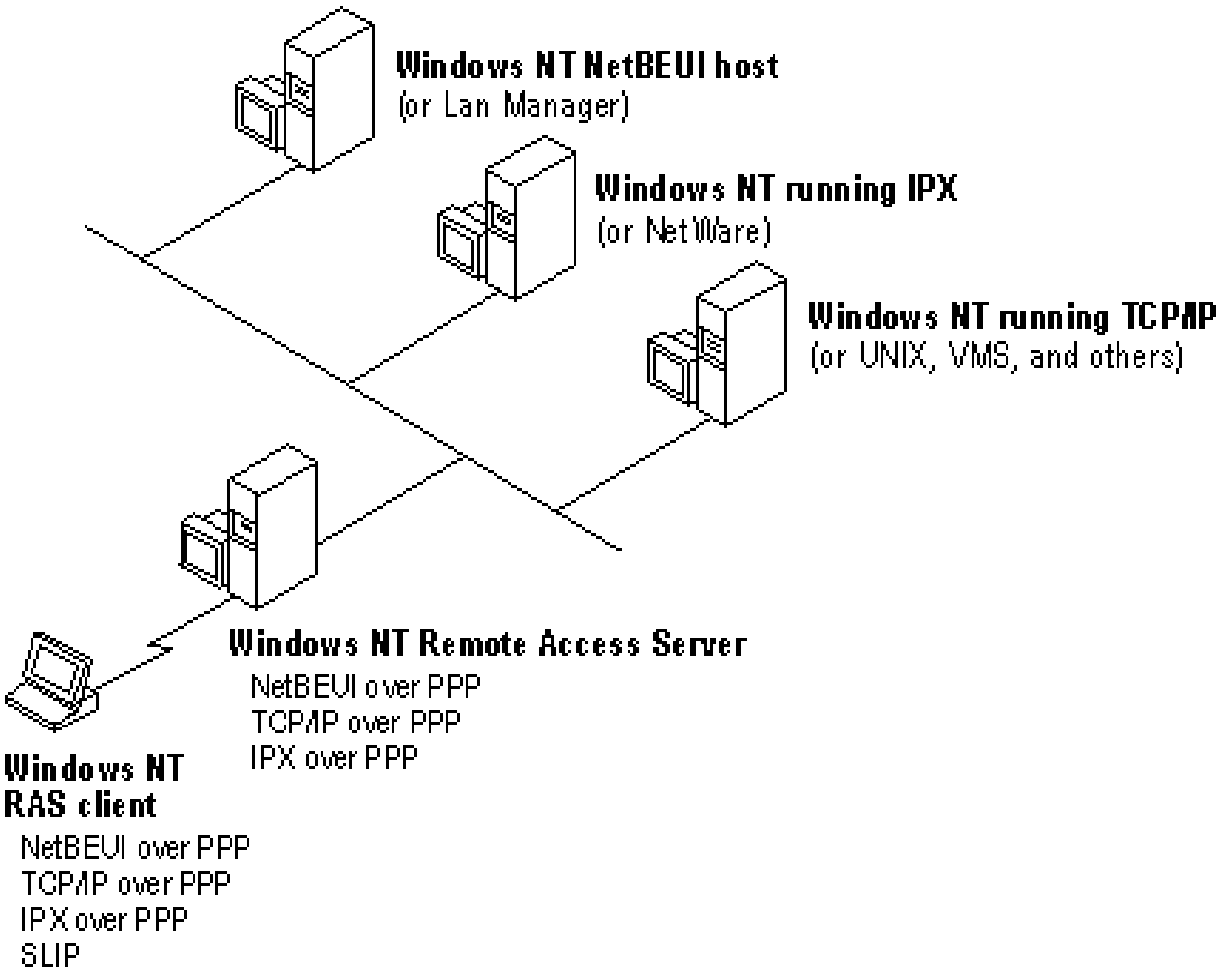
4.11 RAS

RAS Client et RAS Server

Utilisation de la base centralisée des utilisateurs

Accès aux ressources du domaine

Possibilité de faire du rétro-appel.



4.12 Commandes en mode ligne

Commandes de bases :

rexec : exécution sur une machine distante d'une commande avec nom de login et passswd
rsh : idem mais le mot de passe n'est pas demandé si le fichier rhost est renseigné.
rcp : copie distante
telnet
ftp : en mode interactif ou en mode batch (ftp -n -s:script)
tftp
finger
lpr, lpq
arp

Utilitaires de diagnostiques :

Netstat
Nslookup
Nbtstat : résolution de noms NetBIOS
Ping
hostname
tracert
arp -a

Affichage de toute la configuration TCP-IP : IPCONFIG /ALL

Commandes de Routage

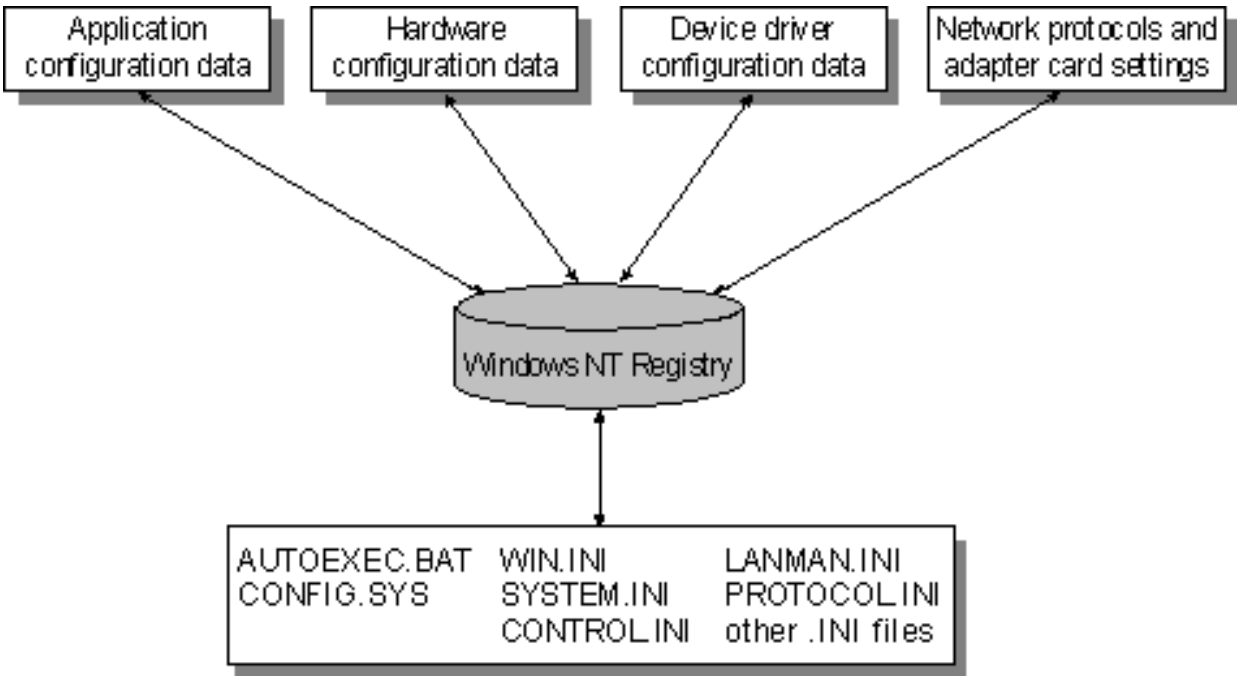
Routage statique : commande ROUTE
Routage dynamique : protocole RIP, transmet les infos de routages IP ou IPX
Test de routage : commande TRACERT

