

Microsoft Windows 2000

# Implémentation d'une infrastructure réseau Microsoft Windows 2000

## **Essentiel** de préparation à la certification 70-216

*Par :*

**NEDJIMI Brahim  
THOBOIS Loïc  
TUDURY Matthieu**



23, rue Château Landon  
75010 – PARIS  
[www.supinfo.com](http://www.supinfo.com)

## Table des Matières :

<b>Module 1 Présentation de l'infrastructure réseau de Microsoft Windows 2000</b>	<b>7</b>
<b>1 Intranet</b>	<b>7</b>
<b>2 Accès distant</b>	<b>7</b>
<b>3 Bureau distant</b>	<b>7</b>
<b>4 Internet</b>	<b>7</b>
<b>5 Extranet</b>	<b>7</b>
<b>Module 2 Attribution automatique d'adresses IP à l'aide du protocole DHCP</b>	<b>8</b>
<b>1 Avantages du serveur DHCP</b>	<b>8</b>
<b>2 Fonctionnement du protocole DHCP :</b>	<b>8</b>
a) Attribution de bail IP :	8
b) Renouvellement de bail :	8
<b>3 Autorisation du service DHCP :</b>	<b>9</b>
<b>4 Configuration du serveur DHCP</b>	<b>9</b>
a) Création et configuration d'une étendue	9
<b>5 Personnalisation des fonctionnalités DHCP</b>	<b>9</b>
a) Regroupement d'étendues à l'aide d'étendues globales	10
b) Création d'adresses de multidiffusion à l'aide d'étendues de multidiffusion	10
<b>6 Configuration du service DHCP sur un réseau routé</b>	<b>10</b>
a) Configuration d'un réseau routé	10
b) Utilisation d'un agent de relais DHCP	10
<b>7 Résolution de problèmes de base de données DHCP</b>	<b>10</b>
<b>Module 3 Implémentation de la résolution de noms à l'aide du système DNS</b>	<b>11</b>
<b>1 Types de requêtes DNS</b>	<b>11</b>
a) Requêtes Itératives	11
b) Requêtes Récursives	11
<b>2 Type de recherche</b>	<b>11</b>
a) Recherche directe	11
b) Recherche inversée	12
<b>3 Installation du service serveur DNS</b>	<b>12</b>
<b>4 Configuration de la résolution des noms pour les ordinateurs</b>	<b>12</b>
<b>5 Configuration des fichiers Hosts</b>	<b>12</b>
<b>6 Création de Zones</b>	<b>12</b>
<b>7 Création de zones de recherche</b>	<b>13</b>
a) Recherche directe	13
b) Recherche inversée	13
<b>8 Configuration des zones</b>	<b>13</b>
a) Configuration de zones standard	13
b) Processus de transfert de zone	13
c) Configuration de transferts de zone	14
d) Création d'un sous domaine	14
e) Configuration de zones intégrées Active Directory	14
f) Migration d'un serveur BIND vers le serveur DNS de Windows 2000	15
<b>9 Intégration de serveurs DNS et DHCP</b>	<b>15</b>
a) Principe de fonctionnement des mises à jour DNS dynamiques	15
b) Configuration des mises à jour dynamiques	15

<b>10</b>	<b>Maintenance et dépannage des serveurs DNS</b>	<b>16</b>
a)	Réduction du trafic à l'aide des serveurs de cache	16
b)	Surveillance des serveurs DNS	16
<b>Module 4 Implémentation de la résolution de noms à l'aide de WINS</b>		<b>17</b>
<b>1</b>	<b>Noms NetBIOS</b>	<b>17</b>
a)	Enregistrement de noms NetBIOS	17
b)	Résolution de noms	17
c)	Mise à disposition de noms	17
d)	Cache de noms NetBIOS	17
e)	Fichier Lmhosts	17
<b>2</b>	<b>Interopérabilité entre le service WINS et le Système DNS.</b>	<b>18</b>
<b>3</b>	<b>Mappages Statiques</b>	<b>18</b>
<b>4</b>	<b>Proxy WINS</b>	<b>18</b>
<b>5</b>	<b>Duplication WINS</b>	<b>18</b>
a)	Partenaires Emetteur/Collecteur (Push/Pull)	18
<b>6</b>	<b>Maintenance de la base de données d'un serveur WINS</b>	<b>18</b>
a)	Compactage de la base de données WINS	18
b)	Sauvegarde et restauration de la base de données WINS	18
<b>Module 5 Configuration de la sécurité du réseau à l'aide de clé publique</b>		<b>20</b>
<b>1</b>	<b>Présentation de l'infrastructure de clé publique</b>	<b>20</b>
a)	Cryptage par clé publique	20
b)	Authentification par clé publique	20
c)	Autorité de certification	20
d)	Infrastructure de clé publique de Windows 2000	21
<b>2</b>	<b>Déploiement de services de certificats</b>	<b>21</b>
a)	Choix d'un modèle d'Autorité de certification	21
b)	Sauvegarde et restauration des services de certificats	22
<b>3</b>	<b>Utilisation des certificats</b>	<b>22</b>
a)	L'assistant de requête de certificat	22
b)	Pages Web des services de certificats	22
<b>4</b>	<b>Gestion des certificats</b>	<b>22</b>
a)	Délivrance des certificats	22
b)	Révocation des certificats	22
c)	Importation et exportation de certificats	22
<b>Module 6 Configuration de la sécurité du réseau à l'aide du protocole IPSec</b>		<b>24</b>
<b>1</b>	<b>Présentation</b>	<b>24</b>
<b>2</b>	<b>Stratégies IPSec</b>	<b>24</b>
a)	Les différentes stratégies IPSec	24
b)	Modes de connexions	24
c)	Personnalisation des stratégies IPSec	24
d)	Modèle de cryptage	24
e)	Optimisation du protocole IPSec	25
<b>Module 7 Configuration de l'accès distant</b>		<b>26</b>
<b>1</b>	<b>Présentation de l'accès distant sous Windows 2000</b>	<b>26</b>
a)	Types de connectivité d'accès distant	26
b)	Protocoles de transport de données	26
c)	Protocoles VPN	27
<b>2</b>	<b>Configuration du serveur d'accès distant</b>	<b>27</b>
a)	Configuration des connexions entrantes d'accès distantes	27
b)	Configuration des paramètres d'accès entrant d'un utilisateur	27

<b>3</b>	<b>Configuration des clients d'accès distant</b>	<b>27</b>
a)	Mise en place d'une connexion à un serveur d'accès distant	27
b)	Configuration de connexions à liaison multiples	28
c)	Les protocoles d'authentification standard	28
d)	Configuration des protocoles de cryptage	28
<b>4</b>	<b>Intégration du protocole DHCP avec le service de Routage et d'accès distant</b>	<b>28</b>
<b>Module 8 Prise en charge de l'accès distant à un réseau</b>		<b>29</b>
<b>1</b>	<b>Stratégies d'accès distant</b>	<b>29</b>
a)	Composants d'une stratégie	29
b)	Examen de l'évaluation des stratégies d'accès distant	29
<b>2</b>	<b>Contrôle de l'accès distant</b>	<b>29</b>
<b>Module 9 Extension des fonctionnalités d'accès distant à l'aide du service IAS</b>		<b>30</b>
<b>1</b>	<b>Présentation du service IAS</b>	<b>30</b>
<b>2</b>	<b>Présentation des services IAS et RADIUS sur un réseau Windows 2000</b>	<b>30</b>
<b>3</b>	<b>Installation et configuration du service IAS</b>	<b>30</b>
<b>Module 10 Configuration d'un serveur Windows 2000 en tant que routeur</b>		<b>31</b>
<b>1</b>	<b>Rappel</b>	<b>31</b>
a)	Rôle d'un routeur	31
b)	Tables de routage	31
<b>2</b>	<b>Configuration des connexions réseaux</b>	<b>31</b>
<b>3</b>	<b>Configuration d'itinéraires statiques</b>	<b>31</b>
<b>4</b>	<b>Configuration d'une interface de routage</b>	<b>31</b>
a)	Interface de routage dans le service Routage et Accès distant	31
b)	Filtrage de paquets	31
<b>5</b>	<b>Implémentation du routage à la demande</b>	<b>32</b>
a)	Configuration d'itinéraires statiques pour une interface de numérotation à la demande	32
<b>6</b>	<b>Configuration du protocole RIP</b>	<b>32</b>
a)	Protocoles de routage	32
b)	Fonctionnement du protocole RIP	32
<b>Module 11 Configuration de l'accès Internet pour un réseau</b>		<b>34</b>
<b>1</b>	<b>Méthodes disponibles pour connecter un réseau à Internet</b>	<b>34</b>
a)	Connexion à Internet à l'aide d'un routeur	34
b)	Sécurisation des connexions Internet à l'aide d'un pare-feu	34
c)	Connexion à Internet à l'aide du protocole NAT	34
d)	Connexion à l'aide du partage de connexion Internet	34
e)	Connexion à l'aide d'un serveur proxy	35
<b>2</b>	<b>Configuration de l'accès à Internet</b>	<b>35</b>
a)	Configuration de l'accès Internet à l'aide d'un routeur	35
b)	Configuration de l'accès Internet à l'aide du protocole NAT	35
<b>Module 12 Configuration d'un serveur Web</b>		<b>36</b>
<b>1</b>	<b>Services Internet</b>	<b>36</b>
<b>2</b>	<b>Configuration d'un site Web</b>	<b>36</b>
a)	Configuration de l'identification de sites Web	36
b)	Méthodes d'authentification	36
c)	Affectation d'un document par défaut	36
<b>3</b>	<b>Administration des Services Internet</b>	<b>36</b>
a)	Application des dernières mises à jour de sécurité	36
b)	Analyse des Services Internet	36

<b>Module 13 Déploiement de Windows 2000 Professionnel à l'aide des services RIS</b>	<b>37</b>
<b>1 Vue d'ensemble</b>	<b>37</b>
<b>2 Prérequis pour l'utilisation de RIS</b>	<b>37</b>
a) Services réseau	37
b) Serveurs hébergeant RIS	37
c) Configuration requise pour les ordinateurs clients	37
<b>3 Installation des services RIS</b>	<b>37</b>
<b>4 Configuration des services RIS</b>	<b>38</b>
a) Autorisation du serveur RIS dans Active Directory	38
b) Configuration spécifique aux ordinateurs clients	38
c) Préconfiguration des ordinateurs clients	38
d) Configuration des options d'installation client	39
<b>5 Déploiement d'images</b>	<b>39</b>
a) Modification d'une image de CD-ROM via un fichier de réponse	39
b) Accès aux images par les utilisateurs	39
c) Installation d'une image sur un client RIS	39
<b>6 Images RipRep</b>	<b>40</b>
<b>Module 14 Gestion d'un réseau Windows 2000</b>	<b>41</b>
<b>1 Vue d'ensemble</b>	<b>41</b>
<b>2 Administration à distance via Terminal Server</b>	<b>41</b>
a) Présentation de Terminal Server	41
b) Le protocole RDP	41
c) Caractéristiques des services Terminal Server en mode administration à distance	41
d) Installation des services Terminal Server	42
<b>3 SNMP sous Windows 2000</b>	<b>42</b>
a) Système de gestion SNMP	42
b) Agent SNMP	42
c) Bases MIB	42
d) Communautés SNMP	42
e) Installation du service SNMP	43
f) Configuration du service SNMP	43
g) Validation de la configuration SNMP à l'aide de SNMPUTIL	43
<b>Module 15 Dépannage des services réseau de Windows 2000</b>	<b>45</b>
<b>1 Identification et diagnostic de problèmes réseau</b>	<b>45</b>
a) Problème matériel	45
b) Exploitation des messages d'erreur	45
c) Observateur d'évènements	45
d) Utilitaires de dépannage	45
<b>2 Résolution des problèmes de protocole TCP/IP</b>	<b>45</b>
a) Vérification de la configuration TCP/IP via <i>ipconfig</i>	45
b) Vérification des connexions TCP/IP	46
c) Dépannage du routage IP	46
d) Résolution d'adresses IP en adresses matérielles	46
<b>3 Résolution des problèmes de résolution de noms</b>	<b>47</b>
a) Principe de la résolution de noms	47
b) Ordre de résolution (NetBIOS)	47
c) Problèmes de noms NetBIOS	47
d) Problèmes de noms d'hôtes	48
<b>4 Résolution des problèmes de services réseau</b>	<b>48</b>
<b>5 Surveillance à l'aide du moniteur réseau</b>	<b>48</b>
<b>Module 16 Configuration de la connectivité réseau entre systèmes d'exploitation</b>	<b>50</b>

<b>1</b>	<b>Vue d'ensemble</b>	<b>50</b>
<b>2</b>	<b>Accès aux ressources Netware.</b>	<b>50</b>
<b>3</b>	<b>Connexion à un réseau Novell Netware</b>	<b>50</b>
a)	Clients pour réseau Netware	50
b)	Services Passerelle pour Netware	50
<b>4</b>	<b>Connexion à des hôtes SNA</b>	<b>50</b>
<b>5</b>	<b>Intégration réseau AppleTalk</b>	<b>51</b>
<b>6</b>	<b>Services pour Unix v2.0</b>	<b>51</b>

## Module 1

### Présentation de l'infrastructure réseau de Microsoft Windows 2000

Les produits de la gamme serveur de Windows 2000 proposent un ensemble de technologies permettant de faciliter la gestion de votre infrastructure réseau. Ceci prend en compte l'ensemble des éléments suivants :

#### **1 Intranet**

L'intranet représente le réseau privé d'une entreprise qui utilise des technologies liées à Internet (serveur Web, messagerie) pour diffuser de l'information et partager des ressources.

#### **2 Accès distant**

L'accès distant permet de se connecter au réseau de l'entreprise afin que les travailleurs itinérants ou l'administrateur puissent utiliser les ressources à distance. L'accès distant permet le choix entre la connexion directe (Modem, RNIS) et la connexion via tunnelling (VPN).

#### **3 Bureau distant**

Permet de connecter de façon plus ou moins permanente plusieurs succursales (ou filiales) distantes à leur siège. Cela est couramment mis en place via des lignes spécialisées et des routeurs.

#### **4 Internet**

Windows 2000 permet de connecter l'entreprise à Internet pour permettre aux utilisateurs d'en exploiter les ressources. On fait alors appel à un ISP (pour les petites structures) ou à la location d'une ligne dédiée.

#### **5 Extranet**

Consiste en la mise en place d'une structure facilitant l'accès par différentes entités distinctes (fournisseurs, clients, ...) aux informations de l'entreprise.

## Module 2

### Attribution automatique d'adresses IP à l'aide du protocole DHCP

#### 1 Avantages du serveur DHCP

Le serveur DHCP permet d'alléger la charge administrative; les ordinateurs ont toujours une adresse IP correcte et des informations de configuration correcte. Cette technologie permet de limiter les manipulations administratives à réaliser sur les clients au niveau de la configuration réseau.

#### 2 Fonctionnement du protocole DHCP :

##### a) Attribution de bail IP :

Lorsque vous allumez votre ordinateur pour la première fois, il fait une demande de bail IP en diffusant le message DHCPDISCOVER à l'aide d'une version limitée du protocole TCP/IP.

Tous les serveurs DHCP qui disposent d'une adresse IP valide pour le segment répondent avec un message DHCPOFFER contenant l'adresse matérielle du client, l'adresse IP proposée, un masque de sous réseau, la durée du bail et l'adresse IP du serveur DHCP.

L'adresse IP proposée est réservée par le serveur, pour éviter de la proposer à un autre client durant le laps de temps qui sépare la proposition de la réservation par le client.

