



Avec les Nuls, tout devient facile!

9^e édition

Créer un réseau

POUR LES NULS

- ✓ Choisir un type de réseau
- ✓ Configurer les postes clients
- ✓ Installer et gérer un serveur au quotidien
- ✓ Maintenance et dépannage du réseau

Doug Lowe





Digitized by the Internet Archive
in 2023 with funding from
Kahle/Austin Foundation

<https://archive.org/details/crerunrseau9epou0000doug>

Créer un réseau ***9^e édition*** ***POUR*** ***LES NULS***

Doug Lowe

FIRST
Interactive

Créer un réseau 9^e édition Pour les Nuls

Titre de l'édition originale : *Networking For Dummies 9th*
Pour les Nuls est une marque déposée de Wiley Publishing, Inc
For Dummies est une marque déposée de Wiley Publishing, Inc

Collection dirigée par Jean-Pierre Cano
Édition : Pierre Chauvot
Traduction : Patricia Moritz et Jean-Louis Gréco
Maquette et illustration : MADmac

Tous droits réservés. Toute reproduction, même partielle, du contenu, de la couverture ou des icônes, par quelque procédé que ce soit (électronique, photocopie, bande magnétique ou autre) est interdite sans autorisation par écrit de Wiley Publishing, Inc.

Edition française publiée en accord avec Wiley Publishing, Inc.
© 2010 par Éditions First
Éditions First
60 rue Mazarine
75006 Paris
Tél. : 01 45 49 60 00
Fax : 01 45 49 60 01
e-mail : firstinfo@efirst.com
ISBN : 978-2-7540-1785-5
Dépôt légal : 2^e trimestre 2010
Imprimé en Espagne

Limites de responsabilité et de garantie. L'auteur et l'éditeur de cet ouvrage ont consacré tous leurs efforts à préparer ce livre. Wiley Publishing et l'auteur déclinent toute responsabilité concernant la fiabilité ou l'exhaustivité du contenu de cet ouvrage. Ils n'assument pas de responsabilités pour ses qualités d'adaptation à quelque objectif que ce soit, et ne pourront être en aucun cas tenus responsables pour quelque perte, profit ou autre dommage commercial que ce soit, notamment mais pas exclusivement particulier, accessoire, conséquent, ou autres.

Marques déposées. Toutes les informations connues ont été communiquées sur les marques déposées pour les produits, services et sociétés mentionnés dans cet ouvrage. Wiley Publishing, Inc. et les Éditions First déclinent toute responsabilité quant à l'exhaustivité et à l'interprétation des informations. Tous les autres noms de marque et de produits utilisés dans cet ouvrage sont des marques déposées ou des appellations commerciales de leur propriétaire respectif.

Sommaire



Introduction	1
À propos de ce livre	1
Comment utiliser ce livre ?	2
Ce que vous n'avez pas besoin de lire.....	3
Hypothèses vous concernant.....	3
L'organisation de ce livre	4
Première partie : Tous en réseau !.....	4
Deuxième partie : Construire son propre réseau	4
Troisième partie : Jouer dans la cour des grands.....	4
Quatrième partie : Guide de l'administration réseau pour les Nuls	5
Cinquième partie : Protéger le réseau	5
Sixième partie : Au-delà de Windows	5
Septième partie : Les dix commandements.....	5
Les icônes utilisées dans ce livre	5
À présent, par où commencer ?	6

Première partie : Tous en réseau ! 7

Chapitre 1 : Toute la vérité sur les réseaux.....	9
Qu'est-ce qu'un réseau ?	10
Pourquoi s'encombrer avec un réseau ?	12
Partage de fichiers	12
Partage de ressources	12
Partage de programmes.....	13
Serveurs et clients.....	14
Serveurs dédiés et pairs.....	15
Qu'est-ce qui fait marcher un réseau ?	16
Ce n'est plus un ordinateur personnel !	18
Devenir administrateur réseau	19
Qu'auraient-ils donc que vous n'auriez pas ?	20

Chapitre 2 : La vie sur le réseau.....	23
Différence entre les ressources locales et les ressources réseau.....	24
Qu'est-ce qu'un nom ?	24
Se connecter au réseau.....	26
Les dossiers partagés.....	29
Quatre bonnes utilisations d'un dossier partagé.....	29
Stocker des fichiers dont tout le monde a besoin.....	30

Stocker ses propres fichiers	30
Partager des informations avec d'autres utilisateurs	31
Sauvegarder son disque dur local	31
Explorer le réseau	32
Mapper des lecteurs réseau	34
L'imprimante réseau	37
Ajouter une imprimante réseau	38
Imprimer sur une imprimante réseau	41
Gérer la file d'attente	41
Se déconnecter du réseau	43

Chapitre 3 : Utiliser pleinement le réseau 45

Partager des ressources	45
Activer le partage de fichiers et d'imprimantes (Windows XP)	46
Activer le partage de fichiers et d'imprimantes (Windows Vista)	48
Activer le partage de fichiers et d'imprimantes (Windows 7)	49
Partager un dossier	50
Partager un dossier sous Windows XP	51
Partager un dossier sous Windows Vista ou Windows 7	53
Utiliser des dossiers publics sous Windows Vista et Windows 7	55
Partager une imprimante	56
Partager une imprimante sous Windows XP	56
Partager une imprimante sous Windows Vista ou Windows 7	58
Utiliser Microsoft Office sur un réseau	59
Installer Office sur un réseau (quelques options)	60
Accéder aux fichiers réseau	61
Utiliser des modèles de document en réseau	62
Travailler en réseau avec une base de données Access	64
Travailler avec des fichiers hors connexion	65

Deuxième partie : Construire son propre réseau 69

Chapitre 4 : Concevoir son réseau 71

Concevoir un réseau	72
Être rationnel	72
Faire l'inventaire	73
Ce que vous devez savoir	74
Les programmes qui rassemblent les informations	76
Avez-vous besoin d'un serveur dédié ?	77
Différents types de serveurs	78
Serveurs de fichiers	78
Serveurs d'impression	78
Serveurs Web	79
Serveurs de messagerie	79
Serveurs de bases de données	79

Choisir un système d'exploitation serveur	79
Planifier l'infrastructure	80
Dessiner les plans	81
Quelques exemples de plans	82
Créer un petit réseau : California Sport Surface	82
Connecter deux réseaux : Creative Course Development	84
Augmenter les performances du réseau : DCH Compta	86
Chapitre 5 : S'empêtrer dans la toile : câbles, cartes et autres matériels bizarres	89
Qu'est-ce qu'Ethernet ?	90
Tout sur les câbles	92
Différentes catégories de câbles	93
Combien de paires ?	94
Blindé ou non ?	94
Quand utiliser du câble plenum ?	95
Monobrin ou multibrin ?	95
Conseils d'installation	96
Brocher un câble à paires torsadées	98
Fixer les connecteurs RJ-45	100
Câbles croisés	101
Prises murales et panneaux de raccordement	102
Concentrateurs et commutateurs	103
Concentrateurs ou commutateurs ?	104
Installer des commutateurs	105
Commutateurs connectés en guirlande	105
Cartes réseau	107
Choisir une carte réseau	108
Installer une carte réseau	108
Autres périphériques réseau	110
Répéteurs	110
Ponts	113
Routeurs	113
Chapitre 6 : Protocole TCP/IP	117
Système binaire	117
Compter avec des 1	118
Un peu de logique	119
Se familiariser avec les adresses IP	120
Décimales pointées	121
Classes d'adresses IP	121
Adresses de classe A	122
Adresses de classe B	123
Adresses de classe C	124
Découpage en sous-réseaux	125
Sous-réseaux	125
Masques de sous-réseau	126

Limites des sous-réseaux.....	128
Adresses privées et adresses publiques.....	128
Comprendre la traduction des adresses de réseau.....	129
Configurer le réseau pour le service DHCP	130
Comprendre le DHCP	130
Serveurs DHCP.....	131
Comprendre les étendues.....	132
Sentiment d'exclusion ?	133
Réservations recommandées.....	133
Quelle durée de bail ?	134
Gérer un serveur DHCP sous Windows Server 2008	135
Configurer un client DHCP sous Windows	138
Utiliser le service DNS	139
Domaines et noms de domaines.....	139
Noms de domaines complets	141
Travailler avec un serveur DNS sous Windows.....	141
Configurer un client DNS sous Windows.....	143

Chapitre 7 : Installer un serveur 145

Fonctions d'un système d'exploitation réseau	145
Support réseau	146
Services de partage de fichiers.....	146
Multitâche.....	147
Services d'annuaire.....	148
Services de sécurité.....	148
Différentes versions de Windows Server 2008	150
Autres systèmes d'exploitation réseau.....	151
Linux.....	151
Apple Mac OS X Server.....	152
Méthodes d'installation d'un système d'exploitation réseau.....	152
Installation complète ou mise à niveau	152
Installation réseau.....	153
Installations automatisées et à distance	154
Inventaire des ressources nécessaires.....	155
Un serveur digne de ce nom.....	155
Un système d'exploitation serveur.....	156
D'autres logiciels	157
Une connexion Internet opérationnelle.....	157
Un bon livre.....	157
Prendre les bonnes décisions	157
Dernières mises au point	159
Installer Windows Server 2008.....	159
Après l'installation	161
Ouvrir une session.....	162
Activer Windows	162
Télécharger des <i>service packs</i>	162

Tester l'installation.....	163
Configurer les rôles du serveur	163

Chapitre 8 : Configurer les clients Windows XP, Vista et 7..... 167

Configurer des connexions réseau.....	168
Configurer des connexions réseau sous Windows XP.....	168
Configurer des connexions réseau sous Windows Vista et Windows 7.....	174
Configurer l'identité d'un ordinateur client	176
Configurer l'identité d'un ordinateur sous Windows XP	177
Configurer l'identité d'un ordinateur sous Windows Vista et Windows 7	178
Configurer la connexion au réseau.....	181

Chapitre 9 : Réseau sans fil..... 183

Plongée dans les réseaux sans fil	183
Petite leçon d'électronique	184
Ondes et fréquences	185
Longueur d'onde et antennes.....	185
Spectre et ART.....	187
802 point onze et des poussières.....	188
À portée de maison.....	189
Adaptateurs ou cartes réseau sans fil.....	190
Points d'accès sans fil	191
Mode infrastructure.....	192
Points d'accès sans fil multifonctions	193
Itinérance (roaming)	193
Ponts sans fil	194
Réseaux ad hoc.....	194
Configurer un point d'accès sans fil	194
Options de configuration	195
Configurer le serveur DHCP	197
Configurer Windows XP pour un réseau sans fil	197
Se connecter à un réseau sans fil sous Windows Vista ou Windows 7.....	200

Troisième partie : Jouer dans la cour des grands..... 201

Chapitre 10 : Connecter le réseau à Internet203

Se connecter à Internet.....	203
Se connecter par le câble ou l'ADSL.....	204
Se connecter via des lignes privées haut débit T1 et T3.....	205
Partager une connexion Internet.....	206
Sécuriser la connexion avec un pare-feu	206
Utiliser un pare-feu	206
Pare-feu intégré de Windows	208

Chapitre 11 : Gérer la messagerie avec Exchange 2007	211
Administrer des boîtes aux lettres	211
Onglet Exchange Général	212
Onglet Adresses de messagerie	213
Onglet Fonctionnalités Exchange	214
Onglet Exchange Paramètres avancés	215
Configurer Outlook pour Exchange	216
Configurer une autre boîte aux lettres	218
Chapitre 12 : Créer un intranet.....	223
Qu'est-ce qu'un intranet ?	223
Pourquoi utiliser un intranet ?	224
Éléments nécessaires pour installer un intranet	225
Installer un serveur Web IIS.....	226
Créer une page simple d'intranet.....	230
Créer un site Web	232
Chapitre 13 : Téléphone ou ordinateur ? (ou comprendre la voix sur réseau IP !).....	239
Comprendre la VoIP	240
Avantages de la VoIP	241
Inconvénients de la VoIP	241
Quelques fournisseurs de VoIP populaires.....	242
Chapitre 14 : Et les portables ?	243
Différents types de portables.....	244
Configurer Exchange sur un iPhone et un appareil sous Windows Mobile.....	245
Configurer un BlackBerry	248
Garantir la sécurité des appareils mobiles	248
Chapitre 15 : Se connecter au réseau depuis son domicile	251
Utiliser Outlook Web Access (OWA).....	252
Utiliser un VPN (Virtual Private Networks)	254

Quatrième partie : Guide de l'administration réseau pour les Nuls

255

Chapitre 16 : Bienvenue dans l'univers de l'administration réseau	257
Tâches de l'administrateur réseau	258
Administrateur à temps partiel.....	259
Documenter le réseau.....	260
Réaliser les tâches de routine	262
Administrer les utilisateurs du réseau.....	263

Choisir les bons outils logiciels	264
Documentation technique à portée de main	266
Obtenir les certifications.....	267
Chapitre 17 : Gérer des comptes utilisateurs sous Windows.....	269
Comprendre les comptes utilisateurs sous Windows	270
Créer un nouvel utilisateur	271
Configurer les propriétés utilisateur	274
Définir le profil utilisateur	277
Réinitialiser des mots de passe d'utilisateurs	278
Activer et désactiver des comptes utilisateurs.....	279
Supprimer un utilisateur	280
Travailler avec des groupes.....	280
Créer un groupe.....	281
Créer un script d'ouverture de session	283
Chapitre 18 : Gérer le stockage réseau	285
Comprendre le stockage réseau.....	285
Serveur de fichiers	285
Périphérique de stockage	286
Comprendre les autorisations	287
Comprendre les partages.....	289
Configurer le rôle de serveur de fichiers.....	290
Administrer le serveur de fichiers.....	291
Utiliser l'Assistant Configuration d'un dossier partagé.....	291
Partager un dossier sans l'assistant.....	298
Définir des autorisations.....	300
Chapitre 19 : Optimiser les performances du réseau.....	303
Pourquoi les administrateurs ont horreur des problèmes de performances ..	304
Qu'est-ce qu'un goulet d'étranglement ?.....	305
Les cinq goulets d'étranglement les plus courants	306
Le matériel intégré dans les serveurs	306
Les options de configuration du serveur	307
Les serveurs surmenés	308
L'infrastructure du réseau	308
Les dysfonctionnements matériels	309
Améliorer les performances du réseau : la méthode maniaque.....	309
Surveiller les performances du réseau.....	310
Quelques conseils supplémentaires	312
Chapitre 20 : Résoudre des problèmes réseau	315
Quand les ordinateurs en bonne santé rencontrent des problèmes	316
Ressusciter un ordinateur qui semble mort	317
Tester la connexion réseau	318
Perdu dans une nuée de messages d'erreur !	319

Revérifier les paramètres du réseau.....	320
Expérimenter, en désespoir de cause.....	320
On commence par qui ?.....	321
Redémarrer un ordinateur client.....	322
Redémarrer des services du réseau	324
Redémarrer un serveur	325
Consulter les journaux d'événements.....	327
Documenter les interventions sur le réseau.....	328

Chapitre 21 : Conserver la maîtrise du réseau et maintenir les utilisateurs à distance329

Former les utilisateurs.....	329
Constituer une bibliothèque.....	330
Rester informé de l'état de l'art	331
Le spécialiste a besoin d'un maître.....	332
Excuses de l'administrateur réseau.....	333

Cinquième partie : Protéger le réseau 335

Chapitre 22 : Sauvegarder les données.....337

Sauvegarder les données	337
Tout sur les bandes et les lecteurs de bandes	338
Logiciels de sauvegarde	339
Types de sauvegarde	340
Sauvegardes normales	341
Copies de sauvegarde.....	342
Sauvegardes journalières	342
Sauvegardes incrémentielles.....	343
Sauvegardes différentielles.....	344
Sauvegardes locales ou sauvegardes sur le réseau ?	345
Combien de jeux de sauvegardes faut-il conserver ?	346
Un mot sur la fiabilité des bandes	347
Nettoyer les têtes de lecture.....	348
Sécurité des sauvegardes	349

Chapitre 23 : Sécuriser le réseau351

Besoin de sécurité ?	352
Deux approches de la sécurité.....	353
Sécurité physique : fermer la porte	354
Sécuriser les comptes utilisateurs.....	355
Brouiller les noms d'utilisateurs	356
Utiliser des mots de passe efficaces	356
Générer des mots de passe pour les Nuls.....	358
Sécuriser le compte administrateur	359

Gérer la sécurité des utilisateurs	359
Comptes utilisateurs	360
Comptes intégrés	360
Droits du système de fichiers (qui peut faire quoi)	362
Thérapie de groupe	363
Profils d'utilisateurs	364
Scripts d'ouverture de session	365
Sécuriser les utilisateurs	365

Chapitre 24 : Renforcer la sécurité du réseau367

Pare-feu	368
Types de pare-feu	369
Filtrer les paquets	369
Inspection dynamique des paquets (SPI)	371
Passerelle applicative	372
Pare-feu intégré de Windows	373
Se protéger contre les virus	373
Qu'est-ce qu'un virus ?	373
Programmes antivirus	375
Travailler en toute sécurité	376
Installer des correctifs	376

Sixième partie : Au-delà de Windows..... 379

Chapitre 25 : Mettre en œuvre un serveur Linux381

Linux versus Windows	382
Choisir une distribution Linux	383
Installer Linux	385
Ouvrir et fermer une session	387
Ouvrir une session	387
Fermer la session	388
Éteindre	388
Utiliser GNOME	389
Utiliser l'interpréteur de commandes	390
Gérer les comptes utilisateurs	390
Configurer le réseau	393
Redémarrer le réseau	394
Danser la samba	396
Comprendre Samba	396
Installer Samba	397
Démarrer et arrêter Samba	397
Utiliser l'outil de configuration du serveur Samba sous Fedora	399

Chapitre 26 : Créer un réseau Macintosh403

Tout ce qu'il faut savoir pour monter un réseau Macintosh.....	403
Protocoles réseau Mac	403
Mac OS X Server	404
Tout ce qu'il faut savoir pour utiliser un réseau Macintosh.....	405
Configurer un Mac pour travailler en réseau	405
Accéder à une imprimante réseau.....	406
Partager des fichiers avec les autres utilisateurs	407
Accéder aux fichiers partagés	407
Tout ce qu'il faut savoir pour mettre en réseau des Mac et des PC.....	408

Septième partie : Les dix commandements411**Chapitre 27 : Plus de dix grosses erreurs réseau413**

Économiser sur le câble	414
Éteindre ou redémarrer un serveur alors que des utilisateurs sont connectés	415
Supprimer des fichiers importants sur le serveur.....	415
Copier un fichier du serveur, le modifier et le recopier sur le serveur	416
Relancer une impression parce que l'imprimante ne réagit pas	416
Supposer que le contenu du serveur est toujours correctement sauvegardé	417
Se connecter à Internet sans se soucier de la sécurité	417
Installer un point d'accès sans fil sans autorisation.....	418
Penser qu'il est impossible de travailler quand le réseau ne fonctionne pas ..	418
Manquer d'espace sur un serveur	419
Accuser systématiquement le réseau	419

Chapitre 28 : Les dix commandements du réseau421

I. Tu sauvegarderas ton disque dur religieusement.....	422
II. Tu protégeras ton réseau contre les infidèles	422
III. Tu préserveras la pureté de ton disque réseau et le débarrasseras des vieux fichiers	422
IV. Tu ne bidouilleras point les fichiers de configuration du réseau, à moins que tu ne saches ce que tu fais	423
V. Tu ne convoiteras point le réseau d'autrui.....	423
VI. Tu préviendras tes utilisateurs avant d'intervenir sur le réseau.....	423
VII. Tu conserveras un stock raisonnable de matériel de rechange	424
VIII. Tu ne voleras point le programme d'autrui sans licence.....	424
IX. Tu formeras tes utilisateurs sur l'art d'utiliser le réseau	424
X. Tu graveras la configuration du réseau sur des tables de pierre	425

Chapitre 29 : Dix choses à conserver dans son placard427

Ruban adhésif	428
Outils	428

Câbles de rechange.....	428
Connecteurs supplémentaires	428
Barres chocolatées.....	429
Cartes réseau supplémentaires	429
Commutateurs réseau bon marché.....	429
Documentation complète du réseau, gravée sur des tables de pierre	429
Manuels et CD du réseau.....	430
Dix exemplaires de ce livre.....	430
Chapitre 30 : Dix couches du modèle OSI.....	431
Couche 1 : Physique	432
Couche 2 : Liaison des données	432
Couche 3 : Réseau.....	434
Couche 5 : Session	435
Couche 6 : Présentation.....	435
Couche 7 : Application.....	435
Index.....	437

Introduction

Bienvenue dans la neuvième édition des *Réseaux pour les Nuls*, livre spécialement écrit à l'intention des personnes qui partagent la certitude qu'elles devraient mettre en réseau leurs ordinateurs mais qui ne savent absolument pas par où commencer.

Copiez-vous souvent une feuille de calcul sur un CD pour partager vos données avec votre collègue du bureau voisin ? Êtes-vous frustré parce que vous ne pouvez pas vous servir de la superbe imprimante laser connectée à l'ordinateur du comptable ? Faites-vous la queue pour utiliser l'ordinateur qui contient la base de données des clients ? Vous avez besoin d'un réseau !

Ou peut-être avez-vous déjà un réseau qui est aussi un problème : on vous a promis que le réseau vous rendrait la vie plus facile mais il a, en fait, bouleversé votre vie informatique. À peine aviez-vous enfin compris à quoi servait votre ordinateur que quelqu'un a fait irruption dans votre bureau, a branché un câble et vous a lancé un « Bonne chance avec le réseau ! » qui vous a donné envie d'hurler.

Dans un cas comme dans l'autre, vous avez trouvé le livre adéquat. L'aide que vous cherchez est ici même.

Ce livre traite des réseaux avec un langage simple et souvent irrévérencieux ; pas besoin d'avoir fait des études poussées pour le comprendre. Il bouscule un peu les sacro-saintes traditions en introduisant un peu d'humour dans un sujet plutôt austère. L'objectif est de ramener sur terre l'orgueilleux vocabulaire réseau, là où vous pourrez le toucher, le manipuler et enfin déclarer : « Qu'y a-t-il de compliqué là-dedans ? Je peux le faire ! »

À propos de ce livre

Ce livre n'est pas du genre à être lu du début à la fin comme s'il s'agissait d'un roman. Si je vous vois le lire à la plage, je risque de vous jeter du sable à la figure. En effet, ce livre est plutôt une référence, le genre que vous attrapez, feuillotez rapidement et commencez à lire. Il compte 30 chapitres et chacun d'eux traite d'un aspect différent du réseau, comme l'impression sur le réseau, la connexion des câbles du réseau ou la configuration de la sécurité de sorte que les « méchants » ne puissent pas pénétrer par effraction. Reportez-vous simplement au chapitre qui vous intéresse et lisez-le.

Chaque chapitre est divisé en plusieurs sections dont les sujets sont en relation avec le thème du chapitre. Par exemple, le chapitre qui traite de la connexion de câbles réseau contient des titres de section comme :

- ✓ Qu'est-ce qu'Ethernet ?
- ✓ Tout sur les câbles.
- ✓ Blindé ou non ?
- ✓ Prises murales et panneaux de raccordement.
- ✓ Concentrateurs et commutateurs.

Vous n'avez rien à mémoriser de ce livre. Vous le prenez juste quand vous avez besoin d'un renseignement. Vous voulez savoir ce qu'est le 100BaseT ? Ouvrez le livre. Vous voulez savoir comment créer de bons mots de passe ? Ouvrez le livre. Sinon, laissez-le de côté et continuez à vivre normalement.

Comment utiliser ce livre ?

Ce livre s'utilise comme une référence. Commencez par le sujet sur lequel vous recherchez des explications. Reportez-vous à la table des matières ou à l'index pour vous y retrouver. La table des matières est suffisamment détaillée pour que vous puissiez localiser la plupart des sujets qui vous intéressent. Si elle ne vous donne pas entière satisfaction, référez-vous à l'index, qui est encore plus précis.

Après avoir localisé votre sujet dans la table des matières ou dans l'index, rendez-vous aux pages concernées.

Bien entendu, ce livre regorge d'informations et je vous invite donc à aller directement vers le sujet qui vous préoccupe. Si vous voulez avoir une vue générale de la sécurité, lisez tout le chapitre qui traite de la sécurité. Si vous voulez simplement savoir comment générer un mot de passe correct, ne lisez que la section qui traite des mots de passe. Il me semble que vous avez compris.

Si vous devez entrer quelque chose sur votre ordinateur, vous verrez le texte à saisir apparaître ainsi : **Tapez ceci**. Dans cet exemple, vous devez taper **Tapez ceci**, puis appuyer sur Entrée. Une explication suit généralement, au cas où vous seriez en train de vous gratter la tête en vous demandant de quoi il retourne.

De plus, dès que je décris une information ou un message affiché à l'écran, je le présente ainsi :

Un message de votre ami le réseau

Ce livre vous renvoie rarement vers d'autres sources d'information ; presque tout ce que vous devez savoir sur les réseaux y figure. Toutefois, si vous avez besoin de plus d'informations, reportez-vous à d'autres ouvrages *Pour les Nuls*. Au cas où vous auriez une question sur les réseaux qui n'est pas traitée dans ce livre, je vous conseille *Networking All-in-One Desk Reference For Dummies*, 3rd Edition (Wiley), un ouvrage de référence plus complet qui étudie des systèmes d'exploitation réseau et des protocoles TCP/IP spécifiques. Vous trouverez aussi d'autres livres de la collection *Pour les Nuls* consacrés aux différents systèmes d'exploitation et programmes d'application qui existent à ce jour.

Ce que vous n'avez pas besoin de lire

Une bonne partie de ce livre peut ne pas être lue. J'ai soigneusement placé les digressions techniques dans des encarts clairement mis en évidence afin que vous puissiez les éviter. Ne les lisez pas, à moins que vous ayez besoin d'explications techniques et vouliez en savoir plus sur ce qui se passe en coulisse. Ne vous inquiétez pas, je ne serai pas du tout vexé si vous n'en lisez pas un mot.

Hypothèses vous concernant

Je vais émettre deux hypothèses vous concernant : vous travaillez avec un PC et vous disposez d'un réseau ou vous pensez en installer un. J'espère que vous connaissez quelqu'un plus à l'aise que vous en informatique (avec qui vous êtes en de bons termes). Mon objectif est de vous défaire de cette personne (du point de vue informatique, bien sûr). Mais ne jetez pas encore son numéro de téléphone !

Ce livre peut-il intéresser un utilisateur Macintosh ? Absolument ! Bien que le gros de ce livre soit consacré à vous expliquer comment connecter des ordinateurs sous Windows pour former un réseau, vous y trouverez aussi des informations sur la mise en réseau d'ordinateurs Macintosh.

Windows 7 ? Pas de souci ! Cet ouvrage regorge d'informations sur la mise en réseau avec le système d'exploitation dernier cri de Microsoft.

L'organisation de ce livre

Vous trouverez des chapitres regroupés en sept parties. Chaque chapitre est divisé en sections qui traitent de divers aspects du sujet du chapitre. Les chapitres sont ordonnés logiquement. Vous pouvez donc les lire dans l'ordre (si vous voulez lire tout le livre). Cependant, le livre est suffisamment modulaire pour que vous puissiez commencer votre lecture à n'importe quelle page.

Voici un aperçu de ce que vous trouverez dans chaque partie :

Première partie : Tous en réseau !

Les chapitres de cette partie proposent aux débutants une introduction au réseau. C'est par là que vous devez commencer si vous n'y connaissez rien. C'est aussi un bon point de départ si vous utilisez déjà un réseau mais ne voyez pas l'utilité « d'optimiser les performances d'un réseau » et voulez simplement savoir ce qu'est un réseau et comment en tirer le meilleur parti.

Atout majeur de cette partie : elle traite de l'utilisation d'un réseau sans entrer dans les détails techniques tels que son installation ou l'administration d'un serveur. En d'autres termes, elle s'adresse à des utilisateurs non avertis qui doivent apprendre à se débrouiller avec un réseau.

Deuxième partie : Construire son propre réseau

Oh, oh ! Le patron vous a lancé un ultimatum : faites en sorte que le réseau fonctionne vendredi ou faites vos valises ! Les chapitres de cette partie traitent de tout ce qu'il vous faut savoir pour créer un réseau, depuis le choix d'un système d'exploitation jusqu'à l'installation des câbles.

Troisième partie : Jouer dans la cour des grands

Maintenant que le réseau est mis en place, il faut le relier au monde extérieur. Les chapitres de cette partie vous permettront de connecter sans risque votre réseau à l'Internet, d'installer un serveur de messagerie, de gérer les appareils mobiles et d'accéder au réseau depuis votre domicile ou en déplacement.

Quatrième partie : Guide de l'administration réseau pour les Nuls

J'espère que vous n'êtes pas chargé de gérer le réseau mais si tel est le cas, les chapitres de cette partie vont vous être utiles. Vous y trouverez tout ce qu'il faut savoir sur les sauvegardes, la sécurité, les performances, le dépoussiérage, le balayage et ce que les administrateurs réseau doivent connaître.

Cinquième partie : Protéger le réseau

Cette partie est consacrée à la sécurité réseau : sauvegarde des données, protection du réseau contre les personnes mal intentionnées susceptibles de l'attaquer et prévention contre des menaces telles que les virus et les spywares.

Sixième partie : Au-delà de Windows

Les réseaux ne sont pas spécifiques à Windows. C'est pourquoi cette partie présente les deux alternatives les plus connues : Linux et Macintosh.

Septième partie : Les dix commandements

Ce ne serait pas un bouquin *Pour les Nuls* sans une liste de précieux conseils : les dix commandements du réseau, les dix choses à conserver dans son placard, les dix plus grosses erreurs réseau et davantage encore !

Les icônes utilisées dans ce livre

Ces petites icônes ne sont pas placées dans la marge pour faire joli. Elles ont une fonction pratique :

Attention ! Il est maintenant question de technique. À ne lire que si vous avez votre capuchon protecteur.

Aux États-Unis, les fondus d'informatique sont appelés *geeks* ou *nerds* (s'ils sont vraiment fondus). Un *geek/nerd* se sert toujours d'un stylo qu'il accroche à sa poche de chemise grâce au capuchon. Ce capuchon est tout un symbole.





Faites attention à cette icône ; elle vous indique qu'une astuce est à portée de main, peut-être un raccourci ou une commande peu employée mais très utile.



Vous ai-je déjà parlé des cours de mémorisation que j'ai suivis ?



Levez les mains du clavier ! Cette icône vous signale quelque chose qui peut vous éviter un désastre.

À présent, par où commencer ?

Vous avez déjà commencé. Maintenant, vous êtes paré pour traverser la jungle des réseaux. Consultez la table des matières et décidez du sujet par lequel vous voulez débiter. Soyez courageux ! Audacieux ! Téméraire ! Et, par-dessus tout, amusez-vous bien !

Première partie

Tous en réseau !



« Regarde, ça doit être un de ces PC assemblés par des détenus.
Il y avait une lime cachée dans le tapis de souris. »

Dans cette partie...

Un jour, des brutes font irruption dans votre bureau et vous placent un revolver sur la tempe : « Ne bougez pas jusqu'à ce que nous vous ayons connecté au réseau ! » dit l'un d'entre eux, tandis que l'autre éventre votre PC, y installe une carte étrange remplie de circuits électroniques, referme votre PC et plante un câble à l'arrière. « C'est fait », disent-ils en partant. « Et surtout, n'appellez pas les flics. Nous savons qui vous êtes. »

Si cela vous est déjà arrivé, vous allez apprécier les chapitres de cette partie. Ils proposent une introduction aux réseaux informatiques, spécialement rédigée pour les utilisateurs réticents.

Si vous n'avez pas de réseau et que vous êtes censé en installer un, les chapitres suivants vous permettront de mieux comprendre ce qu'est effectivement un réseau. De cette manière, vous serez prêt à affronter les chapitres (malheureusement plus techniques) de la deuxième partie et des suivantes.

Chapitre 1

Toute la vérité sur les réseaux

Dans ce chapitre :

- ▶ Qu'est-ce qu'un réseau ?
- ▶ Pourquoi est-ce une bonne idée d'utiliser un réseau ?
- ▶ Différence entre serveurs et clients.
- ▶ Système d'exploitation d'un réseau.
- ▶ Comment fonctionne un réseau ?
- ▶ Comment un réseau change-t-il la vie informatique ?
- ▶ Être administrateur réseau.
- ▶ Qu'ont-ils donc que vous n'avez pas ?

Les réseaux informatiques jouent les mauvais rôles dans les films. Dans la série des *Terminator*, un réseau informatique du futur, nommé Skynet, prend le contrôle de la planète, construit des robots terminator effrayants et les envoie dans le passé pour assassiner toute personne ayant la malchance de porter le nom de Sarah Connor. Dans *Matrix*, un réseau très puissant transforme des êtres humains en esclaves en les enfermant dans une simulation du monde réel. Et dans *War Games*, l'un des premiers films de Matthew Broderick, un adolescent, génie de l'informatique, manque de déclencher la Troisième Guerre mondiale en piratant un jeu (la « guerre thermonucléaire totale ») après s'être connecté au réseau du ministère américain de la Défense.

Ne craignez rien. Ces méchants réseaux n'existent que dans l'imagination des auteurs de science-fiction. Dans la réalité, les réseaux sont bien plus posés. Ils ne pensent pas par eux-mêmes, ils ne peuvent pas mal tourner sans votre consentement et ils ne vous feront aucun mal, même si vous vous appelez Sarah Connor.

Maintenant que vous avez surmonté votre peur des réseaux, vous êtes prêt à attaquer ce chapitre. Il s'agit d'une introduction aux réseaux informatiques, parfois superficielle, mais qui aborde sous un angle nouveau les concepts vous permettant de vous servir d'un ordinateur connecté à un réseau. Ce chapitre n'entre pas trop dans les détails ; ces derniers (ennuyeux, il est vrai) figurent plus loin.

Qu'est-ce qu'un réseau ?

Un *réseau* n'est rien de plus que deux ordinateurs (ou plus) reliés par un câble (ou dans certains cas par ondes radio) afin de pouvoir échanger des informations.

Bien entendu, il existe d'autres moyens d'échanger de l'information entre des ordinateurs sans avoir recours à des réseaux. La plupart d'entre nous a déjà utilisé ce que les mordus d'informatique appellent le *réseau itinérant* : c'est-à-dire lorsque vous copiez un fichier sur un CD, un DVD ou une clé USB pour transférer des données sur un autre ordinateur. Le terme *réseau itinérant* est un magnifique trait d'humour caractéristique des mordus d'informatique.

Le principal problème du réseau itinérant est sa lenteur, sans compter qu'il use la moquette ! Un jour, un fondu d'informatique radin découvrit qu'il était moins coûteux de relier les ordinateurs entre eux par des câbles que de remplacer la moquette tous les six mois. C'est ainsi que le concept moderne de réseau informatique est né.

Pour créer un réseau, vous devez relier tous les ordinateurs de votre bureau avec des câbles et utiliser une *carte réseau* (une carte dotée d'un circuit électronique à intégrer dans votre ordinateur et qui dispose d'une prise spéciale à l'arrière de l'ordinateur). Ensuite, vous configurez votre système d'exploitation pour que le réseau fonctionne. Et voilà, vous disposez d'un réseau opérationnel.

Si vous ne voulez pas vous encombrer de câbles, vous pouvez opter pour un *réseau sans fil*. Chaque ordinateur est doté d'un adaptateur spécial équipé d'antennes en forme d'oreilles de lapin. Les ordinateurs peuvent ainsi communiquer entre eux sans l'aide de câbles.

La Figure 1.1 représente un réseau type composé de quatre ordinateurs. Vous pouvez voir que les quatre ordinateurs sont connectés via un câble à un appareil central nommé *switch* ou *commutateur*. Vous pouvez aussi remarquer que l'ordinateur de Lucien est connecté à une superbe imprimante laser. Grâce au réseau, Julie, Gilbert et Jean-Jacques peuvent utiliser cette imprimante laser. Notez que Jean-Jacques a collé le chewing-gum qu'il mâchait hier à l'arrière de son ordinateur. Bien qu'elle ne soit pas recommandée, la présence d'un chewing-gum ne devrait pas affecter le bon fonctionnement du réseau.