Commandes du Kit de ressources Windows NT 4.0 server :

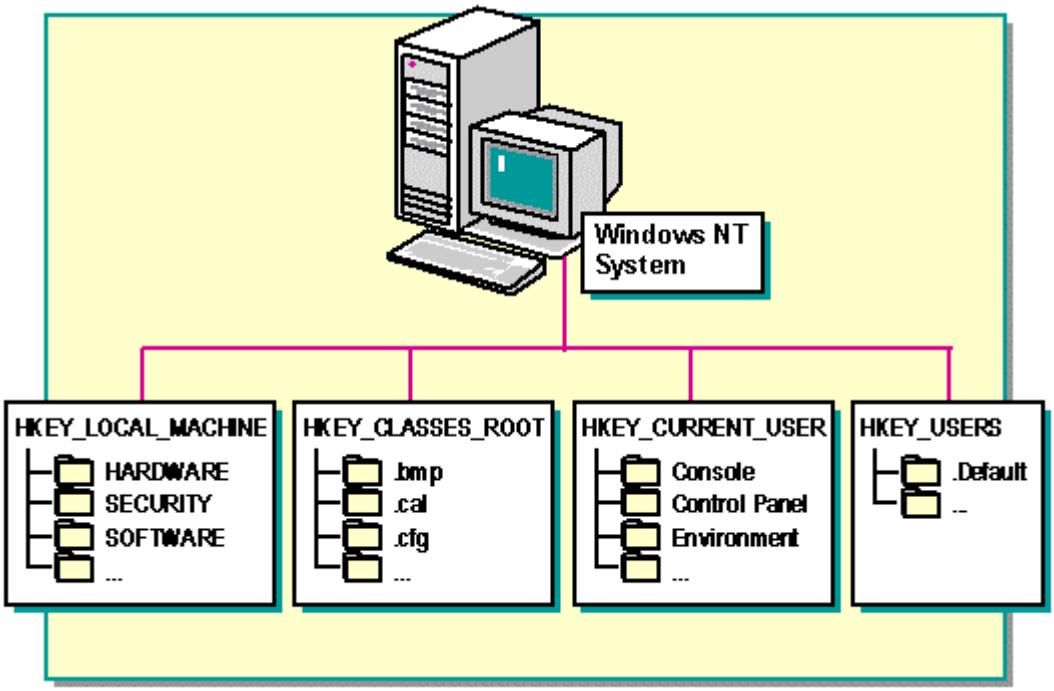
Browmon.exe, browstat.exe
Dommon.exe
Rconsole
Gestion de la registery en mode batch (reddmp, regdel …)
Gestion des process (pview, rkill)

5. ADMINISTRATION D'UN SERVEUR WINDOWSNT

5.1 Les registres



Structure des registres



Exemples :

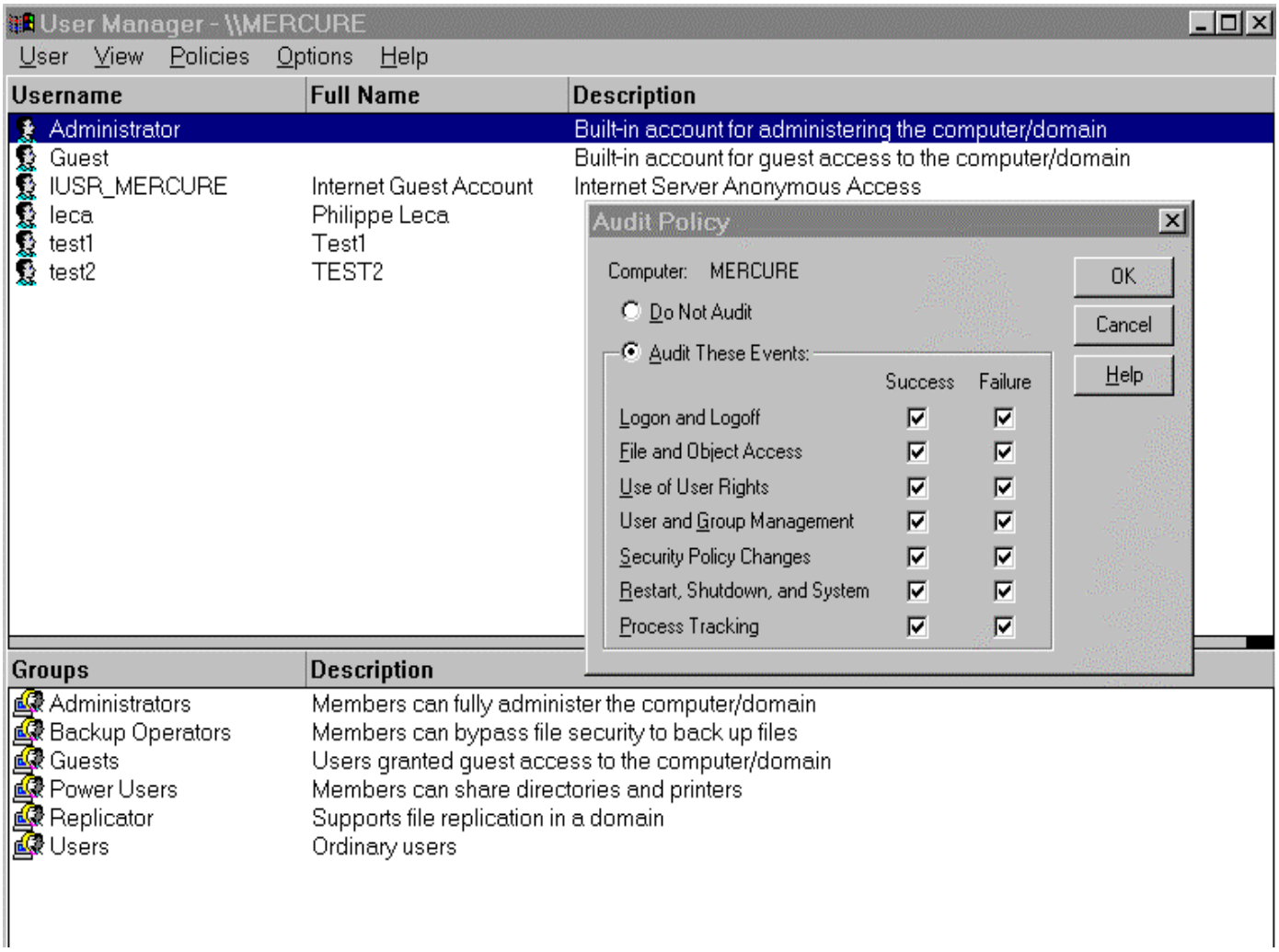
Modification de la taille de la mémoire paginée :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session\Memory\

explorateur de réseaux :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\parameters\

Informations sur les protocoles réseaux utilisés :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NBF\

5.2 Les audits

L'audit permet de contrôler certains événements. La réussite et/ou l'échec des événements contrôlés sont inscrits dans le journal des événements.