Si le client ne reçoit pas de réponse d'un serveur DHCP, il renvoie un DHCPDISCOVER au bout de 2 puis 4, 8, 16 secondes à laquelle on ajoute une durée aléatoire entre 0 et 1000 ms.

Si le client n'a pas obtenu de réponse, il utilise une adresse IP comprise dans la plage d'adresse 169.254.0.1 et 169.254.255.254 (APIPA). Le client continue de rechercher un serveur DHCP toutes les 5 minutes.

Lorsque le client reçoit une offre d'adresse IP, il répond à la première qu'il reçoit en diffusant un message DHCPREQUEST pour l'accepter. Toutes les adresses IP proposées par les autres serveurs DHCP sont alors libérées.

Le serveur DHCP qui a émis l'offre acceptée envoie un accusé de réception DHCPACK. Ce message contient le bail ainsi que les informations de configuration.

Lorsque le client DHCP reçoit l'accusé de réception, il initialise le protocole TCP/IP.

##### b) Renouvellement de bail :

Un client DHCP tente automatiquement de renouveler son bail à 50% de sa durée. Pour cela, il envoie un message DHCPREQUEST au serveur DHCP qui lui a fourni son bail. Le serveur DHCP lui retourne un DHCPACK contenant la durée du nouveau bail ainsi que les paramètres de configuration mis à jour.

Si le serveur DHCP n'est pas présent, il réessayera à 75% de la durée du bail puis à 87,5% ; s'il n'a pas reçu de réponse à 87,5% alors il enverra un message DHCPDISCOVER auprès de tous les serveurs DHCP. S'il reçoit un DHCPOFFER pour mettre à jour son bail en cours, alors il effectuera le renouvellement auprès de ce serveur DHCP à compter de ce moment.

Si le bail expire, alors, le client cesse immédiatement d'utiliser l'adresse IP et recommencera toute la procédure d'attribution

Lorsque vous démarrez un ordinateur qui dispose d'un bail toujours valide, il commence par tenter le renouvellement de bail.

Si un client demande le renouvellement d'un bail non valide (machine déplacée) ou en double, le serveur DHCP répond par un DHCPNAK, le client est alors contraint d'obtenir une nouvelle adresse IP.

Il est possible de demander le renouvellement du bail manuellement à l'aide de la commande **ipconfig /renew**.

Il est aussi possible de forcer l'abandon d'un bail avec la commande **ipconfig /release**. Le message DHCPRELEASE sera envoyé au serveur DHCP et le protocole TCP/IP sera stoppé.

### 3 Autorisation du service DHCP :

Sur un réseau avec un domaine Windows 2000, vous devez autoriser le serveur DHCP, sinon, celui-ci ne répondra pas aux clients.

✍ Seul les serveurs DHCP Windows 2000 vérifient l'autorisation.

Un serveur DHCP, pendant son initialisation, diffuse le message DHCPINFORM. Les serveurs DHCP en fonctionnement lui retournent un DHCPACK contenant les informations du domaine racine Active Directory, à l'aide desquelles il contacte le contrôleur de domaine pour vérifier qu'il fait partie de la liste des serveur DHCP autorisés puis démarre. S'il n'est pas autorisé, le service DHCP ajoute un message d'erreur au journal des événements et ne répond pas aux clients.

### 4 Configuration du serveur DHCP

#### a) Création et configuration d'une étendue

Pour utiliser l'adressage IP dynamique, vous devez créer une étendue sur le serveur. Chaque étendue se caractérise par un nom, une description, une plage d'adresses IP avec le masque de sous réseau correspondant, une durée de bail et les plages d'IP exclues (facultatif).

Il faut activer une étendue pour qu'elle soit disponible.

#### Configuration de la durée de bail :

Une durée de bail courte est conseillée lorsque vous avez plus d'adresses IP que de machines. Dans ce cas, lorsque l'on éteint des machines, leur adresse IP est plus rapidement libérée. C'est aussi utile lorsque les paramètres du réseau changent souvent.

Une durée de bail plus longue permet de diminuer le trafic réseau engendré par le renouvellement des IP.

Une durée de bail illimitée supprime le trafic engendré par le protocole DHCP. En effet, les clients ne l'utilisent qu'au démarrage de la machine.

#### Options d'étendues :

Les options d'étendues permettent de fournir diverses informations en même temps que l'adresse IP.

Les options d'étendues courantes sont l'adresse de la passerelle par défaut, le nom de domaine DNS, l'adresse des serveurs DNS et WINS, le type de Nœud WINS.

Les options d'étendues peuvent être définies à plusieurs niveaux, cela simplifie l'administration.

Au niveau du serveur, les options s'appliquent à tous les clients DHCP.

Au niveau de l'étendue, les options s'appliquent uniquement sur les clients DHCP qui reçoivent un bail de cette étendue, elles sont prioritaires sur les options de serveur.

Au niveau de la classe, les options sont appliquées sur les clients qui appartiennent à la classe. Les classes doivent être définies sur les clients. Les options de classe sont prioritaires sur les options d'étendues et les options de serveur.

Au niveau du client réservé, les options que vous définissez au niveau du client sont prioritaires sur toutes les autres options.

#### Réservations d'adresse IP pour les ordinateurs clients :

Vous pouvez réserver une adresse IP spécifique pour un client en faisant une réservation (basée sur l'adresse MAC du client).

### 5 Personnalisation des fonctionnalités DHCP

### a) Regroupement d'étendues à l'aide d'étendues globales

Une étendue globale est un groupe de deux ou plusieurs étendues combinées pour que vous puissiez les gérer sous la forme d'une seule unité. Lorsqu'un client demande un bail à un serveur DHCP ayant plusieurs étendues combinées dans une étendue globale, alors le serveur « piochera » indifféremment dans l'une ou l'autre des étendues. Les étendues globales permettent de ne pas avoir à supprimer et recréer des étendues existantes.

### b) Création d'adresses de multidiffusion à l'aide d'étendues de multidiffusion

Pour permettre l'utilisation d'adresses de multidiffusion dynamiques, vous devez créer une étendue de multidiffusion sur le serveur DHCP (DCP dans ce cas précis) les clients doivent pouvoir utiliser le protocole MADCAP et les routeurs entre l'ordinateur source et les ordinateurs de destination doivent être configurés pour reconnaître l'adresse de multidiffusion.

## 6 Configuration du service DHCP sur un réseau routé

Le protocole DHCP étant basé sur la diffusion, il existe des problèmes liés aux réseaux routés car les routeurs sont généralement configurés pour ne pas envoyer les messages de diffusion aux autres sous réseaux.

### a) Configuration d'un réseau routé

Inclure un serveur DHCP dans chaque sous réseau physique.  
Configurer un routeur conforme à la RFC 1542 pour l'envoi de messages DHCP entre sous réseaux.  
Configuration d'agents de relais DHCP.

### b) Utilisation d'un agent de relais DHCP

Si votre réseau physique est séparé en deux par un routeur non conforme à la RFC 1542, et que vous ne souhaitez pas installer plusieurs serveurs DHCP, vous pouvez installer dans le sous réseau qui ne contient pas de serveur DHCP un agent de relais DHCP qui transférera les requêtes des clients au serveur DHCP à l'aide de paquets dirigés.

Il est aussi possible d'utiliser un agent de relais DHCP pour assurer la tolérance aux pannes.

 Le service RRAS doit être activé sur la machine pour que le relais DHCP puisse fonctionner.

## 7 Résolution de problèmes de base de données DHCP

La base de donnée DHCP se situe dans Racine\_système\System32\dhcp.  
Les sauvegardes se situent dans Racine\_système\System32\dhcp\backup\jet\new.  
L'utilitaire JetPack.exe permet de compacter et de réparer la base de donnée.

Si la réparation de la base de donnée échoue, vous pouvez la restaurer à partir du répertoire de sauvegarde.

## Module 3

### Implémentation de la résolution de noms à l'aide du système DNS

Le système de noms DNS est une base de données distribuée utilisée sur les réseaux IP pour transposer et résoudre les noms d'ordinateurs en adresse IP. C'est la principale méthode de résolution de noms de Windows 2000.

La structure hiérarchique de l'espace de noms de domaines est telle que :

- Le domaine racine, qui se trouve en haut de la structure du nom de domaine, est représenté par un point.
- Les domaines de premier niveau suivent directement les domaines racines ; ils peuvent être représentés par le type d'organisation ou la localisation géographique (ex : com, org, fr, de, ...)
- Les domaines de deuxième niveau sont enregistrés directement auprès des entreprises et peuvent posséder de nombreux sous domaines.

Le Nom de Domaine Pleinement Qualifié ou FQDN (Fully Qualified Domain Name) décrit la relation exacte entre un hôte et son domaine.

Dans les FQDN suivant : web.labo-microsoft.supinfo.com, le domaine racine est le '.' A partir de la droite du nom de domaine, le '.com' est le nom de domaine de 1<sup>er</sup> niveau, le '.supinfo' est le nom de domaine du deuxième niveau et le reste sont des sous domaines dans la présente arborescence de noms de domaines.

Le serveur DNS contient des informations de la portion de l'espace de noms DNS qu'il va fournir au client. Le serveur DNS va stocker des noms / adresses IP de sa zone dans un fichier de zone. Lorsqu'un ordinateur client envoie une requête de résolution de nom à un serveur DNS, ce dernier va consulter sa base de données de noms et va, soit répondre au client s'il possède la correspondance nom / adresse IP, soit interroger les autres serveurs DNS en cas d'échec de la recherche dans sa base de données locale.

## 1 Types de requêtes DNS

### a) Requêtes Itératives

Elle sont envoyées par un client à un serveur DNS. Ce dernier renvoie la meilleure réponse qu'il possède à partir de ses données de cache ou de zone. S'il ne possède pas la réponse exacte, il renvoie le client vers un serveur de référence dans un niveau inférieur de l'espace de nom de domaine. Le client va alors interroger le serveur correspondant. Ce processus se poursuit jusqu'à ce que le client localise le serveur qui pourra résoudre le nom en adresse IP ou bien jusqu'à ce qu'une erreur se produise ou encore que le délai soit dépassé.

### b) Requêtes Récursives

Le serveur DNS doit absolument fournir un résultat au client pour ce type de requête. Dans le cas où il ne possède pas la réponse à la requête, il va effectuer (pour le compte du client) des requêtes itératives séparées vers d'autres serveurs qui l'aident à répondre à la requête récursive.

## 2 Type de recherche

Le type de recherche détermine les tâches qu'effectuera le serveur DNS. Ainsi, une zone sera utilisée pour la résolution par recherche directe ou inversée. Il suffit d'indiquer au moment de sa création quel sera son type, c'est-à-dire directe ou inversée.

### a) Recherche directe

Elle est utilisée pour retrouver l'adresse IP d'une machine sur le réseau local ou sur Internet à partir de son nom de machine. Elle nécessite une résolution de nom de machine en adresse IP par le serveur DNS. L'adresse IP trouvée sera renvoyée à la machine cliente.

## b) Recherche inversée

Elle est utilisée pour retrouver le nom d'une machine à partir de son adresse IP. On peut imaginer qu'en cas de surveillance des connexions IO qui sont faites à un serveur, on veuille localiser le nom de domaine de la machine associée à l'adresse IP utilisée pour se connecter. Elle nécessite donc une résolution d'adresse IP en nom de machine.

## 3 Installation du service serveur DNS

Il est nécessaire de configurer le futur serveur DNS pour qu'il utilise une adresse IP fixe au lieu d'une adresse attribuée dynamiquement par un serveur DHCP. Il faut pour cela configurer le protocole TCP/IP, et entrer une adresse statique dans la boîte de dialogue **Propriétés de protocole Internet**. Microsoft recommande également de configurer le nom de domaine sur le serveur DNS, dans **Propriétés de protocole Internet** (TCP/IP).

L'installation se fait via l'assistant « ajout / suppression de programmes ». Le service Serveur DNS fait partie des services de mise en réseau. (Composants intégrés de Windows 2000).

## 4 Configuration de la résolution des noms pour les ordinateurs

Les ordinateurs clients vont émettre des requêtes de résolution de noms de machines en adresses IP aux serveurs DNS du réseau.

Dans les propriétés du protocole Internet (TCP/IP), on peut indiquer que les adresses IP des serveurs DNS sont fournies par un serveur DHCP ou l'on peut indiquer manuellement les adresses des serveurs DNS (primaire et auxiliaire) à utiliser.

## 5 Configuration des fichiers Hosts

Un fichier Hosts est un fichier texte qui contient les correspondances statiques entre les noms d'hôte et les adresses IP. Windows 2000 peut utiliser un fichier Hosts local pour la résolution de nom, ce qui permet d'obtenir une réponse plus rapide aux requêtes DNS puisque le fichier Hosts est interrogé avant d'interroger n'importe quel serveur DNS. La mise à jour de ces fichiers se fait manuellement, et l'éditeur de texte de Windows 2000 peut être utilisé à cet effet.

## 6 Création de Zones

Une zone est une portion contiguë de l'espace de noms de domaine pour laquelle un serveur DNS sert de référence pour la résolution des requêtes DNS. Elle permet de stocker des noms concernant un ou plusieurs domaines DNS ou des portions de domaines DNS.

Un serveur DNS peut héberger différents types de zones tout comme un ou différents types de zones peuvent être hébergés sur plusieurs serveurs DNS pour fournir une tolérance aux pannes et répartir la résolution des noms et de la charge de travail.

Un enregistrement de ressource stocké dans un fichier de zone définit une zone. Le fichier de zone stocke des informations pour effectuer la résolution de noms. Toutes les tâches administratives liées aux serveurs DNS se font à travers le snap-in mmc DNS.

Pour effectuer ces tâches sur une serveur DNS non contrôleur de domaine, vous devez faire partie du groupe Administrateurs sur cet ordinateur ; dans le cas d'un contrôleur de domaine, vous devez faire être membre de l'un des groupes suivants : Administrateurs DNS, Administrateurs du domaine ou Administrateurs de l'entreprise.

Il existe différents types de zone :

<b>Principale standard</b>	Contient une version en lecture écriture dans un fichier texte. Récupère toute les modifications de la zone. Doit toujours être créée en premier pour une nouvelle zone.
----------------------------	--

<b>Secondaire standard</b>	Contient la copie en lecture seule du fichier de la zone principale standard. Toute modification effectuée sur le fichier de zone principale standard est répliquée sur celui-ci. Permet de répartir la charge de résolution de noms des serveurs DNS.
<b>Intégrée Active Directory</b>	Les informations contenant la zone DNS sont stockées dans la base Active Directory et non dans un fichier texte. Les mises à jour ont lieu automatiquement pendant la réplication d'Active Directory. Cette méthode améliore la tolérance aux pannes en éliminant le point unique d'échec.

## 7 Création de zones de recherche

Les clients DNS réalisent principalement deux types de recherche, les recherches directes et les recherches inversées.

### a) Recherche directe

Lorsque vous créez une zone de recherche directe, l'assistant vous proposera les trois types de zone disponibles, puis il vous invitera à entrer le nom de la zone à gérer et enfin il vous demandera de valider le nom du fichier contenant la zone DNS. Une fois ces étapes passées, l'assistant va créer automatiquement la zone, le fichier et des enregistrements de type "Source de nom" (Serveur ayant l'autorité sur la zone) et "Serveurs de noms" (Serveur pouvant répondre aux requêtes des clients).

### b) Recherche inversée

Lorsque vous créez une zone inversée, l'assistant vous propose d'indiquer l'ID (Partie réseau de votre adresse IP). Pendant que vous entrez l'ID, le nom de la zone de recherche inversée s'affiche sous la forme des nombres de votre ID en ordre inverse suivi de ".in-addr.arpa" (ex : Pour "172.16.0.0/16"  $\rightarrow$  "16.172.in-addr.arpa"). Le nom in-addr.arpa représente un domaine spécial au niveau DNS, il est réservé à la résolution d'adresses IP en noms d'hôtes.