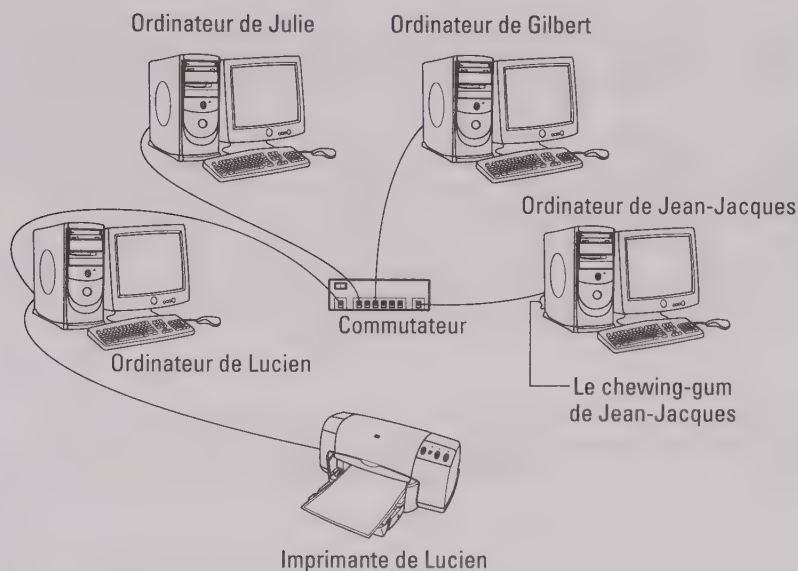


Figure 1.1 : Exemple de réseau type.

L'univers des réseaux informatiques requiert un vocabulaire étrange. Vous n'avez, fort heureusement, pas à connaître tous les termes obscurs. En voici quelques-uns :

- ✓ **LAN :** Les réseaux sont souvent appelés LAN. LAN est un acronyme qui signifie *Local Area Network* (réseau local). C'est le premier *STL*, ou *Sigle de Trois Lettres* – différent d'un ATL (abréviation de trois lettres ; l'acronyme étant un sigle qui se prononce comme un mot) –, que vous rencontrerez dans ce livre. Vous n'avez pas besoin de vous en souvenir, pas plus que des nombreux STL qui vont suivre. En fait, le seul sigle de trois lettres dont vous devez vous souvenir est STL.
- ✓ **SQL :** Vous pensez peut-être qu'un sigle de quatre lettres est un SQL, mais vous avez tort. Un sigle de quatre lettres est nommé *STLE*, ce qui signifie *Sigle de Trois Lettres Étendu*.
- ✓ **Sur le réseau :** Chaque ordinateur connecté au réseau est dit *sur le réseau*. Le terme technique (que vous pouvez oublier) désignant un ordinateur sur un réseau est *nœud*.
- ✓ **En ligne :** Quand un ordinateur est allumé et peut accéder au réseau, l'ordinateur est dit *en ligne*. Quand un ordinateur ne peut pas accéder au réseau, il est *hors ligne*. Un ordinateur peut être hors ligne pour plusieurs raisons : il est éteint, un utilisateur l'a déconnecté du réseau, il est cassé, le câble qui le relie au réseau est débranché ou le morceau de chewing-gum est coincé dans le disque dur.



✓ **Mettre en route** : Quand un ordinateur est allumé et fonctionne correctement, il est dit *en route*. Allumer un ordinateur se dit le *mettre en route*.

Ne confondez pas les réseaux locaux avec *Internet*. Internet est un énorme regroupement de réseaux informatiques répartis sur toute la planète. Mettre en réseau les ordinateurs de votre domicile ou du bureau afin de pouvoir partager de l'information et connecter votre ordinateur au réseau mondial Internet sont deux tâches bien distinctes mais liées. Si vous voulez utiliser le réseau local pour connecter vos ordinateurs au réseau Internet, reportez-vous au Chapitre 10.

Pourquoi s'encombrer avec un réseau ?

Franchement, les réseaux informatiques sont assez pénibles à mettre en place. Alors, pourquoi le faire ? Parce que les avantages que procure un réseau annulent largement la peine que représente son installation.

Nul besoin de faire une thèse sur les réseaux pour comprendre leurs avantages. En fait, vous le savez depuis la maternelle : les réseaux sont synonymes de partage. Pour être plus précis, les réseaux permettent de partager trois éléments : les fichiers, les ressources et les programmes.

Partage de fichiers

Les réseaux vous permettent de partager de l'information avec d'autres ordinateurs connectés au réseau. Vous pouvez partager les fichiers de plusieurs manières, en fonction de la configuration de votre réseau. Le moyen le plus direct consiste à envoyer un fichier en pièce jointe à un courrier électronique, depuis votre ordinateur sur l'ordinateur de votre ami. Ce dernier peut aussi accéder à votre ordinateur par le réseau et récupérer le fichier sur votre disque dur. Vous avez également la possibilité de copier le fichier sur le disque dur d'un autre ordinateur puis d'indiquer son emplacement à votre ami pour qu'il puisse le récupérer plus tard. D'une manière ou d'une autre, les données circulent jusqu'à l'ordinateur de votre ami via le câble réseau et non pas via un CD, un DVD ou une clé USB comme dans le réseau itinérant.

Partage de ressources

Vous pouvez configurer certaines ressources informatiques comme un lecteur ou une imprimante pour que tous les ordinateurs du réseau puissent y accéder. Par exemple, l'imprimante laser reliée à l'ordinateur de Lucien

dans la Figure 1.1 est une ressource partagée, ce qui signifie que n'importe qui sur le réseau peut s'en servir. Sans le réseau, Julie, Gilbert et Jean-Jacques devraient acheter leur propre imprimante laser.

Les lecteurs peuvent aussi être des ressources partagées. En fait, vous devez configurer un lecteur en tant que ressource partagée pour pouvoir partager des fichiers avec les autres utilisateurs. Supposez que Gilbert veuille partager un fichier avec Jean-Jacques et qu'un lecteur partagé ait été installé sur l'ordinateur de Julie. Gilbert n'a qu'à copier le fichier sur le lecteur partagé de l'ordinateur de Julie puis indiquer à Jean-Jacques où il l'a stocké. Alors, quand Jean-Jacques sera disponible, il pourra copier le fichier depuis l'ordinateur de Julie vers le sien (à moins bien sûr que le fouineur de service ne l'ait supprimé).



Vous pouvez aussi partager d'autres ressources, par exemple une connexion Internet. En fait, le partage d'une connexion Internet est l'une des principales motivations pour la mise en place d'un réseau.

Partage de programmes

Au lieu de conserver des copies distinctes de programmes sur chaque ordinateur, il est parfois conseillé de stocker le logiciel sur un ordinateur partagé auquel chacun peut accéder. Par exemple, dans le cas de dix utilisateurs qui choisissent tous le même programme, vous pouvez soit acheter et installer dix exemplaires du programme (un par utilisateur), soit acheter une licence pour dix utilisateurs et installer le logiciel une seule fois, sur le disque partagé. Chacun des dix utilisateurs peut alors accéder au programme depuis le disque dur partagé.

Cependant, dans la plupart des cas, il est très lent de faire fonctionner un logiciel sur le réseau. Une solution plus communément adoptée pour partager des programmes via un réseau consiste à copier le logiciel sur un disque partagé puis à l'installer sur le disque local de chaque utilisateur. Par exemple, Microsoft Office vous permet d'opter pour cette solution si vous achetez une licence Microsoft pour chacun des ordinateurs sur lesquels vous installez Office.

L'installation d'Office depuis un disque partagé présente un avantage évident : vous n'êtes pas obligé de balader les CD d'installation sur chaque poste. De plus, l'administrateur système peut personnaliser l'installation réseau, de sorte que le logiciel s'installe de la même manière sur tous les ordinateurs. Notez toutefois que cette solution est surtout intéressante pour les grands réseaux. Si le vôtre compte moins de dix ordinateurs, il vaut mieux installer Office sur chaque machine à partir des CD d'installation.



Rappelez-vous qu'il est illégal d'acheter un exemplaire d'un programme pour un seul utilisateur si c'est pour le stocker sur un lecteur partagé afin que tous les utilisateurs du réseau puissent y accéder. Si cinq personnes veulent utiliser un logiciel, vous devez acheter soit cinq exemplaires du programme, soit une licence réseau qui autorise cinq utilisateurs (ou plus).



Cela dit, beaucoup de fabricants vendent leurs logiciels avec une *licence multiutilisateur*. Dans ce cas, vous pouvez installer le logiciel sur autant de postes que vous voulez mais son utilisation simultanée est limitée à un certain nombre de personnes. Généralement, un logiciel à licence spéciale, exécuté sur l'un des serveurs du réseau, surveille le nombre de personnes qui utilisent le logiciel en même temps. Ce type de licence est couramment utilisé pour des logiciels spécialisés (et chers) tels que des programmes de comptabilité ou d'infographie.



Autre avantage du réseau : il permet aux utilisateurs de communiquer entre eux, surtout par l'intermédiaire de messageries électroniques ou de services de messagerie instantanée. Cependant, le réseau offre également d'autres moyens de communication : il peut vous servir à organiser des réunions en ligne. Les utilisateurs disposant de caméras vidéo sur leur ordinateur (*webcams*) peuvent participer à des visioconférences. Vous pouvez même jouer à la « dame de pique » via le réseau, pendant votre pause déjeuner, bien évidemment.

Serveurs et clients

L'ordinateur du réseau qui possède les disques, l'imprimante et les autres ressources partagées avec les autres ordinateurs du réseau est un *serveur*. Ce terme sera souvent utilisé, vous devez vous en souvenir. Écrivez-le au dos de votre main gauche.

Tout ordinateur qui n'est pas un serveur est un *client*. Vous aurez aussi à vous souvenir de ce terme. Écrivez-le sur le dos de votre main droite.

Il n'y a que deux types d'ordinateurs sur un réseau : des serveurs et des clients. Regardez votre main gauche puis votre main droite. Ne vous lavez pas les mains tant que vous n'avez pas mémorisé ces termes.

La distinction entre un client et un serveur sur un réseau serait quelque chose d'amusant à étudier en sociologie. C'est le type de différence qui existe entre ceux qui ont des biens et ceux qui n'en ont pas.



- ✓ Les ordinateurs les plus puissants et les plus coûteux dans un réseau sont généralement les serveurs. C'est logique car chaque utilisateur du réseau a recours à leurs ressources.

- ✓ Les ordinateurs les moins chers et les moins puissants sont les clients. Ce sont les ordinateurs utilisés pour le travail quotidien. Les clients n'ayant pas à partager de ressources, ils n'ont pas besoin d'être très performants.
- ✓ La plupart des réseaux comportent plus de clients que de serveurs. Par exemple, un réseau de dix clients comptera probablement un seul serveur.
- ✓ Sur de nombreux réseaux, il existe une véritable ségrégation entre les serveurs et les clients. Autrement dit, un ordinateur est un serveur ou un client mais pas les deux à la fois. Un serveur ne peut pas devenir client et un client ne peut pas devenir serveur.
- ✓ D'autres réseaux, généralement plus petits, sont plus progressistes. Ils autorisent n'importe quel ordinateur du réseau à devenir serveur et à être simultanément serveur et client.

Serveurs dédiés et pairs

Dans certains réseaux, un ordinateur serveur est un ordinateur serveur et rien d'autre. Il est affecté à la seule tâche de partager des ressources, comme des disques et des imprimantes, afin qu'elles soient accessibles aux clients du réseau. Un tel serveur est nommé *serveur dédié* car il ne peut effectuer d'autres tâches que celles liées au réseau.

L'approche moderne des réseaux autorise chaque ordinateur d'un réseau à fonctionner à la fois comme client et comme serveur. Ainsi, n'importe quel ordinateur peut partager son imprimante ou ses disques avec les autres ordinateurs du réseau. Et tandis qu'un ordinateur se comporte en serveur, vous pouvez continuer à l'utiliser pour faire du traitement de texte. Ce type de réseau est nommé *réseau pair-à-pair* (*peer-to-peer* en anglais) car tous les ordinateurs sont des pairs, c'est-à-dire qu'ils sont égaux.

Voici quelques réflexions sur les différences entre les réseaux à serveurs dédiés et les réseaux pair-à-pair. Pensez-y demain matin, pendant que vous promènerez votre chien :

- ✓ Les fonctionnalités de réseau pair-à-pair sont intégrées à Windows. Si votre ordinateur fonctionne sous Windows, vous n'aurez donc pas à acheter d'autres logiciels pour transformer cet ordinateur en serveur. Vous devrez tout simplement activer les fonctionnalités serveur de Windows.
- ✓ Les fonctionnalités serveur des versions grand public de Windows (comme Windows XP, Vista ou Windows 7) ne sont pas très efficaces car ces versions n'ont pas été conçues pour être des serveurs de réseau.



Si vous projetez de transformer un ordinateur en serveur permanent, vous devez avoir recours à un système d'exploitation spécial à la place de Windows. Un système d'exploitation réseau, aussi nommé NOS (*Network Operating System*), est spécialement conçu pour gérer efficacement les fonctions liées au réseau.

- Les systèmes d'exploitation réseau les plus employés sont les versions serveur de Windows.

À l'heure où j'écris ce chapitre, la dernière version serveur de Windows est *Windows Server 2008*. Toutefois, de nombreuses entreprises utilisent encore la version précédente (*Windows Server 2003*) et certaines ne parviennent pas à se défaire de leur prédécesseur, *Windows 2000 Server*.

- Il existe d'autres systèmes d'exploitation réseau tels que *Linux* et *Novell NetWare*.

✓ De nombreux réseaux sont à la fois des réseaux pair-à-pair *et* des réseaux à serveurs dédiés. Ces réseaux disposent :

- d'au moins un ordinateur *serveur* qui utilise un NOS tel que *Windows Server 2008*.
- d'ordinateurs *clients* qui utilisent les fonctionnalités serveur de Windows pour partager des ressources avec le réseau.

✓ Vos serveurs doivent non seulement être dédiés mais aussi sincères.



Qu'est-ce qui fait marcher un réseau ?

Pour vous servir d'un réseau, vous n'avez pas vraiment besoin de savoir comment il fonctionne. Cependant, vous pourriez vous sentir mieux si vous réalisiez qu'il ne fonctionne pas par magie. Un réseau peut sembler magique mais il ne l'est pas. Voici la liste des différents éléments qui composent un réseau :

- ✓ **Carte réseau.** Elle se trouve dans un ordinateur connecté au réseau ; c'est une carte électronique qui porte le nom de *carte réseau* mais est aussi appelée *NIC* (pour *Network Interface Card*).

Si votre carte réseau est active en permanence et qu'elle vous sert à mettre à jour des logiciels et à sauvegarder des données, de jour comme de nuit, veillez à ce qu'elle soit suffisamment performante.





Bien que la carte réseau soit en général intégrée à la carte mère de votre ordinateur, sur les ordinateurs récents, vous avez la possibilité d'utiliser une interface réseau externe reliée à l'ordinateur par le port USB de ce dernier.

C'est cette interface réseau intégrée à la carte mère de l'ordinateur qui est en général appelée NIC, bien que ce ne soit pas réellement une carte séparée.

- ✓ **Câble réseau.** Le câble réseau relie les ordinateurs. Il se branche dans le port de la carte réseau, à l'arrière de la tour de votre ordinateur.

La plupart des réseaux utilisent un type de câble qui ressemble à un câble de réseau téléphonique. Mais les apparences sont trompeuses. Le câble pour le téléphone est de moins bonne qualité et ne fonctionnera pas avec un réseau informatique. Sur ce dernier, chaque paire de fils du câble doit être inversée d'une certaine manière. C'est pourquoi ce type de câble est aussi appelé *câble à paires torsadées*. Les fils des câbles téléphoniques standards ne sont pas inversés.

Rendez-vous au Chapitre 5 pour tout savoir sur les câbles réseau.

Vous pouvez vous passer de câbles en installant un réseau sans fil. Je traite les réseaux sans fil au Chapitre 9.



- ✓ **Commutateur réseau.** Si votre réseau utilise un câble à paires torsadées, il aura probablement aussi besoin d'un *commutateur* (également appelé *switch*). Le commutateur est une petite boîte avec plein de connecteurs. Chaque ordinateur du réseau est connecté au commutateur par un câble. Le commutateur connecte ainsi tous les ordinateurs entre eux.

Au début des réseaux à paires torsadées, on utilisait des dispositifs appelés *concentrateurs* (*hubs*), dont les performances ont été largement dépassées par les commutateurs. Les concentrateurs ont cessé d'être utilisés après l'an 2000 !



- ✓ **Logiciel réseau.** Bien entendu, il faut installer plusieurs logiciels pour faire fonctionner un réseau. Pour un réseau pair-à-pair tournant sous Windows, vous devrez passer par le Panneau de configuration. Des systèmes d'exploitation réseau, tels que Windows Server 2008, requièrent une longue configuration avant de pouvoir fonctionner convenablement.

Reportez-vous au Chapitre 7 pour plus d'informations sur le choix d'un système d'exploitation réseau.



Ce n'est plus un ordinateur personnel !

S'il y a bien une chose dont je voudrais que vous vous souveniez avant tout, c'est qu'une fois que vous avez connecté votre ordinateur personnel (PC) au réseau, ce n'est plus un ordinateur personnel. Vous faites maintenant partie d'un réseau d'ordinateurs et, d'une certaine manière, vous avez dépouillé votre PC de l'attrait qui l'a rendu si populaire : l'indépendance.

J'ai commencé à faire de l'informatique à l'époque où les ordinateurs mainframes étaient ce qu'il y avait de mieux. Les *ordinateurs mainframes* étaient des machines énormes et complexes qui remplissaient des pièces entières et devaient être refroidies à l'eau. Mon premier ordinateur était un Hex Core Model 2000 de chez Binford à refroidissement liquide. Si, si, je vous assure ! Je n'invente pas cette histoire d'eau froide. Il fallait souvent avoir recours à un plombier pour installer un ordinateur mainframe. En fait, les plus gros d'entre eux étaient refroidis par de l'azote liquide. En revanche, j'ai inventé ce que j'ai dit à propos du Binford 2000.

Il fallait des équipes de programmeurs et d'opérateurs rien que pour veiller au bon fonctionnement des ordinateurs mainframes. Ils devaient être gérés avec soin. Toute une bureaucratie s'est bâtie autour de la gestion des mainframes.

Les ordinateurs mainframes dominaient le monde du travail. Les ordinateurs personnels ont tout changé. Ils ont déplacé la puissance informatique de la pièce où s'entassaient les gros ordinateurs vers le bureau d'un utilisateur, où elle est restée. Les PC ont coupé le lien avec le contrôle centralisé qu'exerçait l'ordinateur mainframe. Un utilisateur de PC peut regarder son ordinateur et se dire : « C'est le mien... rien que le mien ! » Les mainframes existent toujours mais ils ne sont plus autant utilisés qu'auparavant.

Les réseaux ont à leur tour tout bouleversé. D'une certaine manière, c'est un retour en arrière, vers la pensée mainframe. Il est vrai que le réseau n'est pas hébergé au sous-sol et qu'il n'y a pas besoin d'un plombier pour l'installer. Mais votre PC ne vous appartient plus totalement. Vous faites partie d'un réseau et, tout comme un mainframe, un réseau doit être géré avec soin.

Voici comment un réseau vous vole votre indépendance :

- ✓ **Vous ne pouvez pas supprimer des fichiers aveuglément sur le réseau.** Ils pourraient ne pas vous appartenir.
- ✓ **Avec le réseau, la sécurité est toujours un souci.** Par exemple, avant de vous permettre d'accéder aux fichiers du réseau, le serveur doit pouvoir vous identifier. Pour cela, vous devez saisir votre nom d'utilisateur et votre mot de passe. Le but est d'éviter qu'un gamin de quinze ans ne pénètre par effraction sur le réseau de votre entreprise via sa connexion Internet et dérobe tous les jeux installés sur votre ordinateur.

- ✓ **Il faut parfois attendre pour accéder aux ressources partagées.** Que Gilbert ait envoyé quelque document à l'imprimante de Lucien ne signifie pas que le document va être imprimé immédiatement. Jean-Jacques peut avoir commandé auparavant une impression qui va durer deux heures. Gilbert devra attendre.
- ✓ **L'espace de stockage n'est pas illimité.** Si vous copiez un fichier de base de données de 600 Mo sur le disque du serveur, des collaborateurs mécontents risquent de vous appeler pour se plaindre parce qu'il ne leur reste plus assez d'espace disque sur le serveur pour sauvegarder leurs fichiers importants.
- ✓ **Vos fichiers peuvent être infectés par un virus transmis par un autre utilisateur du réseau.** Puis, à votre tour, vous pouvez infecter accidentellement d'autres utilisateurs.
- ✓ **La sauvegarde de fichiers sensibles sur le serveur doit être une décision mûrement réfléchie.** Si vous sauvegardez sur le disque dur du serveur une note dans laquelle vous exprimez toute la haine que vous ressentez pour votre patron, sachez que ce dernier pourrait facilement la trouver et donc la lire.
- ✓ **Le serveur doit être allumé et opérationnel en permanence.** Si l'ordinateur de Lucien est un serveur, Lucien ne peut pas éteindre son ordinateur quand il quitte le bureau. S'il le fait, vous ne pouvez pas accéder aux fichiers stockés sur son ordinateur.
- ✓ **Si votre ordinateur est un serveur, vous ne pouvez pas l'éteindre sans prévenir.** Quelqu'un d'autre pourrait être en train d'accéder à un fichier sur votre disque dur ou d'imprimer un document avec votre imprimante.

Pourquoi Lucien récupère-t-il toujours la meilleure imprimante ? S'il ne tenait qu'à Jean-Jacques, je parie que c'est Julie qui l'aurait !

Devenir administrateur réseau

Vous n'êtes pas à l'abri de tout un tas de problèmes, même avec un réseau simple ; il est donc important de nommer un *administrateur réseau* qui sera chargé de veiller à ce que le réseau ne « tombe » pas ou ne devienne incontrôlable.

L'administrateur réseau n'a pas besoin d'être un génie de la technique. En fait, quelques-uns des meilleurs administrateurs réseau se révèlent être dénués de toutes connaissances techniques. Ce qui est important, c'est que l'administrateur soit bien organisé. Son travail est de s'assurer qu'il reste plein d'espace libre sur le serveur de fichiers, que ce dernier soit sauvegardé régulièrement, que les nouveaux employés puissent accéder au réseau, etc.

Il incombe aussi à l'administrateur réseau de résoudre les problèmes de base que les utilisateurs ne peuvent pas traiter par eux-mêmes et de savoir quand il convient d'appeler un expert si quelque chose de grave survient. C'est un métier difficile mais quelqu'un doit le faire. Voici quelques conseils :

- ✓ La quatrième partie de ce livre est entièrement consacrée au malheureux administrateur réseau. Si vous êtes concerné, lisez les chapitres de cette partie. Si vous êtes assez chanceux pour que la tâche soit attribuée à quelqu'un d'autre, fêtez cela en lui offrant un exemplaire de ce livre.
- ✓ Dans les petites structures, il arrive souvent que l'administrateur réseau soit choisi à la courte paille. La personne qui tire la paille la plus courte perd et devient l'administrateur réseau.
- ✓ Bien entendu, l'administrateur réseau ne peut pas être totalement incompetent techniquement parlant. J'ai un peu exagéré pour vous faire sentir combien les capacités organisationnelles sont plus importantes que les capacités techniques. L'administrateur doit être en mesure d'effectuer divers travaux de maintenance du réseau. Dans la pratique, il faut un minimum de savoir-faire technique mais l'essentiel tient aux capacités d'organisation.

Qu'auraient-ils donc que vous n'auriez pas ?

Au vu de tout ce qu'il faut prendre en compte, vous devez vous demander si vous êtes assez futé pour manipuler votre ordinateur après l'avoir connecté au réseau. Bien sûr que vous l'êtes ! Si vous êtes assez rusé pour acheter ce livre parce que vous savez que vous avez besoin d'un réseau, vous avez tout ce qu'il vous faut pour utiliser le réseau après l'avoir mis en place. Vous pourrez aussi l'installer et le gérer vous-même. Ce n'est pas de la recherche fondamentale.

Je connais certaines personnes qui se servent de réseaux à longueur de journée. Elles n'ont rien d'exceptionnel mais elles possèdent quelque chose que vous n'avez pas : un *certificat*. Donc, en vertu des pouvoirs qui me sont conférés par la Société des diminués de l'informatique, je vous remets le certificat de la Figure 1.2, vous confirmant que vous avez accédé au titre convoité de Nullité Réseau Certifiée ou NRC. Dans certains cercles, ce titre est bien plus prestigieux que l'indigeste badge CNE qu'arborent les véritables experts en réseau.

Félicitations et partez l'esprit tranquille !



Figure 1.2 : Certificat officiel NRC.

Chapitre 2

La vie sur le réseau

Dans ce chapitre :

- Utiliser les ressources locales et les ressources réseau.
- Jouer au jeu des noms.
- Se connecter au réseau.
- Utiliser des dossiers partagés.
- Explorer le réseau.
- Mapper des lecteurs réseau.
- Utiliser une imprimante réseau.
- Se déconnecter du réseau.

Une fois que votre PC aura été connecté au réseau, il ne sera plus une île séparée du reste du monde par quelque fanatique isolationniste brandissant un drapeau « Ne me marchez pas dessus ». La connexion au réseau change votre PC pour toujours. Votre ordinateur fait maintenant partie d'un « système », connecté aux « autres ordinateurs » sur le « réseau ». Vous devez alors vous préoccuper des détails ennuyeux de la vie en réseau comme avoir recours à des ressources locales ou partagées, vous connecter et accéder à des disques réseau, utiliser des imprimantes en réseau, vous déconnecter et qui sait quoi encore.

Quel ennui ! Ce chapitre veut vous montrer en quoi consiste la vie en réseau. Malheureusement, il devient parfois technique, si bien que vous risquez d'avoir besoin de votre capuchon de stylo.

Différence entre les ressources locales et les ressources réseau

Au cas où vous ne l'auriez pas compris dans le Chapitre 1, l'une des différences fondamentales entre un ordinateur isolé et un ordinateur en réseau est la distinction entre les ressources locales et les ressources réseau. Les *ressources locales* sont des choses telles que les disques, les imprimantes et les lecteurs de CD-ROM ou DVD qui sont connectés directement à votre ordinateur. Que vous soyez connecté ou non au réseau, vous pouvez toujours vous servir des ressources locales. Les *ressources réseau* sont les disques, les imprimantes et les lecteurs de CD-ROM qui sont connectés aux ordinateurs serveurs du réseau. Vous ne pouvez travailler avec les ressources réseau qu'une fois votre ordinateur connecté au réseau.

Toute l'astuce pour utiliser un ordinateur en réseau consiste à distinguer les ressources *locales* (qui vous appartiennent) des ressources *réseau* (qui appartiennent au réseau). Dans la plupart des réseaux, votre lecteur C est un disque local, comme votre dossier Mes documents. Si une imprimante se trouve à côté de votre PC, c'est probablement une imprimante locale. Vous pouvez faire tout ce que vous voulez avec ces ressources sans affecter le réseau ou les autres utilisateurs du réseau (du moment que ces ressources locales ne sont pas partagées sur le réseau).

- ✓ Vous ne pouvez pas dire d'une ressource qu'elle est locale ou réseau au premier coup d'œil. L'imprimante qui se trouve à côté de votre ordinateur est probablement votre imprimante locale mais, encore une fois, il peut s'agir d'une imprimante réseau. La même chose pour les lecteurs : le disque dur qui se trouve dans votre PC est probablement le vôtre mais il peut aussi être un disque réseau, employé par d'autres utilisateurs du réseau.
- ✓ Puisque les serveurs de réseau dédiés contiennent des ressources, vous pouvez dire qu'ils sont non seulement dédiés mais également un lieu de ressource.

Qu'est-ce qu'un nom ?

À peu près tout ce qui se trouve sur un réseau informatique porte un nom : les ordinateurs portent un nom, les utilisateurs portent un nom, les imprimantes et les disques partagés sur le réseau portent un nom et le réseau lui-même porte un nom. Il n'est pas essentiel de connaître chacun des noms utilisés sur le réseau mais il est important d'en connaître certains.

Voici quelques détails concernant les noms réseau :



- ✓ **Toute personne qui peut se servir du réseau dispose d'un *identifiant utilisateur* (ID utilisateur, pour abréger).** Vous devez connaître votre ID utilisateur afin de vous connecter au réseau. Vous devez aussi connaître les ID de vos copains, tout particulièrement si vous voulez leur chiper des fichiers ou leur envoyer des vacheries.

Nous reviendrons sur les ID utilisateur et la connexion dans la section suivante, intitulée « Se connecter au réseau ».



- ✓ **Il est tentant de laisser les utilisateurs du réseau se servir de leur nom comme ID utilisateur mais ce n'est pas une bonne idée.** Vous irez droit dans le mur, même dans une petite structure : souvenez-vous de cette Mrs. McCave qui eut vingt-trois enfants et les prénomma tous Dave.



Je suggère que vous adoptiez une méthode rigoureuse pour créer les ID utilisateur. Par exemple, vous pourriez choisir votre prénom et les deux premières lettres de votre nom de famille. L'ID de Gilbert serait alors *gilbertcl* et celui de Jean-Jacques *jeanjacquescl*. Vous pourriez aussi prendre la première lettre de votre prénom suivie de votre nom en entier. L'utilisateur Gilbert sera alors identifié par *gcleaver* et Jean-Jacques deviendra *jjcleaver* (notez que la casse importe peu dans la plupart des réseaux ; par conséquent, *jjcleaver* est identique à *JJcleaver*).



- ✓ **Chaque ordinateur sur le réseau doit disposer d'un nom unique de machine.** Vous n'avez pas à connaître le nom de tous les ordinateurs du réseau mais il peut être nécessaire de connaître le nom de votre ordinateur ainsi que les noms des ordinateurs serveurs auxquels vous devez accéder.

Le nom d'un ordinateur est souvent identique à l'ID de la personne qui utilise cet ordinateur. Cette pratique n'est pas recommandée car, dans beaucoup d'entreprises, les personnes vont et viennent plus rapidement que les ordinateurs. Le nom reflète parfois une localisation géographique telle que *bureau-12* ou *arrière-boutique*. Les ordinateurs serveurs portent des noms qui correspondent au groupe d'utilisateurs se servant le plus souvent du serveur comme *serveur-dao* ou *serveur-dev*.

Ici encore, certains fondus d'informatique se plaisent à se distinguer en utilisant des noms bizarroïdes tels que *BL3K5-87a*. Vous pourriez aussi préférer des noms tirés de la science-fiction. *HAL*, *Colossus*, *M5* et *Data* viennent à l'esprit. Les noms mignons comme *Herbie* ne sont pas autorisés. Cependant, *Tigrou* et *Winnie* sont parfaitement acceptables, même recommandés. Les tigres aiment les réseaux...



La technique la plus sensée consiste à attribuer des noms contenant des chiffres tels que *ordinateur001* ou *ordinateur002*.

- ✓ **Les ressources réseau telles que les disques et les imprimantes portent aussi un nom.** Par exemple, un serveur réseau peut disposer de deux imprimantes, nommées *laser* et *jetdencre* (pour indiquer le type d'imprimante) et de deux disques, nommés *disque-C* et *disque-D*.
- ✓ **Les serveurs réseau disposent d'un ID utilisateur réservé à l'administrateur.** Si vous vous connectez avec l'ID de l'administrateur, vous pourrez faire tout ce que vous voulez : ajouter de nouveaux utilisateurs, définir de nouvelles ressources réseau, changer le mot de passe de Gilbert, bref : tout. L'ID de l'administrateur réseau est parfois très subtil, du genre *administrateur*.
- ✓ **Le réseau lui-même a un nom.**

L'univers Windows comprend deux types de réseaux de base :

- Les *réseaux de domaine* sont la norme pour les grands environnements d'entreprise qui ont les serveurs consacrés et le personnel informatique pour les maintenir.
- Les *réseaux de groupe de travail* sont plus communs dans la sphère privée ou les petits bureaux qui ne possèdent pas de serveurs dédiés ou d'administrateurs.

Un réseau de domaine est représenté par un *nom de domaine* tandis qu'un réseau de groupe de travail est identifié par un *nom de groupe de travail*. Indépendamment du type de réseau que vous employez, vous devez connaître ce nom pour accéder au réseau.

Se connecter au réseau

Pour utiliser des ressources réseau, vous devez connecter votre ordinateur au réseau et passer par un processus confidentiel nommé *identification*. Le but de l'identification est de faire savoir au réseau qui vous êtes, de sorte qu'il décide si vous êtes un gentil ou un méchant.

S'identifier, c'est un peu comme encaisser un chèque. Le processus requiert deux types d'identification :

- ✓ **Votre ID utilisateur** : le nom sous lequel le réseau vous connaît. Votre ID utilisateur est généralement une variante de votre vrai nom, comme *jjacques* pour Jean-Jacques. Toute personne qui se sert du réseau doit disposer d'un ID utilisateur.
- ✓ **Votre mot de passe** : un mot secret que seuls vous et le réseau connaissez. Si vous tapez le bon mot de passe, le réseau croit que vous êtes qui vous dites être.

Chaque utilisateur a un mot de passe spécifique et ce mot de passe doit rester confidentiel.

Dans les premiers temps de l'informatique en réseau, vous deviez taper une commande d'identification à une invite MS-DOS puis saisir votre ID utilisateur et votre mot de passe. À l'heure de Windows, vous vous connectez au réseau via une boîte de dialogue spécialisée qui apparaît lorsque vous démarrez votre ordinateur. La Figure 2.1 représente la version Windows 7 de cette boîte de dialogue.



Voici quelques remarques à méditer :

- ✓ Les termes *nom d'utilisateur* et *nom de login* sont parfois employés à la place d'ID utilisateur. Ils signifient la même chose.
- ✓ Tant que nous parlons de mots qui signifient la même chose, sachez que *se connecter* et *se logger*, c'est pareil.
- ✓ En matière de réseau, vous et votre ordinateur êtes deux entités distinctes. Votre ID utilisateur se réfère à vous et non à votre ordinateur. C'est pourquoi vous avez un ID utilisateur tandis que votre ordinateur a un nom d'ordinateur. Vous pouvez vous connecter au réseau au moyen de votre ID utilisateur depuis n'importe lequel des ordinateurs connectés au réseau. De même, les autres utilisateurs peuvent se connecter au réseau depuis votre ordinateur avec leur propre ID.

Quand les autres se connectent à votre ordinateur à l'aide de leur propre ID, ils ne peuvent pas accéder à vos fichiers réseau si ces derniers sont protégés par un mot de passe. Cependant, ils *ont la possibilité* d'accéder aux fichiers locaux que vous n'avez pas protégés. Faites donc attention à bien choisir les personnes que vous autorisez à utiliser votre ordinateur.

- ✓ Si vous vous connectez à un réseau avec nom de domaine, la boîte de dialogue de connexion de Windows XP comprend un champ dans lequel vous devez entrer ce nom de domaine. Avec un peu de chance, il contiendra la valeur par défaut appropriée et vous pourrez ignorer ce champ sans aucun danger. Si ce n'est pas le cas, votre administrateur réseau se fera une joie de vous indiquer comment entrer cette information.
- ✓ Windows Vista et Windows 7 ne proposent pas de champ dans lequel vous pouvez spécifier le nom de domaine. Au lieu de cela, vous devez indiquer le nom de domaine, suivi de votre ID, en les séparant par une barre oblique inverse. Par exemple :

```
persepolis\jjacques
```

Ici, le nom de domaine est *persepolis* et le nom d'utilisateur est *jjacques*.

Notez que Windows Vista et Windows 7 retiennent les noms de domaine et d'utilisateur saisis lors de la précédente connexion. Il ne vous reste alors qu'à taper votre mot de passe. Pour vous connecter à un autre domaine ou comme autre utilisateur, cliquez sur **Changer d'utilisateur**. Cliquez ensuite sur l'icône **Autre utilisateur** et entrez un autre nom de domaine et d'utilisateur ainsi que le mot de passe approprié.