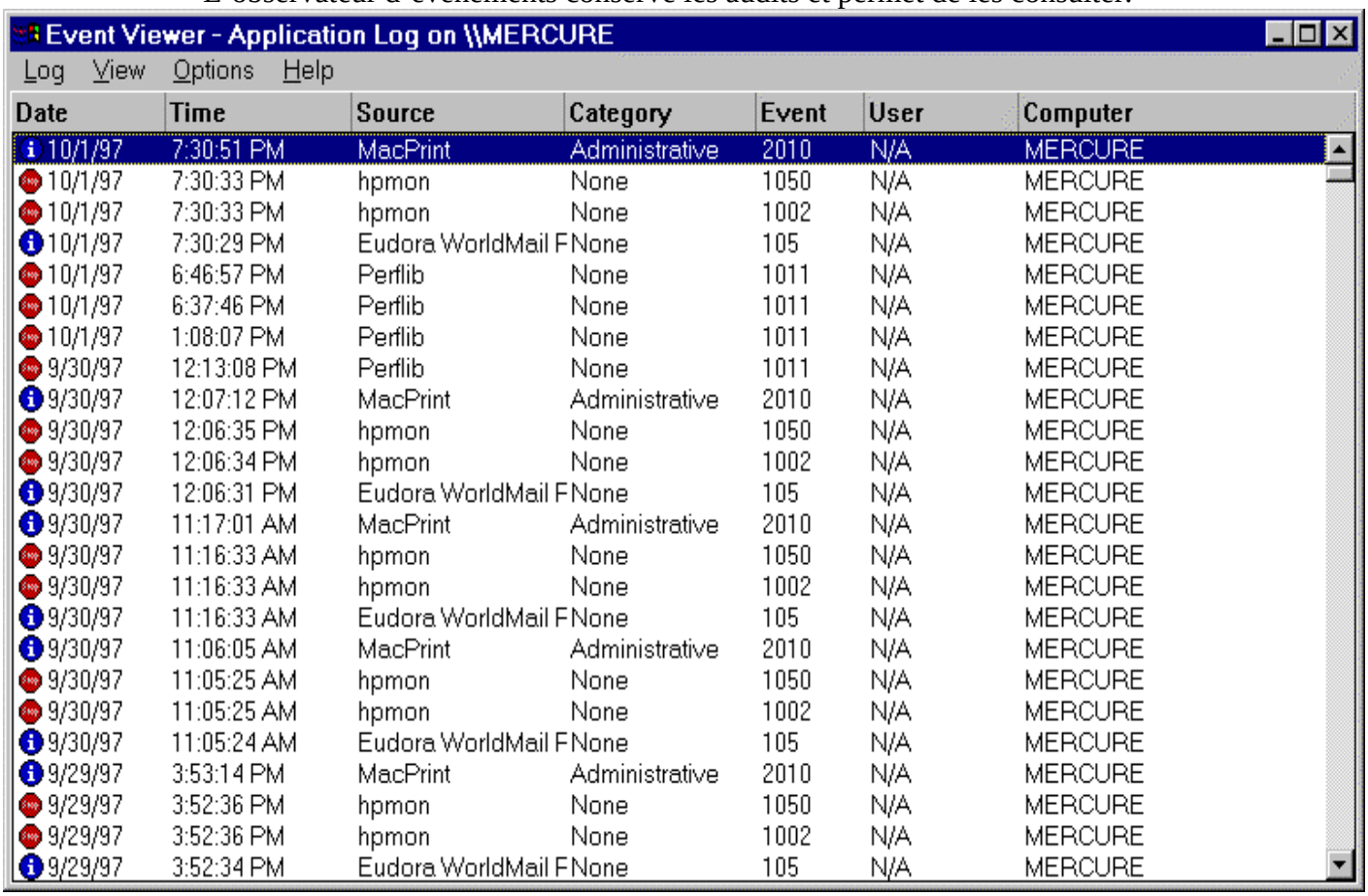
De plus, dans le cas des actions sur les répertoires et les fichiers, il faut préciser quels sont les répertoires et fichiers à auditer (car, sinon, le journal des événements serait rempli trop vite !). Après avoir sélectionné un dossier ou un fichier dans ***POSTE DE TRAVAIL*** ou ***EXPLORATEUR,*** il faut appeler la commande ***FICHIER / PROPRIETE / SECURITE / AUDIT***. Le bouton ***AJOUTER*** permet de sélectionner les groupes et/ou les utilisateurs à auditer. Pour chaque groupe ou utilisateur, il faut ensuite spécifier les événements à auditer : lecture, écriture, suppression...

Il est également possible de faire un audit pour l'imprimante.

Il est également possible de spécifier si l'audit doit être fait dans le cas des erreurs fatales, dans le ***PANNEAU DE CONFIGURATION***, par la commande ***SYSTEME / ARRET/DEMARRAGE***.

5.3 L'observateur d'événements

L'observateur d'événements conserve les audits et permet de les consulter.



Date	Time	Source	Category	Event	User	Computer
10/1/97	7:30:51 PM	MacPrint	Administrative	2010	N/A	MERCURE
10/1/97	7:30:33 PM	hpmon	None	1050	N/A	MERCURE
10/1/97	7:30:33 PM	hpmon	None	1002	N/A	MERCURE
10/1/97	7:30:29 PM	Eudora WorldMail F	None	105	N/A	MERCURE
10/1/97	6:46:57 PM	Perflib	None	1011	N/A	MERCURE
10/1/97	6:37:46 PM	Perflib	None	1011	N/A	MERCURE
10/1/97	1:08:07 PM	Perflib	None	1011	N/A	MERCURE
9/30/97	12:13:08 PM	Perflib	None	1011	N/A	MERCURE
9/30/97	12:07:12 PM	MacPrint	Administrative	2010	N/A	MERCURE
9/30/97	12:06:35 PM	hpmon	None	1050	N/A	MERCURE
9/30/97	12:06:34 PM	hpmon	None	1002	N/A	MERCURE
9/30/97	12:06:31 PM	Eudora WorldMail F	None	105	N/A	MERCURE
9/30/97	11:17:01 AM	MacPrint	Administrative	2010	N/A	MERCURE
9/30/97	11:16:33 AM	hpmon	None	1050	N/A	MERCURE
9/30/97	11:16:33 AM	hpmon	None	1002	N/A	MERCURE
9/30/97	11:16:33 AM	Eudora WorldMail F	None	105	N/A	MERCURE
9/30/97	11:06:05 AM	MacPrint	Administrative	2010	N/A	MERCURE
9/30/97	11:05:25 AM	hpmon	None	1050	N/A	MERCURE
9/30/97	11:05:25 AM	hpmon	None	1002	N/A	MERCURE
9/30/97	11:05:24 AM	Eudora WorldMail F	None	105	N/A	MERCURE
9/29/97	3:53:14 PM	MacPrint	Administrative	2010	N/A	MERCURE
9/29/97	3:52:36 PM	hpmon	None	1050	N/A	MERCURE
9/29/97	3:52:36 PM	hpmon	None	1002	N/A	MERCURE
9/29/97	3:52:34 PM	Eudora WorldMail F	None	105	N/A	MERCURE

L'observateur d'événements est donc la *seule interface disponible*, pour les services ou les applications, pour communiquer de façon unifiée et directe avec l'administrateur.