## 8 Configuration des zones

### a) Configuration de zones standard

Il est possible, lors de la configuration d'un serveur DNS sous Windows 2000, de configurer sur le même serveur une zone en tant que principale standard (ex : microsoft.supinfo.com) et une zone en tant que secondaire standard (ex : supinfo.com).

De plus lorsque l'on configure une zone secondaire standard, il est possible de lui spécifier une liste de serveurs DNS maîtres à partir desquels les informations de zone seront récupérées. Dans cette liste pourront apparaître aussi bien des serveurs maintenant une zone secondaire que principale.

### b) Processus de transfert de zone

Le transfert de zone consiste en la diffusion des entrées contenues dans une zone à l'ensemble des serveurs DNS secondaires de cette zone.

Sous Windows 2000, il est possible de mettre en place des transferts de zone incrémentiels qui ne diffusent que les modifications du fichier de zone.

Le processus de transfert de zone intervient dans 2 cas :

- Un serveur maître envoie une notification de modification de la zone aux serveurs DNS secondaires de la zone. Une fois cette notification reçue, les serveurs secondaires envoient une requête de mise à jour au serveur maître.
- Chaque serveur DNS secondaire interroge à intervalles réguliers ses serveurs maîtres sur les modifications sur la zone. Cette requête est lancée aussi à chaque démarrage du service DNS.

### c) Configuration de transferts de zone

Toutes les informations liées à la fréquence d'exécution des transferts de zone sont stockées dans les enregistrements de ressource de noms (SOA – Start of Authority).

Un certain nombre de paramètres sont modifiables (dans les propriétés de la zone) :

<b>Numéro de série</b>	Le numéro de série fonctionne comme un numéro de version (il est donc incrémenté à chaque version) permettant de savoir si, lors de la synchronisation avec le serveur maître, la zone doit être mise à jour.
<b>Serveur principal</b>	Le serveur principal précise le nom de domaine complet du serveur principal.
<b>Personne responsable</b>	La personne responsable sera avertie par e-mail à chaque fois qu'une erreur se produit lors d'un transfert de zone.
<b>Intervalle d'actualisation</b>	L'intervalle d'actualisation spécifie la fréquence à laquelle un serveur secondaire va envoyer une requête de mise à jour à son serveur maître.
<b>Intervalle avant nouvelle tentative</b>	L'intervalle avant nouvelle tentative détermine l'intervalle de temps qu'un serveur secondaire va prendre pour re-contacter son serveur maître suite à l'échec de la tentative d'une mise à jour.
<b>Expire après</b>	Définit le délai d'expiration d'un serveur secondaire s'il n'arrive pas à contacter son serveur maître. A la suite de l'expiration il ne répondra plus aux requêtes de la zone.
<b>Durée de vie minimale</b>	La durée de vie (TTL) minimale indique le temps durant lequel un serveur peut mettre en cache des informations pour une zone.
<b>Durée de vie pour cet enregistrement</b>	Spécifie la durée TTL de l'enregistrement SOA.

Il est possible de limiter le nombre de serveurs que vous allez autoriser à recevoir les zones. Ceci est défini soit par une liste d'adresse IP de serveurs DNS soit en limitant les transferts aux serveurs DNS situés dans le même domaine. De la même manière, il est possible de définir une liste de serveur DNS secondaires qui recevront une notification des mises à jour d'un fichier de zone.

### d) Création d'un sous domaine

Un sous domaine est un domaine (appelé domaine enfant) hiérarchiquement situé sous un autre domaine (appelé domaine parent). Cette structure permet une meilleure organisation d'une zone ainsi qu'une délégation de pouvoir facilitée. Par exemple, dans **labo-microsoft.supinfo.com**, **labo-microsoft** est le domaine enfant, **supinfo** est le domaine parent et **com** le domaine de rang primaire).

La création d'un sous domaine peut passer par deux méthodes selon que l'on désire que le nouveau domaine soit géré par le même serveur DNS que le domaine parent ou que l'on désire que le domaine enfant soit stocké et géré sur un autre serveur DNS.

### e) Configuration de zones intégrées Active Directory

L'intégration des zones DNS dans l'Active Directory permet de stocker les zones DNS dans l'Active Directory et ainsi bénéficier d'un certain nombre d'avantages :

<b>Pas de point faible unique</b>	Les mises à jour de la zone ne sont plus limitées à un seul serveur (DNS principal standard) mais peuvent être réalisées sur l'ensemble des serveurs DNS de la zone et toutes les modifications sont alors répliquées sur l'ensemble des serveurs DNS de la zone.
<b>Topologie de duplication unique</b>	La topologie de duplication est alors liée à celle de l'Active Directory ce qui permet d'éviter une configuration de réplication isolée pour le DNS.
<b>Mises à jour dynamiques sécurisées</b>	Il est alors possible de limiter les mises à jour dynamiques à un certain nombre d'ordinateurs autorisés.

☞ Il n'est possible de créer des zones intégrées Active Directory que sur les contrôleurs de domaine sur lesquels le service DNS a été installé.

## f) Migration d'un serveur BIND vers le serveur DNS de Windows 2000

Les fichiers de zones DNS sous Windows 2000 sont stockés dans le répertoire %SYSTEMROOT%\System32\Dns.

On y trouve les fichiers suivants :

<b>Domaine.dns</b>	Fichier de recherche directe de la zone <i>domaine</i> .
<b>z.y.x.w.in-addr- arpa.dns</b>	Fichier de recherche inversée de la plage IP z.y.x.w.
<b>Cache.dns</b>	Fichier contenant des informations sur des enregistrements issus de zones non gérées par le serveur.
<b>Boot</b>	Fichier d'amorçage contrôlant le mode de démarrage du service serveur.

La structure des fichiers BIND et des fichiers Windows 2000 étant identique, il est alors possible de procéder à une migration simplement en copiant les fichiers BIND dans le répertoire de Windows 2000 et en les renommant avec la nomenclature de Windows 2000. Ex : **db.supinfo.com** en **supinfo.com.dns** ou **db.0.168.192** en **0.192.168.in-addr.arpa.dns**.

## 9 Intégration de serveurs DNS et DHCP

### a) Principe de fonctionnement des mises à jour DNS dynamiques

Lorsqu'un client DHCP reçoit une adresse IP, les enregistrements DNS le concernant doivent être mis à jour. Ainsi, les machines exécutant Windows 2000 (aussi bien les serveurs que les clients) sont capables de mettre à jour les informations du serveur DNS.

Dans le cas d'une machine Windows 2000 cliente DHCP, lorsque celle-ci va envoyer une requête DHCP pour obtenir une adresse IP elle va joindre à sa requête le nom de domaine complet (FQDN). Le serveur DHCP envoie l'adresse IP au client. Une fois l'adresse IP reçue, le client DHCP envoie une mise à jour de son enregistrement de recherche directe (A) au serveur DNS et le serveur DHCP envoie une mise à jour de l'enregistrement de recherche inversée (PTR) au serveur DNS.

Dans le cas d'une machine exécutant une version antérieure de Windows, celle-ci ne peut mettre à jour elle-même les enregistrements du DNS. Il est alors nécessaire de configurer le serveur DHCP afin qu'il puisse mettre à jour à la fois les enregistrements A et PTR de la machine.

### b) Configuration des mises à jour dynamiques

Pour que les mises à jour dynamiques soient possibles, il est nécessaire de configurer le serveur DNS afin qu'il les accepte. Pour configurer le serveur DNS, on dispose de trois options:

- **Non** : Interdit les mises à jour dynamiques pour la zone.
- **Oui** : Autorise les mises à jour dynamiques pour la zone.
- **Uniquement les mises à jour sécurisées** : Autorise les mises à jour dynamiques pour la zone uniquement aux ordinateurs spécifiés (Uniquement lorsque la zone est intégrée à Active Directory).

☞ Les mises à jour sécurisées n'autorisent que les nouveaux enregistrements issus des ordinateurs possédant un compte dans l'Active Directory et les mises à jour provenant des ordinateurs qui ont créé l'enregistrement.

Ensuite le serveur DHCP doit être configuré selon le mode d'utilisation :

Il faut tout d'abord activer l'option **Mettre à jour automatiquement les informations de client DHCP dans DNS** puis choisir l'une des options suivantes :

- **Mettre à jour uniquement si un client DHCP le demande** : Le client mettra à jour l'enregistrement A et le serveur DHCP l'enregistrement PTR.
- **Toujours mettre à jour DNS** : Indique que le serveur DHCP va mettre à jour à la fois les enregistrements A et PTR.

De plus, si vous disposez de clients exécutant des versions antérieures de Windows, assurez vous que l'option **Activer des mises à jour pour les clients DNS qui ne prennent pas en charge la mise à jour dynamique** est activée.

Pour finir, il faudra configurer les clients (uniquement ceux tournant sous Windows 2000) :

Dans la configuration DNS des clients, il faudra activer les options **Enregistrer les adresses de cette connexion dans le système DNS** et **Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS**.

## 10 Maintenance et dépannage des serveurs DNS

### a) Réduction du trafic à l'aide des serveurs de cache

Les serveurs dédiés à la mise en cache permettent, dans un réseau étendu par exemple, de minimiser le trafic intersites en créant un cache de toutes les requêtes fréquemment émises.

Pour configurer un serveur de mise en cache, il suffit d'installer le service DNS et de ne configurer aucune zone dessus.

Lorsqu'une requête est émise, si le serveur cache ne dispose pas de l'enregistrement correspondant dans sa base, il va émettre une requête au serveur DNS (spécifié dans la liste des redirecteurs du serveur cache) et lorsqu'il en récupère la réponse, il la stocke dans sa base et l'envoie au client. Par la suite, si un autre client émet la même requête, le serveur cache pourra répondre lui-même, directement.

Aussi il est nécessaire que le serveur de cache réalise des requêtes récursives plutôt que itératives afin de réduire encore une fois le trafic sur le réseau. Afin de réaliser cela, il faut définir l'adresse IP du serveur DNS dans les redirecteurs.

### b) Surveillance des serveurs DNS

Il existe plusieurs utilitaires permettant de tester son serveur DNS :

- Les outils de la console d'administration DNS permettent de visualiser le résultat de requêtes simples ou récursives ainsi qu'un test automatique avec intervalle.
- L'activation d'un système d'enregistrement de chaque action réalisée par le serveur DNS.
- L'outil en ligne de commande nslookup permet d'interroger le contenu de la base DNS à distance.

## Module 4

### Implémentation de la résolution de noms à l'aide de WINS

Le service WINS a été créé dans le but de limiter le trafic de diffusion et de permettre la résolution de noms NetBIOS sur plusieurs segments de réseau.

Dans Windows 2000, le principal moyen pour la résolution de noms est le système DNS, mais, pour les ordinateurs clients utilisant des versions antérieures de Windows, il faut utiliser un serveur WINS pour leur permettre de communiquer efficacement.

#### 1 Noms NetBIOS

Un nom NetBIOS est constitué de 15 caractères représentant le nom de la machine plus un 16ème qui indique le service fourni.

Un nom NetBIOS ne peut être utilisé qu'une fois sur un réseau ; ils peuvent correspondre à un nom de machine ou à un nom de groupe. Il est enregistré dynamiquement sur un réseau lors du démarrage de l'ordinateur.

##### a) Enregistrement de noms NetBIOS

Au démarrage de l'ordinateur, le service NetBT sur le protocole TCP/IP va envoyer une demande d'enregistrement du nom NetBIOS à un serveur WINS (dirigée ou par diffusion suivant le type de nœud). Si un autre hôte a déjà enregistré ce nom NetBIOS, alors la demande est refusée et l'ordinateur sera dans l'impossibilité de communiquer à l'aide du protocole NetBIOS.

##### b) Résolution de noms

Il y a plusieurs possibilités en fonction du type de nœud :

- Nœud B : Utilise la diffusion pour l'enregistrement et la résolution de noms.
- Nœud P : Utilise un serveur de noms (WINS) pour la résolution.
- Nœud M : Méthode B et P : si aucun résultat par la méthode B utilisation de la méthode P.
- Nœud H : Méthode B et P : si aucun résultat par la méthode P utilisation de la méthode B.

##### c) Mise à disposition de noms

Lors de l'arrêt d'un ordinateur ou d'un service NetBIOS, une requête est effectuée au serveur de noms dans le but de libérer le nom NetBIOS.

##### d) Cache de noms NetBIOS

Le cache de noms NetBIOS contient les derniers noms NetBIOS résolus et leur adresse IP correspondante.

##### e) Fichier Lmhosts

Un fichier LMHOSTS contient des correspondances entre noms NetBIOS et adresses IP. Le fichier LMHOSTS est interrogé lorsque les autres méthodes échouent.

Le fichier LMHOSTS est une succession de lignes contenant des IPs et leur nom NetBIOS correspondant. On peut ajouter à ces lignes des mots clés précédés d'un '#'.

Mots clés :

- #PRE (charge l'entrée dans le cache)
- #DOM :[domaine] (l'ordinateur spécifié est contrôleur de domaine)
- #INCLUDE chemin\fichier (inclut un fichier externe. 'chemin' peut correspondre à un chemin UNC).
- #MH (pour ajouter un ordinateur Multi-Host)

Le fichier LMHOSTS doit obligatoirement se trouver dans le dossier : 'racine\_systeme\System32\drivers\etc\'. Ce fichier ne doit pas avoir d'extension.

Un fichier exemple (LMHOSTS.SAM) se trouve dans le répertoire cité ci-dessus.

Il est possible de désactiver l'utilisation du fichier LMHOSTS en allant dans les propriétés avancées du protocole TCP/IP.

## **2 Interopérabilité entre le service WINS et le Système DNS.**

Pour permettre la résolution par des clients Windows 2000 de noms NetBIOS, il est possible d'activer sur le DNS la recherche WINS. Lorsque le service DNS ne trouve pas d'enregistrement dans sa base pour la requête, il peut la passer au service WINS.

## **3 Mappages Statiques**

Vous avez la possibilité d'ajouter manuellement une entrée dans le serveur WINS. Toutefois, il ne faut utiliser cette possibilité que pour les ordinateurs qui ne peuvent s'enregistrer dynamiquement (ex : machine UNIX)

## **4 Proxy WINS**

Un proxy WINS est un ordinateur configuré pour transmettre les requêtes de résolution, d'enregistrement et de libération de noms NetBIOS effectuées par diffusion à un serveur WINS. Il n'est utile que dans un réseau routé où les clients ne supportent la résolution de noms NetBIOS que par diffusion (clients UNIX).

Une station de travail Windows peut se transformer en Proxy WINS en définissant l'entrée EnableProxy à 1, dans la clé HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters du Registre.

## **5 Duplication WINS**

La duplication de bases de données WINS réplique les enregistrements tous les serveurs WINS.

### **a) Partenaires Emetteur/Collecteur (Push/Pull)**

Un partenaire Collecteur demande les copies des nouvelles entrées de la base de données à ses partenaires de réplication à intervalles réguliers. Vous pouvez configurer cet intervalle. Ce type de partenaires est généralement utilisé dans le cas de liaisons lentes.

Un partenaire Emetteur avertit ses partenaires de réplication lorsque le nombre de modifications dans sa base de données atteint un seuil que vous pouvez configurer. Ce type de partenaires est utilisé dans le cas de liaisons rapides.

Un partenaire Emetteur/Collecteur demande la copie des nouvelles entrées à intervalles réguliers et avertit ses partenaires de réplication lorsque le nombre de modifications atteint le seuil. Par défaut un serveur WINS est configuré en partenaire Emetteur/Collecteur.