- ✓ Votre ordinateur peut avoir été configuré pour vous connecter automatiquement dès que vous l'allumez. Dans ce cas, vous n'avez pas à saisir votre ID utilisateur et votre mot de passe. Cette configuration rend la connexion plus conviviale mais elle en retire toute la saveur. Sans oublier que c'est carrément stressant si vous êtes un tant soit peu inquiet à l'idée que des méchants puissent accéder à vos fichiers personnels.
- ✓ Conservez votre mot de passe toute votre existence. Je vous dirais bien le mien mais je serais obligé de vous faire disparaître.



Figure 2.1 : Vous devez saisir votre ID et votre mot de passe pour accéder au réseau.

Les dossiers partagés

Avant l'ère des réseaux (Av. Rx), votre ordinateur ne disposait probablement que d'un disque nommé C. Peut-être deux, C et D, le second pouvant être un autre disque ou un lecteur de CD-ROM ou de DVD-ROM. Quoi qu'il en soit, ces disques sont physiquement présents dans votre PC. Ce sont des *disques locaux*.

Maintenant que vous êtes sur un réseau, vous aurez probablement accès à des disques qui ne sont pas sur votre PC mais qui se trouvent plutôt dans d'autres ordinateurs connectés au réseau. Ces disques réseau peuvent se situer sur un ordinateur serveur dédié ou, dans le cas d'un réseau pair-à-pair, sur un autre ordinateur client.

Vous pouvez, dans certains cas, accéder à l'intégralité d'un disque réseau via le réseau. Mais, dans la plupart des cas, vous ne pouvez accéder qu'à certains dossiers (*répertoires* dans le jargon MS-DOS) de ces disques réseau. D'une manière ou d'une autre, les disques ou les dossiers partagés sont désignés dans la terminologie Windows par *dossiers partagés*. Un dossier partagé est généralement appelé *disque réseau* parce qu'il est possible d'accéder au dossier partagé comme si c'était un disque séparé, avec sa propre lettre d'identification.

Il est possible de limiter l'utilisation des dossiers partagés. Par exemple, vous pouvez avoir un accès total à certains dossiers partagés, si bien que vous pouvez copier les fichiers qu'ils contiennent, les supprimer, créer ou déplacer des fichiers, etc. Dans les autres dossiers partagés, votre accès peut être limité de diverses manières. Par exemple, vous pouvez copier des fichiers depuis et vers un dossier partagé mais n'avez pas l'autorisation de supprimer, de modifier des fichiers ou de créer de nouveaux dossiers. Un mot de passe peut aussi être exigé pour vous autoriser à accéder à un dossier protégé. L'espace disque utilisable pour un dossier partagé peut également être limité. Pour plus d'informations sur les restrictions relatives au partage de fichiers, reportez-vous au Chapitre 18.



Gardez à l'esprit qu'en plus de pouvoir accéder aux dossiers partagés qui résident sur d'autres ordinateurs, vous pouvez aussi désigner votre ordinateur comme serveur afin de permettre aux utilisateurs du réseau d'accéder aux fichiers que vous partagez. Pour savoir comment partager des dossiers sur votre ordinateur avec les autres utilisateurs du réseau, reportez-vous au Chapitre 3.

Quatre bonnes utilisations d'un dossier partagé

Une fois que vous savez quels dossiers partagés sont à votre disposition sur le réseau, il faut réfléchir à ce que vous pouvez en faire ! Cette section décrit quatre bonnes raisons d'utiliser un dossier partagé.

Stocker des fichiers dont tout le monde a besoin

Un dossier partagé en réseau est un bon endroit pour entreposer des fichiers auxquels plusieurs utilisateurs doivent avoir accès. Sans réseau, vous devez stocker une copie des fichiers sur chaque ordinateur et veiller à ce que les copies soient correctement synchronisées. Vous pouvez aussi les transférer sur un support amovible, clé USB, CD-ROM ou DVD-ROM réinscriptible et les faire passer d'un utilisateur à l'autre ou encore conserver les fichiers sur un ordinateur et inviter les utilisateurs à venir les consulter sur place !

En réseau, il suffit de placer les fichiers dans un dossier partagé pour que toute personne autorisée puisse y accéder.

Stocker ses propres fichiers

Vous pouvez également considérer un dossier partagé comme une extension de votre disque dur local. Par exemple, si vous avez téléchargé sur Internet tant d'images, de musiques et de films qu'il n'y a plus d'espace disponible sur votre disque dur et si le serveur réseau possède des milliards et des milliards de gigaoctets d'espace libre, n'hésitez pas, déplacez vos données sur le disque réseau !

Voici quelques directives pour stocker dans de bonnes conditions des fichiers sur des disques réseau :

- ✓ **Une zone réseau peut être configurée pour un usage privé de vos données personnelles de sorte qu'aucun autre utilisateur ne puisse y accéder.** De cette façon, vous n'aurez pas à craindre un collègue fouineur susceptible de venir fourrer son nez dans vos dossiers confidentiels.
- ✓ **N'abusez pas du stockage sur les disques réseau.** Il est probable que d'autres utilisateurs commencent à saturer leur disque dur local et qu'ils seraient heureux de pouvoir bénéficier comme vous d'espace sur les disques réseau.
- ✓ **Avant de stocker des fichiers personnels sur un disque réseau, assurez-vous que vous en avez la permission.**
- ✓ **Sur les réseaux de domaine, la lettre H est généralement affectée aux dossiers personnels des utilisateurs (H pour *home*).** Ce dossier *home* est spécifique à chaque utilisateur ; vous pouvez le considérer comme la version réseau du dossier *Mes Documents* de votre disque local. Si un dossier *home* est à votre disposition sur le réseau, utilisez-le pour tous les fichiers importants plutôt que le dossier local *Mes Documents*. En effet, les zones réseau des utilisateurs (dossiers

home) sont, en général, incluses dans les procédures de sauvegarde quotidiennes du réseau. En revanche, les données des dossiers locaux Mes Documents *ne sont pas* prises en compte dans les sauvegardes.

Partager des informations avec d'autres utilisateurs

« Hé, Lucien, peux-tu me donner les statistiques sur les équipes de rugby de la Coupe du monde ? »

« Bien sûr, Gilbert ! » Mais comment faire ? Si le fichier se trouve sur le disque local de Lucien, comment celui-ci peut-il en donner une copie à Gilbert ? Lucien peut le faire en copiant le fichier sur un disque réseau. Ensuite, Gilbert n'aura plus qu'à le recopier sur son disque dur.

Voici quelques directives à garder à l'esprit quand vous utilisez un disque réseau pour échanger des fichiers avec d'autres utilisateurs :

- ✓ **N'oubliez pas de supprimer les fichiers que vous avez stockés dans le dossier réseau après qu'ils ont été récupérés.** Sinon, ce dernier risque de se remplir rapidement de fichiers inutiles.
- ✓ **Créez sur le disque réseau un dossier destiné spécifiquement au partage de fichiers entre plusieurs utilisateurs.** Nommez-le PARTAGE ou choisissez un nom qui décrit clairement sa fonction.



Dans la plupart des cas, il est plus facile d'envoyer des dossiers avec la messagerie plutôt qu'en faisant appel à un dossier réseau. Pour ce faire, il suffit d'envoyer un message au destinataire et d'insérer le fichier à partager ; vous n'avez pas alors à vous inquiéter de l'endroit où déposer le fichier sur le serveur ni à savoir qui le supprimera ensuite.

Sauvegarder son disque dur local

Si la taille du serveur de fichiers est suffisamment importante, vous pouvez sauvegarder, dans un dossier partagé, les données sensibles de votre disque dur local. Il suffit de copier les fichiers à sauvegarder dans un dossier partagé.

Évidemment, si vous recopiez la *totalité* de votre disque local (et si vos collègues ont les mêmes habitudes), vous risquez rapidement de saturer les disques réseau. Contactez l'administrateur réseau avant de vous lancer dans une telle opération ; il se peut que celui-ci ait déjà installé un disque réseau destiné spécialement aux copies de sauvegarde. Si vous êtes chanceux, votre

administrateur aura peut-être même mis à votre disposition un programme de sauvegarde automatique pour vos données importantes, de sorte que vous n'ayez plus rien à faire !

J'espère que votre administrateur réseau a également l'habitude de sauvegarder les disques réseau sur bande (consultez le Chapitre 22 pour plus de détails). De cette façon, si quelque chose arrive au serveur réseau, les données pourront être récupérées à partir des bandes de sauvegarde.

Explorer le réseau

Windows vous permet d'accéder à des ressources réseau, telles que les dossiers partagés, en parcourant le réseau. Sous Windows XP, il suffit de cliquer sur l'icône Favoris réseau qui se trouve sur votre Bureau. Sous Windows Vista et Windows 7, sélectionnez Réseau dans le menu Démarrer. La Figure 2.2 représente la version Windows 7 de l'explorateur de réseau.

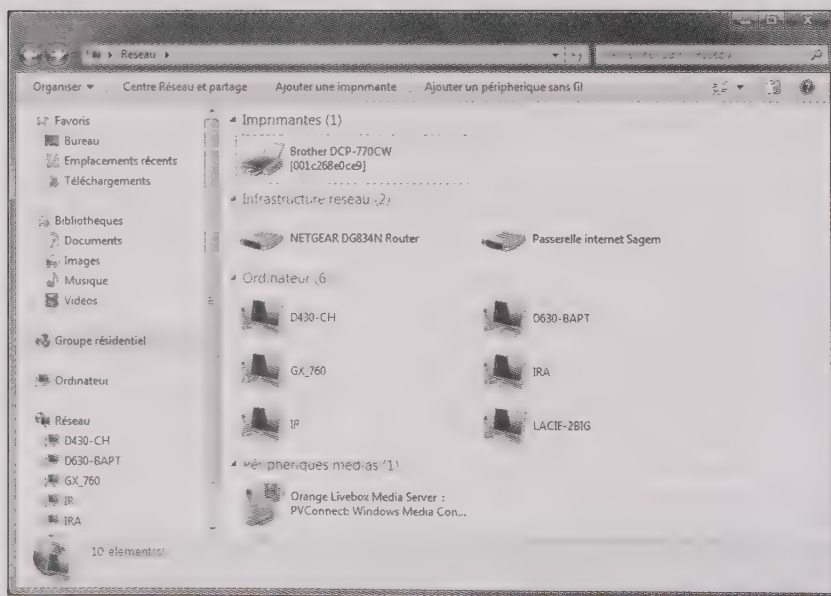


Figure 2.2 : Observation du réseau sous Windows 7.

Le réseau illustré dans la Figure 2.2 compte six ordinateurs, une imprimante, un commutateur ainsi qu'un routeur. Il suffit de double-cliquer sur l'une des icônes pour découvrir une liste des ressources partagées, disponibles sur l'ordinateur. Par exemple, la Figure 2.3 montre les ressources partagées par la machine LACIE-2BIG.

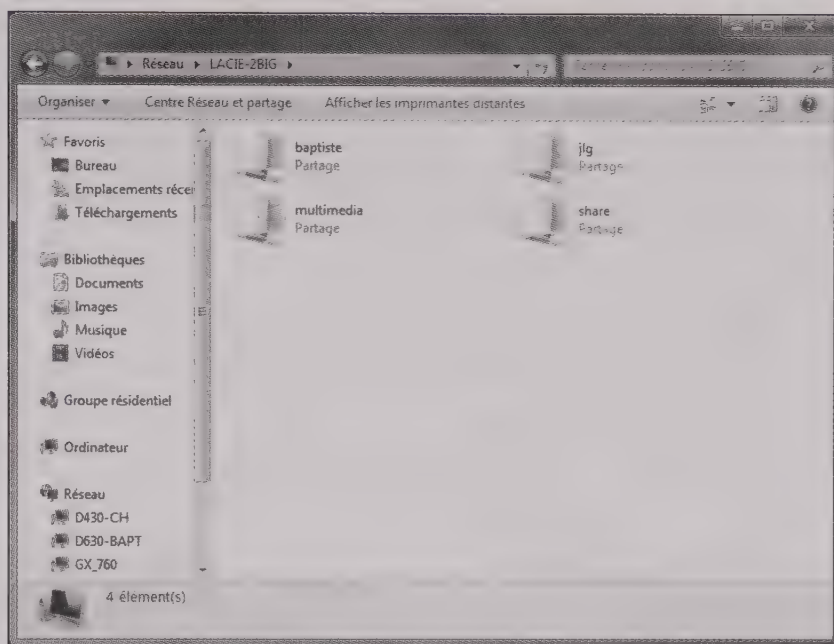


Figure 2.3 : Ressources disponibles sur un ordinateur serveur.

Vous pouvez également explorer le réseau à partir de n'importe quelle application Windows. Par exemple, vous travaillez avec Microsoft Word 2007 et voulez ouvrir un fichier stocké dans un dossier partagé de votre réseau. Pour ce faire, utilisez la commande Ouvrir pour ouvrir la boîte de dialogue du même nom (avec Office 2003, utilisez la commande Fichier/Ouvrir, avec Office 2007, cliquez sur le bouton Office). Sélectionnez Réseau dans la liste qui apparaît dans la partie gauche de la boîte de dialogue et parcourez le réseau pour accéder au fichier recherché (voir la Figure 2.4).



Sous Windows 95 ou 98, les Favoris réseau sont appelés Voisinage réseau. Lorsque vous ouvrez le Voisinage réseau sous Windows 95 ou 98, vous voyez immédiatement la liste des ordinateurs raccordés à votre réseau. Il suffit ensuite de cliquer sur l'un d'eux pour accéder à ses lecteurs et dossiers partagés.

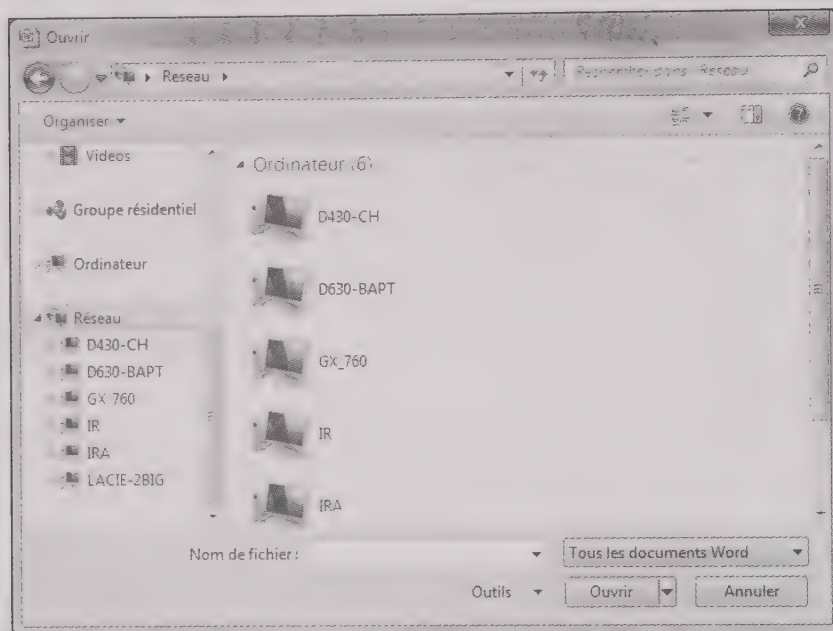


Figure 2.4 : Exploration du réseau à partir d'Office 2007.

Mapper des lecteurs réseau

Si vous réalisez que vous accédez très fréquemment à un dossier partagé, il pourrait être utile de recourir à une petite astuce nommée *mappage* pour accéder au dossier partagé plus rapidement. Le mappage consiste à attribuer une lettre de lecteur au dossier partagé. Vous pouvez alors employer cette lettre pour pénétrer dans le dossier partagé, comme s'il s'agissait d'un lecteur local. De cette manière, vous pouvez accéder au dossier partagé depuis n'importe quel programme Windows, sans avoir à naviguer dans le réseau.

Par exemple, vous pouvez mapper le dossier partagé nommé Fichiers sur le serveur SERVEUR-2BIG avec le lecteur K de votre ordinateur. Ainsi, pour accéder aux fichiers stockés dans le dossier partagé Fichiers, vous consultez simplement le lecteur K.

Procédez comme suit pour mapper un dossier partagé à une lettre de lecteur sous Windows 7 ou Windows Vista :

1. Sélectionnez Démarrer/Ordinateur.

La fenêtre Ordinateur s'ouvre.

2. Cliquez sur Connecter un lecteur réseau dans la barre d'outils.

La boîte de dialogue Connecter un lecteur réseau s'ouvre, comme le montre la Figure 2.5.

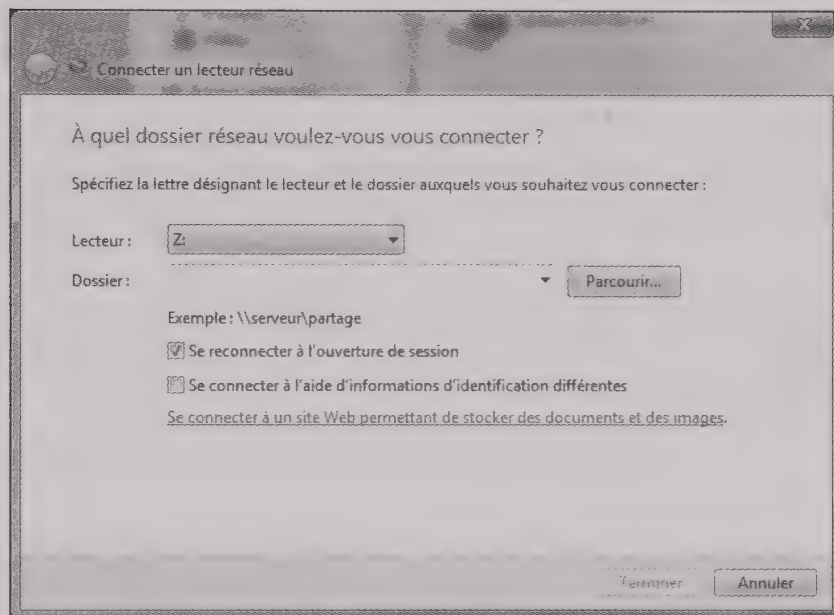


Figure 2.5 : Boîte de dialogue Connecter un lecteur réseau.

3. Si vous le souhaitez, vous pouvez modifier la lettre du lecteur dans la liste déroulante Lecteur.

Vous n'aurez certainement pas à modifier la lettre de lecteur proposée par Windows (Z dans la Figure 2.5). Toutefois, si vous êtes exigeant, vous pouvez choisir une autre lettre dans la liste déroulante Lecteur.

4. Cliquez sur le bouton Parcourir.

Une boîte de dialogue similaire à celle de la Figure 2.6 apparaît.

5. Utilisez la boîte de dialogue Rechercher un dossier pour rechercher et sélectionner le dossier partagé que vous voulez utiliser.

Vous pouvez parcourir tous les dossiers partagés de tous les ordinateurs du réseau.

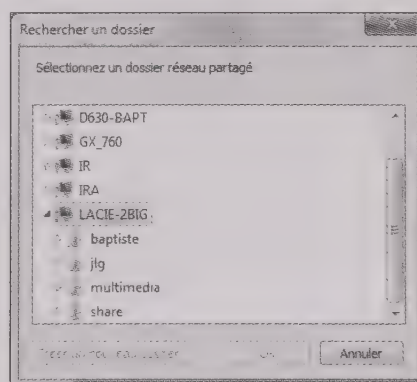


Figure 2.6 : Recherche du dossier à mapper.

6. Cliquez sur OK.

La boîte de dialogue Rechercher un dossier se ferme et vous rebasculiez dans la boîte de dialogue Connecter un lecteur réseau.

7. Si vous voulez que ce lecteur réseau soit automatiquement mappé dès que vous vous connectez au réseau, cochez la case Se reconnecter à l'ouverture de session.

Si vous ne cochez pas la case Se reconnecter à l'ouverture de session, la lettre de lecteur est uniquement disponible jusqu'à ce que vous quittiez Windows ou que vous vous déconnectiez du réseau. Si vous cochez cette option, le lecteur réseau est automatiquement mappé à chaque fois que vous vous connectez au réseau.



Assurez-vous que l'option Se reconnecter à l'ouverture de session est bien cochée, si vous avez souvent recours au lecteur réseau.

8. Cliquez sur Terminer.

Vous rebasculiez dans la fenêtre Ordinateur, illustrée par la Figure 2.7, dans laquelle apparaît désormais le lecteur réseau que vous venez de mapper.

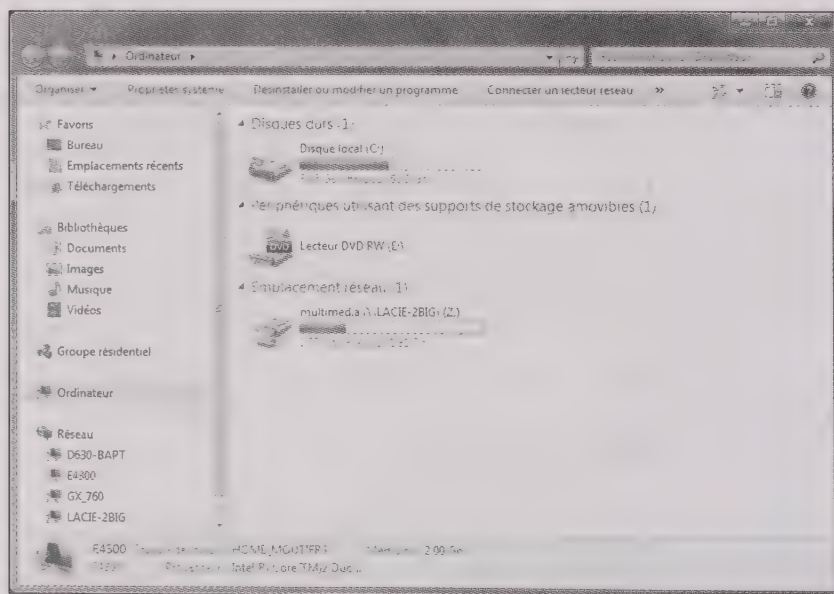


Figure 2.7 : Le lecteur réseau mappé figure dans la fenêtre Ordinateur.

Votre administrateur réseau a peut-être déjà configuré votre ordinateur avec un ou plusieurs lecteurs réseau mappés. Si tel est le cas, demandez-lui de vous indiquer quels sont les lecteurs qui ont été mappés. Autre alternative :

ouvrez simplement la fenêtre Ordinateur (Poste de travail sous Windows XP) pour y jeter un œil.

Voici quelques astuces supplémentaires :

- ✓ **Si vous utilisez Windows XP, la démarche pour mapper un disque réseau est analogue à celle de Windows Vista.** Cliquez sur l'icône Poste de travail et choisissez Outils/Connecter un lecteur réseau, puis suivez la procédure à partir de l'étape 3.
- ✓ **Associer une lettre de lecteur à un dossier partagé correspond à associer un lecteur ou mapper un lecteur.** On dit que « le lecteur H est mappé à un disque réseau ».
- ✓ **Les lettres de lecteur réseau n'ont pas besoin d'être attribuées de la même manière sur tous les ordinateurs du réseau.** Par exemple, un lecteur réseau auquel est assignée la lettre H sur votre ordinateur peut se voir attribuer la lettre Q sur un autre ordinateur. Dans ce cas, le lecteur H et le lecteur Q de l'autre ordinateur sont un seul et même lecteur. Cela peut prêter à confusion. Si votre réseau est organisé de cette manière, mettez du poivre dans le café de l'administrateur.
- ✓ **L'accès à un dossier partagé est beaucoup plus rapide par le lecteur mappé que par les Favoris réseau.** Cela est dû au fait que, lorsque vous ouvrez les Favoris réseau, Windows doit parcourir l'intégralité du réseau pour identifier tous les ordinateurs reliés au réseau, opération que Windows n'a pas à effectuer pour accéder à un lecteur mappé.
- ✓ **Si vous activez l'option Se reconnecter à l'ouverture de session, vous recevez un message d'avertissement si le lecteur n'est pas disponible au moment de la connexion.** La plupart du temps, cela signifie que le serveur n'est pas allumé. Quelquefois c'est aussi dû à une rupture de la connexion réseau. Pour de plus amples informations sur les solutions aux problèmes réseau de ce genre, reportez-vous au Chapitre 20.

L'imprimante réseau

Travailler avec une imprimante en réseau, c'est comme travailler avec un disque réseau. Vous pouvez imprimer sur une imprimante réseau à partir de n'importe quelle application Windows en choisissant une imprimante réseau disponible. Dans Office XP, la commande est localisée dans le menu Fichier. Dans Office 2007, il suffit de cliquer sur le bouton Office.

Rappelez-vous cependant qu'imprimer sur une imprimante réseau et imprimer sur une imprimante locale sont deux choses différentes. Avec une imprimante locale, vous êtes le seul à pouvoir l'utiliser alors que vous

partagez l'imprimante réseau avec les autres utilisateurs. Cela complique les choses de plusieurs manières :

- ✓ **Si plusieurs utilisateurs impriment sur l'imprimante réseau en même temps, le serveur doit bien distinguer les différents travaux d'impression.** S'il ne le faisait pas, il en résulterait un véritable cafouillis, votre rapport de 168 pages serait mélangé avec les fiches de salaire. Heureusement, le serveur fait attention que cela ne se produise pas et ce grâce à une fonctionnalité amusante nommée *spooling*.
- ✓ **L'impression en réseau fonctionne sur le principe du premier arrivé, premier servi (à moins que vous ne connaissiez les astuces présentées dans le Chapitre 3).** Invariablement, quand je me rends dans une grande surface, la personne qui se trouve devant moi à la caisse a choisi un produit qui n'a pas de code-barres et je reste là à attendre des heures que quelqu'un aille vérifier le prix. L'impression en réseau peut ressembler à cela. Si quelqu'un envoie un travail d'impression de deux heures à l'imprimante avant que vous puissiez transmettre une note d'une demi-page, vous devrez attendre.
- ✓ **Vous pouvez avoir accès à l'imprimante locale ainsi qu'à plusieurs imprimantes réseau.** Avant que vous ne soyez forcé d'utiliser un réseau, votre ordinateur disposait probablement d'une imprimante à laquelle il était connecté. Vous pouvez vous servir de votre imprimante jet d'encre bon marché (heu ! je voulais dire... locale) pour imprimer quelques documents et utiliser l'imprimante laser réseau pour des travaux plus importants. Pour cela, vous devez trouver dans vos applications le moyen de basculer d'une imprimante vers une autre.

Ajouter une imprimante réseau

Avant de pouvoir imprimer sur une imprimante réseau, vous devez configurer votre ordinateur pour accéder à l'imprimante réseau que vous avez choisie. Dans le menu Démarrer, sélectionnez le Panneau de configuration et double-cliquez sur l'icône Imprimantes. Si votre ordinateur est déjà configuré pour fonctionner avec une imprimante réseau, une icône représentant cette imprimante apparaît dans le dossier Imprimantes. Vous pouvez distinguer une imprimante réseau d'une imprimante locale par la forme de son icône ; les imprimantes réseau ont un tuyau attaché à leur base.

Si aucune imprimante réseau n'est configurée sur votre ordinateur, vous pouvez en ajouter une avec l'Assistant Ajout d'imprimante. Respectez les étapes suivantes sous Windows Vista ou Windows 7 :

1. Dans le menu Démarrer, sélectionnez Panneau de configuration et double-cliquez sur l'icône Imprimantes.

2. Cliquez sur le bouton Ajouter une imprimante dans la barre d'outils.

L'Assistant Ajout d'imprimante s'ouvre, comme le montre la Figure 2.8.

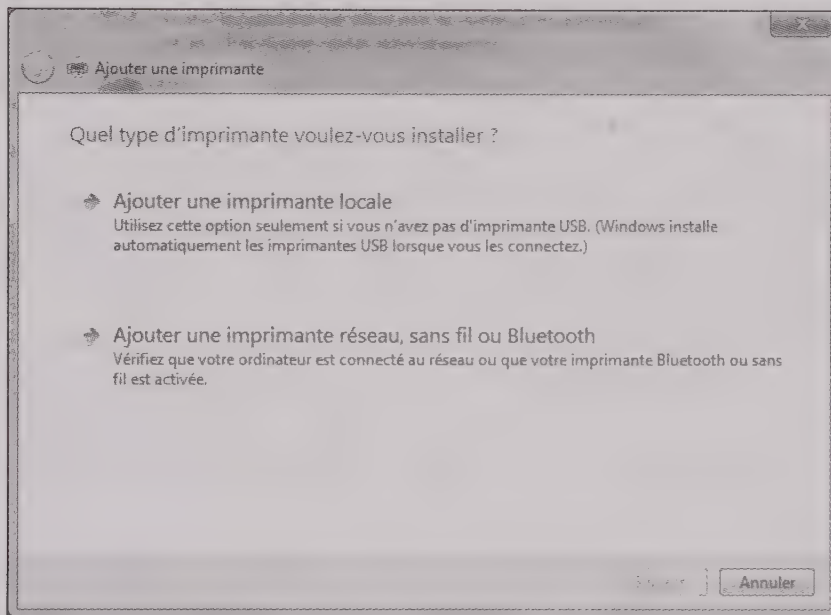


Figure 2.8 : Fenêtre de l'Assistant Ajout d'imprimante.

3. Sélectionnez l'option Ajouter une imprimante réseau, sans fil ou Bluetooth.

L'assistant examine le réseau comme le montre la Figure 2.9, puis affiche les imprimantes disponibles.

4. Sélectionnez l'imprimante de votre choix.

Si vous ne parvenez pas à localiser l'imprimante, demandez à l'administrateur quel est le *chemin UNC* (*Universal Naming Convention*, convention de nom universelle qui l'identifie sur le réseau ou son adresse IP). Cliquez ensuite sur L'imprimante que je veux n'est pas répertoriée puis entrez le chemin UNC ou l'adresse IP quand vous y êtes invité.

5. Cliquez sur Suivant pour ajouter l'imprimante.

L'assistant copie les pilotes d'impression de l'imprimante réseau sur votre ordinateur. Il se peut que l'assistant vous demande de confirmer ce choix. Dans ce cas, cliquez sur Installer le pilote.



L'Assistant Ajout d'imprimante affiche le nom de l'imprimante et demande si l'imprimante en cours d'installation doit devenir l'imprimante par défaut.

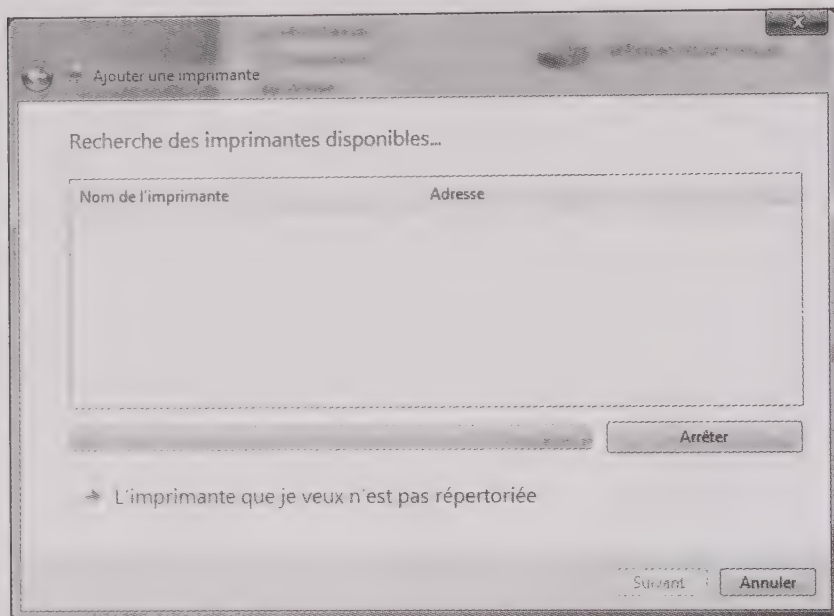


Figure 2.9 : L'Assistant Ajout d'imprimante examine le réseau.

6. Définissez l'imprimante comme votre imprimante par défaut, si vous le souhaitez.

7. Cliquez sur Suivant pour continuer.

Une dernière boîte de dialogue s'affiche.

8. Cliquez sur Terminer.

Vous avez terminé !



Nombre d'imprimantes réseau, principalement les plus récentes, sont connectées directement au réseau via une carte Ethernet intégrée. La configuration de ces imprimantes peut s'avérer délicate. Vous devrez peut-être demander de l'aide à votre administrateur réseau. Certaines imprimantes directement connectées au réseau disposent de leur propre adresse Internet, par exemple *Imprimante.FamilleBrecat.com*. Dans ce cas, vous pouvez paramétrer l'imprimante en allant sur sa page Web à l'aide de votre navigateur. Pour installer l'imprimante, il suffit de cliquer sur un lien.

Imprimer sur une imprimante réseau

Une fois l'imprimante réseau installée sous Windows, rien de plus facile que d'imprimer. Vous pouvez imprimer sur l'imprimante réseau depuis n'importe quel programme Windows grâce à la commande Imprimer qui ouvre la boîte de dialogue Imprimer. Par exemple, la Figure 2.10 montre la boîte de dialogue Imprimer de WordPad, le programme de traitement de texte fourni avec Windows. Les imprimantes disponibles figurent dans la partie supérieure de la boîte de dialogue. Sélectionnez l'imprimante réseau dans cette liste et cliquez sur OK pour imprimer votre document. C'est tout ce qu'il y a à faire !

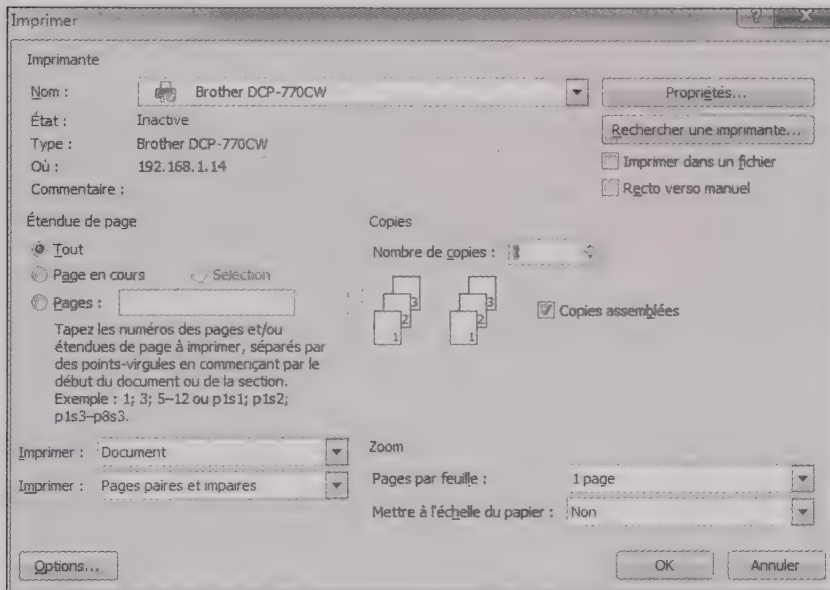


Figure 2.10 : Boîte de dialogue Imprimer type.

Gérer la file d'attente

En général, une fois le travail d'impression envoyé à l'imprimante réseau, vous n'avez plus à vous en soucier. Vous vous rendez simplement à l'endroit où se trouve l'imprimante et voilà, votre document imprimé vous attend.

C'est ce qui se passe dans un monde idéal. Dans le monde réel où nous vivons vous et moi, toutes sortes de choses peuvent arriver à votre travail d'impression entre l'instant où vous l'avez envoyé à l'imprimante réseau et l'instant où celle-ci commence effectivement l'impression :

- ✓ Vous découvrez que quelqu'un a envoyé avant vous un rapport de 50 trillions de pages dont l'impression ne sera achevée que lorsque la dette nationale aura été remboursée.
- ✓ Le prix des vis plaquées a augmenté de deux euros, rendant obsolètes les recommandations que vous formulez dans votre rapport.
- ✓ Votre chef vous appelle et vous dit que son beau-frère va assister à la réunion et que vous seriez bien aimable d'imprimer une version supplémentaire de la proposition à son intention. Une photocopie ne saurait convenir ; des originaux, s'il vous plaît !
- ✓ Vous avez décidé d'aller manger et vous ne voulez pas que votre document soit imprimé avant que vous soyez de retour.