Accessible par la commande ***DEMARRER / PROGRAMMES / OUTILS D'ADMINISTRATIONS / OBSERVATEUR D'EVENEMENTS***, il affiche tous les événements survenus sur l'ordinateur depuis une certaine date (fixée par l'administrateur ou fonction d'un taux de remplissage du disque)

Il est possible de paramétrer le journal par la commande ***JOURNAL / PARAMETRES DU JOURNAL***. : taille de chaque journal, ce qu'il y a lieu de faire lorsque le journal est plein : arrêter d'y écrire, écraser les événements les plus anciens...

Il est à noter qu'il est possible de se connecter aux journaux de toute machine NT en allant dans le menu ***JOURNAL / SE CONNECTER A***

5.3.1 Analyseur de performances

Il s'appelle à partir de la commande ***DEMARRER / PROGRAMMES / OUTILS D'ADMINISTRATIONS / ANALYSEUR DE PERFORMANCES.*** Il est beaucoup plus utilisé pour

l'optimisation des performances que la maintenance simple. Toutefois, son utilisation peut aussi servir à une bonne administration des performances du serveur. (*Cet outil sera détaillé par la suite*)

5.3.2 Moniteur Réseau

Est un analyseur de trafic réseau. Nouveau dans la version 4, cet outil est maintenant intégré en standard avec Windows NT et permet d'analyser le degré de saturation du serveur. Cet outil est aussi fort apprécié pour sa capacité à analyser les trames Netbios ou NBT du réseau ainsi que celle qui lui permet d'identifié les machines par leur nom Netbios plutôt qu'en affichant leur adresse MAC souvent inconnue des administrateurs NT

5.3.3 Gestionnaire de Serveur

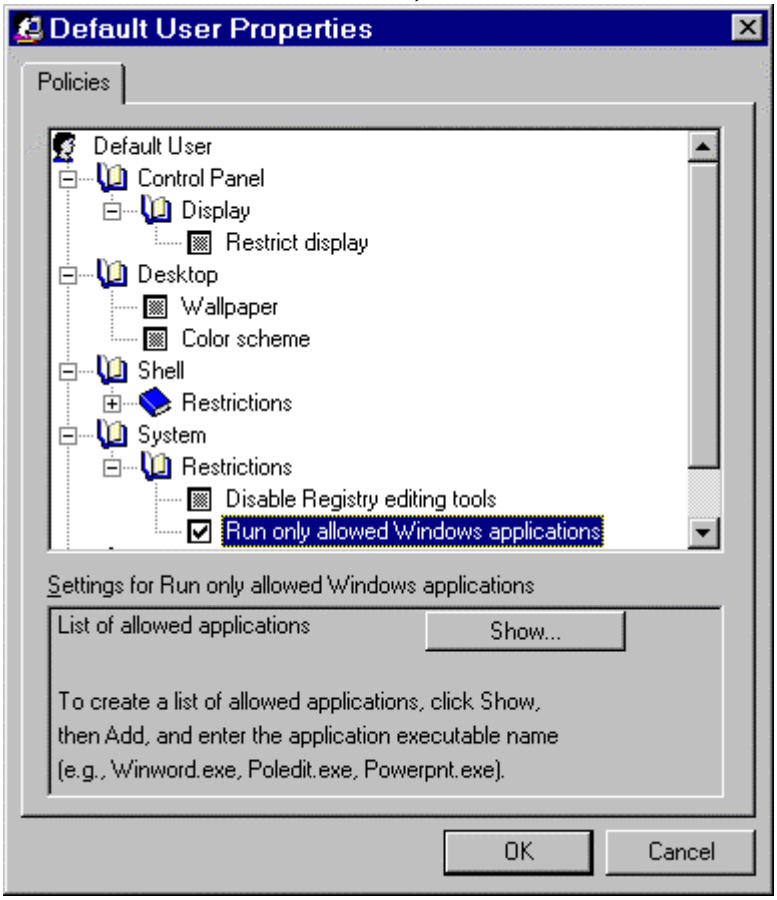
Il s'appelle par la commande ***DEMARRER / PROGRAMMES / OUTILS D'ADMINISTRATIONS / GESTIONNAIRE DE SERVEUR.*** Il est le point central où se regroupent les divers aspects du serveur. C'est également par le biais de cet outil que l'administration à distance d'autres serveurs est possible. (*Cet outil sera détaillé par la suite*)

5.3.4 Gestionnaire de Licences

Il s'appelle par la commande ***DEMARRER / PROGRAMMES / OUTILS D'ADMINISTRATIONS / GESTIONNAIRE DE LICENCES.*** Il permet de rajouter des licences par la commande ***LICENCE / NOUVELLES LICENCES*** et permet aussi de surveiller la répartition des licences au travers d'un domaine ainsi que les éventuels manques de licences.

5.4 L'éditeur de stratégie

L'éditeur de stratégie s'appelle par la commande ***DEMARRER / PROGRAMMES / OUTILS D'ADMINISTRATION / EDITEUR DE STRATEGIES SYSTEME***. Il permet de changer les droits de tous les utilisateurs ou d'un seul, de tous les ordinateurs ou d'un seul



Pour modifier les droits actifs, il faut appeler la commande ***FICHIER / OUVRIR UNE STRATEGIE*** et sélectionner le fichier NTCONFIG.POL du répertoire WINNT \ SYSTEM32 \ REPL \ IMPORT \ SCRIPT.