## **6 Maintenance de la base de données d'un serveur WINS**

La base de données WINS se trouve dans le dossier Racine\_systeme\System32\WINS

### **a) Compactage de la base de données WINS**

Pour compacter la base WINS, il faut arrêter le service WINS et exécuter l'utilitaire JetPack.exe.

Syntaxe : JetPack.exe <fichier a compacter> <fichier temporaire>

### **b) Sauvegarde et restauration de la base de données WINS**

Sauvegarde :

Vous pouvez soit effectuer une sauvegarde manuelle, soit configurer le service pour faire une sauvegarde automatique. Il ne faut pas oublier de définir le répertoire de sauvegarde par défaut.

Restauration :

Arrêtez le service WINS, supprimez tous les fichiers de la base de données actuelle, Effectuez la restauration à partir de la sauvegarde. Redémarrez le service.

Attention : la base de données à restaurer doit être dans le répertoire de sauvegarde par défaut.

## Module 5

### Configuration de la sécurité du réseau à l'aide de clé publique

#### 1 Présentation de l'infrastructure de clé publique

Le cryptage par clé publique permet de sécuriser une transaction entre deux machines. Ceci est beaucoup utilisé dans les domaines de l'authentification ou du transfert de données.

##### a) Cryptage par clé publique

Le cryptage par clé publique utilise deux clés différentes issues d'un d'algorithme mathématique :

- **La clé publique** : Elle transite sur le segment de réseau non sécurisé (Internet) et permet à celui qui la reçoit de crypter les données (ce sera **l'émetteur** des données à transmettre).
- **La clé privée** : Elle est confidentielle et permet à son propriétaire (le **destinataire** des données à transmettre) de décrypter les données cryptées à l'aide la clé publique correspondante.

L'algorithme étant de type asynchrone, il n'est pas possible de retrouver une clé à partir de l'autre. Seule la clé privée va pouvoir décrypter les données cryptées avec la clé publique.

Procédure réalisée par les composants de cryptage lors d'une transaction :

- Le destinataire des données génère la clé publique et la clé privée.
- Le destinataire envoie la clé publique à l'émetteur via le réseau.
- L'émetteur reçoit la clé et crypte les données avec.
- L'émetteur envoie les données cryptées au destinataire.
- Le destinataire reçoit les données et les décrypte à l'aide de la clé privée.

##### b) Authentification par clé publique

L'authentification par clé publique permet d'authentifier et de vérifier l'auteur de données numériques. Cette méthode utilise aussi un duo de clés publique et privée. Mais à la différence du cryptage par clé publique, ces clés ont un rôle inversé :

- **La clé publique** : Elle transite sur le segment de réseau non sécurisé (Internet) et permet à celui qui la reçoit (le **destinataire** du message à transmettre) de vérifier la signature des données transmises.
- **La clé privée** : Elle est confidentielle et permet à son propriétaire (**l'émetteur** des données à transmettre) de signer le message à transmettre.

Procédure réalisée par les composants d'authentification :

- L'émetteur du message génère la clé publique et la clé privée.
- L'émetteur signe le message à l'aide de la clé privée.
- Le destinataire reçoit le message et vérifie la signature du message à l'aide de la clé publique.

Afin d'éviter toute modification du contenu sur le segment de réseau à risque, il est possible d'utiliser des algorithmes de hachage qui vont garantir qu'aucune donnée n'a été modifiée lors du transfert, car si tel est le cas, le traitement du document génère un contenu radicalement différent.

##### c) Autorité de certification

L'autorité de certification fourni et affecte les clés de cryptage, de décryptage et d'authentification. Ces clés sont distribuées via des certificats qui font correspondre les clés publiques à des informations comme le nom ou l'adresse e-mail. Ces certificats peuvent être affectés à un ordinateur, à un utilisateur ou à un service.

Il existe 2 types d'autorités de certificat :

- les compagnies commerciales telles que Verisign qui délivrent des certificats pour des millions d'utilisateurs
- les autorités de certificats internes aux entreprises configurables sous Windows 2000 Server.

Il est possible de créer une hiérarchie d'autorités de certification. Ainsi, on va pouvoir définir une autorité racine qui va, via des règles très strictes, certifier d'autres autorités de certification de rang inférieur, qui elles-mêmes pourront certifier des autorités de certification de rang inférieur.

Ainsi on pourra déléguer toutes les demandes de certificats à des autorités de certification de rang moindre.

#### d) Infrastructure de clé publique de Windows 2000

Afin de pouvoir utiliser le cryptage par clé publique, un certain nombre de composants sont nécessaires au sein de l'infrastructure Windows 2000.

- **Service de certificats** : Permet d'agir en tant qu'autorité de certificat au sein de l'entreprise.
- **Active Directory** : Met à disposition de tous les utilisateurs l'ensemble des certificats et des révocations.
- **Applications gérant l'infrastructure de clé publique** : Applications prenant en compte les clés publiques pour l'authentification (ex : IE, IIS, Outlook,...)

Les composants de l'infrastructure de clé publique utilisent les protocoles de sécurité du marché :

- **SSL** : Protocole assurant la sécurité et la confidentialité des communications sur Internet.
- **Protocole IPSec** : Ensemble de protocoles gérant l'échange sécurisé de paquets au niveau de la couche IP.

## 2 Déploiement de services de certificats

### a) Choix d'un modèle d'Autorité de certification

Lors de la mise en place du service de certificats, vous avez le choix entre deux classes d'autorités de certification :

- **Les certificats d'entreprises** : Permet de mettre en place un service de certificats basé sur un environnement Windows 2000. Aussi toutes les demandes de certificats devront provenir d'utilisateurs et d'ordinateurs possédant un compte dans l'Active Directory.
- **Les certificats autonomes** : Permet de mettre en place un service de certificats basé sur un environnement autre que Windows 2000.

Ces deux classes d'autorités de certification vont pouvoir être déclinées en quatre modèles :

- **Autorité de certification racine d'entreprise** : constitue l'autorité racine de la classe certificats d'entreprise, elle se situe au premier niveau de la hiérarchie de certificats dans un environnement Windows 2000.
- **Autorité de certification secondaire d'entreprise** : constitue l'autorité secondaire de la classe certificats d'entreprise, elle nécessite obligatoirement une autorité de certification d'entreprise à laquelle se rattacher.
- **Autorité de certification racine autonome** : constitue l'autorité racine de la classe certificats autonomes, elle se situe au premier niveau de la hiérarchie de certificats dans un environnement hétérogène.
- **Autorité de certification secondaire autonome** : Il constitue l'autorité secondaire de la classe certificats autonomes, elle nécessite obligatoirement une autorité de certification autonome à laquelle se rattacher.

☞ L'installation d'une autorité de certification d'entreprise nécessite que l'administrateur soit membre du groupe Administrateurs de l'entreprise.

✍ Afin de publier les certificats dans l'Active Directory, il est nécessaire que le compte machine du serveur soit membre du groupe Editeurs de certificats.

### b) Sauvegarde et restauration des services de certificats

La protection des informations de certification est essentielle afin d'éviter toute perte de données cryptées à l'aide de ces dernières. Aussi la base est sauvegardée à chaque utilisation de l'utilitaire **ntbackup** et de l'option de sauvegarde de l'état du système. D'autre part, il est possible de sauvegarder la base indépendamment dans la console d'administration **Autorité de certification**.

## 3 Utilisation des certificats

### a) L'assistant de requête de certificat

L'assistant de requête de certificat ne permet de récupérer des certificats qu'à partir d'autorités de certification d'entreprise.

Ce processus se réalise à partir du composant enfichable MMC **Certificats** ou directement à partir d'une **GPO** pour un déploiement automatique.

### b) Pages Web des services de certificats

Chaque serveur Windows 2000 sur lequel est installée une autorité de certificats dispose de pages Web permettant aux utilisateurs d'envoyer des demandes de certificats courantes ou avancées.

✍ La demande via les pages Web consiste en l'unique méthode pour récupérer un certificat à partir d'une autorité de certification autonome.

✍ Par défaut, toute demande faite à une autorité de certification autonome ne sera délivrée qu'une fois celle-ci validée.

## 4 Gestion des certificats

### a) Délivrance des certificats

Pour les autorités de certification autonomes, il est nécessaire de valider chacune des demandes de certificat.

Cette action se réalise à partir de la console d'administration **Autorité de certification**.

### b) Révocation des certificats

Il est possible à un administrateur de révoquer n'importe quel certificat avant son expiration (ex : licenciement d'un employé, ...).

Cette action se réalise à partir de la console d'administration **Autorité de certification**.

Une fois un certificat révoqué, il doit être publié pour prendre effet (il apparaît dans la liste de révocation). Cette publication est réalisée automatiquement suivant un intervalle de temps défini par l'administrateur de l'autorité de certification. Il est possible de publier manuellement cette liste.

✍ Les ordinateurs clients conservent dans un cache la liste de révocation. Aussi, tant que cette liste n'arrive pas à expiration, la liste de révocation publiée n'est pas prise en compte.

### c) Importation et exportation de certificats

Il est possible via le composant enfichable **Certificats** de procéder à l'import et à l'export de certificats et cela dans différents formats :

- Echange d'informations personnelles (PKCS #12)
- Standard de syntaxe de message cryptographique (PKCS #7)
- Binaire codé DER X.509
- Codé Base64 X.509

## Module 6

# Configuration de la sécurité du réseau à l'aide du protocole IPSec

### 1 Présentation

Le protocole IPSec est une surcouche réseau qui permet de crypter tout le trafic transitant sur le réseau.

### 2 Stratégies IPSec

Les stratégies IPSec permettent une administration simplifiée. Vous pouvez administrer les stratégies d'un ordinateur en particulier comme tous les ordinateurs du domaine. Une console d'administration Gestion de la sécurité sur protocole IP est disponible sur toute machine Windows 2000.

#### a) Les différentes stratégies IPSec

**Client (en réponse seule)** : L'ordinateur n'utilisera l'IPSec que si l'ordinateur distant lui en fait la demande.

**Serveur (demandez la sécurité)** : L'ordinateur tentera d'imposer IPSec, si l'ordinateur distant ne le supporte pas, la communication se fera sans IPSec.

**Sécuriser le serveur (nécessite la sécurité)** : L'ordinateur utilisera toujours IPSec. Si l'ordinateur distant ne peut pas utiliser IPSec, il n'y aura pas de communication.

#### b) Modes de connexions

Il y a deux modes possibles : le mode de transport et le mode tunnel.

Le mode de transport est à utiliser sur un réseau, pour encrypter le trafic dans un réseau. Il prend en charge la connexion avec plusieurs machines.

Le mode de tunnel est réservé à la liaison de deux réseaux. Le trafic qui passe d'un réseau à l'autre sera crypté entre les deux réseaux.

#### c) Personnalisation des stratégies IPSec

**Point de sortie du tunnel** : définit l'ordinateur de tunneling le plus proche de la destination du trafic IP, tel que spécifié par la liste des filtres IP associés. Deux règles sont nécessaires, une dans chaque direction.

**Type de réseau** : permet de définir sur quels types d'interface sera utilisé le protocole IPSec. (Réseau, accès distant).

**Méthode d'authentification** : Windows 2000 (Kerberos v5), Autorité de certification, chaîne (clef définie manuellement, ex : mot de passe).

**Filtres IP** : Définit le trafic sécurisé, les filtres prédéfinis sont Tout le trafic ICMP, Tout le trafic IP.

#### d) Modèle de cryptage

Il y a cinq algorithmes de cryptage ; deux d'entre eux sont réservés au cryptage des authentifications, et les trois autres aux paquets de données.

Méthode de cryptage des authentifications :

- \_ SHA : Cryptage haute sécurité (militaire) : 160bits
- \_ MD5 : Cryptage haute sécurité (commercial) : 128bits

Méthode de cryptage des paquets :

- \_ DES 56 bits : Faible sécurité, une clé de 56bits
- \_ DES 40 bits : Méthode restreinte imposée par le gouvernement français. Non-conforme aux RFC. Utilise une clé de 40bits
- \_ 3DES : triple couche de cryptage DES utilisant trois clés de 56bits. Haute sécurité (nécessite 2,5 fois plus de temps processeur que le DES).

## e) Optimisation du protocole IPSec

Niveau de sécurité requis :

N'implémentez pas le protocole IPSec s'il n'est pas nécessaire. Le cryptage des données consomme du temps processeur. Le trafic et la taille des paquets IP augmente. Si les données sont moyennement sensibles ou hautement sensibles, en fonction de ce paramètre utilisez une méthode de cryptage différente. Vous pouvez aussi n'activer le cryptage IPSec que vers un ordinateur, le trafic vers les autres restant en clair.

✍ Certaines cartes réseau sont équipées d'un processeur dédié pour le cryptage et le décryptage des trames IPSec, cela permet d'augmenter sensiblement les performances.

Nombre d'entrées de filtre de stratégie IpSec :

Le protocole IPSec peut bloquer les accès non autorisés en utilisant des filtres IP et des stratégies de négociation.

## Module 7

### Configuration de l'accès distant

#### 1 Présentation de l'accès distant sous Windows 2000

L'accès distant permet à des utilisateurs de joindre votre réseau pour travailler de manière déportée. Ils peuvent ainsi utiliser les ressources informatiques de votre entreprise n'importe où dans le monde.

La mise en place d'un service d'accès distant se fait via l'outil d'administration **Routage et accès distant** coté serveur et via un logiciel d'accès distant coté client. Le serveur permet d'authentifier l'utilisateur distant désirant se connecter et de donner l'accès au réseau de l'entreprise.

La connexion entre le client et le serveur utilise un protocole d'accès distant spécifique comme le PPP (Point-to-Point Protocol). Les données vont être encapsulées dans un protocole réseau (ex :TCP/IP), puis dans le protocole d'accès distant qui transportera les données entre le réseau de l'entreprise et le client.

##### a) Types de connectivité d'accès distant

Deux types de connexions d'accès distant sont disponibles :

- Connexion d'accès à distance :

Ce type de connexion utilise souvent du matériel spécifique pour exploiter des média de communication existants comme les lignes RTPC (Réseau téléphonique). Ce type de connexion assure un débit garanti et une sécurité accrue car le serveur et le client sont directement connectés l'un à l'autre. Par contre, la vitesse de connexion est très souvent lente et le coup de connexion pour des entreprises comptant un très grand nombre d'employés distants est très important.

- Connexions de réseau virtuel (VPN) :

Une connexion VPN permet d'utiliser l'infrastructure d'Internet pour relier le client et le serveur. Chacun d'entre eux va se connecter à Internet via son ISP puis une encapsulation par un protocole sécurisé va mettre en place un tunnel virtuel entre les deux entités permettant une connexion sécurisée. L'utilisation d'Internet permet de réduire les coûts de connexion et d'atteindre des vitesses de connexion difficilement envisageable dans le cas de connexions directes.

##### b) Protocoles de transport de données

Deux types de protocoles vont être utilisés lors de connexions distantes :

- Les protocoles LAN

Les protocoles LAN suivant seront pris en charge par le service Routage et accès distant et permettrons au serveur Windows 2000 de s'intégrer à différents types de réseaux.

<b>TCP/IP</b>	Le protocole <b>TCP/IP</b> est le protocole par défaut des environnements Microsoft et UNIX.
<b>NWLink</b>	NWLink permet l'intégration avec les environnements NetWare.
<b>NetBEUI</b>	NetBEUI permet la connexion avec les environnements Microsoft (souvent anciens) utilisant ce protocole.
<b>AppleTalk</b>	TCP/IP est le protocole des environnements Macintosh (Apple).

- Les protocoles d'accès distant :

Les protocoles d'accès distant vont permettre de réaliser les connexions distantes en encapsulant les protocoles LAN.