Heureusement, vous n'avez pas perdu tout contrôle sur votre travail d'impression. Vous pouvez facilement changer l'état des travaux d'impression que vous avez envoyés à l'imprimante. En effet, il vous est possible de modifier l'ordre dans lequel les travaux sont imprimés, de suspendre un travail de sorte qu'il ne soit pas imprimé tant que vous ne l'avez pas demandé ou carrément de le supprimer.

Nul doute que vous êtes assez doué pour apprendre à vos travaux à faire d'autres choses, comme se serrer les mains, se retourner et faire le mort. Mais les astuces de base (suspendre, annuler et changer l'ordre des impressions) suffiront pour débiter.

Pour gérer la file d'attente, ouvrez le Panneau de configuration (Démarrer/Panneau de configuration) puis cliquez sur Imprimantes. Double-cliquez ensuite sur l'icône de l'imprimante que vous voulez gérer. Une fenêtre s'ouvre, semblable à celle représentée dans la Figure 2.11. Un seul document est en attente.

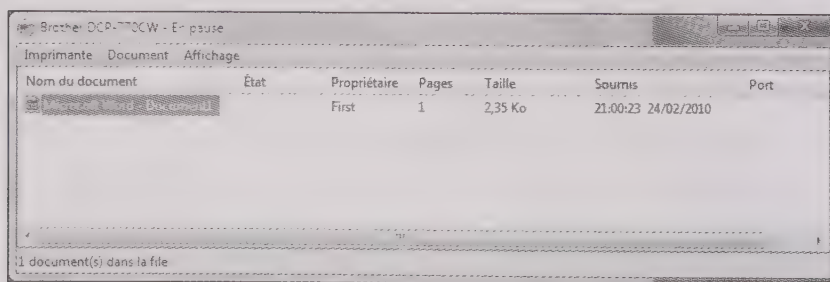


Figure 2.11 : Gestion de la file d'attente des impressions.

Voici quelques astuces pour gérer les travaux d'impression qui figurent dans la file d'attente ou dans l'imprimante elle-même :

- ✓ **Pour suspendre temporairement un travail**, sélectionnez-le et utilisez la commande Document/Suspendre l'impression. Cette commande relance aussi l'impression.
- ✓ **Pour supprimer un travail d'impression**, sélectionnez-le et exécutez la commande Document/Annuler l'impression.
- ✓ **Pour arrêter l'imprimante**, exécutez Imprimante/Suspendre l'impression. Utilisez cette même commande pour la relancer.
- ✓ **Pour supprimer tous les travaux**, cliquez sur la commande Imprimante/Purger les documents d'impression.
- ✓ **Pour placer un travail en tête de la file d'attente**, glissez-le en haut de la liste.

Toutes ces astuces ne s'appliquent évidemment qu'à vos travaux d'impression. Vous ne pouvez heureusement pas supprimer ceux d'autrui.

Ce qu'il y a de bien dans la gestion de l'impression sous Windows, c'est qu'elle vous décharge de tous les détails inhérents aux différents systèmes d'exploitation réseau. Que vous imprimiez sur une imprimante NetWare, sur une imprimante sous Windows 2003 ou sur une imprimante partagée sous Windows, la fenêtre d'impression gère les travaux de la même manière.

Se déconnecter du réseau

Vous devriez vous déconnecter quand vous avez fini d'utiliser le réseau. Se déconnecter d'un réseau rend les disques et les imprimantes réseau indisponibles. Votre ordinateur est toujours physiquement connecté au réseau (à moins que vous n'ayez coupé le câble réseau avec des cisailles ; mauvaise idée, ne le faites pas !) mais vous ne pouvez plus accéder au réseau et à toutes ses ressources.

Voici quelques conseils à garder à l'esprit lorsque vous vous déconnectez :

- ✓ Après avoir éteint votre ordinateur, vous êtes automatiquement déconnecté du réseau. Lorsque vous démarrez votre ordinateur, vous devez vous reconnecter.

C'est une bonne idée que de se déconnecter du réseau si vous comptez ne pas avoir besoin de votre ordinateur pendant un certain temps. Tant que votre ordinateur est connecté, n'importe qui peut s'en servir pour accéder au réseau. Alors, dans le cas où des utilisateurs non autorisés se serviraient de votre ID utilisateur, vous seriez responsable des éventuels dégâts.



- ✓ Sous Windows, cliquez sur le bouton Démarrer et sélectionnez l'option Fermer la session pour vous déconnecter. Cette action vous déconnecte du réseau sans redémarrer Windows.
 - *Sous Windows XP*, vous accédez directement à cette commande à partir du menu Démarrer.
 - *Sous Windows Vista*, cliquez sur Démarrer puis sur la flèche qui apparaît à côté du petit cadenas.

Chapitre 3

Utiliser pleinement le réseau

Dans ce chapitre :

- Transformer un ordinateur en serveur réseau.
- Partager des dossiers avec d'autres utilisateurs.
- Utiliser le dossier Public avec Windows Vista et Windows 7.
- Partager une imprimante.
- Utiliser Microsoft Office en réseau.
- Travailler avec des fichiers hors connexion.

Le Chapitre 2 pose les bases de l'utilisation d'un réseau : connexion au réseau, accès aux données stockées dans des dossiers partagés, impression et déconnexion. Dans ce chapitre, je vous invite à aller au-delà de ces bases. Vous allez découvrir comment transformer votre ordinateur en serveur pour partager vos propres fichiers et imprimantes, comment utiliser l'une des applications informatiques les plus populaires, la messagerie, et comment travailler avec Office en réseau.

Partager des ressources

Comme vous le savez probablement déjà, il existe deux types d'ordinateurs sur un réseau : les ordinateurs clients et les ordinateurs serveurs. Dans le système économique du réseau, les *ordinateurs clients* sont les consommateurs, ceux qui utilisent les ressources du réseau telles que les imprimantes et les disques partagés. Les *serveurs* sont les fournisseurs, ceux qui mettent à disposition leurs propres imprimantes et leurs propres disques sur le réseau de sorte que les ordinateurs clients puissent y accéder.

Ce chapitre montre comment vous pouvez transformer votre ordinateur client Windows en un ordinateur serveur pour que les autres ordinateurs du réseau se servent de votre imprimante et de tous les dossiers que vous déciderez de partager. De cette manière, votre ordinateur fonctionne à la fois comme un client et comme un serveur :

- ✓ C'est un ordinateur **client** lorsque vous envoyez un document à une imprimante réseau ou quand vous accédez à un fichier stocké sur le disque d'un autre serveur.
- ✓ C'est un ordinateur **serveur** quand quelqu'un d'autre envoie un travail d'impression à votre imprimante ou accède à un fichier stocké sur le disque de votre ordinateur.

Activer le partage de fichiers et d'imprimantes (Windows XP)

Avant que vous ne partagiez vos fichiers et votre imprimante avec les autres utilisateurs du réseau, vous devez activer une fonctionnalité Windows nommée *Partage de fichiers et d'imprimantes*. Si cette fonctionnalité n'est pas activée, votre ordinateur peut se comporter en client mais pas en serveur. Cette section montre comment mettre en œuvre ces fonctionnalités avec Windows XP. Pour Windows Vista, consultez la section suivante, « Activer le partage de fichiers et d'imprimantes (Windows Vista) ».

Avec un peu de chance, le partage des fichiers et des imprimantes est déjà activé sur votre ordinateur. Pour le savoir, double-cliquez sur Poste de travail sur le Bureau, sélectionnez l'icône de votre lecteur C et cliquez sur le menu Fichier. Si ce dernier comporte une commande de partage, le partage des fichiers et des imprimantes est activé et vous pouvez sauter le reste de cette section. Si vous ne trouvez pas de commande de partage dans le menu Fichier, vous devrez installer le partage des fichiers et des imprimantes avant de pouvoir partager un fichier ou une imprimante avec les utilisateurs du réseau.

Pour activer le partage de fichiers et d'imprimantes sous Windows XP, procédez de la manière suivante :

- 1. Dans le menu Démarrer, sélectionnez Paramètres puis Panneau de configuration.**

Le Panneau de configuration s'ouvre.

- 2. Double-cliquez sur l'icône Connexions réseau.**

La boîte de dialogue Connexions réseau s'ouvre.

3. Effectuez un clic droit sur Connexion au réseau local et cliquez sur Propriétés.

La boîte de dialogue Propriétés de Connexion au réseau local s'affiche, comme le montre la Figure 3.1.

4. Cochez la case Partage de fichiers et d'imprimantes pour les réseaux Microsoft.

5. Cliquez sur OK.



Lorsque vous êtes dans la boîte de dialogue Connexions réseau, ne vous amusez pas à changer les autres paramètres du réseau. Vous pouvez modifier les options de partage de fichiers et d'imprimantes en toute sécurité mais, de grâce, ne touchez pas aux autres options.

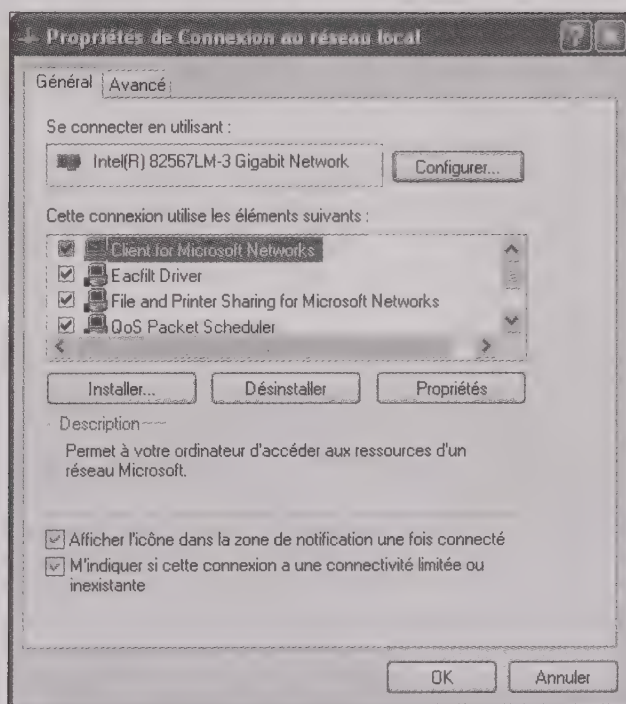


Figure 3.1 : Boîte de dialogue Propriétés de Connexion au réseau local.

Activer le partage de fichiers et d'imprimantes (Windows Vista)

Pour activer le partage de fichiers et d'imprimantes sous Windows Vista, procédez de la manière suivante :

1. Cliquez sur Démarrer/Réseau.

La fenêtre Réseau s'ouvre.

2. Cliquez sur le bouton Centre Réseau et partage dans la barre d'outils.

La boîte de dialogue Centre Réseau et partage apparaît, comme le montre la Figure 3.2.

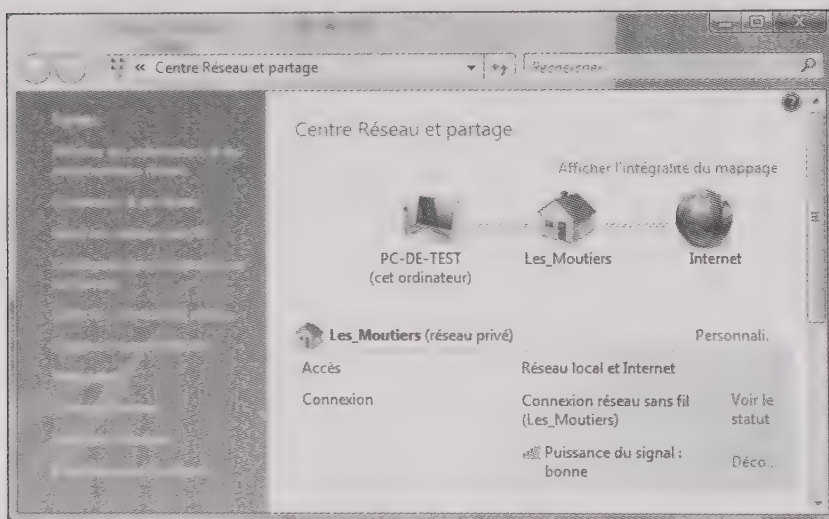


Figure 3.2 : Boîte de dialogue Centre Réseau et partage.

3. Sélectionnez l'option Partage de fichiers.

Cette étape affiche les commandes qui vous permettent d'activer le partage de fichiers, comme le montre la Figure 3.3.

4. Sélectionnez Activer le partage de fichiers et cliquez sur Appliquer.

Le partage de fichiers est activé.

5. Sélectionnez l'option Partage d'imprimante.

Cette étape affiche les commandes qui vous permettent d'activer le partage d'imprimante.

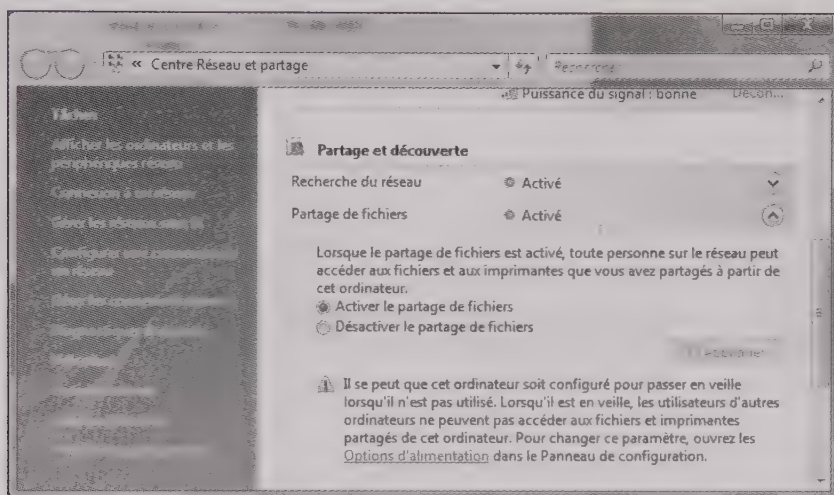


Figure 3.3 : Le sous-menu Partage et découverte.

6. Sélectionnez Activer le partage d'imprimante et cliquez sur Appliquer.

Le partage d'imprimante est activé.

7. Fermez le Centre Réseau et partage.

Vous pouvez maintenant partager vos fichiers et imprimantes.

Activer le partage de fichiers et d'imprimantes (Windows 7)

Suivez ces étapes pour activer le partage de fichiers et d'imprimantes sous Windows 7 :

1. Cliquez sur le bouton Démarrer, tapez Paramètres de partage avancés et appuyez sur Entrée.

Cette étape ouvre la fenêtre Paramètres de partage avancés dans laquelle figurent les paramètres réseau de tous les réseaux auxquels vous êtes connecté. Deux réseaux sont mentionnés pour un ordinateur domestique : Résidentiel ou professionnel et Public. Un troisième réseau nommé Domaine existe pour un ordinateur connecté à un réseau de domaine.

2. Cliquez sur la flèche en regard du réseau pour lequel vous voulez activer le partage de fichiers et d'imprimantes.

Pour un ordinateur domestique, cliquez sur la flèche qui pointe vers le bas, correspondant à Résidentiel ou professionnel. Pour un ordinateur connecté à un réseau de domaine, cliquez sur la flèche en regard de Domaine.

La Figure 3.4 représente les paramètres d'un réseau Résidentiel ou professionnel.

N'activez *pas* le partage de fichiers ou d'imprimantes pour le réseau Public.

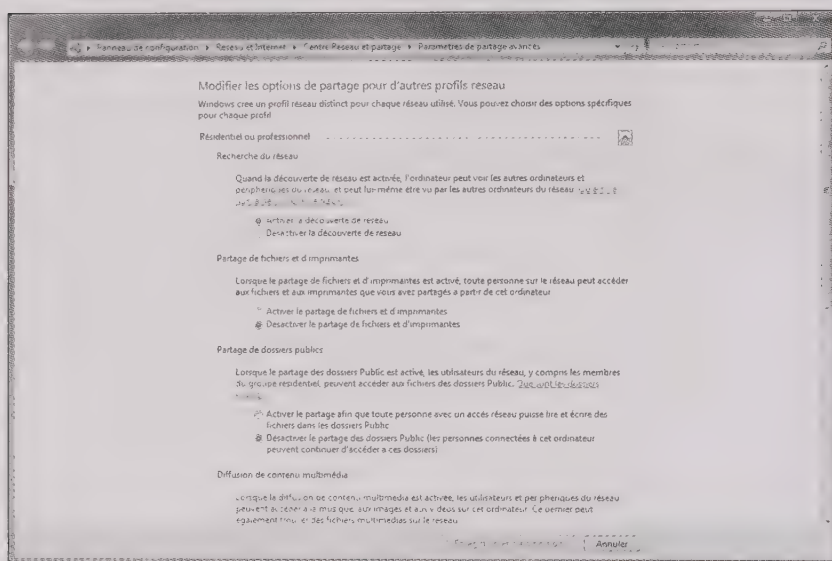


Figure 3.4 : Activation du partage de fichiers et d'imprimantes sous Windows 7.

3. Activez l'option Activer le partage de fichiers et d'imprimantes.

4. Cliquez sur Enregistrer les modifications.

Cette action enregistre vos modifications et ferme la fenêtre Paramètres de partage avancés.

Partager un dossier

Pour permettre aux autres utilisateurs du réseau d'accéder aux fichiers stockés sur votre disque dur, vous devez partager le disque entier ou désigner un dossier du disque comme dossier *partagé*. Si vous partagez un disque entier, les autres utilisateurs du réseau pourront accéder à tous les fichiers et répertoires de ce disque. Si vous partagez un dossier, les

utilisateurs du réseau ne pourront accéder qu'aux fichiers figurant dans le dossier que vous partagez (si le dossier que vous partagez contient d'autres dossiers, les utilisateurs du réseau pourront aussi accéder aux fichiers que contiennent ces dossiers).



Je vous recommande de ne pas partager votre disque tout entier, à moins que vous ne vouliez permettre à *n'importe qui sur le réseau* de farfouiller dans vos fichiers. Vous devriez plutôt vous contenter de partager un ou des dossiers qui contiennent les documents spécifiques que vous voulez mettre à disposition des autres utilisateurs du réseau. Par exemple, si vous stockez vos documents Word dans le dossier Mes documents, vous pouvez partager ce dossier de sorte que les autres utilisateurs du réseau puissent accéder à vos documents Word.

Partager un dossier sous Windows XP

Pour partager un dossier sur un ordinateur équipé de Windows XP, procédez comme suit :

1. Double-cliquez sur l'icône Poste de travail de votre Bureau.

La fenêtre Poste de travail s'affiche à l'écran.

2. Sélectionnez le dossier que vous souhaitez partager.

Cliquez sur l'icône du disque qui contient le dossier que vous souhaitez partager puis localisez et sélectionnez le dossier concerné.

3. Faites un clic droit sur le dossier et sélectionnez Partage et sécurité.

La boîte de dialogue Propriétés du dossier que vous voulez partager s'affiche. Notez que les options de partage sont grisées.

4. Cochez l'option Partager ce dossier sur le réseau.

Les autres options ne sont plus grisées, comme le montre la Figure 3.5.

Si vous le souhaitez, vous pouvez sauter les étapes 2 à 4. Il vous suffit d'effectuer un clic droit sur le dossier que vous voulez partager puis de sélectionner Partage et sécurité dans le menu contextuel.

5. Modifiez le nom de partage si vous n'aimez pas celui que Windows propose.

Le *nom de partage* est le nom sous lequel les autres utilisateurs du réseau voient le dossier partagé. Vous pouvez utiliser n'importe quel nom, du moment qu'il compte moins de douze caractères. Les majuscules et les minuscules sont considérées de la même manière : « Mes documents » est identique à « MES DOCUMENTS ».



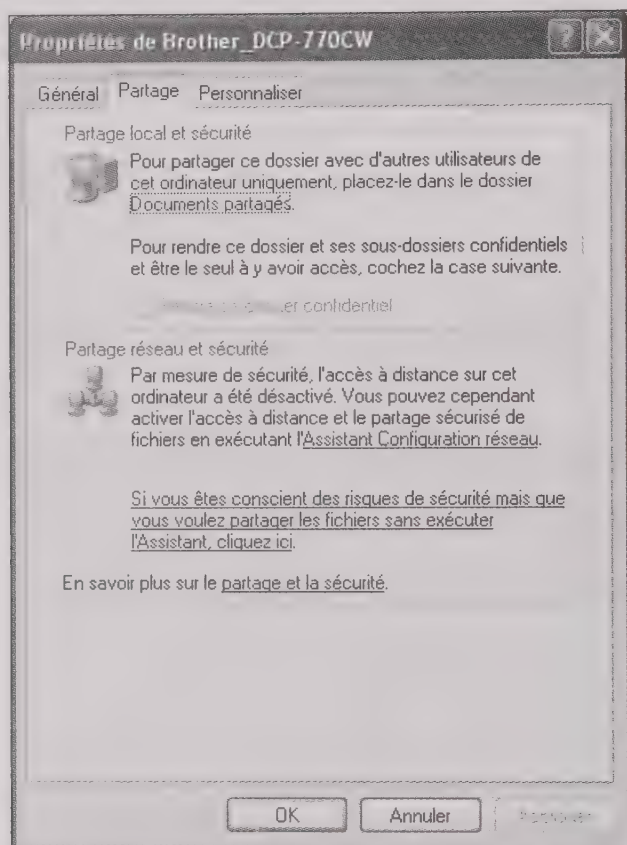


Figure 3.5 : Les options de partage ne sont plus grisées quand vous sélectionnez Partager ce dossier sur le réseau.



Windows propose un nom de partage basé sur le nom courant du dossier. Si le nom du dossier compte douze caractères (ou moins), le nom proposé est identique au nom du dossier. Si le nom du dossier dépasse douze caractères, Windows génère une version abrégée. Par exemple, « Fichiers Multimédia » devient « FICHIERS MUL ».

Si le nom que Windows a choisi n'a pas de sens ou semble bizarre, modifiez-le. Par exemple, je choisirais probablement « MULTIMEDIA » au lieu de « FICHIERS MUL ».

6. Pour permettre aux autres utilisateurs du réseau de modifier les fichiers de ce dossier, cochez la case Autoriser les utilisateurs réseau à modifier mes fichiers.

Si vous n'activez pas cette option, les autres utilisateurs pourront ouvrir vos fichiers mais seront dans l'impossibilité d'enregistrer leurs modifications.

7. Cliquez sur OK.

La boîte de dialogue Propriétés disparaît et une main est ajoutée à l'icône du dossier pour montrer qu'il est dorénavant partagé.

Si vous changez d'avis et décidez de ne plus partager le dossier, double-cliquez sur Poste de travail, sélectionnez le dossier ou le lecteur que vous ne voulez plus partager et exécutez Fichier/Partage et sécurité pour afficher la boîte de dialogue Propriétés. Décochez alors l'option Partager ce dossier sur le réseau puis cliquez sur OK.

Partager un dossier sous Windows Vista ou Windows 7

Pour partager un dossier sur un ordinateur équipé de Windows Vista ou Windows 7, procédez comme suit :

1. Choisissez Démarrer/Ordinateur.

La fenêtre Ordinateur apparaît.

2. Repérez le dossier que vous souhaitez partager.

3. Effectuez un clic droit sur le dossier à partager et cliquez sur Propriétés.

La boîte de dialogue Propriétés s'ouvre.

4. Cliquez sur l'onglet Partage puis sur le bouton Partager.

La boîte de dialogue Partage de fichiers s'affiche, comme le montre la Figure 3.6.

5. Cliquez sur la flèche de la liste déroulante, sélectionnez Tout le monde et cliquez sur Ajouter.

Cette action indique que n'importe qui sur votre réseau peut accéder au dossier partagé.

Si vous préférez, vous pouvez limiter l'accès à certains utilisateurs. Pour ce faire, sélectionnez chaque personne à qui vous accordez l'accès et cliquez sur Ajouter.

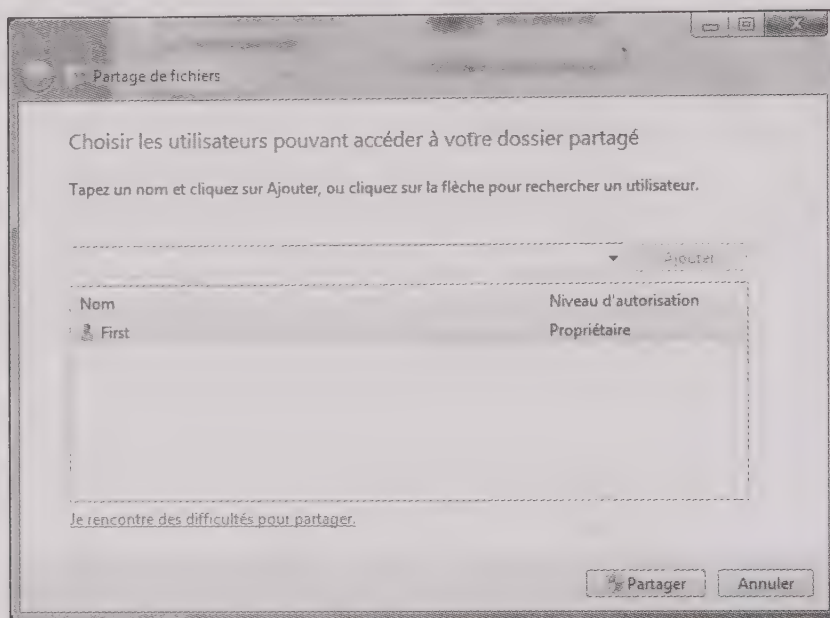


Figure 3.6 : Boîte de dialogue Partage de fichiers (Windows Vista et Windows 7).

6. Sélectionnez ensuite le niveau d'accès que vous affectez à chaque utilisateur.

Utilisez la liste déroulante de la colonne Niveau d'autorisation pour choisir l'un de ces trois niveaux d'accès :

- **Lecteur** : un lecteur peut ouvrir des fichiers ouverts mais ne peut pas modifier ou créer de nouveaux fichiers ou dossiers.
- **Collaborateur** : un collaborateur peut ajouter des fichiers au dossier partagé et seulement modifier ou supprimer ses propres fichiers.
- **Copropriétaire** : un copropriétaire a l'accès total au dossier partagé. Il peut créer, modifier ou supprimer n'importe quel fichier du dossier.

7. Cliquez sur Partager.

La boîte de dialogue qui s'affiche confirme que le dossier a été partagé.

Utiliser des dossiers publics sous Windows Vista et Windows 7

Windows Vista et Windows 7 introduisent une nouvelle méthode de partage des fichiers sur le réseau : le dossier Public. Le *dossier Public* est simplement un dossier affecté à l'accès public. Les fichiers et sous-dossiers de ce dossier Public peuvent être consultés par d'autres utilisateurs du réseau et par n'importe quel utilisateur qui ouvre une session sur votre ordinateur.

Avant de pouvoir utiliser le dossier Public, vous devez l'activer. Sous Windows 7, respectez les étapes de la section « Activer le partage de fichiers et d'imprimantes (Windows 7) » mais sélectionnez l'option Activer le partage dans la zone Partage de dossiers publics. Pour Windows Vista, référez-vous à la section « Activer le partage de fichiers et d'imprimantes (Windows Vista) » mais sélectionnez l'option Partage de dossiers publics au lieu des options Partage de fichiers et Partage d'imprimantes.

Après avoir activé le partage du dossier Public, vous pouvez accéder à ce dossier sur votre ordinateur. Pour ce faire sous Windows Vista, exécutez la commande Démarrer/Ordinateur puis cliquez sur le dossier Public dans la partie gauche de la fenêtre. Pour ouvrir un dossier Public sous Windows 7, cliquez sur Démarrer/Ordinateur puis sur Bibliothèques dans la partie gauche. Vous avez alors accès aux dossiers Documents, Musique, Images ou Vidéos. La Figure 3.7 vous propose un exemple de dossier Public sous Windows 7.

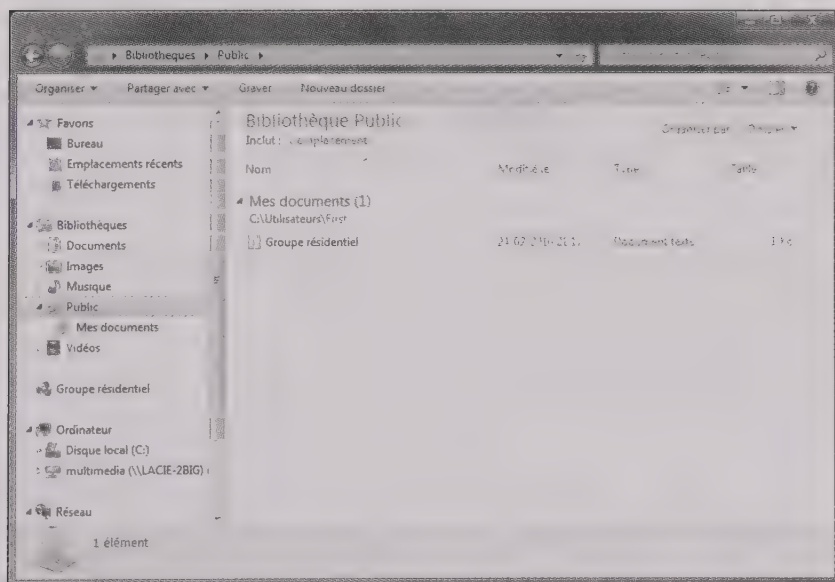


Figure 3.7 : Exemple de dossier Public sous Windows 7.

Comme vous pouvez le voir, le dossier Public comporte plusieurs sous-dossiers prédéfinis, destinés à partager des documents, des images, de la musique, des fichiers téléchargés et des vidéos. Vous pouvez les utiliser ou bien créer vos propres sous-dossiers pour organiser au mieux vos données dans votre dossier Public.



Pour accéder au dossier Public d'un autre ordinateur, utilisez les techniques décrites dans le Chapitre 2 pour parcourir le dossier Public ou le mapper au lecteur réseau.

Partager une imprimante

Partager une imprimante est bien plus traumatisant que de partager un disque. Quand vous partagez un disque, les autres utilisateurs du réseau accèdent à vos fichiers de temps en temps. Quand ils le font, vous entendez le clic-clic du disque pendant quelques instants et votre ordinateur peut se figer une demi-seconde. Les interruptions causées par les autres utilisateurs sont parfois perceptibles mais jamais gênantes.

Quand vous partagez une imprimante, votre collègue de l'étage du dessous peut commander l'impression d'un rapport de 140 pages à l'instant même où vous voulez imprimer cette note d'une page que votre patron veut voir sur son bureau dans deux minutes. L'imprimante peut se retrouver à court de papier ou, pire, être victime d'un bourrage pendant l'impression du travail de quelqu'un d'autre et vous serez chargé de régler ce problème.

Aussi importunes que ces interruptions puissent être, il est parfois très judicieux de partager une imprimante. Si vous disposez de la seule imprimante décente de votre bureau ou groupe de travail, tout le monde va vous ennuyer pour pouvoir l'utiliser. Vous feriez mieux de partager cette imprimante sur le réseau, de sorte que personne ne fasse plus la queue pour imprimer à partir de votre ordinateur.

Partager une imprimante sous Windows XP

Pour partager une imprimante sous Windows XP, procédez comme suit :

- 1. Dans le menu Démarrer, sélectionnez Paramètres et cliquez sur Imprimantes et télécopieurs.**

La boîte de dialogue Imprimantes et télécopieurs s'ouvre, comme le montre la Figure 3.8. Dans cet exemple, la boîte de dialogue affiche six imprimantes.

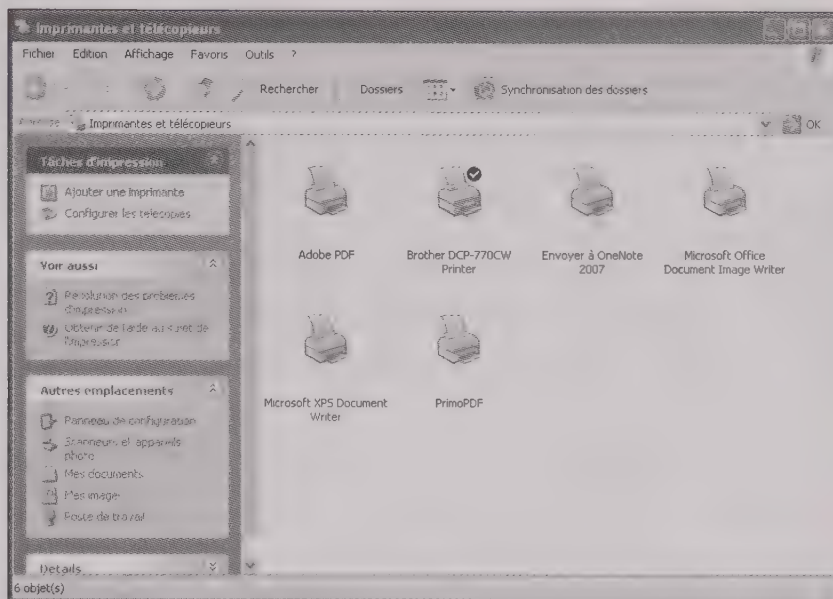


Figure 3.8 : Boîte de dialogue Imprimantes et télécopieurs.

2. Sélectionnez l'imprimante que vous souhaitez partager.

Cliquez sur l'icône de l'imprimante pour la sélectionner.

3. Exécutez la commande Fichier/Partager.

Vous avez raison, ça n'a pas de sens. Vous partagez une imprimante et non un fichier, mais la commande Partager se trouve dans le menu Fichier. Allez savoir pourquoi...

La boîte de dialogue Propriétés s'affiche quand vous exécutez la commande Fichier/Partager.

4. Cochez l'option Partager cette imprimante.

5. Changez le Nom de partage si vous n'aimez pas celui que propose Windows.

Les autres ordinateurs ont recours au Nom de partage pour identifier l'imprimante partagée, aussi convient-il de choisir un nom qui ait un sens.

6. Cliquez sur OK.

Vous retournez dans la boîte de dialogue Imprimantes et télécopieurs. Une main est ajoutée à l'icône de votre imprimante pour montrer que l'imprimante est dorénavant partagée.

Pour désactiver le partage de votre imprimante sur le réseau afin que les autres utilisateurs du réseau n'aient plus la possibilité d'y accéder, reprenez la procédure précédente jusqu'à l'étape 3 pour afficher la boîte de dialogue Propriétés de l'imprimante. Cochez l'option Ne pas partager cette imprimante puis cliquez sur OK. La main disparaît de l'icône de l'imprimante, ce qui indique que l'imprimante n'est plus partagée.

Partager une imprimante sous Windows Vista ou Windows 7

Pour partager une imprimante sous Windows Vista ou Windows 7, exécutez ces étapes :

1. Cliquez sur le bouton Démarrer, tapez Imprimantes et appuyez sur Entrée.

La fenêtre Imprimantes apparaît.

2. Effectuez un clic droit sur l'imprimante à partager et sélectionnez Propriétés.

La boîte de dialogue Propriétés de l'imprimante s'affiche.

3. Ouvrez l'onglet Partage.

Dans l'onglet Partage, représenté dans la Figure 3.9, les options de partage d'imprimante sont grisées.

4. Activez l'option Partager cette imprimante.

5. Modifiez le nom du partage si celui proposé par Windows ne vous convient pas.

Puisque d'autres ordinateurs utiliseront ce nom de partage pour identifier l'imprimante, faites en sorte qu'il soit suffisamment descriptif.

6. Cliquez sur OK.

Vous rebasculez dans la fenêtre Imprimantes. L'icône de l'imprimante a été modifiée pour indiquer qu'elle est à présent partagée.

Pour désactiver le partage de votre imprimante, suivez les étapes 1 à 6 et décochez la case Partager cette imprimante avant de cliquer sur OK.