☐ Action autorisée

☒ Action refusée

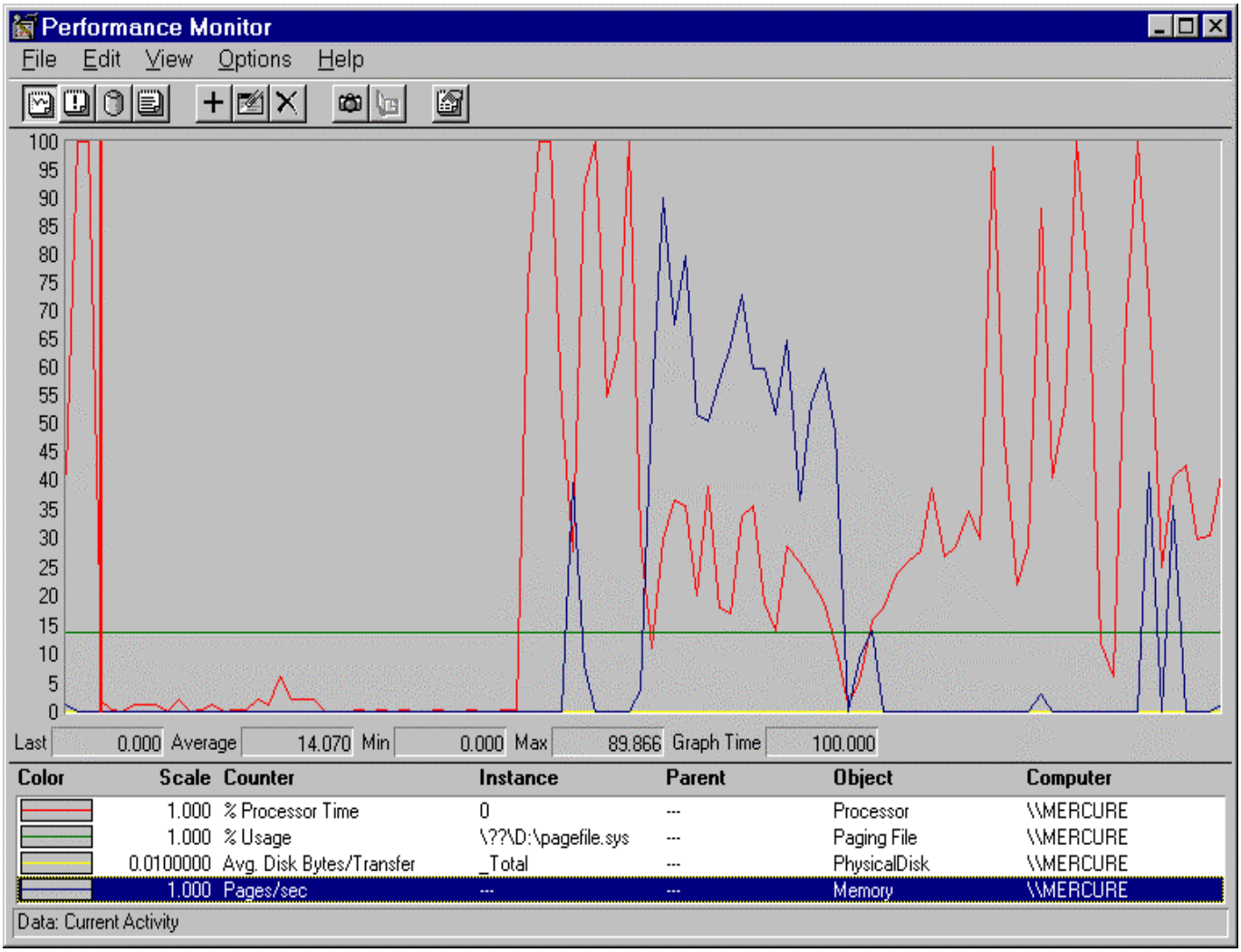
■ Comportement par défaut appliqué

La commande ***FICHIER / ENREGISTRER*** permet d'enregistrer cette nouvelle stratégie dans un fichier *.POL. Seul celui placé dans le partage NETLOGON (répertoire WINNT \ SYSTEM32 \ REPL \ IMPORT \ SCRIPT) sous le nom NTCONFIG.POL sera actif.

Attention : c'est une surcouche qui se rajoute au droits déjà existants

5.5 Mise en œuvre de l'analyseur de performances

Il s'appelle par la commande ***DEMARRER / PROGRAMMES / OUTILS D'ADMINISTRATION / ANALYSEUR DE PERFORMANCES***



5.5.1 Fonctionnement général

L'analyseur de performances est un outil graphique permettant de mesurer les performances des ordinateurs du réseau. Sur chaque ordinateur, il est possible d'afficher le comportement des objets (processeurs, mémoire, cache, threads, processus,...) Chacun de ces objets est associé à un ensemble de compteurs qui fournissent des informations sur l'utilisation des périphériques, les longueurs des files d'attente, les retards, les débits, la surcharge interne... Ces informations peuvent être vues sous forme de graphes, de messages d'alertes, de rapports qui reflètent l'activité.

L'analyseur de performances s'utilise donc :

① pour rechercher les causes de la lenteur ou de l'inefficacité d'un ordinateur ou d'une application

② pour surveiller les systèmes de façon continue et rechercher les goulets d'étranglement intermittent des performances

③ pour savoir s'il faut augmenter la capacité d'une ressource.

Il possède deux modes de fonctionnement : en temps réel ou en différé avec un journal. Par défaut, toute l'analyse se fait en temps réel.

5.5.2 Affichage graphique des performances

Après avoir sélectionné l'affichage graphique par la commande ***AFFICHAGE / GRAPHE***, la commande ***EDITION / AJOUTER AU GRAPHE*** présente une nouvelle fenêtre. Dans celle-ci, il faut successivement :

- sélectionner l'ordinateur à analyser
- sélectionner l'objet (souvent le processeur et la mémoire)
- pour chaque objet, sélectionner l'instance (un objet peut avoir plusieurs instances : un pour chaque disque physique par exemple)
- sélectionner le compteur voulu. En cas de besoin, le bouton ***EXPLIQUER*** définit clairement le rôle du compteur
- sélectionner éventuellement une échelle, une couleur et un type de trait pour le tracé
- terminer la commande par le bouton ***AJOUTER***

Ces différentes étapes sont à refaire pour chaque compteur. Lorsque tous les compteurs sont ajoutés, il faut fermer la fenêtre par le bouton ***TERMINER***. La fenêtre graphique affiche alors ces compteurs en temps réel.

Quels sont les éléments les plus courants à surveiller ?