<b>PPP</b>	Le protocole <b>PPP</b> (Point to Point Protocol) permet d'utiliser le protocole TCP/IP sur une
------------	---

	connexion via ligne téléphonique.
<b>SLIP</b>	Le protocole <b>SLIP</b> (Serial Line Internet Protocol) n'est supporté qu'en tant que client, Windows 2000 ne pouvant être employé en tant que serveur SLIP.
<b>RAS</b>	Ce protocole supporte le transport des protocoles TCP/IP, NetBEUI et NWLink. Il est utilisé pour l'interconnexion avec des environnements Microsoft plus anciens (NT 3.1, MS-DOS, ...).
<b>ARAP</b>	Le protocole <b>ARAP</b> permet le support des clients Macintosh.

### c) Protocoles VPN

Lors d'une connexion VPN, deux protocoles spécifiques peuvent être utilisés, garantissant la sécurité des données sur le réseau publique :

	<b>PPTP</b>	<b>L2TP</b>
<b>Réseau d'interconnexion supporté</b>	IP	IP, X.25, ATM, Relais de trame
<b>Authentification</b>	Sans tunnel	Avec tunnel
<b>Cryptage</b>	PPP intégré	IPSec

## 2 Configuration du serveur d'accès distant

### a) Configuration des connexions entrantes d'accès distantes

La configuration des connexions entrantes se fait via l'outil d'administration Routage et accès distant où il suffit d'activer le routage d'accès distant et de configurer le serveur à l'aide de l'assistant.

Lorsque vous démarrez le service de routage d'accès distant, 5 ports PPTP et 5 ports L2TP sont automatiquement configurés. Lors de la configuration d'un serveur de Réseau privé virtuel (VPN), dans l'assistant, le nombre de ports configurés de base est fixé à 128 par protocole. Pour modifier ce nombre, il suffit de modifier les paramètres de propriétés des ports.

### b) Configuration des paramètres d'accès entrant d'un utilisateur

Pour qu'un utilisateur puisse bénéficier de l'accès distant, il est nécessaire de lui en attribuer les droits. Ainsi trois choix s'offrent à l'administrateur :

- **Permettre l'accès** : L'utilisateur peut se connecter au serveur d'accès distant.
- **Refuser l'accès** : L'utilisateur ne peut pas se connecter au serveur d'accès distant.
- **Contrôler l'accès via la stratégie d'accès distant** : Les droits d'accès de l'utilisateur seront définis via des stratégies d'accès directement configurées sur le serveur.

Il est possible de spécifier le numéro d'appel de l'utilisateur afin que le serveur puisse le vérifier lors d'une connexion, ou encore, spécifier des propriétés de rappel afin que la communication soit prise en charge par l'entreprise. Il est aussi possible d'affecter une adresse IP statique que l'utilisateur va utiliser à chacune de ces connexions.

## 3 Configuration des clients d'accès distant

Il existe 3 types de connexions sortantes :

- les connexions d'accès à distance (vers un réseau privé ou un ISP)
- les connexions à un serveur VPN
- les connexions distantes utilisant un câble ou un port infrarouge.

### a) Mise en place d'une connexion à un serveur d'accès distant

Afin de se connecter à un serveur d'accès distant à partir de Windows 2000 Professionnel, il faut afficher les propriétés des Favoris réseau et lancer l'assistant Etablir une nouvelle connexion.

## b) Configuration de connexions à liaison multiples

Il est possible de configurer la connexion pour qu'elle utilise plusieurs liaisons physiques afin d'augmenter la bande passante. Pour cela, il faut que le client et le serveur autorisent les liaisons multiples.

Pour configurer le serveur, il suffit d'afficher les propriétés du serveur et d'activer l'option Connexions à liaisons multiples et Contrôle de largeur de bande passante dans l'onglet PPP.

Pour configurer le client, il suffit d'afficher les propriétés de la connexion sur laquelle vous souhaitez utiliser la numérotation de plusieurs périphériques et de spécifier les connexions que vous allez utiliser.

## c) Les protocoles d'authentification standard

Différents protocoles permettent d'authentifier les utilisateurs lors des accès distants avec plus ou moins de sécurité :

<b>PAP (Password Authentication Protocol)</b>	Protocole utilisant des logins et des mots de passe en clair.
<b>SPAP (Shiva Password Authentication Protocol)</b>	Dépendant du constructeur matériel Shiva. Les mots de passe sont protégés par un cryptage réversible.
<b>CHAP (Challenge Handshake Authentication Protocol)</b>	Aussi connu sous le nom MD5-CHAP, il permet d'obtenir un niveau de cryptage plus élevé.
<b>MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)</b>	Protocole d'authentification propriétaire à Microsoft permettant d'authentifier les clients utilisant Windows et utilisant le principe de CHAP. Il supporte le MPPE qui permet de crypter l'ensemble des données qui transitent entre le serveur et le client. Tous les OS Microsoft depuis Windows 95 supportent le MS-CHAP.
<b>MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol Version 2)</b>	Nouvelle version de MS-CHAP utilisant des clés de cryptage plus robustes ainsi que l'authentification mutuelle. Les ordinateurs sous Windows 95 et antérieur ne supportent pas ce protocole d'authentification (Windows 98 et ultérieur le supportent)
<b>EAP (Extensible Authentication Protocol)</b>	Le client et le serveur négocient la méthode d'authentification qui sera utilisée. Le protocole MD5-CHAP, TLS et des méthodes propriétaires de fournisseurs tiers peuvent être utilisés. Ce protocole garantit la prise en charge des futures méthodes d'authentification.
<b>TLS (Transport Layer Security)</b>	Est utilisé principalement avec des systèmes d'authentification à l'aide de cartes à puce (SmartCard).

## d) Configuration des protocoles de cryptage

Le cryptage de données va permettre de protéger les données en cryptant l'ensemble des données qui vont transiter entre le client et le serveur. L'utilisation des protocoles de cryptage de données est possible uniquement si le protocole d'authentification est MS-CHAP, MS-CHAP v2 ou TLS. Deux protocoles de cryptage sont disponibles avec Windows 2000 :

- **MPPE** : MMPE permet de protéger les données sur une connexion PPTP avec 3 niveaux d'encodage (128 bits, 56 bits et 40 bits).
- **IPSec** : IPSec permet de sécuriser les transferts du réseau en cryptant directement les trames IP.

## 4 Intégration du protocole DHCP avec le service de Routage et d'accès distant

Les clients qui vont se connecter au réseau peuvent obtenir une adresse IP à partir du serveur DHCP de l'entreprise. Si le serveur DHCP est déconnecté, une adresse de type APIPA ne permettant pas d'accéder aux ressources de l'entreprise est attribuée au client.

Il est possible de configurer le serveur d'accès distant avec une plage d'adresse IP destinées aux clients d'accès distant.

## Module 8

### Prise en charge de l'accès distant à un réseau

#### 1 Stratégies d'accès distant

Les stratégies d'accès distant permettent de spécifier si une connexion est autorisée ou refusée. Une stratégie d'accès distant est stockée sur le serveur local, et n'est pas disponible dans Active Directory.

##### a) Composants d'une stratégie

Une stratégie d'accès distant contient trois composants : une condition, une autorisation et un profil.

##### Conditions

Comprend des paramètres tel que l'heure, des groupes utilisateurs, l'identité de l'appelant ou encore des adresses IP.

##### Autorisations

Il s'agit d'autoriser ou de refuser l'accès si l'appel correspond aux conditions.

##### Profil

Permet de définir les protocoles autorisés, le niveau de cryptage accepté, des filtrages IP, la durée de connexion maximum, la possibilité d'utiliser des liaisons multiples...

##### b) Examen de l'évaluation des stratégies d'accès distant

**En mode natif ou sur un serveur autonome :**

1<sup>ère</sup> étape : comparaison des conditions et de la tentative de connexion

2<sup>ème</sup> étape : comparaison de l'autorisation d'appel entrant de l'utilisateur (Refuser, permettre, contrôler via stratégie).

3<sup>ème</sup> étape : application à la connexion entrante des paramètres du profil de la stratégie (la connexion est coupée s'ils ne peuvent pas s'appliquer).

Une stratégie d'accès distant est définie par défaut. Elle interdit l'accès.

En mode mixte, l'autorisation de l'accès ne se fait pas par une stratégie d'accès, mais par un refus ou une permission explicite sur le compte. Toutefois, si l'on permet l'accès à l'utilisateur, il devra quand même remplir les conditions d'une stratégie pour se voir autoriser l'accès.

Si la stratégie par défaut Interdire l'accès est toujours présente et qu'aucune autre stratégie n'est présente, le passage de mode mixte en mode natif n'a aucune incidence.

##### Stratégies multiples

Les stratégies sont traitées dans l'ordre. Dès que les conditions d'une stratégie concordent à une tentative de connexion, l'autorisation est évaluée en fonction du profil et du compte utilisateur. Si l'autorisation n'est pas accordée, aucune autre stratégie n'est vérifiée et la connexion est annulée.

#### 2 Contrôle de l'accès distant

Il est possible de tracer les connexions au serveur d'accès distant. Dans le registre, la clef **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Tracing**

contient quatre valeurs :

EnableFileTracing, FileDirectory, FileTracinMask, MaxFileSize.

Mettre à 1 la valeur EnableFileTracing permet d'activer le traçage des connexions.

## Module 9

### Extension des fonctionnalités d'accès distant à l'aide du service IAS

L'expansion géographique des entreprises devenant de plus en plus importante, il est souvent nécessaire d'avoir à authentifier l'ensemble des utilisateurs à partir d'un point unique. Des services d'authentification à distance comme RADIUS (Remote Authentication Dial-In User Service) s'avèrent alors très utiles.

#### 1 Présentation du service IAS

Le service IAS permet l'authentification, l'autorisation, l'audit et la comptabilisation des connexions d'accès à distance, des connexions sur réseau privé (VPN) et des connexions à la demande, et tout cela, de façon centralisée.

#### 2 Présentation des services IAS et RADIUS sur un réseau Windows 2000

Le protocole RADIUS permet de répondre aux demandes d'authentification des clients et à la comptabilisation des connexions de ces derniers.

Un client RADIUS peut être configuré sur un serveur d'accès réseau (basé sur PPP) ou sur un serveur d'accès distant (Windows 2000 avec le service Routage et accès distant).

Le serveur RADIUS est un serveur Windows 2000 qui exécute le service IAS.

Pour effectuer une authentification RADIUS :

L'utilisateur se connecte au serveur d'accès.

Le serveur d'accès envoie la requête d'authentification au serveur IAS.

Le serveur IAS récupère les informations de compte sur un contrôleur de domaine.

Si les informations d'authentification sont correctes et si la connexion est autorisée, le serveur IAS autorise alors l'accès et enregistre les connexions sous forme d'événements de comptabilisation.

L'avantage majeur du protocole RADIUS est sa faculté à s'intégrer dans des solutions hétérogènes.

#### 3 Installation et configuration du service IAS

L'installation du service IAS se fait via l'Assistant Composants de Windows, dans les services de mise en réseau en sélectionnant **Service d'authentification Internet**.

Une fois l'installation terminée, la configuration du serveur se fait en deux étapes :

Autoriser le serveur RADIUS à accéder à l'Active Directory pour qu'il puisse valider les requêtes d'authentification.

Définir la liste des clients RADIUS (les serveurs d'accès) pouvant utiliser le serveur IAS.

Ensuite il faut configurer les clients RADIUS pour qu'ils transmettent leurs requêtes d'authentification au serveur IAS et qu'ils utilisent la gestion de comptes RADIUS.

Afin de traiter les informations de connexion, trois types d'événements peuvent être audités :

- **Enregistrer les requêtes de gestion des comptes**
- **Enregistrer les requêtes d'authentification** (échec ou réussite)
- **Inscrire l'état périodique** (très gourmand en espace disque)

## Module 10

### Configuration d'un serveur Windows 2000 en tant que routeur

#### 1 Rappel

##### a) Rôle d'un routeur

Un routeur permet d'acheminer des paquets entre différents réseaux. Il permet aussi de segmenter un réseau pour préserver la bande passante.

##### b) Tables de routage

Un routeur utilise ses tables de routage pour déterminer sur quelle interface il va envoyer un paquet : Lorsque le routeur reçoit un paquet, il compare l'adresse de destination avec les entrées de la table de routage, ce qui détermine l'interface de sortie.

La commande « route print » permet d'afficher la table de routage.

Les éléments qui constituent une entrée de la table de routage sont les suivants :

- Destination réseau
- Masque réseau
- Passerelle : adresse IP de l'hôte pouvant router vers le réseau de destination
- Interface : adresse IP locale permettant d'atteindre la passerelle
- Métrique : coût de l'itinéraire
- Nombre de sauts : Indique le nombre de routeurs avant la destination
- Retard : Indique la durée nécessaire pour atteindre la destination
- Débit
- Fiabilité : Mesure de la constance d'un chemin

#### 2 Configuration des connexions réseaux

Pour configurer vos interfaces réseau, vous devez disposer d'une adresse IP. Les adresses IP conseillées pour un réseau privé sont sur les plages 10.0.0.0/8, 172.16.0.0./12, 192.168.0.0/16. Pour une connexion à Internet, utilisez l'adresse que vous fournit votre FAI. Il vous faudra aussi un masque de sous-réseau et une adresse de serveur DNS.

La commande « ipconfig /all » vous permet de voir la configuration de toutes vos interfaces réseau.

#### 3 Configuration d'itinéraires statiques

Si votre réseau n'est pas trop grand, vous pouvez générer la table de routage « à la main » . Par défaut la table de routage contient déjà les entrées de routage pour les réseaux directement connectés. Il vous suffit de rajouter les entrées pour les réseaux qui ne sont pas connectés directement.

Attention, le maintien d'un réseau à l'aide de tables de routage statiques accroît la charge administrative et n'est pas conseillé si le réseau doit évoluer.

#### 4 Configuration d'une interface de routage

##### a) Interface de routage dans le service Routage et Accès distant

Il existe trois types d'interface de routage :

- 1) interface LAN.
- 2) Interface de numérotation à la demande. (représente une connexion Point à Point)
- 3) Interface de tunnel IP dans IP. (typiquement utilisé pour faire traverser à des paquets multi-diffusion, des réseaux ne les supportant pas).

##### b) Filtrage de paquets

Il est possible grâce au filtrage IP d'autoriser ou d'interdire l'acheminement de types de trafic IP spécifiques.

Le filtrage de paquets peut être configuré de deux façons différentes :

- 1) Rejet de tous les paquets sauf ceux qui répondent aux règles que vous définissez.
- 2) Acceptation de tous les paquets sauf ceux qui répondent aux règles que vous définissez.

Pour définir une règle, vous pouvez choisir un réseau source et/ou un réseau de destination (ne pas définir de réseau équivaut à tout le trafic passant par l'interface), puis vous devez choisir un protocole dans la liste :

- a) TCP
- b) TCP [établi]
- c) UDP
- d) ICMP
- e) N'importe lequel
- f) Autre (nécessite un numéro de protocole, tous les protocoles compatibles avec Windows 2000 sont dans le fichier `racine_systeme\system32\drivers\etc\protocol`)

## 5 Implémentation du routage à la demande

Le service Routage et accès distant permet de router des paquets sur plusieurs réseaux de communication. Lorsqu'un paquet à destination d'un réseau distant arrive, la connexion est initialisée vers le site distant. Si, après un certain délai, il n'y a plus de trafic sur la connexion, alors, celle-ci est déconnectée.

Le routage à la demande permet de réduire de façon significative les coûts de communication.