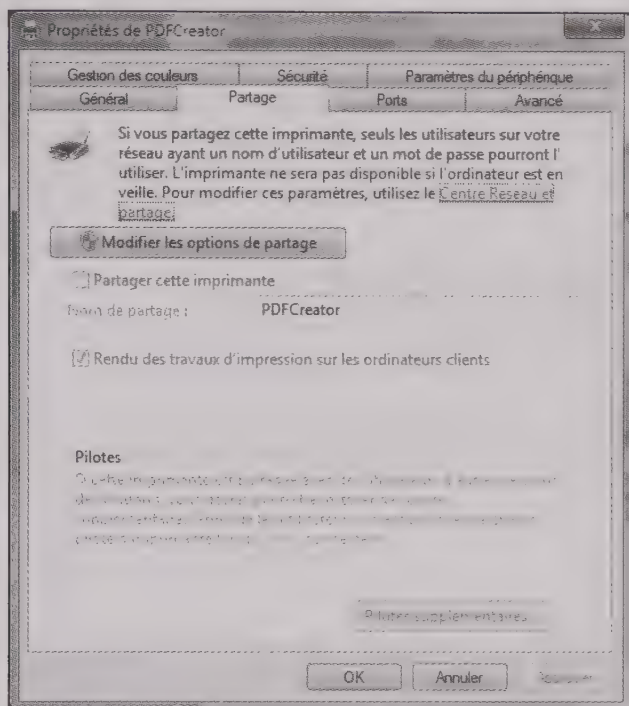


Figure 3.9 : Partage d'une imprimante sous Windows 7.

Utiliser Microsoft Office sur un réseau

Microsoft Office est de loin la plus populaire des suites d'applications utilisées sur les ordinateurs personnels et elle comprend les programmes les plus employés dans un bureau : un programme de traitement de texte (Word), un tableur (Excel), un programme de présentation (PowerPoint) et un excellent programme de messagerie électronique (Outlook). En fonction de la version d'Office achetée, vous aurez aussi droit à un programme de base de données (Access), à un outil de création de formulaires dynamiques (InfoPath), à un programme de développement de sites Internet (FrontPage) et à un programme de PAO (Publisher).

Cette section présente les fonctionnalités réseau de Microsoft Office 2007, la dernière version d'Office. Quelques-unes de ces fonctionnalités s'appliquent aussi aux versions antérieures d'Office.



Pour vous servir au mieux d'Office sur un réseau, je vous conseille d'acheter le Kit de ressources de Microsoft Office. Ce kit (aussi appelé *ORK – Office Resource Kit*) contient des informations relatives à l'installation et à l'utilisation d'Office en réseau et il est livré avec un CD comprenant de précieux outils. Si vous ne voulez pas acheter ORK, vous pouvez l'utiliser en ligne et télécharger les outils ORK sur le site TechNet de Microsoft (technet.microsoft.com).

Installer Office sur un réseau (quelques options)

Avant d'installer Microsoft Office sur un réseau, vous devez prendre quelques décisions élémentaires. En particulier, voici quelques approches possibles quant à l'installation de Microsoft Office sur les ordinateurs clients du réseau :

- ✓ Vous pouvez tout bonnement ignorer le fait que vous disposez d'un réseau et acheter un exemplaire d'Office pour chacun des ordinateurs du réseau. Ensuite, vous pouvez installer Office sur chaque poste à partir du CD. Cette solution est envisageable si :
 - le réseau est de petite taille.
 - chaque ordinateur est doté d'un disque dur de taille suffisante pour héberger Office.
 - chaque ordinateur est équipé d'un lecteur de CD-ROM.
- ✓ Pour un réseau de plus grande envergure, vous pourrez utiliser le programme d'installation d'Office en mode Installation d'administration. Il permet de créer un type d'installation spéciale sur le disque d'un serveur de réseau à partir duquel vous pourrez installer Office sur les ordinateurs du réseau. L'installation d'administration permet de contrôler les fonctionnalités personnalisées sélectionnées pour chacun des ordinateurs du réseau et réduire ainsi les interactions requises lors de l'installation d'Office sur chaque machine.

Si vous optez pour le mode Installation d'administration, vous pouvez vous servir de l'Assistant d'installation réseau livré avec le Kit de ressources d'Office. Cet assistant permet de personnaliser les paramètres d'installation d'Office sur les ordinateurs clients. Par exemple, vous pouvez choisir les composants d'Office à installer, donner des réponses par défaut aux questions oui/non que le programme d'installation pose à l'utilisateur et limiter les interactions entre l'utilisateur et le programme d'installation.





Quelle que soit la solution retenue pour votre réseau, vous devrez acheter soit un exemplaire d'Office, soit une licence pour l'installer sur chacun des ordinateurs. Il est illégal d'acheter un seul exemplaire d'Office et de l'installer sur plusieurs ordinateurs.

Accéder aux fichiers réseau

Ouvrir un fichier stocké sur un disque réseau est presque aussi simple que d'ouvrir un fichier sur un disque local. Tous les programmes Office utilisent la commande Office/Ouvrir pour afficher la boîte de dialogue Ouvrir. La Figure 3.10 montre celle d'Excel (la boîte de dialogue est à peu près identique dans tous les autres programmes d'Office).

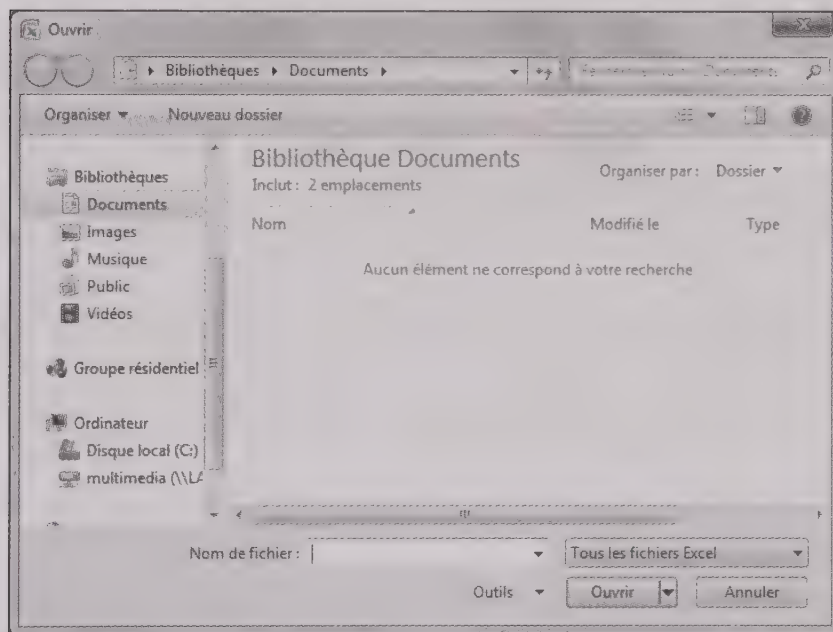


Figure 3.10 : Boîte de dialogue Ouvrir d'Excel 2007.

Pour accéder à un fichier stocké sur un volume réseau mappé à une lettre de lecteur, il suffit de choisir le lecteur réseau dans la liste déroulante en haut de la boîte de dialogue. Si le volume réseau n'a pas été mappé à un lecteur, cliquez sur Favoris réseau, dans l'angle inférieur gauche de la boîte de dialogue Ouvrir, sélectionnez Réseau et parcourez le réseau à la recherche du fichier que vous voulez ouvrir.

Vous pouvez mapper un lecteur réseau directement depuis la boîte de dialogue Ouvrir. Pour ce faire, il suffit de localiser le dossier à mapper, d'effectuer un clic droit et de sélectionner la commande Connecter un lecteur réseau.



Si vous tentez d'ouvrir un fichier déjà ouvert par un autre utilisateur du réseau, Office vous signale que le fichier est utilisé et vous propose de l'ouvrir en lecture seule. Vous pouvez lire et imprimer un fichier ouvert en lecture seule mais Office ne vous autorise pas à modifier cette version du fichier. Pour enregistrer vos modifications dans un nouveau fichier, vous devrez utiliser la commande Enregistrer sous.

Utiliser des modèles de document en réseau

Un *modèle* est un type particulier de document qui contient des informations de mise en forme, du texte standard et d'autres paramètres personnalisés que vous pouvez employer comme base d'un nouveau document.

Quatre programmes Office (Word, Excel, Access et PowerPoint) vous permettent de spécifier un modèle dès que vous créez un nouveau document. En utilisant la commande Office/Nouveau dans Excel, Word ou PowerPoint pour créer un nouveau document, vous voyez apparaître une boîte de dialogue qui permet de choisir un modèle pour ce nouveau document.

Office est livré avec un ensemble de modèles pour les types de documents les plus courants. Ces modèles sont regroupés dans les divers onglets qui apparaissent dans la boîte de dialogue Nouveau.

En plus des modèles livrés avec Office, vous pouvez créer vos propres modèles Word, Excel et PowerPoint. C'est notamment très utile pour homogénéiser l'apparence des documents créés par les utilisateurs de votre réseau. Par exemple, vous pouvez créer un modèle Lettre qui contient le papier à en-tête de votre entreprise ou un modèle Proposition qui affiche le logo de la société.

Office vous permet de stocker les modèles à deux endroits qui dépendent de ce que vous voulez en faire :

- ✓ **Dans le dossier Modèles utilisateur, généralement situé sur le disque local de l'utilisateur.** Si quelqu'un a besoin d'un modèle particulier, c'est là qu'il ira le chercher.
- ✓ **Dans le dossier Modèles groupe de travail, figurant normalement sur un disque réseau partagé.** Cela vous autorise donc à stocker sur un serveur des modèles que vous voulez mettre à disposition de tous les utilisateurs du réseau, tout en permettant à chaque utilisateur de créer ses propres modèles, inaccessibles aux autres.

Lorsque vous vous servez à la fois du dossier Modèles utilisateur et du dossier Modèles groupe de travail, Office mélange les modèles des deux dossiers et les affiche par ordre alphabétique dans la boîte de dialogue Nouveau. Par exemple, supposons que le dossier Modèles utilisateur

contienne des modèles nommés Document vierge et Page Web et que le dossier Modèles groupe de travail comprenne un modèle nommé Lettre société. Alors, les trois modèles apparaîtront dans la boîte de dialogue Nouveau, dans l'ordre suivant : Document vierge, Lettre société et Page Web.

Pour définir l'emplacement des dossiers Modèles utilisateur et Modèles groupe de travail dans Microsoft Word, exécutez les étapes suivantes :

1. Cliquez sur le bouton Office puis sur Options Word.

La boîte de dialogue Options Word apparaît.

2. Ouvrez Options avancées.

Vous accédez aux options avancées.

3. Descendez jusqu'à la section Général et cliquez sur le bouton Emplacement des fichiers.

La boîte de dialogue Dossiers par défaut s'affiche, comme le montre la Figure 3.11.

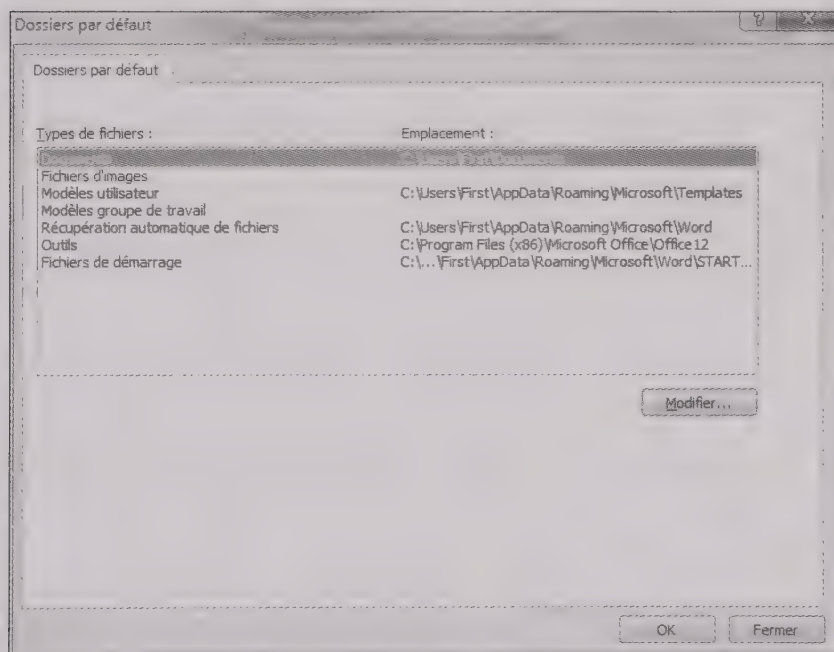


Figure 3.11 : Définition de l'emplacement des fichiers dans Word 2007.

4. Double-cliquez sur Modèles groupe de travail.

Cette étape ouvre la boîte de dialogue Changer de dossier.

5. Spécifiez l'emplacement des fichiers modèles puis cliquez sur OK.

Vous revenez à la boîte de dialogue DoSSIers par défaut.

6. Cliquez sur OK pour fermer la boîte de dialogue.

Vous rebasculez dans la boîte de dialogue Options Word.

7. Cliquez encore une fois sur OK.

La boîte de dialogue Options Word se ferme.



Bien que les paramètres des Modèles utilisateur et Modèles groupe de travail concernent Word, Excel et PowerPoint, vous ne pouvez les modifier que dans Word. Les boîtes de dialogue Options d'Excel et de PowerPoint ne proposent pas ces options.

Lorsque vous installez Office, les modèles standards, fournis avec Office, sont copiés dans un dossier, sur le disque local de l'ordinateur, et l'option Modèles utilisateur concerne ce dossier. L'option Modèles groupe de travail reste vide. Vous pouvez partager le dossier Modèles groupe de travail en cliquant sur Modèles groupe de travail puis sur Modifier et en spécifiant le dossier réseau partagé qui contient vos modèles de document.

Travailler en réseau avec une base de données Access

Si vous voulez partager une base de données Access entre plusieurs utilisateurs du réseau, vous devez être au courant de certaines choses. Voici les plus importantes :

- ✓ Quand vous partagez une base de données, plusieurs utilisateurs peuvent vouloir modifier un enregistrement en même temps. Cette situation peut engendrer des problèmes si deux utilisateurs tentent de mettre à jour l'enregistrement. Pour gérer cela, Access verrouille l'enregistrement si bien que seul un utilisateur peut y accéder à un instant T. Access emploie une des trois méthodes suivantes pour verrouiller des enregistrements :
 - **Enr modifié** qui verrouille l'enregistrement dès qu'un utilisateur commence à le modifier. Par exemple, si un utilisateur récupère un enregistrement via un formulaire qui permet de le mettre à jour, Access verrouille l'enregistrement pendant l'édition, si bien que les autres utilisateurs ne peuvent pas modifier l'enregistrement tant que le premier utilisateur n'a pas terminé.

- **Aucun** qui ne signifie pas réellement que l'enregistrement n'est pas verrouillé. En fait, Aucun signifie que l'enregistrement n'est pas verrouillé tant qu'un utilisateur ne modifie pas le contenu de la base de données. Cette méthode peut induire en erreur les autres utilisateurs car elle permet à un utilisateur d'écraser les modifications apportées par un autre utilisateur.
- **Général** qui verrouille une table entière dès qu'un utilisateur modifie un enregistrement de cette table.
- ✓ Access vous permet de partager une table de sorte que les formulaires, les requêtes et les états soient stockés sur le disque dur de chaque utilisateur mais que les données elles-mêmes demeurent sur le disque réseau. Cette fonctionnalité peut rendre l'accès à une base de données plus rapide sur le réseau mais elle est un peu plus complexe à mettre en œuvre. Pour partager une base de données, exécutez la commande Outils de base de données/Base de données Access/Fractionner la base de données.
- ✓ Access dispose de fonctionnalités de sécurité intégrées à utiliser si vous partagez une base de données d'un ordinateur client Windows de type Windows XP ou Windows Vista. Si vous la stockez sur un serveur de domaine, vous pouvez vous servir des fonctionnalités de sécurité du serveur pour protéger la base de données.
- ✓ Access rafraîchit automatiquement les formulaires et les feuilles de données toutes les soixante secondes. De cette manière, si un utilisateur ouvre le formulaire ou la feuille de données et qu'un autre utilisateur modifie les données quelques secondes plus tard, le premier voit les modifications dans la minute qui suit. Si vous trouvez que soixante secondes est un délai trop long (ou trop court), vous pouvez changer la vitesse de rafraîchissement grâce à la commande Avancé de la boîte de dialogue Options d'Access.

Travailler avec des fichiers hors connexion

Les ordinateurs de bureau sont par nature privés de pieds. Par conséquent, ils sont en permanence connectés à leurs réseaux. Les ordinateurs portables, quant à eux, peuvent se promener d'un endroit à l'autre sans obligation de connexion à un réseau. Si vous avez un réseau sur votre lieu de travail, vous vous y connectez lorsque vous êtes au travail. Mais quand vous vous trouvez à votre domicile avec votre portable, par exemple pour le week-end, vous n'êtes plus connecté à votre réseau.

Naturellement, votre patron préfère que vous passiez vos week-ends à travailler et que vous puissiez accéder de chez vous à vos fichiers réseau sans être connecté au réseau ! C'est là que le mécanisme des fichiers hors

connexion entre en jeu. Il vous permet d'accéder à vos fichiers réseau même si vous êtes déconnecté du réseau.

Tout cela ressemble à de la magie mais il n'en est rien. En fait, comment cela se passerait-il si ce mécanisme n'existait pas ? Il faudrait copier les fichiers sur le disque dur de votre portable à partir du réseau, les modifier en local de retour à votre domicile puis les recopier sur le réseau une fois de retour sur votre lieu de travail.

C'est exactement de cette manière que fonctionne le dispositif de fichiers hors connexion sauf que Windows s'occupe de tout sans aucune intervention de l'utilisateur. Bien que vous soyez déconnecté du réseau, Windows vous donne l'impression d'être réellement sur le réseau. Par exemple, si vous mappez un lecteur réseau (le lecteur M, par exemple) et si vous le rendez disponible hors connexion, vous pouvez encore y accéder lorsque la connexion réseau est coupée. En fait, Windows détecte la déconnexion du réseau et réoriente l'accès au lecteur M vers sa copie sur le disque dur local.

Les complications surgissent lorsque des fichiers hors connexion ont été modifiés par plusieurs utilisateurs. Windows tente bien de remédier à ce désordre mais il lui est quasiment impossible d'y parvenir. La solution consiste à n'utiliser le dispositif de fichiers hors connexion qu'avec des ressources réseau qui sont susceptibles de ne pas être modifiées simultanément par plusieurs utilisateurs. En d'autres termes, rendre votre disque personnel disponible hors connexion ne pose aucun problème quand vous êtes la seule personne à y avoir accès. En revanche, je ne vous conseille pas de le faire pour des ressources partagées à moins qu'il s'agisse de ressources en lecture seule qui ne contiennent pas de fichiers susceptibles d'être modifiés.

Les fichiers hors connexion sont configurés de la manière suivante, en fonction du système d'exploitation :

- ✓ **Sous Windows Vista ou Windows 7**, ouvrez la fenêtre Ordinateur, effectuez un clic droit sur le lecteur réseau auquel vous souhaitez accéder hors connexion et choisissez Toujours disponible hors connexion.
- ✓ **Sous Windows XP**, ouvrez le Poste de travail, effectuez un clic droit sur le lecteur réseau auquel vous souhaitez accéder hors connexion et sélectionnez Rendre disponible hors connexion.

Si vous ne voulez pas rendre disponible l'intégralité du lecteur, vous pouvez désigner différents dossiers en utilisant la même technique : effectuez un clic droit sur le dossier souhaité puis sélectionnez Toujours disponible hors connexion (Windows Vista ou Windows 7) ou Rendre disponible hors connexion (Windows XP).

Lorsque vous rendez un lecteur ou un dossier disponible hors connexion, Windows copie tous les fichiers du lecteur ou du dossier sur le disque local. La durée de ce processus dépend de la taille du lecteur ou du dossier.

Une fois qu'un lecteur a été rendu disponible hors connexion, Windows s'occupe de tout : chaque fois que vous vous connectez ou déconnectez du réseau, Windows synchronise les fichiers hors connexion. Pour ce faire, il compare le couple date et heure de chaque fichier sur le serveur et sur la zone locale et conserve la version la plus récente.

Voici quelques autres remarques au sujet des fichiers hors connexion :

- ✓ Vous pouvez forcer la synchronisation des fichiers hors connexion. Effectuez un clic droit sur le lecteur ou le dossier et exécutez la commande Synchronisation.
- ✓ Assurez-vous que les fichiers du dossier que vous êtes en train de rendre disponible hors connexion sont bien fermés. Si un fichier est ouvert, vous allez recevoir un message d'erreur. Vous devrez alors fermer le fichier ouvert avant de pouvoir rendre le dossier disponible hors connexion.
- ✓ La boîte de dialogue Propriétés des lecteurs réseau mappés comporte un onglet Fichiers hors connexion, comme le montre la Figure 3.12.

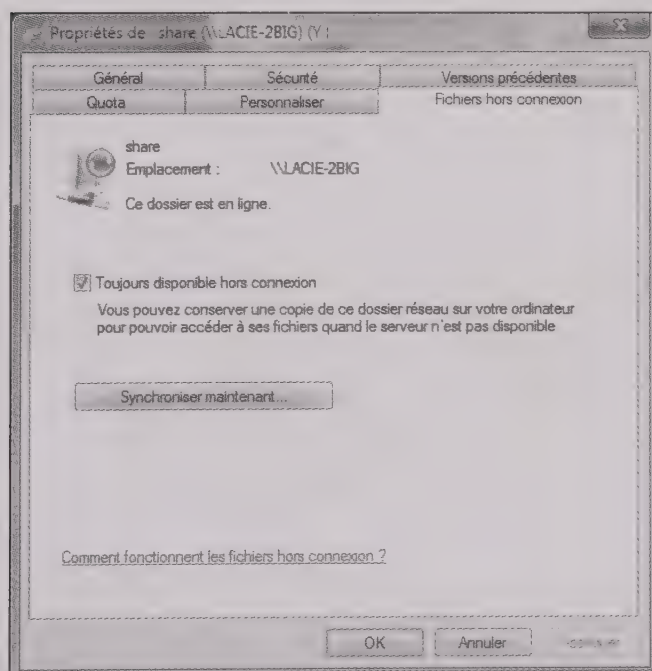


Figure 3.12 : Propriétés de l'onglet Fichiers hors connexion.

Deuxième partie

Construire son propre réseau



Dans cette partie...

Vous allez apprendre à mettre en œuvre votre propre réseau, c'est-à-dire à le concevoir puis l'installer. Vous découvrirez les différents types de câbles, de systèmes d'exploitation réseau disponibles ainsi que tous les autres éléments avec lesquels vous aurez à vous battre.

Eh oui, ces chapitres contiennent quelques notions techniques. Mais ne craignez rien ! Je vous apporte une bonne nouvelle : un réseau opérationnel est à portée de main et vous, oui, même vous, pouvez le concevoir et l'installer tout seul.

Chapitre 4

Concevoir son réseau

Dans ce chapitre :

- ▶ Concevoir un réseau.
- ▶ Travailler avec un objectif.
- ▶ Inventorier son stock informatique.
- ▶ Vérifier l'utilité d'un réseau.
- ▶ Comparer différents types de serveurs.
- ▶ Choisir son système d'exploitation serveur.
- ▶ Planifier l'infrastructure et dessiner les plans.
- ▶ Observer un exemple de réseau.

Bien, vous êtes convaincu que vous devez mettre vos ordinateurs en réseau. Et maintenant ? Allez-vous faire un saut à la boutique d'informatique en allant au travail, installer le réseau avant le café du matin et vous attendre à ce qu'il soit opérationnel vers midi ?

Je ne pense pas !

Mettre en réseau vos ordinateurs n'est pas une tâche comme les autres : il faut un peu de méthode. Ce chapitre vous aide à réfléchir sur votre réseau avant que vous ne commenciez à dépenser de l'argent. Il vous explique comment produire une spécification qui sera tout aussi valable que celle qu'un consultant réseau vous aurait facturée 1 000 euros.

Vous voyez ; ce livre vous fait déjà économiser de l'argent !

Concevoir un réseau

Avant de commencer ce projet de réseau, qu'il s'agisse d'une nouvelle installation ou d'une mise à niveau d'un réseau existant, commencez par établir un plan détaillé. Si vous prenez des décisions techniques trop rapidement, avant d'étudier toutes les conséquences qui risquent d'affecter le projet, vous le regretterez ! Vous découvrirez trop tard qu'une application majeure ne tourne pas en réseau ou bien que ses performances en réseau sont extrêmement dégradées ou encore que les éléments clés du réseau ne fonctionnent pas ensemble.

Voici quelques règles générales à garder à l'esprit pour vous aider à concevoir votre réseau :

- ✓ **Ne bâclez pas la phase de conception.** Les erreurs les plus coûteuses sont celles que vous faites avant d'installer le réseau. Accordez-vous le temps de la réflexion et imaginez plusieurs solutions.
- ✓ **Mettez par écrit la spécification de votre réseau.** Elle n'a pas besoin de faire 500 pages. Si vous voulez qu'elle ait l'air professionnel, reliez-la avec une spirale de 2 cm de diamètre. La spirale sera bien assez grosse pour contenir toute votre spécification.
- ✓ **Avant d'acheter quoi que ce soit, demandez conseil.** Demandez, de préférence à quelqu'un qui connaît mieux l'informatique que vous, de lire votre spécification.
- ✓ **Actualisez la spécification.** Si un ordinateur vient s'ajouter au réseau, revoyez sa conception, dépoussiérez-la et procédez à la mise à jour.



Le schéma d'un réseau n'est pas gravé dans le marbre. Si quelque chose ne fonctionne pas comme prévu, vous pourrez toujours le corriger en fonction des circonstances.

Être rationnel

Quand vous préparez une mise en réseau, vous devez avant tout vous demander à quelles fins vous en avez besoin. Voici quelques-unes des raisons (toutes bonnes) qui justifient la création d'un réseau :

- ✓ Mes collègues et moi échangeons quotidiennement des données enregistrées sur des clés USB. Un réseau nous éviterait de les utiliser.



- ✓ Je n'ai pas l'intention d'acheter une imprimante laser à chacun alors que, la plupart du temps, la seule que nous ayons est sous-utilisée. Une mise en réseau permettra de la mettre à disposition de tout le monde.
- ✓ Je veux fournir un accès Internet à tous mes ordinateurs. C'est l'unique raison d'être de beaucoup de réseaux, notamment les plus petits.
- ✓ Quelqu'un m'a fait remarquer que, dans mon entreprise, l'impression des notes et rapports correspondait à la destruction de sept arbres par jour. Installer une messagerie électronique permettra de préserver les forêts.
À vrai dire ça ne servira à rien, car, selon l'une des dures lois de la bureautique, plus vous essayez de ne plus recourir au papier, plus vous finissez par en utiliser.
- ✓ Les affaires vont si bien qu'une seule personne n'arrive plus à suivre les commandes. Avec un réseau, chacun entrera les commandes lui-même et je ne serai plus obligé de payer quelqu'un pour faire ce travail.
- ✓ Mon beau-frère vient de créer un réseau dans son bureau et je ne veux pas passer pour un ringard.

Vérifiez bien que vous avez identifié les motifs qui vous poussent à envisager l'installation d'un réseau et écrivez-les noir sur blanc. Ne vous souciez pas d'obtenir le prix Goncourt pour votre prose. Inscrivez simplement ce que vous attendez de votre réseau.

Si vous rédigez une proposition de 500 pages, vous devriez placer les raisons pour lesquelles un réseau est nécessaire dans la section « Justification ».



Tandis que vous identifiez les raisons susceptibles de vous pousser à installer un réseau, vous pouvez très bien en arriver à la conclusion que vous n'avez pas besoin de réseau. Rien de grave. Vous pouvez toujours employer le carnet à spirales pour votre collection de timbres.

Faire l'inventaire

L'une des phases les plus délicates de la spécification d'un réseau est de trouver le moyen de faire fonctionner ensemble les ordinateurs dont vous disposez déjà. Autrement dit, comment aller de A à Z ? Avant de parvenir à Z, vous devez savoir ce que vous possédez en A. En d'autres termes, vous devez faire un inventaire détaillé de votre matériel informatique.

Ce que vous devez savoir

Vous devez disposer des informations suivantes sur chacun de vos ordinateurs :

- ✓ **Le type de processeur et, si possible, sa fréquence d'horloge.** L'idéal serait que tous vos ordinateurs soient au moins des Pentium IV cadencés à 3 ou 4 GHz. Mais, dans la plupart des cas, vous trouverez un mélange d'ordinateurs : des neufs, des vieux, des prêtés. Vous pourriez même trouver quelques reliques appartenant à l'ère du pré-Pentium.

Vous ne pouvez généralement pas deviner le type du processeur d'un ordinateur en observant la tour. Cependant, la plupart des ordinateurs affichent le type du processeur quand vous les allumez ou les redémarrez. Si cette information apparaît trop brièvement à l'écran pour que vous puissiez la lire, appuyez sur la touche Arrêt défil afin de suspendre l'affichage. Lorsque vous avez fini de lire l'information, appuyez de nouveau sur la touche Arrêt défil pour que votre ordinateur continue son initialisation.

- ✓ **La capacité du disque dur et la configuration de ses partitions.** Sur un ordinateur fonctionnant sous Windows, vous pouvez obtenir la taille du disque dur en ouvrant la fenêtre Ordinateur, en effectuant un clic droit sur l'icône d'un lecteur et en exécutant la commande Propriétés du menu contextuel. La Figure 4.1 représente la boîte de dialogue Propriétés d'un disque de 15,8 Go disposant de 8,94 Go d'espace libre.

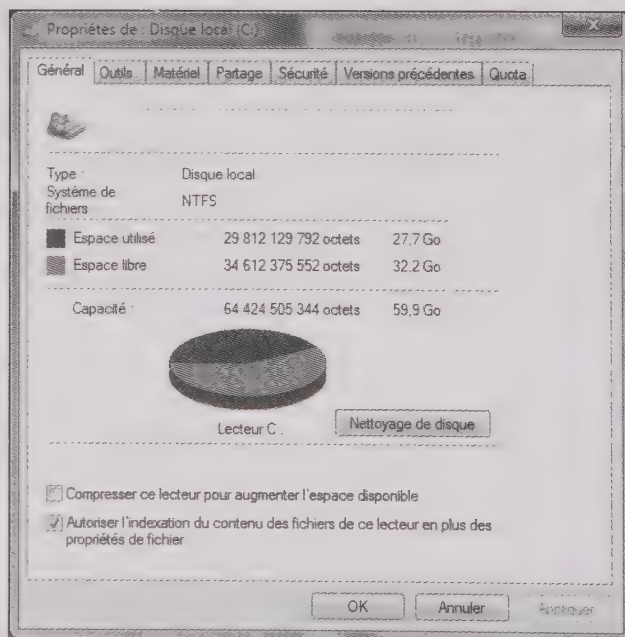


Figure 4.1 : La boîte de dialogue Propriétés d'un disque indique sa capacité totale et la quantité d'espace disponible.

Si votre ordinateur dispose de plusieurs disques durs, Windows affiche une icône pour chacun d'eux ou pour les partitions dans la fenêtre Ordinateur. Prenez note de la capacité totale et de l'espace disponible sur chaque disque dur. Une *partition* est une partie du disque dur considérée comme un lecteur à part. Nous n'y reviendrons plus.

- ✓ **La quantité de mémoire.** Sous Windows, vous pouvez obtenir cette information facilement : effectuez un clic droit sur Ordinateur et exécutez la commande Propriétés. La quantité de mémoire dont dispose votre ordinateur est affichée dans la boîte de dialogue qui apparaît. Par exemple, la Figure 4.2 présente la boîte de dialogue Système d'un ordinateur sous Windows 7 avec 2 Go de RAM.

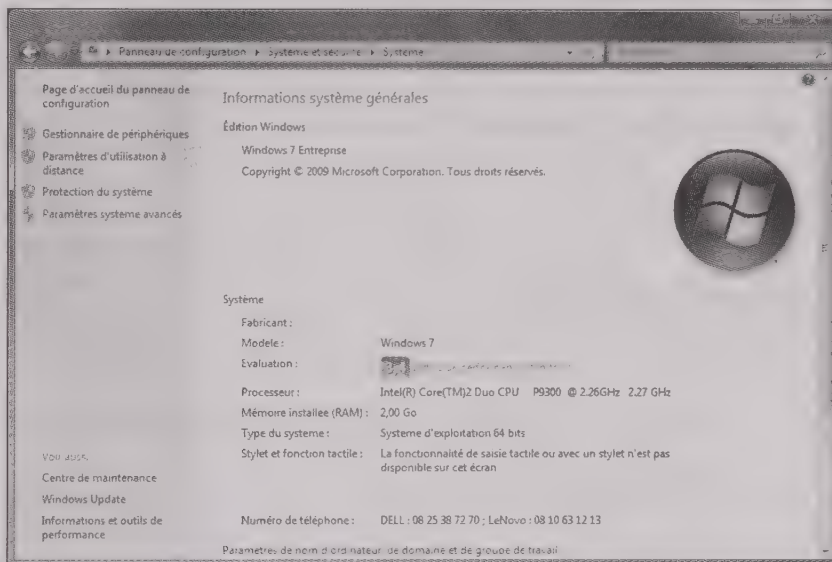


Figure 4.2 : Fenêtre Système d'un ordinateur sous Windows 7 avec 2 Go de RAM.

- ✓ **La version du système d'exploitation.** Elle figure dans la boîte de dialogue Système. En guise d'exemple, la Figure 4.2 représente la fenêtre Système d'un ordinateur équipé de Windows 7 Edition Intégrale. Il est important que tous les ordinateurs du réseau disposent de la dernière mise à jour du service pack.
- ✓ **Le type de carte réseau installée.** Pour trouver le modèle exact, ouvrez le menu Démarrer, effectuez un clic droit sur Ordinateur, sélectionnez Propriétés puis Gestionnaire de périphériques. La boîte de dialogue Gestionnaire de périphériques s'ouvre et affiche le nom de la carte réseau de l'ordinateur.

Le Gestionnaire de périphériques est aussi commode pour découvrir les autres périphériques installés dans l'ordinateur ou pour vérifier quels pilotes sont utilisés par tel ou tel matériel.



- ✓ **Les protocoles réseau utilisés.** Pour déterminer cette information sous Windows XP, ouvrez le Panneau de configuration, double-cliquez sur l'icône Connexions réseau pour ouvrir la boîte de dialogue Connexions réseau, effectuez un clic droit sur la connexion réseau et exécutez la commande Propriétés. Sous Windows Vista ou Windows 7, cliquez sur le bouton Démarrer, tapez « Connexions réseau », effectuez un clic droit sur Connexion au réseau local et sélectionnez Propriétés.
- ✓ **Le type d'imprimante connectée à l'ordinateur, s'il y en a une.** Généralement, il suffit de jeter un œil à l'imprimante. Vous pouvez également obtenir cette information dans la fenêtre Imprimantes.
- ✓ **Les autres périphériques connectés à l'ordinateur.** Un lecteur de CD, DVD ou CD-RW ? Un scanner ? Un lecteur Zip ou Jaz ? Un lecteur de bandes ? Un caméscope ? Un androïde ? Un bain à remous ?
- ✓ **Les pilotes et les disques d'installation sont-ils disponibles ?** J'espère que vous savez où sont rangés les CD nécessaires pour faire fonctionner des périphériques comme la carte réseau, les imprimantes, les scanners, etc. Dans le cas contraire, vous devriez les trouver sur Internet.
- ✓ **Les logiciels installés sur l'ordinateur.** Microsoft Office ? AutoCAD ? Paint Shop Pro ? Dressez-en la liste complète, sans oublier les numéros de version.

Les programmes qui rassemblent les informations

C'est un long travail que de rassembler des informations sur vos ordinateurs quand ils sont nombreux. Heureusement, il existe plusieurs logiciels qui ont la faculté de rassembler automatiquement les informations à votre place. Ces programmes inspectent l'ordinateur sous tous les angles, déterminant le type et la fréquence du processeur, la quantité de RAM et la capacité des disques. Ils affichent ensuite ces informations à l'écran et vous permettent de les sauvegarder dans un fichier ou de les imprimer.

Windows est livré avec un programme de ce type nommé Informations système Microsoft. Ce programme rassemble et affiche des informations sur votre ordinateur. Pour le lancer, sélectionnez Démarrer/Tous les programmes/Accessoires/Outils système/Informations système.