✓ La mémoire avec les compteurs :

- Nombre de pages allouées par seconde
- Nombre de bits disponibles
- Nombre de fautes d'allocation de pages

✓ Le serveur avec les compteurs

- Nombre d'octets total par seconde
- Nombre d'accès aux ressources externes
- Nombre de connexions par seconde

✓ Le processeur

✓ Les disques physiques et logiques

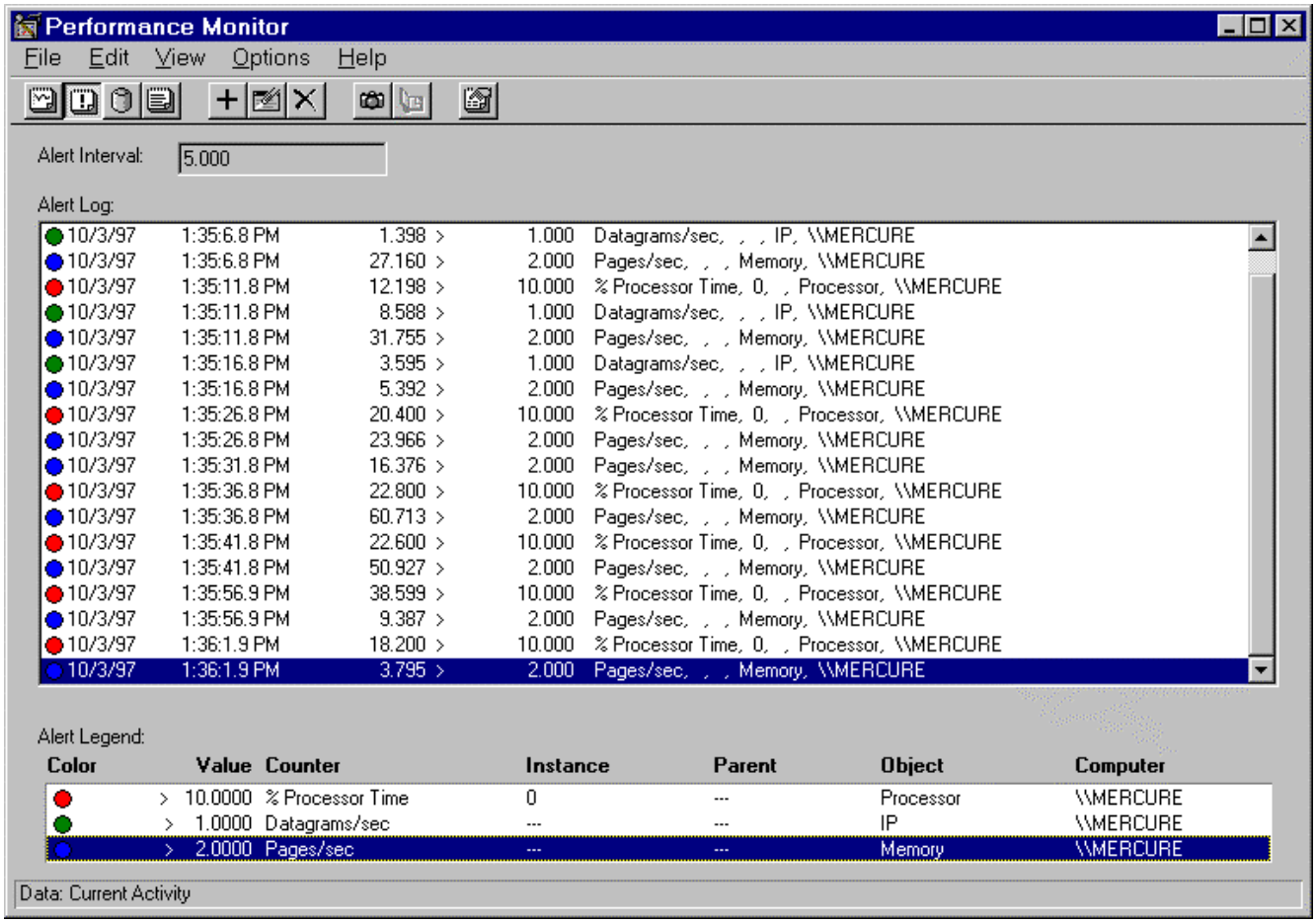
Qu'en déduire ?

✓ S'il y a plus de 5% de fautes d'allocations de page, la mémoire virtuelle n'est pas assez grande

✓ Si le processeur est saturé à 50 % pendant plusieurs minutes, il atteint ses limites

- ✓ Si le réseau est saturé à 60% en permanence avec des pics à 80%, il doit être amélioré (par exemple, augmenter le débit de la connexion)
- ✓ Si le disque est occupé à 80% sur une semaine, il faut augmenter la RAM

5.5.3 Mise en place d'alertes / de journal / de rapport



✍ *Les alertes*

La commande ***AFFICHAGE / ALERTES*** permet de gérer les alertes. La commande ***EDITION / AJOUTER DES ALERTES*** permet de sélectionner les compteurs de la même façon que pour le graphe. L'alerte se déclenche lorsque le compteur est au-dessus ou en-dessous du seuil indiqué. Elle permet de lancer un programme au moment de l'alerte. Ce programme peut être par exemple un message à envoyer à tous les utilisateurs (`NET SEND* "Serveur saturé"`). Ce programme peut être envoyé la première fois ou chaque fois que le compteur atteint le seuil critique.

✍ *Les rapports*

La commande ***AFFICHAGE / RAPPORTS*** permet de créer des rapports. La commande ***EDITION / AJOUTER*** permet de sélectionner les éléments à rajouter au rapport de la même façon que pour le graphe.

✍ *Le journal*

La commande ***AFFICHAGE / JOURNAL*** permet de créer un journal. La commande ***EDITION / AJOUTER*** permet de sélectionner les objets à rajouter au journal : *l'objet avec tous ses compteurs est rajouté au journal*.

La commande ***OPTIONS / JOURNAL*** permet de spécifier l'intervalle de temps (en millièmes de secondes) entre 2 écritures dans le journal. Elle permet surtout de spécifier dans quel fichier journal (*.LOG) les informations doivent être stockées. Lorsque le nom du fichier et son répertoire sont donnés, l'enregistrement des informations dans le fichier s'effectue par un clic sur le bouton ***DEMARRER LE JOURNAL***. L'enregistrement est continu jusqu'à ce qu'il soit arrêté par un clic sur le bouton ***FERMER LE JOURNAL*** dans cette même commande.

Par la commande ***OPTIONS / JOURNAL / FREQUENCE DE MISE A JOUR / MANUELLE,*** il est possible de ne pas enregistrer en continu les informations choisies. Les informations ne sont alors écrites dans le disque dur que lorsque l'administrateur appelle la commande ***OPTIONS / REACTUALISER*** ou appuie sur ***CTRL + U***.

La commande ***FICHIER / EXPORTER LE JOURNAL*** permet d'enregistrer ces informations dans un fichier au format *.TSV (délimité avec des tabulations) ou au format *.CSV (délimité avec des points virgules). Ces fichiers permettent de faire des statistiques sous Excel par exemple.

Attention : « on peut s'observer soi-même » et fausser l'analyse : par exemple si l'analyse porte sur les écritures sur le disque dur et que l'analyseur doit écrire ses informations sur le même disque dur !

5.5.4 L'analyse en différé

Pour faire une analyse en différé, plusieurs étapes sont nécessaires :

5.5.4.1 Préparation

- Il faut appeler l'***ANALYSEUR DE PERFORMANCES***
- Il faut d'abord sélectionner les objets à analyser par la commande ***EDITION / AJOUTER AU JOURNAL***
- Il faut ensuite configurer l'analyseur de performances par la commande ***OPTIONS / JOURNAL***

  Dans cette commande, il faut indiquer la fréquence d'enregistrements, le répertoire et le nom du fichier *.LOG qui contiendra les informations. Cette commande se termine par un clic sur le bouton ***ENREGISTRER***.
- Cette configuration est enfin sauvée dans un fichier de configuration par la commande ***FICHIER / ENREGISTRER LES PARAMETRES DU JOURNAL***

  Dans cette commande, il faut taper le répertoire et le nom du fichier *.PML qui contient la configuration choisie (objets sélectionnés, fichier *.LOG). Cette commande se termine par un clic sur le bouton ***ENREGISTRER***.