Sur une connexion à la demande, on a la possibilité de définir des filtres d'accès à la demande. Le principe de ces filtres est exactement le même que pour le filtrage de paquets, mais au lieu d'autoriser ou de refuser le paquet, il initialise ou pas la connexion. On peut aussi restreindre à l'aide de plages horaires les appels.

### a) Configuration d'itinéraires statiques pour une interface de numérotation à la demande

Pour permettre des communications bidirectionnelles sur une liaison d'accès à la demande, vous devez définir des itinéraires statiques à chaque extrémité de la liaison.

## 6 Configuration du protocole RIP

RIP est un protocole de routage, il génère dynamiquement les tables de routage à l'aide des informations envoyées par les autres routeurs. Le protocole RIP supprime des charges administratives la gestion des tables de routage.

### a) Protocoles de routage

Windows 2000 supporte deux protocoles de routage : RIP et OSPF.

Le protocole RIP est conçu pour l'échange d'informations de routage sur un réseau de faible ou de moyenne envergure. RIP est simple à configurer et à déployer.

Le protocole OSPF est très efficace sur de grands réseaux. Il est toutefois plus difficile à configurer et sa gestion prend plus de temps.

### b) Fonctionnement du protocole RIP

Un routeur utilisant le protocole RIP va envoyer les informations de sa table de routage à tous les autres routeurs. Il recevra les tables de routage des autres routeurs, et finira donc par pouvoir router sur tous les réseaux.

Configuration du mode de fonctionnement :

Mode de mise à jour autostatique : attend la sollicitation d'autres routeurs pour envoyer les informations de routage. Cette configuration est utilisée pour les interfaces de numérotation à la demande.

Mode de mise à jour périodique : ce mode envoie des annonces RIP périodiquement (délai paramétrable). C'est le paramètre par défaut des interfaces LAN.

Configuration des protocoles pour les annonces RIP :

Vous pouvez configurer RIP pour qu'il émette ses annonces en diffusion RIP v.1, diffusion RIP v.2, Multidiffusion RIP v2 ou en mode silencieux (ne fait qu'écouter).

Vous pouvez aussi choisir de n'accepter que des paquets RIP v.1 ou RIP v.2 ou d'accepter les paquets venant des deux versions.

Configuration du coût :

Vous pouvez choisir une valeur allant de 1 à 15. Le protocole RIP utilise les sauts pour quantifier le coût d'une interface.

Il est possible d'activer l'authentification sur les routeurs RIP pour éviter que des annonces venant de routeurs non autorisés n'ajoutent des entrées dans les tables de routage. Toutefois la sécurité est minimale, car les mots de passe circulent en clair.

Il est aussi possible de filtrer les annonces par plages d'adresses IP.

Les trois choix sont :

- Accepter tous les itinéraires
- Accepter tous les itinéraires dans les plages listées
- Ignorer tous les itinéraires dans les plages d'adresses listées.

Configuration du protocole RIP pour un réseau de non-diffusion

Si votre réseau ne supporte pas la diffusion tel les relais de trames, il vous faudra configurer des « voisins », pour lesquels vous pourrez configurer d'envoyer des annonces en monodiffusion.

## Module 11

### Configuration de l'accès Internet pour un réseau

Il existe différentes technologies pour rendre accessible Internet à votre réseau. La plupart de ces technologies peuvent être mises en place sous Windows 2000 via l'outil d'administration **Réseau et accès distant**.

#### 1 Méthodes disponibles pour connecter un réseau à Internet

##### a) Connexion à Internet à l'aide d'un routeur

Un routeur analyse la destination du paquet pour définir le meilleur itinéraire à l'aide de ses tables de routage. Ainsi tout paquet destiné à Internet sera dirigé directement vers le fournisseur de services Internet (ISP).

L'inconvénient de la connexion à Internet par un routeur est que chaque client sur le réseau doit disposer d'une adresse IP publique. De plus chaque client étant directement connecté à Internet (via son adresse IP publique), aucune sécurité contre l'accès non autorisé des utilisateurs n'est fourni.

##### b) Sécurisation des connexions Internet à l'aide d'un pare-feu

Un pare-feu (firewall) est un dispositif matériel ou logiciel (parfois les deux) qui limite, à l'aide de règles, l'accès des utilisateurs internes ou externes au réseau.

Le pare-feu permettra de spécifier aussi bien le type de trafic entrant que sortant du réseau. Tous les paquets ne correspondant pas à ces règles seront alors supprimés.

##### c) Connexion à Internet à l'aide du protocole NAT

Le protocole NAT permet de donner l'accès à l'ensemble des machines d'une entreprise à partir d'une seule IP publique. Il va transposer des adresses IP privées en une seule adresse IP publique sur Internet.

La procédure exécutée pour la transposition d'adresses est la suivante :

- Le client envoie une requête au serveur NAT ayant pour destination, par exemple, un serveur FTP sur Internet.
- Le serveur NAT modifie l'en-tête de la requête en remplaçant l'adresse IP du client par sa propre adresse IP et ceci sans changer l'adresse IP de destination.
- Le serveur FTP reçoit la requête et envoie la réponse au serveur NAT.
- Le serveur NAT, via une table de mappage de l'ensemble de ses clients, modifie l'en-tête du paquet pour retourner la réponse au client.

☞ Il est possible, dans Windows 2000, de mettre en place un mini serveur DHCP ainsi qu'un redirecteur de requêtes DNS dans la configuration du protocole NAT.

##### d) Connexion à l'aide du partage de connexion Internet

Le partage de connexion Internet (ICS) permet de mettre en place facilement le partage de connexion Internet dans de petits réseaux comme les réseaux domestiques. Cette fonctionnalité met en place un routage NAT « allégé » (sans ses possibilités de paramétrage sont limitées par rapport au routage NAT « normal »).

Il est déconseillé de mettre en place le partage de connexion Internet dans des réseaux ayant un nombre de services IP (DNS, Active Directory, DHCP,...) importants, préférez lui plutôt le protocole NAT.

Pour mettre en place le partage de connexion Internet, il suffit de l'activer dans l'onglet Partage des propriétés de la connexion Internet.

### **e) Connexion à l'aide d'un serveur proxy**

Le serveur proxy permet de réaliser des requêtes mandataires vers Internet. Il permet de diminuer la bande passante utilisée vers Internet en mettant en place un système de cache permettant de réaliser un seul téléchargement d'une page même si plusieurs clients en font la requête.

Lorsqu'un client va faire une requête vers Internet à travers un serveur proxy, il envoie l'URL vers le proxy, puis celui-ci va envoyer la requête sur le réseau en son nom. Une fois la réponse reçue, il va l'envoyer à son client.

Il est possible d'auditer le trafic de navigation des utilisateurs ainsi que de restreindre l'accès à certaines pages.

## **2 Configuration de l'accès à Internet**

### **a) Configuration de l'accès Internet à l'aide d'un routeur**

La configuration de l'accès à Internet peut passer par une connexion permanente ou par une connexion à la demande.

Une fois l'accès configuré, il suffit d'ajouter des itinéraires statiques afin que toutes les informations qui n'ont pas pour destination le réseau interne de l'entreprise, soit transmises sur Internet.

Afin que les clients puissent utiliser ce réseau routé, il leur suffit d'avoir une adresse IP, un masque de sous réseau et comme passerelle, l'adresse du serveur réalisant le routage.

### **b) Configuration de l'accès Internet à l'aide du protocole NAT**

Pour mettre en place le routage NAT, il faut installer le protocole Traduction d'adresses réseau (NAT) dans la console d'administration Routage et accès distant.

Une fois le protocole installé, il faut définir l'interface publique et l'interface privée constituant le routage NAT.

Diverses options sont disponibles avec le protocole NAT comme la possibilité de mapper un port de l'interface publique pour qu'il pointe directement sur une machine interne du réseau et ainsi mettre cette machine à disposition des utilisateurs d'Internet.

## Module 12

### Configuration d'un serveur Web

#### 1 Services Internet

Lorsque vous installez Windows 2000 avec les options par défaut, les services Internet sont installés. Les services Internet comprennent un service WWW, un service FTP, un service SMTP (envoi de mail) et un service NNTP (pour héberger des newsgroups). Il est recommandé de les désinstaller si vous ne prévoyez pas de les utiliser.

#### 2 Configuration d'un site Web

##### a) Configuration de l'identification de sites Web

Paramètres du site Web :

- 1) Adresse IP. (défini sur quelle interface le site sera présent)
- 2) Port TCP. (il est conseillé de laisser le port par défaut 80).
- 3) En-tête de l'hôte (permet de mettre plusieurs sites sur une même IP, indiquez le nom DNS utilisé pour ce site).
- 4) Port SSL. (Pour les communications cryptées, nécessite un certificat SSL, port par défaut : 443).

##### b) Méthodes d'authentification

- Accès anonyme : c'est l'authentification par défaut, les personnes se connectant sont considérées comme l'utilisateur *IUSR\_nom\_ordinateur*, cet utilisateur est membre du groupe Invités.
- Authentification de base : un login et un mot de passe sont demandés à l'utilisateur se connectant, ceux-ci sont envoyés dans la requête http. Cette méthode n'est pas sécurisée car les informations passent en clair.
- Authentification Digest : elle est similaire à l'authentification de base excepté que les informations ne passent pas en clair.
- Authentification Windows : authentification la plus sécurisée. Elle n'est toutefois pas compatible avec les proxy HTTP.

##### c) Affectation d'un document par défaut

Un document par défaut est un fichier que va chercher le service Web lorsque dans la requête HTTP n'est précisé qu'un chemin.

#### 3 Administration des Services Internet

##### a) Application des dernières mises à jour de sécurité

Afin que votre serveur Web n'ai pas de problèmes de sécurité, appliquez régulièrement les mises à jour de sécurité.

##### b) Analyse des Services Internet

Lorsque vous installez le service IIS, des compteurs sont ajoutés au moniteur système.

Internet Information Services Global contient les compteurs qui font état du régulateur de la bande passante et de l'utilisation de l'indicateur Object Cache des Services Internet.

Service Web propose des compteurs qui présentent les données relatives aux connexions anonymes et identifiées vers l'application de service HTTP et aux requêtes HTTP qui ont été traitées depuis le démarrage du service Web.

Active Server Pages contient des compteurs sur l'utilisation des Active Server Pages.

## Module 13

### Déploiement de Windows 2000 Professionnel à l'aide des services RIS

#### 1 Vue d'ensemble

Les services RIS (Remote Installation Services – Services d'installation à distance) simplifient grandement le déploiement de systèmes d'exploitation Windows 2000 Professionnel. Combinés aux technologies Intellimirror (gestion des données utilisateurs, installation à distance d'applications,...), les services RIS constituent un outil puissant, rapide et fiable de déploiement de stations de travail Windows 2000.

Les ordinateurs clients vierges de tout système peuvent se connecter à un serveur exécutant RIS lors de leur démarrage et installer Windows 2000 Professionnel à travers le réseau de façon automatisée.

#### 2 Prérequis pour l'utilisation de RIS

##### a) Services réseau

Avant de pouvoir installer et exécuter RIS, il faut s'assurer de la disponibilité d'un certain nombre de services sur votre réseau :

- **Active Directory** (pour localiser les serveurs RIS, contrôler l'accès aux services d'installation).
- **DNS** (requis pour Active Directory).
- **DHCP** (pour que le client sur lequel on souhaite déployer Windows 2000 Professionnel puisse obtenir une adresse IP et se connecter au serveur RIS).

##### b) Serveurs hébergeant RIS

Le serveur sur lequel le service RIS s'exécutera devra répondre aux critères suivants :

- Les différentes images RIS (qui correspondent chacune une configuration spécifique de Windows 2000 Professionnel qui peut être déployé sur les clients) doivent impérativement se trouver sur une partition (ou un volume) distinct de la partition sur laquelle le système est installé.
- Cette partition (ou volume) doit utiliser le système de fichiers NTFS et doit être partagée.
- La partition ou le volume partagé doit faire au moins 2Go (pour les images et les fichiers systèmes propres à RIS).
- Le volume partagé doit être assez grand pour supporter RIS et les différentes images disques Windows 2000 Professionnel.

##### c) Configuration requise pour les ordinateurs clients

Pour que les ordinateurs clients puissent se connecter au serveur RIS, ils doivent disposer d'une carte réseau PXE (Pre-Boot Execution) (ROM version 99c minimum).

✍ Les cartes réseau PXE doivent disposer d'une version .99c minimum pour être compatible avec le service RIS.

Pour les ordinateurs ne disposant pas de carte compatibles PXE, il est toutefois possible de créer une disquette d'installation RIS en utilisant le Remote Boot Disk Generator (RBDG.EXE). Ces disquettes ne supportent que les cartes réseau PCI. RBDG.EXE se trouve dans le partage **reminst** des serveurs RIS, dans le dossier **admin\i386**.

#### 3 Installation des services RIS

L'installation s'effectue à partir du composant **Ajout/Suppression de programme** du panneau de configuration, dans **Ajouter/Supprimer des composants Windows** en ajoutant les **Services d'installation à distance**.

Ensuite, il faudra créer une image initiale du système à installer grâce à l'**Assistant Installation des services d'Installation à distance**, que l'on exécute en allant dans **Démarrer / Exécuter**, puis en tapant **risetup**.

Windows 2000 générera automatiquement la structure du dossier RIS dans la partition que vous aurez désigné dans **l'Assistant Installation des services d'Installation à distance**.

Il y créera l'image de CD-ROM initiale de Windows 2000 Professionnel ainsi qu'un fichier de réponse par défaut nommé Ristandard.SIF (les fichiers .SIF sont une variante des fichiers unattend.txt).

Enfin, les services RIS démarrent sur le serveur.

☞ Lors d'un déploiement, si vos ordinateurs clients n'arrivent pas à se connecter à un serveur RIS et affichent un message « BINL », il faudra redémarrer le service BINLSVC (Boot Information Negotiation Layer Service).

## 4 Configuration des services RIS

### a) Autorisation du serveur RIS dans Active Directory

Tout comme un serveur DHCP, un serveur RIS devra être autorisé dans Active Directory avant qu'il puisse répondre aux requêtes clientes.

L'autorisation s'effectue d'ailleurs dans la console d'administration DHCP, exactement comme pour un serveur DHCP.

☞ Dans le cas d'une délégation du contrôle d'administration, si vos administrateurs délégués doivent déployer des images grâce à RIS, il faudra veiller à ce qu'ils disposent des privilèges administratifs leur permettant d'ajouter des comptes d'ordinateurs dans Active Directory. Par défaut, chaque utilisateur a le droit de créer 10 comptes d'ordinateur dans Active Directory.

### b) Configuration spécifique aux ordinateurs clients

Il est possible de définir un certain nombre d'options qui influent sur l'installation effectuée sur les ordinateurs clients. Il est ainsi possible de définir une convention de dénomination pour les ordinateurs clients, en utilisant la combinaison de différents paramètres tels le nom de l'utilisateur, le prénom (ou sa première lettre), voir même son adresse MAC. Un générateur de nombres (incrémenté de 1 pour chaque client déployé) est aussi disponible.

Ces options se configurent dans la console **Utilisateurs et Ordinateurs Active Directory**, en faisant un clic droit sur le serveur RIS, en affichant ses propriétés, en allant sur l'onglet **Installation à Distance**, et enfin sur **Paramètres Avancés**.

☞ Les noms des comptes d'ordinateurs générés ne peuvent excéder 64 caractères. Ceux dépassant cette limite sont tronqués.

Il est aussi possible de définir l'emplacement (dans Active Directory) où les comptes d'ordinateurs seront créés. :

- Emplacement par défaut du service d'annuaire (dans le conteneur **Ordinateurs**).
- Même emplacement que celui de l'utilisateur qui paramètre l'ordinateur client
- L'emplacement suivant du service d'annuaire (dans l'unité d'organisation que vous spécifiez manuellement).