Quand vous exécutez Informations système Microsoft, vous voyez apparaître une fenêtre Informations système, comme le montre la Figure 4.3. Elle n'affiche initialement que des informations élémentaires sur votre ordinateur telles que la version de Windows que vous utilisez, le type de processeur, la quantité de mémoire et la quantité d'espace libre sur chacun des disques

de l'ordinateur. Pour obtenir des informations plus détaillées, cliquez sur Ressources matérielles, Composants ou Environnement logiciel sur le côté gauche de la fenêtre.

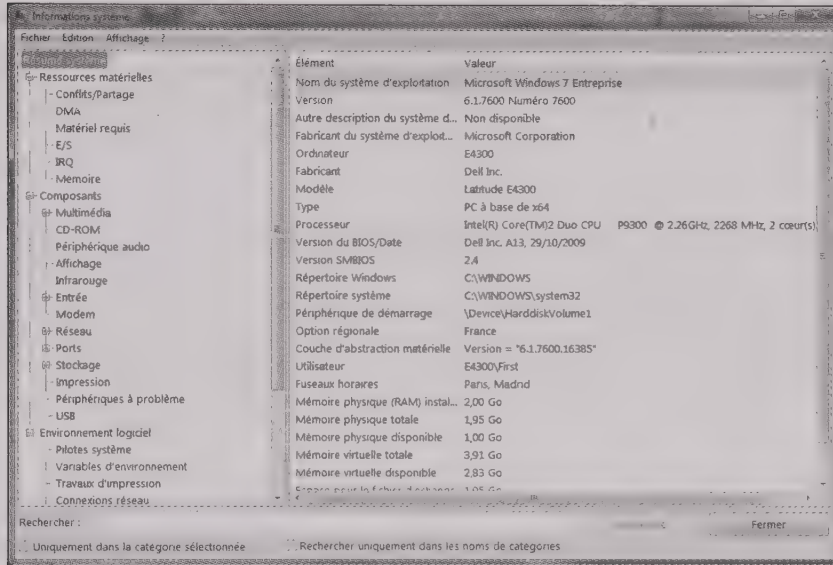


Figure 4.3 : Affichage des informations système.

Avez-vous besoin d'un serveur dédié ?

Une des questions les plus fondamentales que vous devez vous poser est : « Le réseau aura-t-il un ou plusieurs serveurs dédiés, s'appuiera-t-il sur un réseau pair-à-pair, le serveur sera-t-il dédié ? » Si votre réseau ne sert qu'à partager une imprimante et à échanger un fichier de temps en temps, vous n'avez peut-être pas besoin d'un serveur dédié. Un simple réseau pair-à-pair reliant vos ordinateurs fera l'affaire. Cependant, disposer d'un serveur dédié est un avantage indéniable, à part peut-être pour les tout petits réseaux.

Voici quelques points à considérer :

- ✓ **Utiliser un serveur dédié permet de rendre le réseau plus rapide, le travail plus facile et le système plus fiable.** Imaginez ce qui se passe quand l'utilisateur d'un ordinateur serveur, doublé du rôle de station de travail, décide d'éteindre son ordinateur, sans réaliser que quelqu'un est en train d'accéder à des fichiers sur ses disques.

- ✓ Vous ne devez pas obligatoirement utiliser votre ordinateur le plus puissant et le plus rapide comme serveur. J'ai vu des réseaux où l'ordinateur le plus lent tenait le rôle de serveur. C'est particulièrement vrai quand le serveur est principalement utilisé pour partager une imprimante. Par conséquent, si vous devez acheter un ordinateur pour votre réseau, pensez à transformer en serveur une de vos anciennes machines et placez votre nouvel ordinateur en tant que client.

Différents types de serveurs

Partant du principe que votre réseau nécessitera un ou plusieurs serveurs dédiés, vous devrez déterminer le type de serveur(s) que vous devrez installer. Dans certains cas, un seul serveur pourra tenir un ou plusieurs de ces rôles. Chaque fois que c'est possible, il est recommandé de limiter chaque ordinateur serveur à une seule fonction de serveur.

Serveurs de fichiers

Les *serveurs de fichiers* fournissent un espace de stockage centralisé, commodément partagé par tous les ordinateurs du réseau. Leur tâche essentielle est le stockage des fichiers et des programmes. Par exemple, tous les membres d'un petit groupe de travail utiliseront l'espace de stockage du serveur de fichiers pour y placer leurs documents Microsoft Office.

Les serveurs de fichiers doivent s'assurer que deux utilisateurs n'essaient pas de mettre à jour le même fichier en même temps. Pour ce faire, les serveurs de fichiers *verrouillent* le fichier qui vient d'être ouvert et ne permettent qu'au premier utilisateur qui l'a ouvert de le modifier. Pendant ce laps de temps, toute autre personne qui y accède ne peut que le faire en mode lecture seule. Pour des documents (par exemple, traitement de texte ou fichiers tableur), le fichier entier est verrouillé. Pour des bases de données, le verrouillage peut être appliqué seulement à l'enregistrement en cours de modification.

Serveurs d'impression

Le partage d'imprimantes est l'une des principales raisons d'être des petits réseaux. Bien que cela ne soit pas une obligation, vous pouvez faire d'un ordinateur un *serveur d'impression* qui aura pour seule tâche de collecter les données transmises par les ordinateurs clients et les imprimer dans un ordre préétabli.

- ✓ Un seul ordinateur peut à la fois faire office de serveur de fichiers et de serveur d'impression mais les performances seront meilleures si un ordinateur est réservé à chacune de ces tâches.
- ✓ Étant donné que l'on trouve des imprimantes à moins de 60 euros, il peut être tentant d'en installer une directement sur chaque ordinateur. Mais la qualité ne sera pas au rendez-vous ! Plutôt que d'acheter plusieurs imprimantes bas de gamme, il est préférable d'investir dans une bonne imprimante laser et de la partager.

Serveurs Web

Un *serveur Web* est un ordinateur équipé de logiciels lui permettant d'héberger un site Web. Les plus connus sont IIS (*Internet Information Services*), de Microsoft et Apache, un programme serveur Web open source géré par Apache Software Foundation.

Serveurs de messagerie

Un *serveur de messagerie* prend en charge la messagerie du réseau. Il est équipé de logiciels spécialisés comme Microsoft Exchange Server. Il doit être compatible avec le logiciel de messagerie. C'est le cas d'Exchange Server, conçu pour fonctionner avec Outlook, la messagerie client fournie avec Office.

Serveurs de bases de données

Un *serveur de bases de données* est un ordinateur équipé d'un système de gestion de bases de données comme Microsoft SQL Server 2005. Les serveurs de base de données sont généralement utilisés conjointement avec des applications d'entreprise (systèmes comptable, marketing...).

Choisir un système d'exploitation serveur

Après avoir déterminé la nécessité, pour le réseau, de recourir à un ou plusieurs serveurs dédiés, il vous faudra maintenant définir le type de système d'exploitation que ces serveurs utiliseront. Il est préférable que ce soit le même pour tous, si vous tenez à éviter les conflits qui peuvent surgir entre différents systèmes d'exploitation.

Bien que vous puissiez choisir l'un ou l'autre des nombreux systèmes d'exploitation, d'un point de vue pratique, vous vous en tiendrez à ceux-ci :

- ✓ Windows Server 2008.
- ✓ Novell NetWare.
- ✓ Linux ou une autre version d'UNIX.

Pour plus d'informations, reportez-vous au Chapitre 7.

Planifier l'infrastructure

Il vous faudra aussi planifier en détail la manière dont les ordinateurs seront reliés entre eux. Cela consiste notamment à déterminer la topologie de réseau à adopter, les types de câbles à utiliser, comment ils seront routés et aussi les besoins matériels (commutateurs, routeurs...).

Bien que vous ayez le choix entre plusieurs options de câblage, vous choisirez sans doute le câble Cat5 (catégorie 5) ou mieux UTP, pour la liaison de la plupart des ordinateurs au réseau – voire de tous. Outre ces décisions élémentaires, vous devrez en prendre beaucoup d'autres :

- ✓ Où placerez-vous les commutateurs : sur le bureau entre les ordinateurs ou dans une armoire de câblage centrale ?
- ✓ Combien d'ordinateurs clients relierez-vous à chaque commutateur et de combien de commutateurs aurez-vous besoin ?
- ✓ Si vous avez besoin de plusieurs commutateurs, par quel type de câble les relierez-vous ?

Reportez-vous au Chapitre 5 pour en savoir plus sur les câbles de mise en réseau.



Si vous installez un nouveau câble de réseau dans un local, ne lésinez pas sur la qualité. Le coût du câble lui-même ne représente qu'une petite partie de tout le travail qu'exige son installation. En optant maintenant pour un câble de bonne qualité, vous n'aurez pas à le remplacer dans quelques années, lorsque le réseau devra être rénové.

Dessiner les plans

Tracer le schéma du réseau est très utile. Il peut s'agir d'un plan de l'étage indiquant l'emplacement de chaque élément du réseau. Ce schéma est parfois appelé *plan physique* mais si vous le préférez, cela peut aussi être un *plan logique*, plus abstrait, qui ressemblerait à un tableau de Picasso, sans les couleurs. Actualisez-le dès que la configuration du réseau change. Précisez la nature des changements (date, raison de la modification...).

Un petit réseau peut être schématisé sur un feuillet de bloc-notes mais si le réseau est plus vaste, un logiciel de tracé de diagrammes vous aidera. L'un des meilleurs est Microsoft Visio, illustré dans la Figure 4.4.



Figure 4.4 : Utilisation de Visio pour créer un diagramme réseau.

Voici quelques-uns des avantages de ce logiciel :

- ✓ Les formes automatiques et les connecteurs qui les relient peuvent être déplacés sans que les connexions soient rompues.
- ✓ Les gabarits contiennent des douzaines de formes pour représenter les composants d'un réseau : pas seulement des serveurs et des clients mais aussi des routeurs, des concentrateurs, des commutateurs, bref tout ce dont vous avez besoin. Si vous avez des exigences particulières, il est même possible d'acheter des jeux de gabarits pour des équipements particuliers comme les routeurs Cisco ou des ordinateurs mainframes IBM.

- ✓ La possibilité d'ajouter des informations (numéro de série, emplacement physique...) à chaque ordinateur ou périphérique du diagramme. Vous pouvez aussi imprimer un inventaire qui regroupe toutes les informations de chaque élément du diagramme.
- ✓ La création de vastes schémas s'étendant sur plusieurs pages.

Quelques exemples de plans

Dans la suite de ce chapitre, vous trouverez quelques exemples de plans de réseaux réels. Ils illustrent plusieurs des notions abordées jusqu'à présent. Les situations sont réelles mais les noms ont été changés afin de ne pas compromettre des innocents.

Créer un petit réseau : California Sport Surface

California Sport Surface (CSS) est une petite société spécialisée dans la réalisation d'installations sportives en extérieur comme des cours de tennis, des stades de football et des pistes de course. L'équipe administrative de CSS ne compte que quatre personnes. La société possède trois ordinateurs :

- ✓ Un nouvel ordinateur de bureau Dell équipé de Windows 7 Edition Familiale Premium. Il est utilisé par le président (Mark) et le vice-président (Julie) qui s'en servent pour préparer des devis, créer des brochures de publicité, gérer la correspondance et d'autres tâches. L'ordinateur est équipé d'un port réseau Ethernet 10/100/1000 Mbps.
- ✓ Un ordinateur Dell plus ancien qui tourne sous Windows XP Edition Familiale, utilisé par le comptable (Erin). Il se sert du logiciel de comptabilité QuickBooks. Cet ordinateur possède aussi un port réseau intégré mais il s'agit d'un port 10/100 qui ne prend pas en charge le gigabit.
- ✓ Un ordinateur portable sous Windows Vista Edition Intégrale, utilisé par le technicien (Daniel) qui l'emporte souvent pour travailler sur les chantiers. Cet ordinateur est équipé d'un port Ethernet 10/100/1000 Mbps.

La société ne possède qu'une seule imprimante à jet d'encre, peu onéreuse, reliée à l'ordinateur d'Erin. Les ordinateurs ne sont pas en réseau. C'est pourquoi, dès que Mark, Julie ou Daniel veulent imprimer un document, ils copient le fichier sur une clé USB qu'ils remettent à Erin. L'ordinateur que se partagent Mark et Julie est connecté à Internet par une connexion DSL.

La société désire mettre ces trois ordinateurs en réseau pour :

- ✓ Partager l'imprimante afin de ne plus avoir à utiliser de clés USB pour transférer les documents.
- ✓ Partager l'accès à Internet afin que chacun puisse accéder au Web à partir de n'importe quel ordinateur.
- ✓ Permettre l'intégration d'un autre ordinateur de bureau que la société envisage d'acquérir d'ici à six mois mais aussi d'un autre ordinateur portable (si les affaires vont bien, CSS compte embaucher un autre technicien).
- ✓ Le réseau doit être intuitif et ne pas exiger trop de maintenance.

Les besoins de mise en réseau de CSS peuvent être satisfaits par un réseau pair-à-pair simple, semblable à celui représenté par la Figure 4.5.

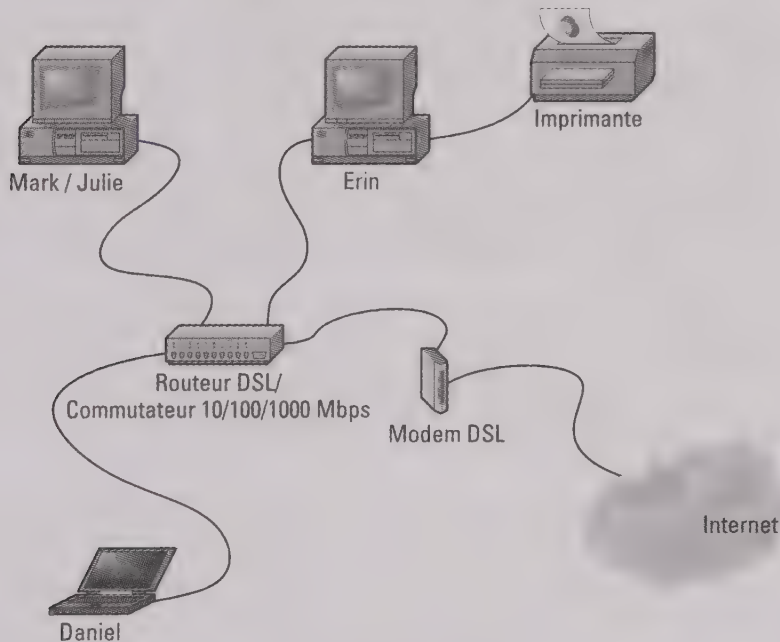


Figure 4.5 : Réseau pair-à-pair de California Sport Surface.

Ce réseau requiert les éléments suivants :

- ✓ Une carte réseau gigabit pour l'ordinateur sous Windows XP, le seul ordinateur qui ne prend pas en charge le gigabit. Une meilleure solution serait de remplacer cet ordinateur par une machine plus récente qui tourne sous Windows 7 et qui possède un port Ethernet intégré.

- ✓ Un ensemble routeur DSL et commutateur à quatre ports 10/100/1000 Mbps. La société devra peut-être étendre les capacités de ce périphérique lorsqu'elle utilisera un ordinateur portable supplémentaire, mais, le moment venu, il sera possible d'ajouter un autre commutateur à 4 ou 8 ports.
- ✓ Il faudra activer la fonction de pare-feu du routeur DSL afin de protéger le réseau des pirates qui écument Internet.
- ✓ Le partage de fichiers et d'imprimante sera activé sur l'ordinateur d'Erin.

Connecter deux réseaux : Creative Course Development

Creative Course Development (CCD) est un petit éditeur d'ouvrages éducatifs situé en Californie. Il est spécialisé dans les ouvrages de mathématiques et de sciences pour les classes primaires et secondaires. La production est variée : livres scolaires, livres de jeux et logiciels sur CD-ROM.

CCD loue deux immeubles de bureau contigus, séparés par une petite cour. L'équipe rédactionnelle, composée d'une douzaine d'auteurs et d'éducateurs, travaille dans l'immeuble A. Les équipes des ventes, du marketing et de l'administration, soit six personnes, se trouvent dans l'immeuble B.

L'équipe de développement de produits et de marketing possède quatorze ordinateurs relativement récents, qui tournent sous Windows Vista Professionnel, et un serveur sous Windows 2003 Server. Toutes ces machines sont reliées par du réseau UTP basé sur un commutateur à 24 ports 100 Mbps. L'accès Internet est fourni par une ligne T1 fractionnelle reliée à un petit routeur Cisco.

L'équipe administrative dispose d'ordinateurs disparates, certains exécutés sous Windows Vista, d'autres sous Windows XP, et même d'un ordinateur sous Windows 98. Un petit serveur sous Windows 2000 Server répond à leurs besoins. Les ordinateurs les plus anciens sont équipés de cartes réseau 10BaseT, les plus récents de cartes 10/100 Mbps. Tous ces ordinateurs sont reliés à un concentrateur Ethernet 10 Mbps assez ancien, à 12 ports. Le débit sur le réseau est donc limité à 10 Mbps. L'accès Internet est assuré par une connexion DSL.

Les deux groupes sont satisfaits de leurs ordinateurs et de leur réseau. Le problème est que les réseaux ne peuvent pas communiquer. Par exemple, l'équipe du marketing de l'immeuble A travaille sur les rapports imprimés fournis par l'équipe des ventes de l'immeuble B, d'où des allers et venues fréquents entre les deux bâtiments lorsqu'il faut suivre une affaire de près.

Bien qu'il existe plusieurs solutions à ce problème, la plus simple consiste à relier les réseaux par un pont à l'aide d'une paire de commutateurs sans fil. À cette fin, CCD achètera deux points d'accès sans fil. L'un sera branché au commutateur de l'immeuble A, l'autre au commutateur situé dans l'immeuble B. Ces points d'accès configurés, les deux réseaux n'en formeront plus qu'un seul. La Figure 4.6 propose un schéma logique du réseau final.

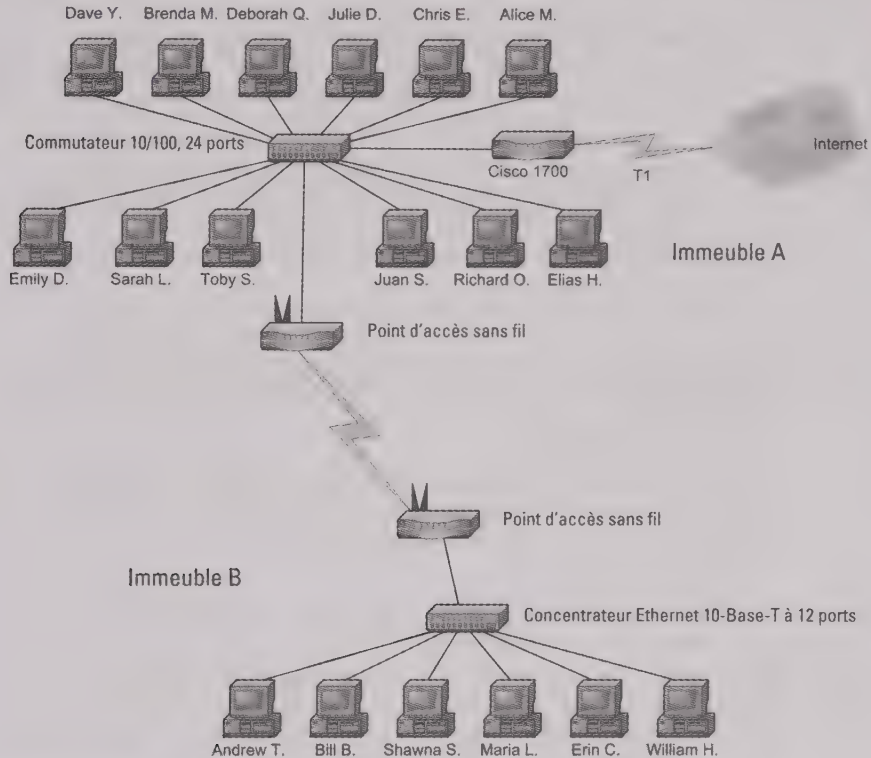


Figure 4.6 : Solution de réseau sans fil pour Creative Course Development.

Bien que la solution sans fil semble simple, quelques complications sont à redouter, notamment :

- ✓ Si l'environnement est défavorable, les points d'accès sans fil peuvent avoir du mal à établir la connexion entre les immeubles. Il faudra peut-être placer les appareils sur le toit. Dans ce cas, CCD devra déboursier un peu plus pour protéger le matériel des intempéries.
- ✓ Comme le point d'accès sans fil de l'immeuble A sera connecté à un commutateur au lieu d'un concentrateur, le commutateur isolera quelque peu les deux réseaux. Mais les performances du réseau final ne devraient pas être affectées.

- ✓ Avant que les réseaux soient connectés, chacun possédait son propre serveur DHCP qui assignait les adresses IP aux utilisateurs. Malheureusement, chacun de ces serveurs DHCP a la même adresse IP locale (192.168.0.1). Lors de la fusion des réseaux, un de ces serveurs DHCP devra être désactivé.
- ✓ De plus, les deux réseaux ont chacun leur propre connexion Internet. Les deux réseaux étant pontés, la société CCD peut à présent se passer de la connexion DSL. Dans les deux immeubles, les utilisateurs peuvent accéder à Internet via la connexion T1 partagée.
- ✓ L'administrateur du réseau devra également déterminer comment gérer les services du réseau. Précédemment, chaque réseau possédait son propre domaine. Après le pontage, la société CCD peut opter pour le maintien de la séparation des domaines ou leur fusion en un seul (cette solution exigeant beaucoup de travail, elle optera probablement pour le maintien de la séparation).

Augmenter les performances du réseau : DCH Compta

DCH Compta est un cabinet d'experts-comptables qui est passé en quelques années de quinze à trente-cinq employés, travaillant tous dans un même immeuble. Voici un bref descriptif de leur réseau :

- ✓ Il est constitué de trente-cinq ordinateurs clients et de trois serveurs exécutés sous Windows 2000 Server.
- ✓ Les trente-cinq ordinateurs clients sont exécutés sous Windows XP Professionnel.
- ✓ Les ordinateurs clients sont équipés de cartes Ethernet 10/100 Mbps. Certains possèdent des cartes 10/100/1000 Mbps.
- ✓ Les serveurs sont équipés de cartes 10/100 Mbps.
- ✓ Tous les bureaux de l'immeuble sont reliés à une armoire de câblage par du câble de catégorie 5. À cet endroit, se trouve un rack comportant deux commutateurs 10/100 Mbps à 24 ports.
- ✓ L'accès Internet est fourni par une connexion T1 et un routeur Cisco 1700.

Ces derniers temps, les performances du réseau étaient nettement insuffisantes, notamment au niveau de l'accès Internet et des transferts de gros fichiers entre les ordinateurs clients et les serveurs. Les utilisateurs avaient commencé à se plaindre des lenteurs du système.

Le problème est double :

- ✓ Les commutateurs 100 Mbps sont trop anciens pour supporter le réseau. Tout le trafic du réseau transite par eux et le débit est limité à 100 Mbps. De ce fait, les nouveaux ordinateurs équipés de ports réseau gigabit sont connectés au réseau à 100 Mbps et non à 1000 Mbps.
- ✓ Le réseau est devenu trop grand pour les capacités du serveur Windows 2000 Server. Les serveurs eux-mêmes sont vieux et le système d'exploitation est obsolète.

Les performances de ce réseau peuvent être considérablement améliorées en deux étapes :

1. Améliorer l'infrastructure réseau.

Remplacer les vieux commutateurs par trois commutateurs 24 ports 10/100/1000 Mbps.

2. Remplacer les vieux serveurs par des serveurs plus rapides exécutés sous Windows Server 2008.

Le réseau est restructuré, comme le montre la Figure 4.7.

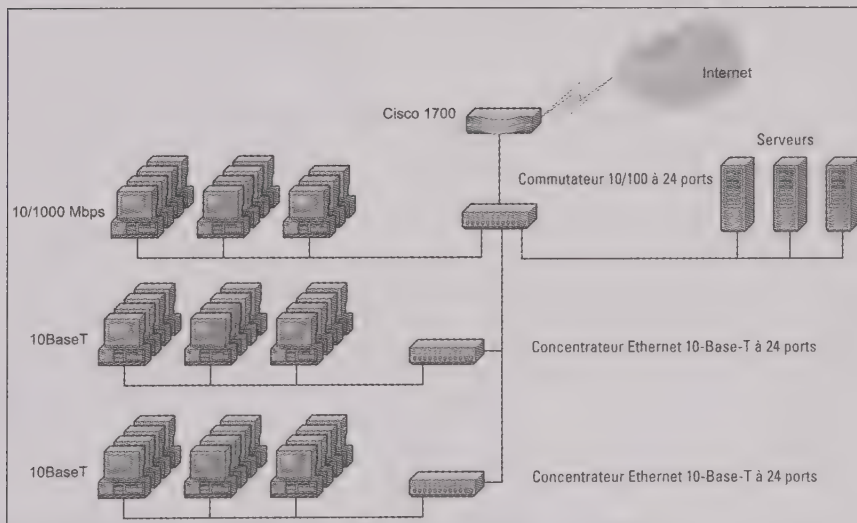


Figure 4.7 : Nouveau réseau de la société DCH Compta.

Chapitre 5

S'empêtrer dans la toile : câbles, cartes et autres matériels bizarres

Dans ce chapitre :

- ▶ Apprendre ce qu'est Ethernet.
- ▶ Découvrir les différents types de câbles réseau.
- ▶ Installer un câble à paires torsadées.
- ▶ Travailler avec des concentrateurs et des commutateurs.
- ▶ Installer une carte réseau.
- ▶ S'initier aux autres périphériques : répéteurs, ponts et routeurs.

Les câbles sont la plomberie de votre réseau. Leur utilisation ressemble beaucoup à celle des tuyaux d'un système d'arrosage : vous devez avoir le bon type de tuyaux (câbles), les bonnes valves et les bons répartiteurs (commutateurs et répéteurs) ainsi que les bonnes têtes d'arrosage (cartes réseau).



Les câbles réseau ont un avantage par rapport aux tuyaux d'un système d'arrosage : vous n'êtes pas mouillé s'ils fuient.

Ce chapitre vous en apprendra probablement plus que vous n'aurez jamais besoin d'en savoir sur les câbles réseau. Je vais vous présenter *Ethernet*, la technologie la plus répandue en matière de câble pour petits réseaux. Vous verrez ensuite comment vous servir des câbles servant à monter un réseau Ethernet. Vous découvrirez aussi comment choisir les bonnes cartes réseau qui vous permettent de connecter les câbles à vos ordinateurs.

Qu'est-ce qu'Ethernet ?

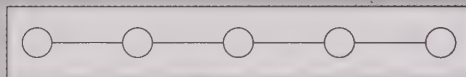
Ethernet est une technologie normalisée permettant de connecter des ordinateurs pour former un réseau.



Encadré inutile sur les topologies de réseaux

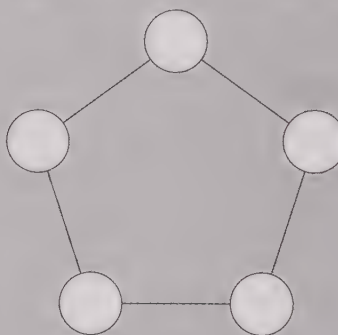
Un livre sur les réseaux ne serait pas complet s'il ne comprenait pas la sacro-sainte présentation des différentes *topologies de réseaux*. La première de ces topologies est le *bus*, dans lequel les nœuds du réseau (les ordinateurs) sont liés les uns aux autres en ligne, comme ceci :

Le *bus* est la plus simple des topologies mais il a ses inconvénients. Si le câble se rompt, le réseau est coupé.



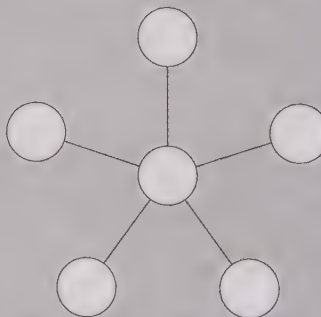
Le deuxième type de topologie est appelé *anneau* :

Un *anneau* ressemble beaucoup à un bus sans fin : le dernier nœud de la ligne est relié au premier nœud, formant ainsi une boucle infinie.



Le troisième type de topologie est l'*étoile* :

Dans un réseau *en étoile*, tous les nœuds sont connectés à un commutateur central. En réalité, chaque nœud dispose d'une connexion indépendante au réseau, donc lorsqu'un câble est rompu, cela n'affecte pas les autres.



Les réseaux Ethernet reprennent la topologie du bus. Cependant, quelques astuces de câblage permettent, lorsque l'on utilise du câble à paires torsadées, de donner au réseau Ethernet l'aspect d'une étoile.

Vous pouvez vous représenter Ethernet comme une espèce de manuel de construction pour réseaux : il spécifie le type de câbles à utiliser, la manière de les connecter entre eux, leur longueur, la façon dont les ordinateurs se transmettent des données via les câbles et j'en passe...



Ethernet n'a pas toujours régné sur l'univers des réseaux comme aujourd'hui. Il y a bien longtemps, Ethernet était concurrencé par deux normes :

- ✓ **Token Ring** est une norme réseau d'IBM toujours utilisée dans certaines entreprises encore dotées de vieux ordinateurs mainframes ou de machines de milieu de gamme.
- ✓ **ARCnet** a pratiquement disparu du monde des réseaux professionnels mais sert encore pour certaines applications réseau industrielles, de l'immotique (techniques appliquées dans le secteur du bâtiment) et de la robotique, par exemple.

De nos jours, ces réseaux sont totalement dépassés. Mieux vaut les oublier. Ethernet est désormais le choix numéro un pour qui veut monter un réseau modeste ou important.

Voici quelques informations intéressantes au sujet des normes Ethernet :

- ✓ Ethernet est un ensemble de normes concernant l'infrastructure de base d'un réseau. Tous les systèmes d'exploitation réseau dont je parle dans ce livre (toutes les versions de Windows, NetWare, Linux et OS X de Macintosh) peuvent fonctionner sur un réseau Ethernet. Si vous bâtissez un réseau sur une base Ethernet solide, vous pourrez changer de système d'exploitation par la suite.
- ✓ Les spécialistes réseau se réfèrent souvent à Ethernet en parlant de 802.3 (prononcé *huit cent deux point trois*) qui correspond à la désignation officielle de l'IEEE (prononcé *itroizeu*). Ces spécialistes sont un groupe d'ingénieurs qui portent des nœuds-papillons et n'ont rien de mieux à faire que de parler d'inductance toute la journée. Ce n'est pas plus mal car s'ils n'étaient pas là, vous ne pourriez pas mélanger des composants Ethernet fabriqués par des sociétés différentes.
- ✓ Le débit de l'Ethernet standard est de 10 millions de bits par seconde ou 10 Mbps. Puisque 8 bits forment un octet, ce débit correspond à peu près à 1,2 million d'octets par seconde. En pratique, Ethernet ne peut véhiculer les données aussi rapidement car celles-ci doivent être transmises par *paquets* de 1 500 octets maximum. Un fichier de 150 Ko doit donc être découpé en cent paquets.

Ce débit n'a rien à voir avec la vitesse à laquelle le signal électrique se propage dans le câble. Les signaux électriques circulent à 70 % de la vitesse de la lumière, ce que le capitaine Picard appellerait : « Facteur warp point sept zéro. En avant. »



- ✓ La nouvelle version d'Ethernet, nommée *Fast Ethernet* ou *Ethernet 100 Mbps*, déplace les données dix fois plus vite que l'Ethernet classique. Dans la mesure où Fast Ethernet déplace les données à un débit de 100 Mbps et utilise du câble à paires torsadées, il est aussi appelé *100BaseT* (et parfois *100BaseTX*).
- ✓ Il existe également une version d'Ethernet encore plus rapide, *Gigabit Ethernet*. Le Gigabit Ethernet est la version la plus utilisée pour les nouveaux réseaux même si beaucoup de réseaux existants fonctionnent encore en 100 Mbps.
- ✓ La plupart des composants réseau commercialisés aujourd'hui supportent les trois débits, 10 Mbps, 100 Mbps et 1000 Mbps. On les appelle souvent *composants 10/100/1000 Mbps*.

Tout sur les câbles

Bien que vous puissiez recourir aux technologies sans fil pour créer des réseaux sans tirer des câbles, la plupart des installateurs de réseaux préfèrent relier les ordinateurs physiquement par des câbles. Au fil des années, de nombreux types de câbles ont été utilisés pour les réseaux Ethernet. Aujourd'hui, presque tous les réseaux sont créés avec des *câbles à paires torsadées*. Dans ce type de câble, les deux brins sont enroulés l'un autour de l'autre afin de réduire les interférences électriques (comme il faut au moins un doctorat en physique pour comprendre comment des câbles torsadés réduisent les interférences, je ne m'attarde pas sur cette notion).

Vous trouverez aussi d'autres types de câbles sur les réseaux. Par exemple, sur les plus anciens, vous rencontrerez deux types de câbles *coaxiaux* (du *coax*, comme on dit dans les milieux branchés). Le premier, qui ressemble à du câble d'antenne de télévision, est appelé « câble RG-58 ». Le second type de câble est un épais câble jaune qui n'était utilisé que pour Ethernet. Vous trouverez aussi des câbles en fibre optique qui relient à grande vitesse des sites très éloignés ou, dans les grands immeubles de bureaux, des gros câbles à multiples paires torsadées. Pour la plupart des réseaux, ce sont cependant des câbles à simple paire torsadée qui sont communément utilisés.

Le câble à paires torsadées est parfois appelé *UTP* (*Unshielded Twisted-Pair*, câble à paires torsadées non blindé). La Figure 5.1 montre un connecteur de câble à paires torsadées.

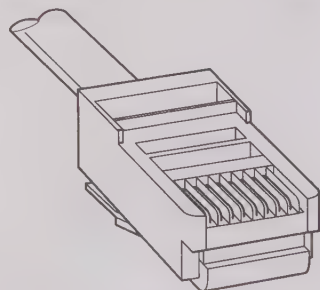


Figure 5.1 : Connecteur de câble à paires torsadées.

Quand vous utilisez du câble UTP pour créer un réseau Ethernet, vous connectez les ordinateurs en étoile, comme le montre la Figure 5.2. Au centre se trouve le *concentrateur* ou le *commutateur*. Selon leur modèle, les concentrateurs et commutateurs Ethernet permettent de connecter de quatre à quarante-huit (ou plus) ordinateurs au moyen de câbles à paires torsadées.

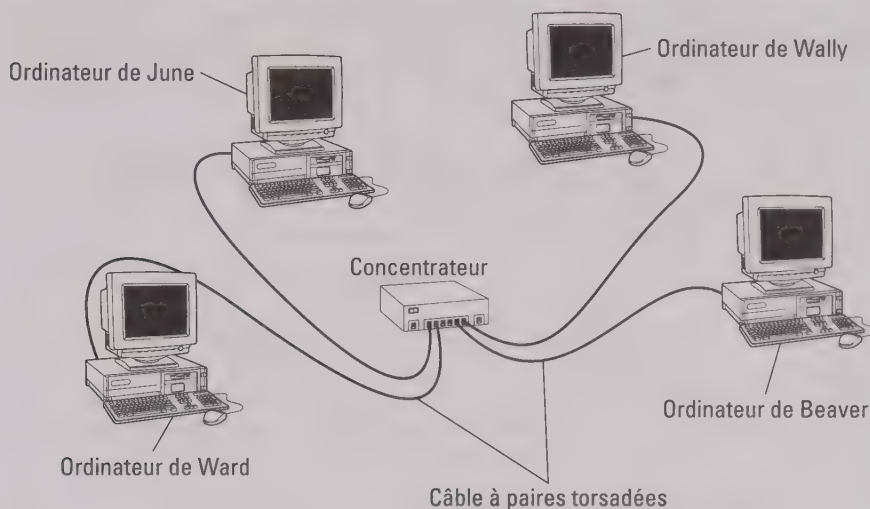


Figure 5.2 : Exemple de réseau avec des câbles à paires torsadées.