5.5.4.2 Mise en route de l'enregistrement

Par la suite, à chaque fois que l'administrateur désire enregistrer des données, il lui suffit de rappeler la configuration. Pour cela :

- Il faut appeler l'***ANALYSEUR DE PERFORMANCES***
- Il faut appeler la commande ***FICHIER /OUVRIR***

Dans cette commande, il faut sélectionner le fichier *.PML et cliquer sur le bouton ***OUVRIR***. A partir de là, les données sont enregistrées.

- Il est possible de placer des signets par la commande ***OPTIONS / SIGNETS***. Ils servent à repérer des événements marquants.

5.5.4.3 Utilisation du fichier journal ainsi obtenu

Après chargement du fichier journal ainsi obtenu, les informations s'étudient de façon « classique ».

- Il faut appeler l'***ANALYSEUR DE PERFORMANCES***.
- Il faut ensuite appeler la commande ***OPTIONS / DONNEES DEPUIS*** et sélectionner le fichier *.LOG qui contient les informations désirées.
- Il faut ensuite choisir le type d'affichage : ***AFFICHAGE / GRAPHE***, ***AFFICHAGE / ALERTE*** ou ***AFFICHAGE / RAPPORT***.
- La commande ***EDITION / AJOUTER*** permet de sélectionner les compteurs à afficher. Seuls les compteurs des objets enregistrés dans le journal peuvent être choisis.
- La commande ***EDITION / FENETRE TEMPORELLE*** permet de n'afficher qu'une partie des informations en spécifiant un point de départ et un point d'arrivée. Si des signets ont été placés pendant l'enregistrement, ils peuvent être utilisés comme point de départ et comme point d'arrivée.

5.6 Les ressources faisant l'objet d'analyses

5.6.1 La mémoire

L'utilisation de la mémoire peut être aussi surveillée en temps réel par le ***GESTIONNAIRE DE TACHES.***

En cas de saturation, plusieurs solutions sont possibles. Dans le ***PANNEAU DE CONFIGURATION***, la commande ***SYSTEME / PERFORMANCE*** permet de privilégier certaines fonctions par rapport à d'autres. Elle permet également de modifier la taille de la mémoire virtuelle. Mais la solution la plus sûre consiste à rajouter de la RAM !

5.6.2 Les processeurs

L'utilisation du temps CPU peut être aussi surveillée en temps réel par le ***gestionnaire de tâches.*** Un temps CPU important pendant quelques secondes ne constitue pas un problème particulier. Dans le cas d'une activité CPU importante pendant plusieurs minutes, voire plusieurs heures, il est important de vérifier, grâce notamment au gestionnaire de tâches, l'application ou les applications qui posent problèmes. Cela peut être le fait d'un service qui monopolise le serveur de façon anormale. Dans ce cas, il suffit de tuer l'application ou le service et de le relancer.

5.6.3 Le disque dur

Lorsque le disque est saturé, cela se traduit par un excès d'activité. Une solution consiste à rajouter un deuxième disque dur avec une deuxième carte contrôleur de façon à répartir l'activité sur les 2 disques. Par exemple, il est possible de mettre les fonctionnalités serveurs sur un disque et les applications comme SQL sur le deuxième. Dans le cas d'un serveur simple par exemple, il est possible de placer l'application SQL sur un disque et les données sur le deuxième.

5.6.4 Les réseaux

Windows NT gère **n** cartes réseaux. En cas de saturation, il est possible d'installer un service réseau par carte. Dans le ***PANNEAU DE CONFIGURATION***, la commande ***RESEAU / LIAISONS*** permet de sélectionner une carte et pour elle d'***ACTIVER*** ou de ***DESACTIVER*** une activité réseau. Cette même commande permet de ***MONTER*** et ***DESCENDRE*** la priorité de la carte pour une activité spécifique.

5.7 Surveillance et optimisation du service serveur de NT

5.7.1 par Performance Monitor

5.7.2 par la commande NETSTAT -s pour IP, NET et NET STATISTICS SERVER

Ces commandes doivent être tapées à partir de ***DEMARRER / PROGRAMMES / INVITE DE COMMANDES***.

La commande ***NETSTAT*** fournit des informations sur le réseau jusqu'au niveau protocole. Elle permet également, avec des paramètres, d'ajouter ou de supprimer des éléments. La commande ***NETSTAT /?*** donne une liste des paramètres possibles. Parmi ceux-ci, les plus utiles sont :

`NETSTAT -E`	Affiche des statistiques Ethernet générale
`NETSTAT -S`	Affiche des statistiques par protocole pour tous les protocoles actifs

La commande ***NET*** fournit des informations sur les échanges au niveau application. La commande ***NET /?*** affiche toutes les options possibles. Pour chacune, l'option ***/?*** donne des indications sur les possibilités de la commande. Parmi celles-ci, les plus utiles sont :

`NET ACCOUNTS`	Affiche des informations sur les comptes
`NET SHARE`	Affiche ou modifie des informations sur les partages
`NET USER USERNAME MOTDEPASSE` `NET USER USERNAME MOTDEPASSE`	Crée ou supprime un compte (paramètres `/ADD et /DELETE`)
`NET GROUP` `NET LOCALGROUP`	Ajoute ou supprimer un groupe (paramètres `/ADD et /DELETE`)
`NET COMPUTER \\NOMORDINATEUR` `NET COMPUTER \\NOMORDINATEUR`	Ajoute ou supprime un ordinateur (paramètres `/ADD et /DELETE`)
`NET CONFIG`	Change la configuration
`NET FILE`	Ferme un accès fichier
`NET PRINT`	Imprime
`NET SEND`	Envoie un message
`NET USE`	Se connecte à distance à un ordinateur ou une imprimante
`NET VIEW`	Affiche les ordinateurs du réseau

Les commandes ***NET STATISTICS SERVER*** et ***NET STATISTICS WORKSTATION*** fournissent des informations sur le réseau (nombre de sessions actives depuis le démarrage du réseau par

exemple). Les commandes ***NET STATISTICS SERVER*** ***\\NOMORDINATEUR*** fournit des informations sur le serveur indiqué.