### c) Préconfiguration des ordinateurs clients

La préconfiguration, utilisée généralement pour sécuriser l'accès aux images RIS, consiste en l'affectation de comptes d'ordinateur créés précédemment à un serveur RIS particulier.

Ainsi, un ordinateur client ne pourra s'adresser qu'à un serveur RIS spécifique pour récupérer le compte d'ordinateur qui lui correspond.

Lorsque ce dernier est configuré pour **ne pas répondre aux clients inconnus**, la préconfiguration évite qu'un ordinateur client non autorisé installe une image du système.

En outre, étant donné que chaque ordinateur client s'adressera à un serveur RIS particulier, la préconfiguration permet de contrôler le nombre d'installations effectuées par chaque serveur RIS. On peut alors mettre en place un système d'équilibrage de charge en répartissant les comptes d'ordinateurs entre les différents serveurs RIS.

Pour pouvoir préconfigurer un ordinateur client, il faut disposer de son GUID (Globally Unique ID). Il est normalement fourni en tant que paramètre émanant de la spécification PXE. Il est soit noté sur la carte réseau, soit affichable dans le BIOS.

L'identificateur unique pour les ordinateurs dont la carte réseau n'est pas compatible PXE est l'adresse MAC de cette dernière, complété de 20 zéros à la fin pour que sa longueur soit de 32 caractères.

#### d) Configuration des options d'installation client

Lors d'une installation classique de Windows 2000 Professionnel, un certain nombre d'options de configuration sont proposées à l'utilisateur par l'assistant d'installation.

Lors d'un déploiement à distance avec RIS, vous avez la possibilité de les configurer automatiquement.

Cette configuration s'effectue via une ou plusieurs stratégies de groupe (GPO) qui seront liées à une unité d'organisation et/ou au domaine.

Les paramètres de la stratégie de groupe se trouvent dans **Configuration de l'utilisateur / Paramètres Windows / Services d'installation à distance**.

### 5 Déploiement d'images

#### a) Modification d'une image de CD-ROM via un fichier de réponse

L'image de CD-ROM initiale contient les paramètres de base de Windows 2000 Professionnel.

Lorsque l'on souhaite spécifier automatiquement certains paramètres (résolution de l'écran, paramètres régionaux,...), on a recours aux fichiers de réponses.

Le fichier de réponses par défaut risetup.sif généré lors de la mise en place de RIS peut être modifié pour prendre en compte vos exigences.

Vous avez aussi la possibilité de créer un fichier de réponses grâce au **Gestionnaire d'installation** (setupmgr.exe), disponible sur le CD-ROM de Windows 2000 (.\\Support\\Outils\\Deploy.cab).

Lorsque vous créez un fichier de réponses, vous devez l'associer à une image.

Ceci s'effectue dans la console **Utilisateurs et Ordinateurs Active Directory**, en faisant un clic droit sur le serveur RIS, en affichant ses propriétés, en allant sur l'onglet **Installation à Distance**, puis sur **Paramètres Avancés**, et enfin dans l'onglet **Images**.

 Vous pouvez associer plusieurs fichiers de réponses à une même image.

#### b) Accès aux images par les utilisateurs

Vous avez la possibilité gérer l'accès aux images par les utilisateurs.

Ainsi, si vous disposez de quatre images, vous pourrez spécifier pour chacune la liste des utilisateurs qui pourront y accéder et les télécharger.

Ce contrôle d'accès s'effectue sur les fichiers de réponse correspondant aux images via des permissions NTFS.

Pour qu'un utilisateur puisse accéder à une image, il faut que son compte d'utilisateur (ou un groupe auquel il appartient) dispose des permissions Lecture/Exécution sur le fichier .SIF correspondant.

#### c) Installation d'une image sur un client RIS

Lors du démarrage d'un ordinateur client compatible PXE, il faudra appuyer sur F12 pour effectuer un démarrage réseau (les clients non compatibles PXE utiliseront la disquette d'amorçage créée via RBF).

Après avoir contacté un serveur RIS et ouvert une session, l'assistant d'installation propose quatre options :

- Automatic Setup : choix de l'image à installer
- Custom Setup : permet à l'utilisateur (disposant des privilèges nécessaires) de modifier le nom d'ordinateur fourni automatiquement, de modifier l'emplacement dans Active Directory où sera placé le compte d'ordinateur

- Restart a Previous Setup Attempt : utilisé lorsque la procédure d'installation a déjà échoué
- Maintenance and Troubleshooting : permet d'exécuter des utilitaires de maintenance et de dépannage de fournisseurs tiers.

## 6 Images RipRep

Les images CD-ROM supportent que les ordinateurs soient constitués de matériel hétérogène à condition que les composants utilisent la même HAL (Hardware Abstraction Layer).

Si vous désirez déployer des images sur différentes machines utilisant des HAL différentes ou si vous souhaitez tout simplement déployer des images pourvues d'applications pré-installées, vous ne pouvez pas utiliser d'images CD-ROM. Il vous faudra utiliser des images RipRep.

En effet, contrairement aux images CD-ROM de base, qui contiennent uniquement le système d'exploitation, les images RIPRep peuvent contenir des applications pré-installées. (il vous faudra une image RipRep par HAL différente).

En plus du serveur RIS, il faudra utiliser un ordinateur source, qui servira de « modèle ».

Sur cet ordinateur source, il faudra installer Windows 2000 Professionnel, le configurer, y installer toutes les applications voulues, en somme préparer une image telle qu'on voudrait la voir déployée sur l'ensemble des machines clientes.

☞ Généralement, lorsque vous préparez ce type de machine, vous ouvrez une session en tant qu'Administrateur. Si vous apportez des modifications à l'environnement utilisateur (Bureau,...), n'oubliez pas de copier le profil de l'administrateur dans celui de l'utilisateur par défaut (Default User) afin que chaque profil utilisateur bénéficie de l'ensemble des paramètres personnalisés.

Il faut ensuite exécuter l'assistant de **Préparation de l'installation à Distance** (riprep.exe) sur l'ordinateur source. Riprep.exe est localisé dans le partage **reminst** des serveurs RIS, dans le dossier **admin\i386**.

On l'exécute en allant dans **Démarrer**, puis en sélectionnant **Exécuter** et en spécifiant le chemin UNC complet de Riprep.exe (Ex : \\RIS-SERVER1\reminst\admin\i386\riprep.exe).

Une image de l'ordinateur source est alors créée sur le serveur RIS. Cette image est automatiquement dépersonnalisée (suppression des informations spécifiques à l'ordinateur telles que l'utilisateur/entreprise enregistré, le numéro de série, le SID,...)

Si vous apportez une modification à votre ordinateur source après avoir créé l'image, il faudra recréer cette dernière pour qu'elle prenne en compte les changements effectués.

☞ Bien qu'une image RipRep soit destinée à être déployée en lieu et place d'une image CD-ROM, cette dernière ne doit pas être effacée. D'ailleurs, la création d'une image RipRep sur un serveur RIS requiert la présence d'une image de CD-ROM.

## Module 14 Gestion d'un réseau Windows 2000

### 1 Vue d'ensemble

Windows 2000 fournit aux administrateurs plusieurs outils leur permettant d'administrer leur environnement Windows 2000 à distance et de façon centralisée. Parmi ceux-ci, on compte les services Terminal Server et SNMP (*Simple Network Management Protocol*).

Avec Terminal Server, vous avez la possibilité d'ouvrir une session distante sur un serveur comme si vous le faisiez localement.

Le service SNMP de Windows 2000 permet de récupérer des informations sur vos machines Windows 2000 au moyen du protocole standard SNMP.

### 2 Administration à distance via Terminal Server

#### a) Présentation de Terminal Server

Le serveur Terminal Server gère les ressources liées à la session de l'utilisateur qui s'y connecte. Il reçoit les frappes au clavier et les clics de souris et achemine le résultat du système d'exploitation au client.

Pour pouvoir disposer des services Terminal Server, un ordinateur doit impérativement fonctionner sous un système d'exploitation de la famille Windows 2000 Server

☞ Les fonctionnalités serveur de Terminal Server ne sont pas disponibles sous Windows 2000 Professionnel. Sous Windows XP Professionnel, ils sont dénommés « Bureau à Distance ».

Au niveau du client, la session Terminal Server se présente sous la forme d'une fenêtre. L'ordinateur client a uniquement besoin de la puissance de traitement nécessaire pour la connexion au serveur. Ce dernier exécute la quasi-totalité des traitements.

Le client Terminal Server est disponible pour les systèmes d'exploitation suivants : Windows 2000, NT, 9x/Me, 3.1 et CE / Pocket PC.

☞ Si vous souhaitez disposer de clients sous d'autres systèmes d'exploitation, vous devrez recourir au client Web Terminal Server ou à l'addon Citrix Metaframe.

#### b) Le protocole RDP

Le protocole Remote Desktop Protocol prend en charge la communication entre l'ordinateur client et le serveur. Il est optimisé pour l'affichage des éléments de l'interface graphique sur l'ordinateur client. Il s'agit d'un protocole de la couche application qui utilise TCP/IP pour effectuer le transfert des données sur le réseau. Le protocole RDP repose sur le standard ITU T 120.

#### c) Caractéristiques des services Terminal Server en mode administration à distance

Lors de l'installation, vous aurez le choix entre les modes « administration à distance » et « serveur d'applications ». Pour administrer vos serveurs, vous devrez choisir le mode administration à distance. En voici les caractéristiques :

- Windows 2000 va limiter à 2 le nombre de connexions à simultanées
- Deux licences Terminal services (TSCAL) sont incluses (en mode serveur d'applications, vous pourrez utiliser plus de deux connexions pour lesquelles il faudra acheter des TSCAL).
- Par défaut, seuls les membres du groupe Administrateurs sont autorisés à se connecter aux serveurs Terminal Server.

## d) Installation des services Terminal Server

Deux méthodes permettent d'installer les services Terminal Server :

- Au cours de l'installation de Windows 2000
- Après l'installation en utilisant l'icône Ajout/Suppression de programmes du Panneau de configuration et en ajoutant « Services Terminal Server » dans les composants Windows.

## 3 SNMP sous Windows 2000

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 2000 peut communiquer ses informations d'état à un système de gestion SNMP situé sur le réseau TCP/IP.

Le service SNMP envoie des informations sur l'état d'un ou plusieurs composants d'un système à un hôte (ou plusieurs) lorsque celui-ci le demande.

### a) Système de gestion SNMP

La principale fonction d'un système de gestion SNMP consiste à demander des informations à un agent SNMP. 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 get-bulk et set.

get est une requête portant sur une valeur spécifique, telle que la quantité d'espace disque disponible.

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.

get-bulk est une requête portant sur une grande quantité de données. Elle est utilisée pour limiter le nombre de requêtes get/get-next effectuées.

set permet de modifier une valeur. On y a rarement recours dans la mesure où la plupart des valeurs n'autorisent qu'un accès en lecture seule, et ne peuvent donc pas être redéfinies.

### b) Agent SNMP

La principale fonction d'un agent SNMP est de réaliser les opérations get, get-next, get-bulk et set que seul un système de gestion SNMP peut demander. 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.

Lorsqu'un agent SNMP envoie de lui-même des informations à un système de gestion SNMP sans que ce dernier ne les demande, il exécute une opération nommée interruption (trap). L'opération trap alerte les systèmes de gestion lorsqu'il se produit un événement significatif, tel que l'absence totale d'espace disque ou une erreur de mot de passe.

✍ Sous Windows 2000, un agent SNMP est fourni, mais pas de gestionnaire SNMP.

### c) Bases 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 la version du système d'exploitation qu'il exécute ou le nombre de connections qu'il maintient à un moment donné. 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.

### d) Communautés SNMP

Une communauté est un groupe fonctionnel d'agents et de systèmes de gestion SNMP.

Seuls les systèmes de gestion et les agents SNMP appartenant à la même communauté peuvent communiquer. La communauté par défaut à laquelle les agents et les systèmes de gestion appartiennent est nommée « public ». Les noms de communauté sont sensibles à la casse.

✍ Un agent SNMP peut appartenir à plusieurs communautés.

### e) Installation du service SNMP

L'installation du service SNMP s'effectue via **Ajout/Suppression de programmes** dans le panneau de configuration. Dans les composants de Windows, il faut cliquer sur **Outils de gestion et d'analyse**, sur **Détails**, puis cocher **SNMP (Protocole simplifié de gestion réseau)**.

✍ Pour installer et configurer l'agent SNMP, vous devez disposer des privilèges Administrateurs.

### f) Configuration du service SNMP

La configuration du service SNMP est accessible via la console de Gestion de l'ordinateur.

Dans les **services**, en affichant les propriétés du service SNMP, on dispose de différents onglets dont **Agent**, **Interruptions** et **Sécurité**.

#### Configuration de l'agent

Dans l'onglet **Agent**, nous pouvons définir le nom d'un contact responsable de l'agent et les services fournis sur le réseau par l'agent, et notamment les couches du modèle OSI auxquelles il fonctionne.

#### Configuration des interruptions

Pour configurer une interruption (onglet **Interruptions**), sélectionnez le nom de communauté qui doit recevoir l'interruption (ajoutez-en un si nécessaire) puis dans la zone **Destination des interruptions**, ajoutez le nom d'hôte DNS, l'adresse IP ou IPX des systèmes de gestion SNMP auxquels vous désirez envoyer ces interruptions.

#### Configuration de la sécurité

Le service SNMP dispose d'un certain nombre de paramètres de sécurité (de base). Ils se configurent via l'onglet **Sécurité** des propriétés du service SNMP.

Envoyer une interruption d'authentification (case à cocher)

Noms de communautés acceptées (liste à fournir)

Accepter les paquets SNMP provenant de n'importe quel hôte (case à cocher)

Accepter les paquets SNMP provenant de ces hôtes (liste à fournir).

Pour une plus grande sécurité, sélectionnez **Envoyer une interruption 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 que Windows 2000 puisse envoyer des interruptions, il faut impérativement que l'option **Envoyer une interruption d'authentification** soit activée.

### g) Validation de la configuration SNMP a l'aide de SNMPUTIL

L'utilitaire snmputil contenu dans le kit de ressources techniques de Windows 2000 Server permet de vérifier la configuration et le bon fonctionnement d'un agent SNMP.

**Sa syntaxe est la suivante :**

`snmputil commande nom_ou_IP_Agent communauté Object_ID`

### Principales commandes:

**get** : permet d'obtenir la valeur de l'objet spécifié

**get-next** : permet d'obtenir la valeur de l'objet situé après l'objet spécifié en paramètre.

Identificateurs d'objets : ces identificateurs dépendent de la structure MIB employée. L'identificateur employé dans la MIB DHCP pour spécifier le nombre d'adresses IP louées par un serveur DHCP est 1.3.6.1.4.1.311.1.3.2.1.1.1.

## Module 15

### Dépannage des services réseau de Windows 2000

Windows 2000 permet la mise en œuvre d'une infrastructure réseau complexe, exploitant de nombreux services et protocoles réseaux. Dans une telle architecture, la localisation d'un élément défectueux ou mal configuré peut se révéler difficile. Windows 2000 inclut pour cela un ensemble d'outils destinés au dépannage des services réseau.

Le dépannage d'un service réseau s'effectue en trois étapes :

- la recherche des symptômes (par exemple, l'impossibilité d'un utilisateur à s'authentifier sur le réseau)
- l'identification des causes potentielles du problème (ex : problème de câble réseau,...) puis diagnostic du problème (ex : mauvais masque de sous-réseau)
- résolution du problème (ex : correction du masque)

#### 1 Identification et diagnostic de problèmes réseau

##### a) Problème matériel

En premier lieu, il faut vérifier que votre matériel (ex : carte réseau) fonctionne correctement. (Afin d'éviter de se lancer dans une recherche de problème logicielle qui pourrait être relativement longue).