L'avantage de la répartition en étoile réside dans le fait que si un câble pose problème, seul l'ordinateur relié par ce câble est affecté. Le reste du réseau continue de fonctionner normalement.

Différentes catégories de câbles

Les câbles à paires torsadées sont proposés en différentes qualités ou *catégories*. Ces catégories sont spécifiées par le standard ANSI/EIA 568 (ANSI sont les initiales d'*American National Standards Institute*, EIA celles d'*Electronic Industries Alliance*). Ces standards indiquent le débit (ou *bande passante*) de ces câbles. Le Tableau 5.1 liste les différentes catégories de câbles à paires torsadées.

Bien que les câbles de catégorie supérieure soient plus chers, le véritable coût d'installation d'un réseau Ethernet est le travail fourni pour passer les câbles à travers les murs. Je vous conseille de ne jamais utiliser de câbles de catégorie inférieure à 5. Si possible, investissez même dans des câbles de catégorie 6 pour permettre les prochaines mises à jour de votre réseau.

Pour avoir l'air cool, dites « cat 6 » plutôt que « catégorie 6 ».



Tableau 5.1 : Catégories de câbles à paires torsadées.

Catégorie	Débit maximal	Utilisation
1	1 Mbps	Voix uniquement
2	4 Mbps	Token Ring 4 Mbps
3	16 Mbps	Ethernet 10BaseT
4	20 Mbps	Token Ring 16 Mbps
5	100 Mbps (2 paires)	Ethernet 100BaseT
	1 000 Mbps (4 paires)	1000BaseTX
5e	1 000 Mbps (2 paires)	1000BaseT
6	1 000 Mbps (2 paires)	1000BaseT et applications à plus gros débits
6a	10 000 Mbps (2 paires)	Le futur standard destiné à l'Ethernet 10 Gbps

Combien de paires ?

La plupart des câbles à paires torsadées ont quatre paires de fils, soit huit en tout. L'Ethernet standard n'utilise en réalité que deux de ces paires. Les deux autres sont inutilisées. Vous pourriez par conséquent être tenté d'acheter du câble à deux paires de fils mais ce serait une mauvaise idée. En effet, si un câble présente un problème, il est parfois possible de le résoudre en passant de la paire défectueuse à une paire inutilisée. Si votre câble est à deux fils, vous ne bénéficierez pas de cette option.



Vous pourriez aussi être tenté d'utiliser les fils inutiles à d'autres fins, comme le transport de la voix ou de données. Dans ce cas, le bruit électromagnétique produit par les signaux vocaux risquerait d'interférer avec les signaux du réseau.

Blindé ou non ?

Le câble UTP (*Unshielded Twisted-Pair*, câble à paires torsadées non blindé) a été conçu pour un usage bureautique dans un environnement normal. Quand vous tirez ce type de câble dans un local, vous devez veiller à ne pas le faire passer trop près des éclairages fluorescents, des climatiseurs ou des moteurs électriques (porte automatique, moteur d'ascenseur...). Le câble UTP est le type de câble le moins cher.

Dans des environnements riches en interférences électromagnétiques (une usine, par exemple), vous opterez pour du câble STP (*Shielded Twisted-Pair*, câble à paires torsadées blindé). Comme il est trois fois plus cher qu'un câble UTP, vous ne l'utiliserez que si c'est nécessaire. En l'installant judicieusement, le câble STP protège même contre de fortes interférences.

La plupart des câbles STP sont protégés par une feuille d'aluminium. Mais si l'environnement est vraiment défavorable, un blindage à base de fils de cuivre tressés assurera une protection encore plus efficace.

Quand utiliser du câble plenum ?

La gaine externe des câbles à paires torsadées est fabriquée en deux matériaux : PVC et plenum.

- ✓ Le *câble en PVC* est le plus courant et le moins onéreux.
- ✓ Le *câble plenum* est un câble spécial ignifugé, conçu pour être installé dans le plenum d'un immeuble (voir description ci-dessous). Le câble plenum est doublé d'un revêtement en Téflon qui non seulement résiste à la chaleur mais dégage peu de fumées toxiques lors de sa combustion. Le câble plenum est malheureusement deux fois plus cher que du câble ordinaire en PVC.



Les normes de sécurité des immeubles de bureau exigent souvent que du *câble plenum* soit utilisé si les câbles du réseau sont installés dans le *plenum* (espace qui fait partie du système d'aération d'un immeuble, généralement situé au-dessus d'un faux plafond ou sous un plancher surélevé).



Notez que la zone au-dessus du plafond suspendu *n'est pas un plenum*, si les canalisations d'aller et de retour de l'air conditionné ou du système de chauffage sont dans des conduits. Du câble plenum n'est indispensable que si la climatisation ou le système de chauffage ne sont pas dans des conduits. Dans le doute, il est préférable qu'un spécialiste examine votre installation avant de tirer les câbles.

Monobrin ou multibrin ?

Les brins de cuivre qui forment le câble existent en deux variétés : à un seul brin ou à brins multiples. Dans un réseau, vous aurez les deux.



- ✓ Dans un *câble multibrin*, chaque conducteur est constitué d'un faisceau de fils minces torsadés. Le câble multibrin est plus souple que le câble monobrin et a moins tendance à se rompre. Il est toutefois plus onéreux et ne transmet pas bien les signaux à longue distance. Le câble multibrin est surtout utilisé pour les raccordements (du panneau de raccordement aux concentrateurs et aux commutateurs, par exemple).

Les câbles d'alimentation de votre unité centrale et de l'écran sont aussi multibrins.

- ✓ Dans un *câble monobrin*, chaque conducteur est un épais brin métallique. Ce type de câble est meilleur marché que le câble multibrin et il transporte le signal sur une plus grande distance mais il n'est pas très souple. Tordu trop souvent, il se rompt. Ce genre de câble est utilisé pour les câblages permanents, dans les murs et les plafonds d'un immeuble.

Conseils d'installation

Le plus dur, lors de l'installation des câbles, est la tâche très physique qui consiste à les tirer à travers les murs, les plafonds et le long du plancher. Ce travail est suffisamment délicat pour que je vous déconseille de le faire vous-même, hormis dans de petits locaux. S'il faut desservir plusieurs bureaux ou s'il faut percer des passages de câbles, faites appel à un professionnel.

Voici quelques recommandations à garder à l'esprit si vous décidez d'installer les câbles vous-même :



- ✓ Le câble à paires torsadées peut être acheté en longueur définie (5, 15 ou 25 mètres...). Mais vous pouvez en commander de n'importe quelle dimension. Le sertissage des connecteurs aux extrémités d'un câble acheté en vrac n'est pas très difficile.

Je ne conseille l'achat de câbles prêts à l'emploi que pour de petits réseaux ou s'il n'est pas nécessaire de traverser des cloisons ou des plafonds.

- ✓ Prévoyez toujours un peu plus de câble qu'il n'en faut, notamment s'il doit traverser une cloison. S'il traverse un faux plafond, laissez quelques mètres de rab ; vous aurez ainsi plein de câble en réserve si, par la suite, vous devez effectuer des réparations.
- ✓ Quand vous tirez les câbles, évitez les sources d'interférences électromagnétiques comme les éclairages fluorescents, les gros moteurs électriques, les machines émettant des rayonnements, etc.



Les éclairages fluorescents sont les sources d'interférences les plus communes. Faites passer les câbles à au moins un mètre de distance.

- ✓ La longueur maximale de câble entre le commutateur et l'ordinateur est de 100 mètres.
- ✓ Si le câble doit franchir un lieu très passant, couvrez-le afin que personne ne se prenne les pieds dedans. Vous trouverez des passages de câbles à poser au sol dans les magasins de bricolage.
- ✓ Quand vous tirez des câbles à travers des cloisons, étiquetez-les à chaque extrémité. Les magasins d'électricité vendent des étiquettes prédécoupées. C'est beaucoup plus professionnel que de coller un morceau de chatterton vaguement griffonné au marqueur.

Bien sûr, vous pouvez aussi écrire directement sur le câble avec un feutre indélébile.



Si vous installez des câbles dans une construction nouvelle, étiquetez chaque extrémité du câble au moins trois fois et laissez environ 30 centimètres entre les étiquettes. Les artisans risquent de laisser du plâtre ou de la peinture sur les câbles, ce qui rendra les étiquettes illisibles.

- ✓ Si plusieurs câbles passent par un même endroit, liez-les avec des liens en plastique (en vente dans les magasins d'électricité). Évitez autant que possible d'utiliser du ruban adhésif ; il ne dure en effet pas très longtemps et laisse des traces de colle. Des années plus tard, ce n'est pas très ragoûtant.



Pour tirer du câble à travers un faux plafond insonorisant, prenez des liens en plastique, des crochets ou des colliers afin de fixer le câble directement sur le plafond ou sur l'armature métallique sur laquelle reposent les panneaux du plafond. Le câble ne doit pas simplement reposer sur les panneaux.

Bien entendu, un bon ouvrier doit avoir de bons outils :

- ✓ Démarrez par la boîte à outils informatique que vous pouvez acheter pour environ 10 euros dans n'importe quelle boutique d'informatique ou de fournitures de bureau. Ces kits comprennent des tournevis et des clés pour ouvrir vos ordinateurs et y insérer des cartes.

La boîte à outils informatique contient probablement tout ce dont vous avez besoin si :

- tous vos ordinateurs sont dans la même pièce.
- vous comptez faire courir le câble sur le sol.
- vous utilisez des câbles déjà assemblés.





Si vous n'avez pas de boîte à outils informatique, assurez-vous que vous avez des tournevis plats et cruciformes de diverses tailles.

- ✓ Au cas où vous utilisez du câble nu sur lequel vous envisagez de fixer vos propres connecteurs, vous devez avoir les outils suivants, en plus de ceux figurant dans la boîte à outils informatique :
 - **Des pinces coupantes.** Une grosse pour le câble coaxial, une plus petite pour le câble à paires torsadées. Des tenailles en titane pour le câble jaune.
 - **Une pince à sertir adaptée au type de câble.** Vous avez besoin d'une pince à sertir pour attacher les connecteurs à vos câbles. N'utilisez pas un modèle bas de gamme à 25 euros. Un modèle digne de ce nom vous coûtera plus de 100 euros mais à l'usage il vous évitera bien des problèmes.
 - **Une pince à dénuder.** Vous n'en aurez besoin que si la pince à sertir ne fait pas fonction de pince à dénuder.
- ✓ Si vous projetez de faire courir le câble à travers les murs, vous aurez aussi besoin des outils suivants :
 - **Un marteau.**
 - **Une scie à guichet.** Utile si vous envisagez de percer des trous dans les murs pour tirer votre câble.
 - **Une lampe de poche.**
 - **Une échelle.**
 - **Quelqu'un pour tenir l'échelle.**
 - **Un guide, probablement.** C'est un morceau de métal rigide enroulé sur lui-même. Pour l'utiliser, vous l'insérez dans une ouverture d'un côté du mur et vous le poussez vers la sortie, où quelqu'un se tient prêt à le saisir quand il sort. Votre collègue attache le câble au guide et crie quelque chose comme « C'est parti ! » ou « Go ! ». Vous tirez alors sur le guide et le câble vient avec (vous pouvez trouver ce type de matériel dans le rayon électricité des bonnes quincailleries).



Si vous envisagez de faire courir le câble à travers un sol en béton, vous devrez louer un marteau-piqueur et un compresseur ainsi que les services de quelqu'un qui brandira un drapeau jaune pendant que vous travaillerez.

Brocher un câble à paires torsadées

Dans un câble à paires torsadées, chaque paire de câble est de l'une de ces couleurs : orange, vert, bleu ou marron. Les deux brins qui forment une paire sont complémentaires : l'un est blanc avec une bande colorée, l'autre coloré avec une bande blanche. Par exemple, la paire orange est constituée d'un

brin orange avec une bande blanche (appelé *brin orange*) et d'un brin blanc avec une bande orange (appelé *brin blanc/orange*). De même, la paire bleue est faite d'un brin bleu avec une bande blanche (le *brin bleu*) et d'un brin blanc avec une bande bleue (le *brin blanc/bleu*).

Lorsque vous reliez un câble à paires torsadées à un connecteur modulaire ou à une prise, il est crucial que les bons brins soient connectés aux bonnes broches. C'est moins évident qu'il n'y paraît car, pour le câblage, vous pouvez adopter n'importe lequel des différents standards. Histoire de compliquer les choses, vous avez le choix entre deux standards très répandus : l'un est le standard EIA/TIA 568A, l'autre le standard EIA/TIA 568B, aussi appelé AT&T 258A. Le Tableau 5.2 montre chacun de ces câblages.



Qu'importe le standard de câblage que vous adoptez, choisissez-en un et tenez-vous-y. Car si vous utilisez un standard à une extrémité du câble et un autre standard à l'autre bout, le câble ne servira à rien.

Tableau 5.2 : Brochage d'un câble à paires torsadées.

Numéro	Fonction	EIA/TIA 568A	EIA/TIA 568B AT&T 258A
Broche 1	Émetteur +	Brin blanc/vert	Blanc/orange
Broche 2	Émetteur -	Brin vert	Orange
Broche 3	Réception +	Brin blanc/orange	Blanc/vert
Broche 4	Inutilisée	Brin bleu	Bleu
Broche 5	Inutilisée	Brin blanc/bleu	Blanc/bleu
Broche 6	Réception -	Brin orange	Vert
Broche 7	Inutilisée	Brin blanc/marron	Blanc/marron
Broche 8	Inutilisée	Brin marron	Marron

Les câbles 10BaseT et 100BaseT n'utilisent en réalité que deux des quatre paires, connectées aux broches 1, 2, 3 et 6. Une paire sert à l'émission des données, l'autre à la réception. La seule différence entre les deux standards de câblage réside dans le choix de la paire pour l'émission et de la paire pour la réception. Dans le standard EIA/TIA 568A, la paire verte sert à l'émission tandis que la paire orange sert à la réception. Dans les standards EIA/TIA 568B et AT&T 258A, la paire orange sert à l'émission et la paire verte à la réception.

Si vous le désirez, vous pouvez vous contenter de ne câbler que les broches 1, 2, 3 et 6. Je vous recommande toutefois d'utiliser toutes les broches, en vous basant sur le Tableau 5.2.

Fixer les connecteurs RJ-45

Les connecteurs RJ-45 d'un câble à paires torsadées ne sont pas difficiles à fixer à condition de posséder la pince à sertir adéquate. La seule précaution importante est de s'assurer que chaque brin sera fixé à la bonne broche puis de serrer la pince suffisamment fort pour assurer une bonne connexion.

Voici comment procéder pour fixer un connecteur RJ-45 :

1. Coupez le câble à la longueur désirée.

Veillez à ce que la coupe soit parfaitement droite et non en diagonale.

2. Insérez le câble dans la partie de la pince qui sert à dénuder le fil, en calant l'extrémité contre le butoir.

Serrez la pince et retirez le câble, toujours bien droit. Cela retire la longueur correcte de revêtement isolant externe sans abîmer l'isolant des brins internes.

3. Disposez les câbles à plat et dans l'ordre, conformément aux indications du Tableau 5.2.

Vous devrez manipuler un peu les brins pour trouver l'ordre correct.

4. Glissez les brins dans les orifices du connecteur.

Vérifiez (plutôt deux fois qu'une) que chaque brin est placé dans l'orifice approprié.

5. Insérez le connecteur et les brins dans la partie de la pince à sertir prévue à cet effet puis serrez-la.

Serrez bien fort !

6. Ôtez le connecteur de la pince puis vérifiez la qualité du sertissage.

C'est terminé !

Voici quelques autres points à garder à l'esprit lorsque vous manipulez des connecteurs RJ-45 et du câble à paires torsadées :



✓ Les broches d'un connecteur RJ-45 ne sont pas numérotées.

Vous pouvez identifier la broche 1 en tenant le connecteur de telle manière que les contacts métalliques soient face à vous, comme le montre la Figure 5.3. La broche 1 est à gauche.

- ✓ Certains câblent le 10BaseT différemment : ils utilisent la paire vert/blanc pour les broches 1 et 2 et la paire orange/blanc pour les broches 3 et 6. Cela n'a aucune influence sur le réseau (il ne distingue pas les couleurs), à condition que les connecteurs RJ-45 soient connectés de la même manière aux deux extrémités du câble !
- ✓ Si vous installez du câble pour un réseau Fast Ethernet, vous devez suivre encore plus scrupuleusement les règles de câblage. Cela signifie que vous devez, entre autres choses, vous assurer que vous travaillez tout du long avec du matériel de catégorie 5. Les câbles et les connecteurs doivent être de catégorie 5. Pour le raccordement des connecteurs, vous ne devez pas défaire plus de 1,5 cm de câble. Et ne tirez pas le câble sur plus de 100 mètres. En cas de doute, confiez l'installation d'un système Ethernet 100 Mbps à des professionnels.

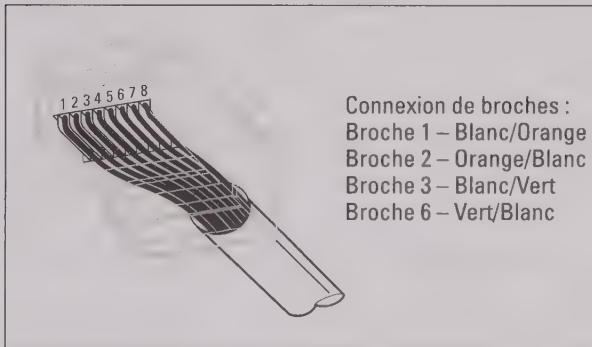


Figure 5.3 : Brochage du connecteur RJ-45 d'un câble à paires torsadées.

Câbles croisés

Un *câble croisé* sert à relier directement deux périphériques sans passer par un concentrateur ou un commutateur. Il sert à relier directement deux ordinateurs mais il est surtout utilisé pour relier en guirlande des concentrateurs et des commutateurs.

Pour créer vos propres câbles croisés, vous devrez inverser les brins à une extrémité du câble, comme l'indique le Tableau 5.3, qui montre le brochage des deux extrémités A et B d'un câble croisé. Reportez-vous respectivement aux informations des colonnes Connecteur A et Connecteur B pour brocher les deux extrémités du câble.

Notez qu'un câble croisé n'est pas indispensable si l'un des concentrateurs ou des commutateurs que vous comptez connecter comporte un port croisé, généralement indiqué sur le boîtier par la mention Uplink (port croisé) ou Daisy-chain (en guirlande). Si l'appareil est équipé d'un port Uplink, vous

pouvez le brancher en guirlande à l'aide d'un câble réseau normal. Pour en savoir plus sur la connexion des concentrateurs et des commutateurs en guirlande, reportez-vous à la section « Concentrateurs et commutateurs », plus loin dans ce chapitre.



En comparant attentivement le Tableau 5.3 avec le Tableau 5.2, vous constaterez qu'un câble croisé n'est en réalité qu'un câble dont le brochage, à une extrémité, est au standard 568A, et à l'autre extrémité au standard 568B.

Tableau 5.3 : Brochage d'un câble croisé.

Broche	Connecteur A	Connecteur B
1	Blanc/vert	Blanc/orange
2	Vert	Orange
3	Blanc/orange	Blanc/vert
4	Bleu	Bleu
5	Blanc/bleu	Blanc/bleu
6	Orange	Vert
7	Blanc/marron	Blanc/marron
8	Marron	Marron

Prises murales et panneaux de raccordement

Si vous le souhaitez, vous pouvez faire courir un seul câble depuis le concentrateur ou le commutateur d'une armoire de câblage et le faire traverser une cloison, monter jusque dans le faux plafond, traverser tout le faux plafond et le faire redescendre à l'autre mur, traverser une autre cloison puis tout le bureau jusqu'à l'ordinateur. Mais, pour une foule de bonnes raisons, ce n'est pas une bonne idée. Entre autres, chaque fois que quelqu'un voudra déplacer l'ordinateur, ne serait-ce que pour nettoyer l'arrière, le câble bougera un peu. La connexion risque même d'être interrompue et la prise RJ-45 devra être remplacée. Dans l'armoire de câblage, les câbles formeront rapidement un beau fouillis.

La solution consiste à tirer le câble entre un *panneau de raccordement* d'une part et une *prise murale* d'autre part. Le câble disparaîtra ainsi dans le mur et au-dessus du faux plafond. Pour connecter un ordinateur au réseau, il suffira de brancher un câble de raccordement entre l'ordinateur et la prise. Passant par l'armoire de câblage, un câble de raccordement relie la prise

murale aux concentrateurs ou aux commutateurs du réseau, comme le montre la Figure 5.4.

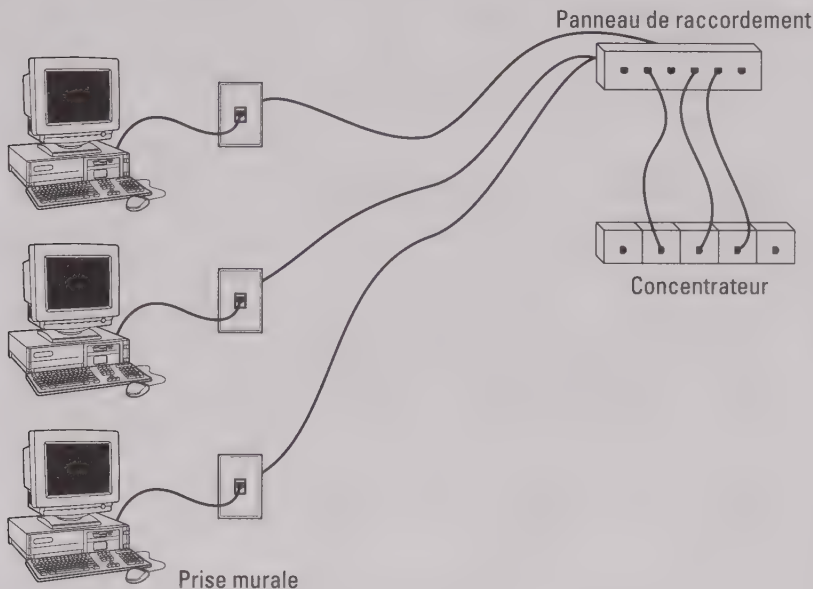


Figure 5.4 : Panneau de raccordement et prises murales.

La connexion d'un câble à paires torsadées à une prise murale ou à un panneau de raccordement est semblable à la connexion à une prise RJ-45. Généralement, aucun outil spécial n'est nécessaire. L'arrière de la prise comporte un emplacement pour chaque brin. Il faut ensuite placer un couvercle amovible sur ces emplacements et appuyer dessus. Les brins sont ainsi plaqués contre les lamelles métalliques qui établissent le contact.



Quand vous connectez un câble à une prise ou à un panneau de raccordement, veillez à défaire aussi peu de longueur de brin que possible. Car si vous en défaites trop, le signal qui passe par ces brins risque de ne plus être fiable.

Concentrateurs et commutateurs

Lorsque vous utilisez du câble à paires torsadées, vous ne reliez pas les ordinateurs directement les uns aux autres. Vous les connectez en fait à un périphérique spécial appelé *commutateur* ou *switch*. Autrefois, ces appareils étaient très onéreux, suffisamment, en tout cas, pour que les amateurs qui savaient monter un petit réseau optent pour le câble coaxial plutôt que pour la paire torsadée car les réseaux à base de câble coaxial n'ont pas besoin de commutateurs.

Aujourd'hui, le coût des commutateurs a baissé à tel point que les avantages du câble à paires torsadées compensent largement le coût et les complications des concentrateurs. Grâce à ce type de câble, il est plus facile de connecter de nouveaux ordinateurs au réseau, de les déplacer, de découvrir et de réparer les problèmes de câbles et d'intervenir sur les ordinateurs que vous devez temporairement ôter du réseau.

Concentrateurs ou commutateurs ?



Un *commutateur* (*switch*, en anglais) est simplement un type de concentrateur sophistiqué.

Leur prix ayant nettement baissé ces dernières années, les commutateurs ont supplanté les concentrateurs sur les nouveaux réseaux. Si votre réseau est assez ancien, doté de concentrateurs et particulièrement lent à vos yeux, vous améliorerez sa vitesse en remplaçant vos vieux concentrateurs par des commutateurs.



Les commutateurs sont plus efficaces que les concentrateurs, pas seulement au niveau de la vitesse :

- ✓ Dans un concentrateur, chaque paquet de données entrant sur un des ports ressort par chacun des autres ports. Ce procédé est inévitable car le concentrateur n'est pas capable de savoir sur quel port est connecté tel ordinateur.

Par exemple, admettons que l'ordinateur de Gilbert soit connecté au port 1 d'un concentrateur à 8 ports et que celui de Lucien soit connecté au port 5. Si la machine de Lucien envoie un paquet d'informations à l'ordinateur de Gilbert, le concentrateur reçoit les données sur le port 1 et les renvoie sur les ports 2 à 8. Tous les ordinateurs connectés au concentrateur vérifient le paquet de données afin de déterminer s'il leur est destiné.

- ✓ Un commutateur sait quel ordinateur est connecté à quel port.

Donc, si l'ordinateur de Gilbert, connecté au port 1, envoie un paquet à l'ordinateur de Lucien, connecté au port 5, le commutateur reçoit le paquet sur le port 1 et l'envoie seulement vers le port 5. Ce procédé est non seulement plus rapide mais il améliore également la sécurité du système car les autres machines n'ont pas accès aux paquets qui ne leur sont pas destinés.

Installer des commutateurs

Voici quelques éléments dont vous devrez tenir compte :



✓ L'installation d'un commutateur est généralement très simple : il suffit de brancher le cordon d'alimentation puis de connecter les câbles de raccordement du réseau.

✓ Chaque port du commutateur est une prise RJ-45 à laquelle est associée une diode électroluminescente (LED) marquée *Link* qui s'allume lorsqu'une connexion est établie sur ce port.

Si l'extrémité d'un câble est branchée au port et l'autre à un ordinateur, la LED *Link* devrait être allumée. Si ce n'est pas le cas, quelque chose ne va pas au niveau du câble, du concentrateur ou du commutateur ou bien du périphérique à l'extrémité du câble.

✓ Chaque port est aussi équipé d'une LED qui clignote selon l'activité sur le réseau.

En observant un concentrateur ou un commutateur pendant un moment, vous finissez par savoir qui utilise le plus le réseau rien qu'en voyant quelle est la LED qui clignote le plus, trahissant une activité soutenue.

Les ports peuvent aussi être équipés d'un indicateur de collision qui clignote dès que des paquets de données entrent en collision sur le port. Des flashes sporadiques sont parfaitement admissibles mais si l'indicateur clignote trop, vous avez peut-être un problème sur le réseau.

- Cela signifie en général que le réseau est surchargé et doit être segmenté par un commutateur afin d'améliorer ses performances.
- Dans certains cas, un indicateur de collision qui flashe trop peut être causé par un nœud fautif qui engorge le réseau avec de mauvais paquets.

Commutateurs connectés en guirlande

Si un seul commutateur ne possède pas suffisamment de ports pour tout le réseau, vous pouvez en relier plusieurs *en guirlande*, comme le montre la Figure 5.5. Pour peu qu'un commutateur soit équipé d'un port croisé, vous pouvez y brancher un câble de raccordement normal vers un autre commutateur. Si aucun de ces périphériques n'est équipé de port croisé, reliez-les par un câble croisé (pour savoir comment confectionner un câble croisé, reportez-vous à la section « Câbles croisés », précédemment dans ce chapitre).

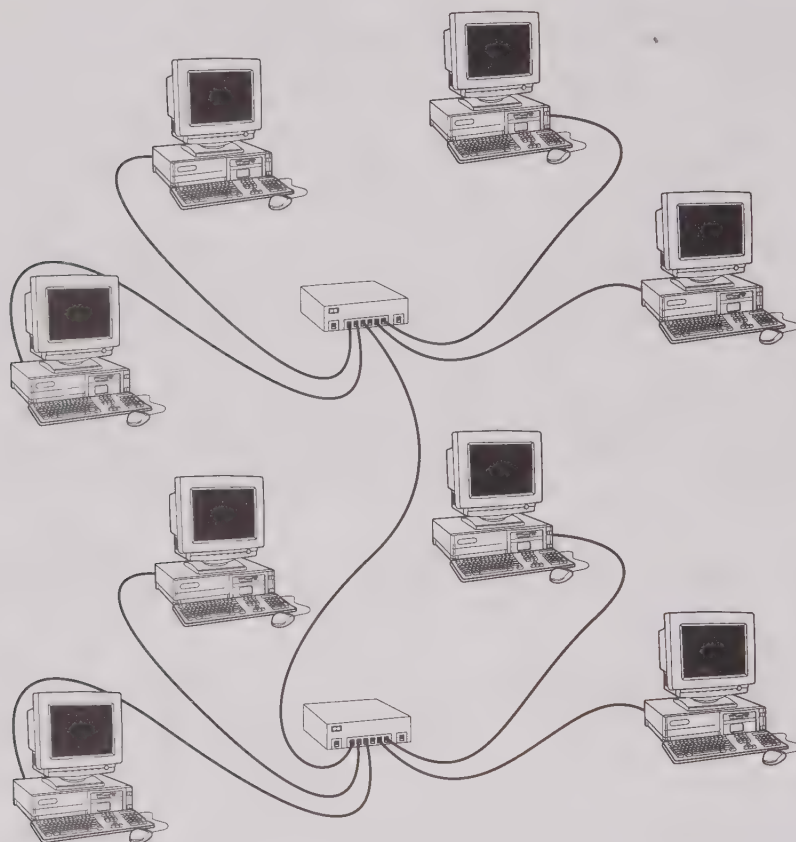


Figure 5.5 : Des commutateurs peuvent être reliés en guirlande.

Sur les commutateurs récents, chaque port peut détecter automatiquement s'il est connecté à un autre commutateur. Dans ce cas, vous ne devez pas utiliser de ports ni de câbles croisés. Vous pouvez employer un câble standard pour connecter les commutateurs en utilisant n'importe quel port disponible.



Vous pouvez souvent augmenter la performance globale de votre réseau en utilisant deux connexions (ou plus) entre les commutateurs. Par exemple, vous pouvez employer deux câbles de connexion pour créer deux connexions entre une paire de commutateurs.

Le nombre de commutateurs pouvant être reliés est limité :

- ✓ Pour un réseau en 10BaseT, vous ne pouvez pas en chaîner plus de trois.
- ✓ Pour un réseau en 100BaseT ou 1000BaseT, vous ne pouvez en relier que deux.

10Base quoi ?

L'IEEE, dans son infinie sagesse, a décrété que les noms suivants devaient être employés pour désigner les trois types de câbles des réseaux 802.3 (autrement dit, Ethernet) :

- ✓ **10Base5** désigne le vieux câble coaxial épais (le machin jaune).
- ✓ **10Base2** désigne le câble coaxial fin (Thinnet).
- ✓ **10BaseT** désigne le câble à paires torsadées non blindé (UTP).

Dans chaque terme, le *10* signifie que le câble fonctionne à 10 Mbps, et *Base* signifie que le câble est employé pour des réseaux à bande de base plutôt que des réseaux à large bande (ne m'en demandez pas plus). Le *5* de 10Base5 donne la longueur maximale d'un segment de câble jaune : 500 mètres. Le *2* de 10Base2 correspond à 200 mètres, ce qui équivaut à peu près aux 185 mètres de longueur maximale d'un segment Thinnet (je trouve que l'IEEE est une curieuse équipe d'ingénieurs ; je ne savais pas qu'« à peu près » faisait partie du vocabulaire d'un ingénieur). Le *T* de 10BaseT signifie *torsadé*.

De tous ces noms, 10BaseT est celui qui est le plus fréquemment utilisé. 10Base5 et 10Base2 sont simplement qualifiés d'*épais* et de *fin*.

En outre, pour le Fast Ethernet, dont le débit est supérieur à celui passant par les câbles 10BaseT, on se sert du terme 100BaseT.



Il est possible de contourner ces limitations en utilisant des *commutateurs empilables*. Ils sont équipés d'une connectique qui fait qu'un ensemble de commutateurs empilés fonctionne comme un seul. Ce matériel est conçu pour les réseaux de grande taille.



Si l'immeuble est précâblé et qu'une prise réseau se trouve dans chaque bureau, vous pouvez utiliser un petit concentrateur ou commutateur pour relier deux ou trois ordinateurs à une seule prise. Branchez le câble de liaison en guirlande à la prise murale et les ordinateurs au concentrateur.

Cartes réseau

Chaque ordinateur qui se connecte au réseau doit être équipé d'une carte d'interface réseau ou carte réseau. Dans la plupart des nouveaux ordinateurs, ces cartes sont intégrées. Mais sur les modèles plus anciens, vous devrez l'installer. Les sections qui suivent expliquent ce qu'il faut savoir pour acheter et installer une carte réseau.

Choisir une carte réseau

Vous trouverez des cartes réseau peu onéreuses dans les boutiques informatiques et dans les grandes surfaces. Voici quelques recommandations utiles :

- ✓ Vos cartes réseau doivent être équipées d'un connecteur adapté au type de câble utilisé. Si vous pensez câbler votre réseau avec du câble Thinnet, vérifiez que vos cartes disposent de connecteurs BNC. Pour du câble à paires torsadées, il vous faut des connecteurs RJ-45.
- ✓ Certaines cartes réseau disposent de deux ou trois connecteurs. Toutes les combinaisons sont possibles : BNC et AUI, RJ-45 et AUI, BNC et RJ-45 et les trois à la fois. Les connecteurs AUI sont en voie d'obsolescence. À l'instar des connecteurs BNC, n'en faites l'acquisition que si votre réseau est déjà câblé en coaxial. Sinon, des cartes à connecteurs RJ-45 conviendront parfaitement.
- ✓ Les cartes les plus récentes sont de type 10/100/1000 Mbps, ce qui signifie qu'elles s'accommodent aussi bien des vieux réseaux à 10 Mbps que de ceux à 100 ou 1000 Mbps. Elles détectent automatiquement le débit et adoptent la bonne vitesse.
- ✓ Achetez une carte compatible avec votre ordinateur. La plupart des ordinateurs peuvent accueillir des cartes au standard ISA 16 bits. Les nouveaux ordinateurs peuvent utiliser des cartes PCI. Si votre ordinateur vous le permet, vous devez acheter une carte PCI. Elles sont non seulement plus rapides que les cartes ISA mais aussi plus faciles à configurer. N'utilisez les cartes ISA que sur les vieux ordinateurs ne pouvant être équipés de cartes PCI.
- ✓ Une carte réseau peut s'avérer assez difficile à configurer car chacune a ses spécificités. Vous vous simplifierez la vie en dotant tous les ordinateurs de votre réseau d'une carte du même modèle. N'essayez pas de mélanger divers types de cartes.
- ✓ Certains ordinateurs sont dotés de ports réseau intégrés. Dans ce cas, vous n'avez pas besoin d'ajouter une carte réseau.

Installer une carte réseau

L'installation d'une carte réseau n'est pas une tâche surhumaine mais vous devrez retrousser vos manches. Si vous savez installer une carte, vous savez les installer toutes. Autrement dit, l'installation d'une carte réseau est comme l'installation d'une carte modem, d'une carte graphique, d'une carte son ou de n'importe quel autre type de carte. Si vous en avez déjà installé une, vous installerez la carte réseau les yeux fermés.

Voici la procédure à suivre pour installer une carte réseau :



1. Quittez Windows, éteignez l'ordinateur et débranchez-le.

N'intervenez jamais dans l'ordinateur s'il n'est pas débranché !

2. Otez le capot de l'ordinateur.

La Figure 5.6 montre l'emplacement classique des vis. Déposez-les à un endroit où elles ne risquent pas de se perdre.

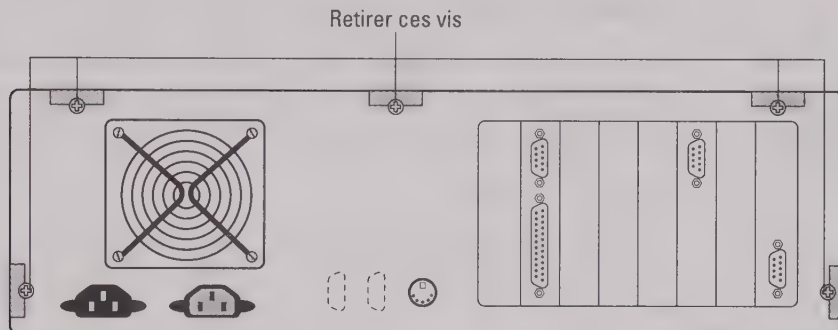


Figure 5.6 : Démontage du capot de la tour.