5.8 Le gestionnaire de serveur

Il s'appelle par la commande ***DEMARRER / PROGRAMMES / OUTILS D'ADMINISTRATION / GESTIONNAIRE DE SERVEUR***

5.8.1 Fonctionnement général

En appelant le gestionnaire de serveur, vous avez une vision globale des ordinateurs qui sont rattachés à votre domaine NT, comme vous pourriez le voir dans le ***VOISINAGE RESEAU***. Cependant, le gestionnaire de serveur vous annonce directement le rôle de vos ordinateurs dans ce domaine, à savoir :

- Contrôleur de domaine principal

- Contrôleur de domaine secondaire

- Serveur indépendant

- Station de Travail NT

- Station de Travail WIN95 ou WIN 3.11

Suivant le type de machine, vous aurez la possibilité d'accéder à plusieurs fonctionnalités. Nous ne parlerons ici que des fonctions actives pour les machines sous Windows NT.

Il est à noter que l'accès à ces fonctions est bien sûr soumis à authentification et qu'il est impossible d'administrer ces machines si vous ne faites pas partie du groupe administrateur. Certaines fonctions sont néanmoins disponibles en lecture uniquement pour le groupe des utilisateurs normaux.

5.8.2 Editer les propriétés

Le gestionnaire de serveurs, bien que son nom ne l'indique pas sert tout autant à administrer à distance les stations de travail NT que les serveurs eux-mêmes. Le premier choix ***EDITER LES PROPRIETES*** permet de voir l'activité de la machine sélectionnée et notamment de voir les utilisateurs connectés, les sessions ouvertes, les partages utilisés.

Il permet de plus de changer la description de la machine, vous donnant ainsi tout loisir de spécifier son utilisation ou son rôle dans le domaine autrement que par son nom NetBios. Enfin, en appuyant sur Alertes, vous pouvez rediriger simplement les alertes administratives issues de cette machine NT à une autre machine ou à un utilisateur déterminé.

5.8.3 Répertoires partagés

Le deuxième choix vous permet d'afficher la liste de tous les partages disponibles sur la machine sélectionnée mais aussi de voir leur point physique (par exemple que le partage **Mon Partage** pointe sur **C:\Mes Documents**) mais aussi d'en afficher les permissions. Il vous est aussi possible de changer ces permissions, d'en restreindre le nombre d'accès

simultanés comme vous pourriez le faire avec l'explorateur NT. Une option permet même d'arrêter un partage déterminé.

Enfin, vous pourrez créer un nouveau partage à distance vous permettant ainsi de créer un accès à cette machine pour vous-même ou pour un groupe d'utilisateur. La seule restriction est qu'il faut connaître impérativement le répertoire physique sur lequel le partage doit s'appuyer avant de le créer , la commande ***PARCOURIR*** n'étant pas disponible dans le gestionnaire de serveur.

5.8.4 Services

Un des problèmes souvent rencontré est le manque d'informations concernant les services qui sont lancés sur les stations et de leurs états. Cette commande permettra de répondre à ce problème en affichant succinctement la liste des services de la machine sélectionnée et ainsi de pouvoir les relancer, les stopper, changer le login de lancement comme si vous le faisiez localement par le panneau de configuration.

5.8.5 Envoyer un message

Permet d'informer l'utilisateur de la station qu'une intervention est en cours. En fait, tout utilisateur connecté à la machine sélectionné sera prévenu, qu'il soit connecté localement ou par réseau.

5.8.6 Promulguer en contrôleur principal de domaine

Cette action n'est disponible que lors de la sélection d'un contrôleur secondaire de domaine et permet de promulguer cette machine en contrôleur principale sans perte d'activité ni redémarrage des serveurs. Il est à noter que cette action est maintenant réversible et que contrairement à NT3.51, l'activation d'un contrôleur de domaine principal dégrade automatiquement le contrôleur principal existant en secondaire.

5.8.7 Synchronisation du domaine

Cette action permet de forcer la resynchronisation de tous les contrôleurs secondaires auprès du contrôleur principal. Cette possibilité est importante lorsque des routeurs séparent deux contrôleurs ou qu'une panne réseau est survenue et que l'on n'est plus sûr de l'état des réplications de la base des utilisateurs.

5.8.8 Ajouter au domaine / Supprimer du domaine

Lorsqu'une nouvelle machine apparaît dans le domaine, il est possible de la faire s'inscrire dans le domaine à partir du panneau de configuration, onglet Réseau. Cette action est tout aussi possible à travers du gestionnaire de serveur mais cette fois-ci en ne quittant pas son siège. Il suffit tout simplement d'aller rajouter le nom de la machine NetBios du nouvel ordinateur devant rentrer dans le domaine. Cette fonction peut être utile de façon dérivée si l'on veut administrer une machine qui ne fait volontairement pas partie du domaine et que l'on veut tout de même administrer. Là encore, il suffira de la rajouter par cette commande, l'administration étant alors soumise aux droits de l'utilisateur sur cette machine.

Une fonctionnalité intéressante est la possibilité de supprimer une machine du domaine ce qui la mettra en quarantaine puisque même si un utilisateur se connecte sur cette machine avec un utilisateur et un mot de passe correct, il ne pourra accéder au domaine car c'est la machine elle-même qui sera interdite.

6. CONCLUSION

Un " serveur réseau " complet qui offre tous les services nécessaires avec le système. Mais encore en pleine évolution (voir Windows NT5.0 : modification de la notion de domaine, amélioration de l'administration à distance, IE 4.0)

Attention aux protocoles utilisés.

Malgré une simplicité apparente d'utilisation et des outils d'administration graphique, un serveur WinNT demande une bonne connaissance de l'administration réseau, des protocoles utilisés et des services mis en place.

Une mise à jour régulière est indispensable (suivie des " Services Packs " et des " Hotfixs") surtout pour la sécurité.

7. REFERENCES

Livres

Au coeur de Windows NT - Helen Custer - Edition Microsoft Press
Ressources Kit NT4 Server - Edition Microsoft Press
Ressources Kit NT4 Worstation - Edition Microsoft Press
TechNet : Technical Information Network (CdRom) - Microsoft
Inside Windows NT Server 4 - Drew heywood, Et Al - New Riders
TCP/IP Environnement NT - Edition ENI

Serveurs WWW

NT FAQ - Savilltech - mirroir sur le site de FWNTUG.
Microsoft : Windows NT Workstation
Microsoft : Windows NT server
Microsoft : Windows NT Server - Technical Support
Microsoft : Windows NT Whitepapers
Microsoft : Internet Resources for Windows NT
Windows NT Magazine : US
Windows NT Networking : cour en ligne de Brian Brown
Mémoire en ligne sur Windows NT de GUIMARD G., LE JAN F., PAGE O., TARDIEU F.
How to Create Internet Site with Windows NT only de John Neystadt
Unix to NT Ressource center
WWW-NT-fr
FWNTUG : French Windows NT User Group
NTSeek - NT Search Engine
NTWorld
WindowsNT ressource center
NTInternals

serveurs FTP (logiciels)

Windows NT Collection at WinSite (mirroir cica)
ENWAC (mirroir)
INDSTATE-Winsock-l (mirroir)
MICROSOFT (mirroir)
YORK (mirroir)

Voir http://www.urec.cnrs.fr/wnt/ pour les URL.