##### b) Exploitation des messages d'erreur

Windows 2000 affiche presque toujours un message d'erreur lorsqu'une opération réseau s'est mal déroulée. En cliquant sur le bouton « ? » du message, vous pourrez obtenir plus de détails sur l'erreur.

La commande **net helpmsg ID\_message** (*ID\_message* représente le numéro d'erreur associé à un message d'erreur) peut aussi vous aider à trouver plus d'informations sur un message d'erreur spécifique.

##### c) Observateur d'évènements

L'observateur d'évènements est un journal consigne un certain nombre d'évènements considérés comme importants ou critiques qui se sont déroulés sur un système.

La plupart des services Windows 2000 inscrivent des informations dans ce journal (journal système), il peut être très utile pour identifier la source d'un problème réseau.

##### d) Utilitaires de dépannage

Un utilitaire de dépannage est un assistant posant une série de questions et dont l'utilité est de résoudre les problèmes courants et généraux (exemple : celui affiché lorsque l'on imprime une page de test et que l'on répond non à la question demandant si l'impression s'est bien déroulée).

Windows 2000 intègre plusieurs utilitaires de dépannage, chacun étant spécifique à un type de problème. Au niveau réseau, on dispose d'utilitaires de dépannage principalement pour TCP/IP, DHCP, DNS, WINS, etc...

#### 2 Résolution des problèmes de protocole TCP/IP

##### a) Vérification de la configuration TCP/IP via *ipconfig*

La première étape de la résolution d'un problème lié à TCP/IP est la vérification des paramètres TCP/IP de la machine incriminée.

En ligne de commande, lancez **ipconfig** pour obtenir votre adresse IP, masque de sous-réseau et passerelle par défaut.

Vérifiez alors la cohérence des paramètres affichés.

☞ Si vous obtenez une adresse en 169.254.x.y, cela signifie que votre machine est configurée pour obtenir une adresse IP via DHCP et que ce dernier n'a pas pu être contacté. APIPA a alors affecté une adresse à votre machine.

✍ Lorsque'il y a un conflit d'adresses IP, l'adresse IP en conflit s'affiche bien mais le masque de sous-réseau est **0.0.0.0**.

La commande **ipconfig /all** vous fournira de plus amples informations sur la configuration TCP/IP de la machine. (Adresse MAC, type de nœud Netbios,...).

### b) Vérification des connexions TCP/IP

Pour vérifier les connexions TCP/IP, on a souvent recours à l'utilitaire **ping**.  
Cet utilitaire emploie le protocole ICMP qui signale l'apparition d'une erreur dans l'environnement IP

✍ Le protocole Internet n'est pas, dans sa définition, absolument fiable. Le but des messages de contrôle ICMP est de pouvoir signaler l'apparition d'un cas d'erreur dans l'environnement IP, et non pas de rendre IP fiable.

Le test de connexion TCP/IP est une procédure à connaître impérativement. Il se déroule en 5 étapes majeures :

1. Ping de l'adresse de bouclage (127.0.0.1) et éventuellement de *localhost*.  
Un problème à cette étape signifie que la pile TCP/IP n'a pas été initialisée, à cause d'un problème de pilote TCP (corrompu, manquant, ...), ou d'un problème matériel (carte réseau défectueuse ou non fonctionnelle).
2. Ping de l'adresse IP de la machine locale.  
Un problème ici peut être dû à un conflit d'adresse IP.
3. Ping de la passerelle par défaut.  
Un problème ici peut vous empêcher d'atteindre un hôte situé sur un autre sous-réseau
4. Ping de l'adresse IP d'un hôte situé sur un autre sous-réseau
5. Ping d'un nom d'hôte distant pour tester la résolution de noms.  
Un problème ici signifierait une défaillance dans la résolution de noms et pas un problème de connectivité TCP/IP.

Lorsque vous utilisez IPSEC sur votre réseau, la commande ping peut vous aider à en diagnostiquer les problèmes. Lorsque **ping** vous renvoie « impossible de joindre l'hôte de destination », cela signifie que l'ordinateur n'a pas pu être contacté. Par contre, si vous obtenez « Délai d'attente de la demande dépassé », il se peut qu'une stratégie IPSEC soit appliquée à l'ordinateur distant et bloque la communication.

### c) Dépannage du routage IP

La première étape du dépannage du routage IP consiste à vérifier les connexions TCP/IP (point précédent). Ensuite, l'utilitaire **tracert** pourra vous permettre de visualiser le chemin (la liste des routeurs) emprunté par les paquets pour arriver à l'hôte de destination ainsi que le temps passé à chaque point avant le transfert vers un autre routeur. Vous pourrez par ce biais déterminer rapidement le routeur fautif.

L'utilitaire **pathping** peut être considéré comme une combinaison évoluée de **ping** et de **tracert**. Il va envoyer des paquets de données à chaque routeur présent sur l'itinéraire menant à l'hôte de destination afin d'établir des statistiques sur la perte de paquets.

### d) Résolution d'adresses IP en adresses matérielles

L'utilitaire Arp.exe est utilisé pour résoudre une adresse IP en adresse matérielle (MAC).  
Le cache local arp (contenant des entrées statiques, saisies manuellement et des entrées dynamiques issues de résolutions par diffusion) est vérifié en premier avant de lancer un broadcast ARP.  
Voici les paramètres de Arp.exe :

- 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

### 3 Résolution des problèmes de résolution de noms

#### a) Principe de la résolution de noms

La résolution de noms consiste, pour un système, à déterminer la correspondance entre un nom « intelligible » et une adresse IP. Il se base pour cela sur des tables maintenues par des serveurs DNS (dans le cas de noms d'hôtes) ou WINS (dans le cas de noms NETBIOS).

La résolution consiste en plusieurs étapes ou méthodes suivant la configuration de chaque ordinateur.

#### b) Ordre de résolution (NetBIOS)

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).

Dans le type de nœud hybride, on interroge en premier lieu un serveur WINS. S'il ne répond pas, on tente une diffusion locale. Puis on interroge le fichier hosts, et si ce dernier ne peut satisfaire la requête, on interroge le serveur DNS (s'il est configuré).

✍ Pour déterminer le type de nœud on utilise la commande **ipconfig /all**.

#### c) Problèmes de noms NetBIOS

Les deux principales commandes employées pour diagnostiquer un problème de résolution de noms NetBIOS sont **nbtstat** et **net view**.

##### Nbtstat

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

En voici les paramètres:

nbtstat [-a Nom Distant] [-A adresse IP] [-c] [-n][-r] [-R] [-RR] [-s] [S] [intervalle]

- a (état carte) Liste la table de noms de l'ordinateur distant (nom connu).
- A (état carte) Liste la table de noms d'ordinateurs distants (adresse IP).
- c (cache) Liste le cache de noms distants y compris les adresses IP.
- n (noms) Liste les noms NetBIOS locaux.
- r (résolus) Liste les noms résolus par diffusion et via WINS.
- R (Recharge) Purge et recharge la table du cache de noms distante.
- S (Sessions) Liste la table de sessions avec les adresses destination IP.
- s (sessions) Liste la table de sessions convertissant les adresses de destination IP en noms d'hôtes NETBIOS.
- RR (ReleaseRefresh) Envoie des paquets de libération de nom à WINS puis actualise

Nom Distant Nom de l'ordinateur hôte distant.

Adresse IP Représentation décimale pointée de l'adresse IP.

Intervalle Réaffiche les statistiques sélectionnées, en marquant un temps d'arrêt égal à "intervalle" secondes entre chaque affichage

✍ **Nbtstat** ne fonctionne que pour les connexions NETBIOS. Pour les connexions TCP/IP, il faut utiliser la commande **Netstat**.

##### Net View

**Net view** permet d'afficher la liste des ressources partagées par une machine (lorsque cette dernière est donnée en paramètre de la commande), ou bien la liste des domaines et/ou les machines qui les composent (commutateur /domain:nom\_du\_domaine).

## d) Problèmes de noms d'hôtes

### Vérification de la configuration

Lorsque l'on parle de noms d'hôtes, on fait indirectement référence au DNS.

La première étape dans la résolution de ce type de problème est la vérification des paramètres DNS : on s'assure, soit via la commande **ipconfig /all** soit dans les propriétés de la connexion réseau que les adresses des serveurs DNS sont correctement configurées.

### Fichier Hosts

Le fichier hosts est associé à la résolution des noms d'hôtes. Suivant le type de nœud de votre machine, Windows 2000 le sollicitera avant ou après un serveur de noms. Les erreurs courantes que l'on y rencontre sont la mauvaise orthographe d'un nom d'hôte ou d'une adresse IP.

Il se trouve dans %winroot%\system32\drivers\etc

### Nslookup

En cas de doute concernant une résolution DNS, il faut utiliser l'utilitaire nslookup (en ligne de commande). Il permet de tracer les requêtes DNS du début à la fin.

## 4 Résolution des problèmes de services réseau

Le dépannage des services réseau se fait par l'intermédiaire de la MMC « Services » située dans les Outils d'administration (accessible aussi via un clic droit sur le poste de travail puis **Gérer**).

Via cette console, vous pourrez visualiser un certain nombre d'informations sur vos services comme leur état (démarré, arrêté, pause) ou leur type de démarrage (manuel, automatique,...).

En double cliquant sur un service, vous pourrez en modifier les paramètres. Parmi ces paramètres, nous avons le type de démarrage (manuel, automatique ou désactivé), la possibilité de définir un compte réseau à utiliser par le service, les options de récupération (après une défaillance du service, le laisse-t-on arrêté ou bien le redémarre-t-on, ...), ou encore les dépendances vis à vis d'autres services.

## 5 Surveillance à l'aide du moniteur réseau

Le Moniteur Réseau, fourni avec Windows 2000 est un outil d'analyse de l'activité du réseau. Il permet de capturer le trafic 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.

L'installation du moniteur réseau se fait en allant dans le **panneau de configuration**, puis dans **Ajout/Suppression de programmes**, puis en cliquant sur **Ajouter/Supprimer des composants Windows**, en sélectionnant **Outils de Gestion et d'analyse**, en cliquant sur **Détails** et enfin, en sélectionnant **Outils d'analyse de réseau**.

L'interface du moniteur réseau se compose de quatre sections:

- Une section graphique qui montre l'activité du réseau (pourcentage d'utilisation du réseau, trames et octets par seconde...)
- Une section référençant les statistiques d'échange 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 2000 peut surveiller le trafic entrant et sortant uniquement sur le système local. La version fournie avec SMS (Systems Management Server) peut surveiller l'ensemble du trafic réseau.

## Module 16

# Configuration de la connectivité réseau entre systèmes d'exploitation

### 1 Vue d'ensemble

Windows 2000 est conçu pour fonctionner en environnement hétérogène. Sa prise en charge de l'interopérabilité avec les systèmes NetWare, Macintosh, IBM et UNIX facilitent son intégration dans la majeure partie des environnements.

### 2 Accès aux ressources Netware.

NWLink (l'implémentation Microsoft du protocole IPX/SPX) est le protocole utilisé par Windows 2000 pour permettre aux systèmes Netware d'accéder à ses ressources. NWLink est tout ce dont vous avez besoin pour permettre à des clients Windows 2000 de faire fonctionner des applications client/serveur depuis un serveur NetWare. NWLink supporte les Sockets Windows et Netbios.

La seule présence de Netware Link va permettre à un client Netware d'accéder à un serveur Windows 2000, notamment à des applications telles SQL Server par exemple.

On peut facilement installer NWLink sur un serveur Windows 2000 et donc intégrer Windows 2000 dans un environnement Netware. En revanche, NWLink ne suffit pas pour partager des ressources car Windows 2000 utilise SMB, non pris en charge par Netware (qui utilise NCP).

Le type de trame standard pour Netware 3.2 est 802.2. Les versions antérieures utilisaient des trames 802.3. Windows 2000 détermine automatiquement le type de trames. Si plusieurs types sont détectés, il prendra 802.2 par défaut.

Le type de trame du protocole NWLink doit correspondre à celui de l'ordinateur avec lequel le système Windows 2000 tente de communiquer. Si le type de trame ne correspond pas, il y aura des problèmes de connexion.

Quand NWLink est configuré pour détecter automatiquement le type de trame, il ne détectera qu'un seul type avec par ordre de préférence : 802.2, 802.3, ETHERNET\_II et 802.5 (Token Ring).

### 3 Connexion à un réseau Novell Netware

#### a) Clients pour réseau Netware

Pour permettre le partage de fichiers et d'imprimantes entre Windows 2000 et un serveur NetWare, CSNW (Services Client pour NetWare) doit être installé sur le système Windows 2000.

#### b) Services Passerelle pour Netware

Les Services Passerelle pour NetWare (Gateway Services for NetWare) peuvent être implémentés sur votre serveur Windows 2000 afin de permettre aux clients Microsoft d'accéder à votre serveur NetWare en utilisant votre serveur Windows 2000 comme passerelle.

Pour configurer SPNW, il faut activer la passerelle et fournir un compte possédant des privilèges de superviseur pour le serveur Netware en question. C'est la passerelle qui va partager les ressources Netware. Toutefois, elle ne peut accorder des permissions plus importantes que ne l'autorisent les droits Netware. Le compte de passerelle doit exister sur le serveur Netware et être membre du groupe NTGATEWAY.

Les serveurs Netware 3 utilisent Bindery Emulation (Preferred Server dans CSNW). Les serveurs Netware 4.x et suivants utilisent NDS (arbre et contexte par défaut).

### 4 Connexion à des hôtes SNA

Les mainframes et systèmes AS/400 IBM utilisent le protocole de gestion réseau SNA. Pour que des clients Windows 2000 se connectent à ces mainframes, un serveur d'intégration d'hôtes Windows 2000 est nécessaire. Ce serveur utilise des protocoles SNA IBM standard tels que DLC ou TCP/IP. DLC est un protocole à utilisation spéciale qui n'est pas routable.

## 5 Intégration réseau AppleTalk

Les services d'intégration réseau AppleTalk permettent aux clients Windows et Macintosh de partager leurs fichiers et imprimantes.

Ces services d'intégration incluent les trois composants :

- Les services de fichiers pour Macintosh : permettent aux clients Windows et Macintosh de partager des fichiers sur un ordinateur sous Windows 2000 Server
- Les services d'impression pour Macintosh : permettent a des clients Macintosh d'imprimer sur des imprimantes connectées a des systèmes Windows 2000 Server. Ils permettent aussi aux clients Windows d'imprimer sur des imprimantes d'un réseau AppleTalk.
- Le protocole AppleTalk : il constitue la base de l'architecture d'un réseau AppleTalk. Il doit etre installé sur les serveurs Windows 2000 pour que ceux-ci soient accessibles par les clients Macintosh.

## 6 Services pour Unix v2.0

Les services pour Unix sont utilisés pour résoudre les problèmes d'interopérabilité Windows 2000 / Unix. (logiciel additionnel non fourni avec Windows 2000).

Par exemple, Windows 2000 utilise CIFS (Common Internet File System), une version évoluée du protocole SMB (Server Message Block), pour partager ses fichiers alors qu'UNIX partage ses ressources fichiers sur le réseau grâce à NFS (Network File System).

Grâce aux services pour Unix:

- le partage de ressources réseau entre Windows NT/2000 et Unix est possible
- on dispose d'utilitaires et d'outils d'administration familiers aux utilisateurs et administrateurs UNIX
- l'administration réseau est simplifiée
- il est possible d'intégrer des comptes UNIX dans Windows 2000.

 Le protocole TCP/IP est requis pour communiquer avec les machines UNIX.