3. Localisez un connecteur d'extension libre dans l'ordinateur.

Les connecteurs d'extension sont disposés à l'arrière de la tour, vous ne pouvez pas les rater.

- Les ordinateurs les plus récents ont au moins deux ou trois connecteurs libres, appelés *connecteurs PCI*. C'est ceux que vous cherchez pour installer votre carte réseau.
- Certains ordinateurs possèdent d'autres types de connecteurs, conçus pour les cartes vidéo ou d'autres cartes. Ils ne sont pas adaptés à votre carte réseau, alors ne forcez pas !

4. Après avoir repéré le bon connecteur libre, ôtez la languette de protection correspondante, placée à l'arrière du châssis de l'ordinateur.

- a. La languette est fixée par une vis cruciforme. Otez-la et déposez-la en lieu sûr.
- b. Retirez ensuite la languette de protection.
- c. Conservez-la dans une boîte, elle peut toujours servir.

Au bout d'un certain temps, vous risquez d'en avoir une belle collection. Gardez-les en souvenir.

5. Insérez la carte réseau dans le connecteur.



Alignez parfaitement le connecteur de la carte réseau avec le connecteur d'extension et appuyez fermement de manière à l'insérer droit. Il faut parfois appuyer très fort. Assurez-vous qu'elle est insérée à fond et pas de travers.

6. Assurez la fixation de la carte en remplaçant sur sa languette la vis ôtée à l'étape 4.

7. Remplacez le capot.



Faites attention aux câbles qui se promènent dans l'ordinateur. N'en pincez pas un par mégarde lorsque vous faites glisser le capot.

Remplacez les vis ôtées à l'étape 2.

8. Rallumez l'ordinateur.

Si la carte est de type plug-and-play (« branchez, ça fonctionne »), elle est automatiquement configurée par Windows dès le redémarrage de l'ordinateur.



Si l'ordinateur ou la carte sont un peu anciens, vous devrez utiliser un logiciel de configuration. Reportez-vous au manuel de la carte pour terminer l'installation.

Autres périphériques réseau

En plus des cartes d'interface réseau, des câbles, des concentrateurs et des commutateurs, certains réseaux exigent l'un ou l'autre des périphériques particuliers décrits dans les sections ci-dessous.

Répéteurs

Un *répéteur* est un appareil qui régénère les signaux de votre réseau de sorte qu'ils puissent circuler sur une distance plus longue. C'est un peu comme les points de ravitaillement sur le parcours d'un marathon. Lorsque le signal passe par le répéteur, il attrape un gobelet, boit une gorgée, s'asperge la tête, jette le gobelet et saute dans un taxi lorsqu'il est sûr que personne ne le regarde.

Vous avez besoin d'un répéteur quand la longueur totale d'un seul brin de câble réseau est plus importante que la longueur maximale autorisée pour ce type de câble :

Câble	Longueur maximale
10Base2 (coax)	185 mètres
10/100BaseT (paire torsadée)	100 mètres

Pour le câble coaxial, les longueurs mentionnées dans le tableau précédent correspondent à des segments et non aux brins. Un *segment* représente tout le câble qui lie un terminateur à un autre et peut comprendre plusieurs ordinateurs. Autrement dit, si vous avez dix ordinateurs que vous devez connecter entre eux avec des brins de 10 mètres de câble coaxial fin, la longueur totale d'un segment sera de 90 mètres. Attention ! Seuls neuf câbles sont requis pour connecter dix ordinateurs. C'est pourquoi ça ne fait pas 100 mètres.

Pour le câble 10BaseT ou 100BaseT, la limite des 100 mètres s'applique au câble qui relie un ordinateur au concentrateur ou au câble qui relie deux concentrateurs entre eux, quand les concentrateurs sont connectés en cascade par du câble à paires torsadées. Autrement dit, vous pouvez connecter chaque ordinateur au concentrateur ou deux concentrateurs entre eux avec au plus 100 mètres de câble.

La Figure 5.7 montre comment utiliser un répéteur afin de connecter deux groupes d'ordinateurs qui sont trop éloignés l'un de l'autre pour permettre l'emploi d'un seul segment. Quand vous vous servez d'un répéteur de cette manière, celui-ci divise le câble en deux segments. La limite de longueur du câble s'applique toujours de chaque côté du répéteur.

Voici quelques points sur lesquels méditer quand vous vous réveillez en pleine nuit en pensant aux répéteurs :



- ✓ Les répéteurs ne s'utilisent que sur des réseaux Ethernet câblés avec du coaxial. Les réseaux 10/100BaseT ne supportent pas les répéteurs. Ce n'est pas tout à fait vrai : le 10/100BaseT autorise les répéteurs. Mais le répéteur n'est pas un engin séparé. Dans un réseau 10/100BaseT, le commutateur est en fait un répéteur à ports multiples. C'est pourquoi le câble employé pour connecter chaque ordinateur au commutateur est traité comme un segment distinct.
- ✓ Certains commutateurs 10/100BaseT possèdent un connecteur BNC. Ce connecteur BNC est un répéteur Thinnet qui vous permet de câbler un segment Thinnet de 185 mètres. Le segment peut relier d'autres ordinateurs, des concentrateurs 10BaseT ou les deux.
- ✓ Une règle de base de l'univers Ethernet est qu'entre deux nœuds un signal ne peut pas passer par plus de trois répéteurs.



Cela ne signifie pas que vous ne pouvez pas utiliser plus de trois répéteurs ou commutateurs mais que si vous le faites vous devez planifier avec précaution le câblage de votre réseau pour que la règle des trois répéteurs ne soit pas enfreinte.

- ✓ Vous pouvez acheter par correspondance des répéteurs à deux ports 10Base2 pour 130 euros. Eh bien ! J'imagine que c'est l'une des raisons pour lesquelles le câble coaxial n'est plus beaucoup utilisé.
- ✓ Les répéteurs sont des composants qu'il est parfaitement normal d'employer sur un réseau conçu dans les règles. Ils n'augmentent pas la longueur maximale d'un segment, ils vous permettent simplement de lier deux segments.



Faites attention à ces petites boîtes noires qui se vantent de repousser la limite de la longueur d'un segment au-delà de 185 mètres pour le Thinnet ou de 100 mètres pour le 10/100BaseT. Généralement, ces produits fonctionnent mais il vaut mieux respecter les règles.

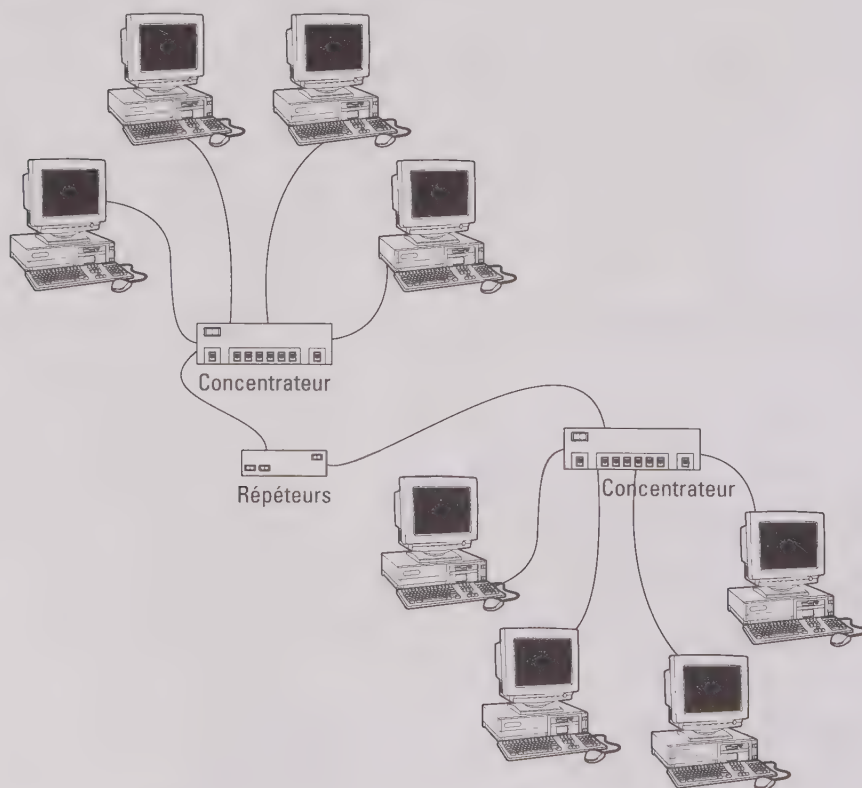


Figure 5.7 : Utilisation d'un répéteur.

Ponts

Un *pont* est un objet qui connecte deux réseaux pour qu'ils n'en forment plus qu'un. Les ponts sont utilisés dans le but de partitionner un grand réseau en deux plus petits pour une question de performances.



Un pont est une espèce de *répéteur intelligent*. Les répéteurs écoutent les signaux qui arrivent sur un câble du réseau, les amplifient puis les renvoient sur un autre câble. Ils procèdent à l'aveugle, sans prêter attention au contenu des messages qu'ils répètent.

Pour sa part, le pont est un répéteur qui manipule les messages plus intelligemment. Pour commencer, la plupart des ponts savent écouter le réseau et détecter automatiquement l'adresse des deux ordinateurs en communication. Ensuite, le pont peut inspecter chaque message qui lui parvient d'un côté et le diffuser si le message est destiné à un ordinateur situé de l'autre côté.

Cette fonctionnalité importante permet au pont de diviser un grand réseau en deux plus petits et plus efficaces. Les ponts fonctionnent mieux sur des réseaux très séparés. Ce serait, par exemple, le cas du service marketing et du service comptabilité, qui auraient chacun leur propre serveur.

Un pont peut partitionner le réseau afin que la partie du réseau réservée au marketing ne soit pas accaparée par la partie réservée à la comptabilité et inversement. Le pont apprend automatiquement à distinguer les ordinateurs appartenant à tel ou tel service et ne fait suivre les messages d'une partie du réseau vers l'autre que si cela s'avère nécessaire. On note une amélioration des performances générales des deux réseaux même si l'emploi d'un pont ralentit un peu le débit.

Voici quelques informations supplémentaires au sujet des ponts :

- ✓ Comme je l'ai déjà mentionné, certains ponts savent transformer le format des messages.
Par exemple, si les gens du marketing bâtissent leur réseau avec Ethernet et que ceux de la comptabilité ont recours au Token Ring, un pont peut relier les deux.
- ✓ Vous pouvez trouver un pont élémentaire pour partitionner deux réseaux Ethernet aux alentours de 400 euros. Des ponts plus évolués peuvent coûter 4 000 euros, voire plus.

Routeurs

Un *routeur* est une sorte de pont mais à une grande différence près : un pont utilise une adresse matérielle (appelée « adresse MAC ») pour savoir à

quel nœud du réseau est envoyé chaque message afin qu'il puisse le diriger vers le segment approprié. Un pont est cependant incapable d'examiner le contenu du message pour savoir quel type d'information est envoyé. Un routeur peut le faire. C'est pourquoi un routeur fonctionne à un niveau plus élevé que celui d'un pont. Il effectue d'autres tâches, comme le filtrage des paquets selon leur contenu. Notez que beaucoup de routeurs bénéficient en plus de fonctions de pontage intégrées, de sorte qu'ils peuvent aussi servir de pont.



Il est possible de configurer un réseau avec plusieurs routeurs travaillant en coopération les uns avec les autres. Par exemple, certains routeurs sont capables de surveiller le réseau afin de déterminer le chemin le plus rationnel pour envoyer des messages à destination. Si une partie du réseau est particulièrement occupée, le routeur saura choisir automatiquement un chemin moins encombré. Il agit un peu comme un hélicoptère de surveillance du trafic routier : s'il repère des ralentissements sur une branche de l'autoroute, il demandera au centre de régulation du trafic d'inciter les automobilistes à prendre une autre route.

Voici quelques informations complémentaires à propos des routeurs :

- ✓ Les routeurs étaient autrefois onéreux et réservés aux grands réseaux. Ces dernières années, le prix des petits routeurs a substantiellement chuté, ce qui les a banalisés même sur les petits réseaux.
- ✓ Les disparités fonctionnelles entre ponts et routeurs (et commutateurs et concentrateurs) tendent à s'amenuiser. Des *routeurs multifonctions*, qui sont à la fois routeur, pont, concentrateur et commutateur, prennent en charge toutes les tâches habituellement confiées à plusieurs périphériques.
- ✓ Certains routeurs ne sont rien de plus que des ordinateurs équipés de plusieurs cartes réseau et de logiciels assurant les fonctions de routage.
- ✓ Des routeurs peuvent connecter des réseaux géographiquement éloignés grâce à des lignes téléphoniques (DSL ou RNIS).
- ✓ L'une des principales raisons d'être des routeurs est la connexion d'un réseau local à Internet. La Figure 5.8 montre un routeur utilisé à cette fin.

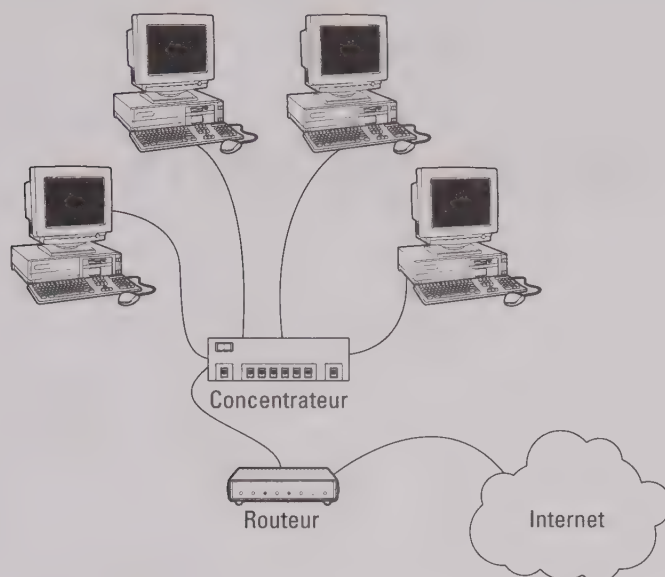


Figure 5.8 : Utilisation d'un routeur pour connecter un réseau local à Internet.

Chapitre 6

Protocole TCP/IP

Dans ce chapitre :

- ▶ S'initier au système binaire.
- ▶ Se familiariser avec les adresses IP.
- ▶ Découpage en sous-réseaux.
- ▶ Adresses IP publiques et privées.
- ▶ Traduction des adresses de réseau.
- ▶ Comprendre les bases du protocole DHCP.
- ▶ Découvrir le service DNS.

L'adressage IP est l'un des éléments fondamentaux du protocole TCP/IP. Chaque équipement, sur un réseau TCP/IP, doit avoir sa propre adresse IP. Dans ce chapitre, vous apprendrez de quoi il s'agit.



Ce chapitre est de loin le plus technique de ce livre. Nous étudierons le système binaire, nous détaillerons la structure des adresses IP et nous découvrirons le fonctionnement des sous-réseaux. Il n'est pas nécessaire d'avoir compris toutes les subtilités de l'adressage IP pour configurer un réseau TCP/IP simple. Mais si vous avez bien assimilé ce chapitre, la notion de protocole TCP/IP sera plus claire. Ceci dit, au travail !

Système binaire

Pour bien comprendre le principe de l'adressage IP, vous devez comprendre ce qu'est le système de numération binaire car il est le fondement de toute adresse IP. Si vous savez déjà de quoi il s'agit, vous pouvez sauter cette section et passer à la section « Adresses IP », plus loin dans ce chapitre. Je ne veux pas vous ennuyer avec ces notions vraiment élémentaires.

Compter avec des 1

Dans le système *binaire*, seuls deux chiffres sont utilisés : 0 et 1. Dans le système décimal, celui qui nous est familier, nous utilisons dix chiffres, de 0 à 9. Dans un nombre décimal ordinaire comme 3 482, le chiffre le plus à droite représente les unités, le chiffre situé juste à sa gauche les dizaines puis arrivent les centaines, les milliers et ainsi de suite. Ces chiffres sont tous des puissances de 10 : d'abord 10^0 (soit 1), puis 10^1 (10), puis 10^2 (100), puis 10^3 (1 000) et ainsi de suite.

En numération binaire, seuls deux chiffres sont utilisés au lieu de dix. C'est pourquoi un nombre binaire se présente d'une manière un peu particulière, comme 110011, 101111 ou 1000001.

La position d'un chiffre binaire (en informatique, il est appelé *bit*, contraction de l'anglais *binary digit*, chiffre binaire) représente une puissance de 2, d'où la progression 1, 2, 4, 8, 16, 32, etc. Pour représenter une valeur décimale sous une forme binaire, il faut multiplier chaque bit par sa puissance de 2 correspondante puis additionner tous ces résultats. Par exemple, la valeur décimale du nombre binaire 10101 est obtenue ainsi :

$$\begin{array}{rcl}
 1 \times 2^0 & = & 1 \times 1 = 1 \\
 + 0 \times 2^1 & = & 0 \times 2 = 0 \\
 + 1 \times 2^2 & = & 1 \times 4 = 4 \\
 + 0 \times 2^3 & = & 0 \times 8 = 0 \\
 + 1 \times 2^4 & = & 1 \times 16 = 16 \\
 \hline
 & & 21
 \end{array}$$

Fort heureusement, la conversion entre des nombres décimaux et binaires est un art dans lequel les ordinateurs excellent. En réalité, vous n'aurez jamais à faire vous-même ce genre de gymnastique intellectuelle. Comprendre le système binaire ne consiste pas à lire un nombre comme 1110110110110 et s'écrier instantanément : « 7606 en décimal ! » Mais si vous savez le faire, Barbara Walters se ferait sans doute une joie de vous interviewer et on tournerait même un film sur vous avec Dustin Hoffman et une vieille Buick.

En fait, il s'agit surtout pour vous d'acquérir des notions de base sur la manière dont les ordinateurs stockent les informations et, ce qui est plus important encore, de comprendre le principe du système hexadécimal, que nous aborderons dans la prochaine section.

Voici quelques caractéristiques intéressantes du système binaire, ainsi que ses similitudes et ses différences avec le système décimal :

- ✓ Le nombre de bits alloué à un nombre binaire détermine la grandeur de ce nombre. Si vous lui allouez 8 bits, la valeur la plus élevée qu'il peut représenter est 1111111, soit 255 en décimal.



Pour vous rendre compte rapidement du nombre de valeurs que peut représenter un nombre binaire d'une longueur donnée, utilisez le nombre de bits comme exposant de deux. Par exemple, un nombre de 8 bits contient 2^8 valeurs. Comme 2^8 est égal à 256, un nombre à 8 bits peut représenter 256 valeurs, de 0 à 255.

- ✓ C'est à cause de ces notions de puissance de 2 que la manière d'évaluer une taille de fichier ou la capacité d'un disque dur est un peu spéciale. En numération décimale, le kilo représente 1000. Mais en informatique (c'est-à-dire en numération binaire), le kilo représente 1024, c'est-à-dire 2^{10} . Par conséquent, un mégaoctet ne représente pas un million d'octets mais 1 048 576, c'est-à-dire 2^{20} .

Un peu de logique

L'un des grands avantages du système binaire est qu'il se prête particulièrement bien à des opérations spéciales appelées *opérations logiques*. Il existe quatre opérations logiques de base, auxquelles s'ajoutent d'autres opérations qui découlent des quatre opérations de base. Trois opérations logiques, ET, OU et XOR (appelé OU exclusif), servent à comparer deux nombres binaires (bits). La quatrième, NON, n'agit que sur un seul bit.

Voici une brève description des opérations logiques de base :

- ✓ **ET.** Une opération logique ET compare deux valeurs binaires. Si les deux sont 1, le résultat est 1. Si l'une des valeurs ou les deux sont 0, le résultat est 0.
- ✓ **OU.** Une opération logique OU compare deux valeurs binaires. Si au moins une des valeurs est 1, le résultat est 1. Si les deux valeurs sont 0, le résultat est zéro.
- ✓ **XOR.** Une opération logique OU exclusif compare deux valeurs binaires. Si exactement l'une d'entre elles est 1, le résultat est 1. Si les deux valeurs sont 0 ou si les deux sont 1, le résultat est 0.
- ✓ **NON.** Une opération logique NON ne compare pas deux valeurs mais change celle d'un chiffre binaire. Si la valeur d'origine est 1, NON renvoie 0. Si la valeur d'origine est 0, NON renvoie 1.

Les opérations logiques sont appliquées à des nombres binaires de plus d'un chiffre en appliquant l'opération à chacun de ses bits. La technique la plus simple est la suivante :

1. Superposez les deux nombres.
2. Écrivez le résultat des opérations logiques sous chacun des nombres binaires.



L'exemple ci-dessous montre le calcul de l'opération logique 10010100 ET 11011101 :

```
  10010100
ET 11011101
  10010100
```

Comme vous le constatez, le résultat est 10010100.

Se familiariser avec les adresses IP

Une *adresse IP* est un ensemble de chiffres qui identifie chaque hôte d'un réseau IP (*Internet Protocol*) d'une manière unique. Comme les adresses IP opèrent au niveau de la couche réseau de la pile du protocole TCP/IP, elles sont indépendantes des adresses MAC de la couche de liaison de données qui se trouve dessous (comme les adresses MAC Ethernet).

Une adresse IP est un nombre binaire de 32 bits. Cela signifie qu'il est possible de définir plus de quatre milliards d'adresses d'hôtes différentes sur Internet. Vous pourriez penser que c'est plus qu'il n'en faut mais le protocole TCP/IP impose certaines restrictions à l'allocation des adresses, qui limitent considérablement le nombre d'adresses IP utilisables. Aujourd'hui, environ la moitié de toutes les adresses IP disponibles a été attribuée. Toutefois, de nouvelles techniques ont réussi à contourner le problème. Un nouveau standard d'adresses IP codées sur 128 bits, appelé *IPv6*, est sur le point d'être adopté. Réseaux et hôtes

La principale fonction de l'IP, dont les initiales signifient « protocole Internet », est de permettre l'établissement des communications entre des réseaux. C'est pourquoi une adresse IP est composée de deux parties :

- ✓ **L'identifiant de réseau (ou ID de réseau ou adresse du réseau)** spécifie le réseau sur lequel un ordinateur hôte peut être trouvé.
- ✓ **L'identifiant d'hôte (ou ID d'hôte ou adresse de l'hôte)** spécifie un périphérique présent sur le réseau selon son identifiant de réseau.

La complexité d'une adresse IP provient surtout du fait qu'il est difficile de déterminer, parmi ses 32 bits, ceux qui appartiennent à l'ID de réseau et ceux qui appartiennent à l'ID d'hôte. Un nouveau système, appelé *adresses IP sans classe*, est en train de supplanter le système à classes d'adresses. Nous reviendrons sur ces deux notions plus tard dans ce chapitre.

Décimales pointées

Une adresse IP est usuellement représentée sous une forme appelée *notation décimale pointée*. Grâce à cette notation, chaque groupe de huit bits, appelé *octet*, est représenté par son équivalent décimal. Prenons par exemple cette adresse IP :

```
11000000101010001000100000011100
```

L'équivalent en notation décimale pointée est :

```
192.168.136.28
```

Dans ce nombre, 192 représente les huit premiers bits (11000000), 168 le deuxième ensemble de huit bits (10101000), 136 le troisième ensemble de huit bits (10001000) et 28 le dernier ensemble de huit bits (00011100). Ce format est celui dans lequel les adresses IP sont généralement représentées.

Classes d'adresses IP

Quand les concepteurs du protocole IP ont développé le système de représentation de l'adressage IP, ils auraient pu affecter un nombre de bits arbitraire à un ID de réseau. Les bits restants auraient été affectés à l'ID d'hôte. Supposons par exemple que les concepteurs aient décidé que la moitié de l'adresse (16 bits) devait être utilisée pour le réseau et l'autre moitié (16 bits) pour l'ID d'hôte. Il en aurait résulté qu'Internet n'aurait pu comporter que 65 536 réseaux, chaque réseau ayant 65 536 hôtes.

Au commencement d'Internet (à la fin des années 1960), ces chiffres auraient semblé plusieurs fois supérieurs aux besoins présents et à venir. Les concepteurs du protocole IP ont réalisé, dès le début, que peu de réseaux comporteraient des dizaines de milliers d'hôtes. Supposons qu'un réseau de mille ordinateurs se connecte à Internet et qu'il reçoive l'un de ces ID de réseau. Comme ce réseau n'utiliserait qu'un millier des 65 536 adresses d'hôtes, les 64 536 autres, non utilisées, seraient gaspillées.

C'est pour résoudre ce problème que la notion de *classe d'adresse* fut introduite. Le protocole IP définit cinq classes d'adresses : A, B, C, D et E. Pour les trois premières, de A à C, la taille des parties d'adresse réservées aux ID réseau et hôte est différente. La classe D est un type d'adresse spécial appelé *multidestinataire*. La classe E est une classe d'adresse expérimentale qui n'est pas utilisée.

Les quatre premiers bits d'une adresse IP sont utilisés pour déterminer la classe à laquelle appartient une adresse :

- ✓ Si le premier bit est à 0, l'adresse est de classe A.
- ✓ Si le premier bit est à 1 et le deuxième à 0, l'adresse est de classe B.
- ✓ Si les deux premiers bits sont à 1 et le troisième à 0, l'adresse est de classe C.
- ✓ Si les trois premiers bits sont à 1 et le quatrième à 0, l'adresse est de classe D.
- ✓ Si les quatre premiers bits sont à 1, l'adresse est de classe E.

Les classes D et E étant réservées à des usages particuliers, le reste de la discussion sera exclusivement consacré aux adresses de classes A, B et C. Le Tableau 6.1 récapitule les caractéristiques de chacune d'elles.

Tableau 6.1 : Classes d'adresses IP.

Classe	Plage d'adresses	Bits de début	Longueur de l'ID réseau	Nombre de réseaux	Nombre d'hôtes
A	1 à 126.x.y.z	0	8	126	16777214
B	128 à 191.x.y.z	10	16	16384	65534
C	192 à 223.x.y.z	110	24	2097152	254

Adresses de classe A

Les adresses de classe A sont conçues pour des réseaux de très grande taille. Dans cette classe, le premier octet de l'adresse est l'identifiant de réseau, les trois autres octets sont ceux de l'identifiant d'hôte. Du fait que huit bits seulement sont alloués à l'ID de réseau et que le premier de ces bits indique que l'adresse est de classe A, seuls 126 réseaux de classe A peuvent exister sur la totalité d'Internet. En revanche, chaque réseau de classe A peut recevoir plus de 16 millions d'hôtes.



Seules 40 adresses de classe A sont actuellement attribuées à des entreprises ou à des organisations. Les autres sont soit réservées à l'usage de l'IANA (*Internet Assigned Numbers Authority*), soit affectées à des organisations qui gèrent les assignations d'adresses IP pour des régions géographiques comme l'Europe, l'Asie et l'Amérique latine.

Le Tableau 6.2 recense quelques sociétés possédant des adresses de classe A. Certaines sont très connues, d'autres moins. Si le sujet vous intéresse, vous trouverez toutes les assignations d'adresses sur le site www.iana.org/assignments/ipv4-address-space.

Tableau 6.2 : Quelques réseaux de classe A.

Réseau	Description	Réseau	Description
3	General Electric Company	20	Computer Sciences Corporation
6	Army Information Systems Center	22,26,	
29, 30	Defense Information Systems Agency		
9	IBM	34	Halliburton Company
11	DoD Intel Information Systems	38	Performance Systems International
12	AT&T Bell Laboratories	40	Eli Lilly and Company
13	Xerox Corporation	43	Administered by APNIC
15	Hewlett-Packard Company	45	Interop Show Network
16	Digital Equipment Corporation	47	Bell-Northern Research
17	Apple Computer, Inc.	48	Prudential Securities Inc.
18	MIT	54	Merck and Co., Inc.
19	Ford Motor Company	56	U.S. Postal Service

Adresses de classe B

Dans une adresse de classe B, les deux premiers octets de l'adresse IP sont utilisés comme identifiant de réseau, les deux autres comme identifiant d'hôte. Par conséquent, les adresses de classe B se rapprochent de la représentation consistant à scinder l'adresse en deux, une moitié étant utilisée pour l'ID de réseau, l'autre pour l'ID d'hôte. La représentation n'est toutefois pas complète car les deux premiers bits du premier octet doivent être à 1 et 0 pour indiquer que l'adresse est de classe B. De ce fait, 16 384 réseaux de classe B peuvent exister. Toutes les adresses de classe B se trouvent dans la plage de 128.x.y.z à 191.x.y.z. Une adresse de classe B peut recevoir jusqu'à 65 000 hôtes.

Le problème avec les réseaux de classe B est qu'en dépit de leur taille inférieure à celle de ceux de classe A, ils allouent de trop nombreux ID d'hôtes. Très peu de réseaux en comportent des dizaines de milliers. C'est pourquoi une assignation sans discernement d'adresses de classe B peut entraîner un gaspillage d'adresses d'hôtes par les organisations qui ne les utilisent pas.



Adresses de classe C

Dans une adresse de classe C, les trois premiers octets sont utilisés pour l'identifiant de réseau et le quatrième pour l'identifiant d'hôte. Ce dernier n'ayant que huit bits, chaque réseau de classe C ne peut recevoir que 254 hôtes. Toutefois, grâce à l'ID de réseau de 24 bits, les adresses de classe C autorisent jusqu'à 2 millions de réseaux.



Le problème des réseaux de classe C est leur petite taille. Bien que peu d'organisations aient besoin des dizaines de milliers d'adresses hôtes que fournit une adresse de classe C, beaucoup d'organisations en requièrent quelques centaines. Ce vaste écart entre les réseaux de classe B et de classe C a entraîné le développement de *sous-réseaux*, sujet abordé dans la prochaine section.

Où en est l'IPv6 ?

La plus grande partie d'Internet est actuellement basée sur la version 4 d'Internet Protocol, appelée IPv4. Elle a rendu de bons et loyaux services pendant plus de vingt ans mais l'expansion du « réseau des réseaux » a démontré les limites d'un adressage sur 32 bits. Ce chapitre est consacré aux évolutions de l'IPv4 pour utiliser au mieux cet adressage mais il est certain qu'à relativement brève échéance l'espace d'adressage de l'IPv4 sera saturé. D'ici là, Internet devra migrer vers la prochaine version d'Internet Protocol : IPv6.

IPv6 est aussi appelé *IP next generation* (IP de prochaine génération) ou *IPng*, en hommage à *Star Trek : The Next Generation*.

IPv6 offre bien des avantages par rapport à IPv4, le plus important étant un adressage Internet sur 128 bits au lieu de 32. Le nombre d'adresses autorisées est si élevé que même les « mille milliards de tonnes de Brest » du Capitaine Haddock seraient loin du compte. Je vous livre ce nombre rien que pour mettre vos neurones à l'épreuve :

340282366920938463463374607431768211456

Ce nombre défie l'entendement. Si l'IANA s'était mis en devoir d'attribuer des adresses IPv6 dès la création de l'univers, au moment du big bang (qui aurait eu lieu il y a quinze milliards d'années) et ce à raison de mille adresses par seconde, moins de 1% des adresses disponibles serait alloué aujourd'hui.

La transition de l'IPv4 vers l'IPv6 n'est pas très rapide. Pendant quelques années encore, l'IPv4 continuera de régir Internet.

Découpage en sous-réseaux

Le découpage en sous-réseaux ou *sous-réseautage* est une technique qui permet à l'administrateur réseau d'utiliser plus efficacement les 32 bits d'une adresse Internet afin de créer des réseaux capables de s'affranchir des limites imposées par les adresses IP de classes A, B et C. Il est ainsi possible de créer des réseaux dont le nombre d'hôtes est mieux adapté aux besoins.

Le découpage en sous-réseaux procure plus de souplesse dans la définition de la partie de l'adresse IP qui représente l'identifiant de réseau et de celle qui représente l'identifiant d'hôte. Les classes d'adresses IP standard ne proposent que trois tailles : 8 bits pour la classe A, 16 bits pour la classe B et 24 bits pour la classe C. Le découpage en sous-réseaux permet de sélectionner arbitrairement le nombre de bits utilisables par l'ID de réseau.

Deux raisons militent en faveur du découpage en sous-réseaux. La première est l'allocation plus efficace de l'espace d'adressage IP. Si Internet était limité aux adresses des classes A, B et C, chaque réseau se verrait attribuer 254, 65 000 ou 16 millions d'adresses IP pour ses équipements hôtes. Bien que les réseaux à plus de 254 périphériques soient nombreux, ceux à 65 000 périphériques le sont beaucoup moins, sans parler des réseaux qui en comptent 16 millions. Malheureusement, tout réseau qui franchirait (de si peu soit-il) la barre des 254 périphériques devrait recevoir une allocation de classe B, ce qui entraînerait un gaspillage de dizaines de milliers d'adresses IP.

La seconde raison qui justifie le découpage en sous-réseaux est que, même si une organisation possède des milliers de périphériques de réseau, les faire fonctionner avec un même ID de réseau ralentirait terriblement le fonctionnement du réseau. Le protocole TCP/IP impose que tous les ordinateurs ayant un même identifiant de réseau soient présents sur le même réseau physique. Le réseau physique comprend un seul *domaine de diffusion*, ce qui signifie qu'une seule installation doit véhiculer tout le trafic du réseau. Pour améliorer les performances, les réseaux sont généralement divisés en domaines de diffusion bien plus petits que l'espace d'adressage d'une classe C.

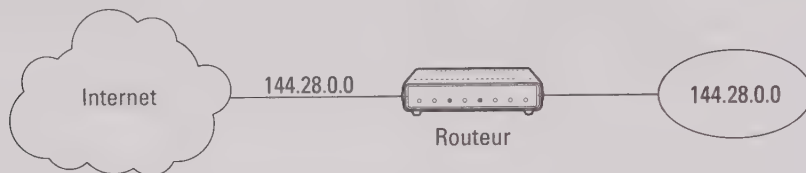
Sous-réseaux

Un *sous-réseau* est un réseau qui fait partie d'un autre réseau (de classe A, B ou C). Les sous-réseaux sont créés en utilisant un ou plusieurs bits d'un hôte de classe A, B ou C pour étendre l'identifiant de réseau. Par conséquent, plutôt que d'avoir un identifiant de réseau standard de 8, 16 ou 24 bits, un sous-réseau peut avoir un identifiant de n'importe quelle longueur.

La Figure 6.1 montre un exemple de réseau avant et après le découpage en sous-réseaux. Dans le réseau découpé, le réseau a reçu l'adresse de classe B

144.28.0.0. Tous les périphériques de ce réseau doivent partager le même domaine de diffusion.

Avant le découpage en sous-réseaux



Après le découpage en sous-réseaux

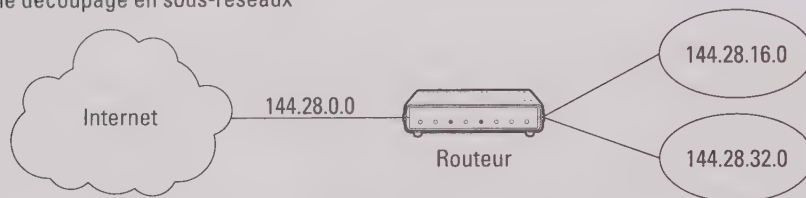


Figure 6.1 : Présentation d'un réseau avant et après son découpage en sous-réseaux.

Dans le second réseau, les quatre premiers bits de l'identifiant d'hôte sont utilisés pour diviser le réseau en deux petits réseaux, identifiés comme sous-réseaux 16 et 32. Dans le monde extérieur, c'est-à-dire de l'autre côté du routeur, ces deux réseaux apparaissent comme un seul réseau identifié par l'adresse IP 144.28.0.0. Par exemple, pour le monde extérieur, le périphérique à l'adresse 144.28.16.22 appartient au réseau 144.28.0.0. Par conséquent, un paquet envoyé à ce périphérique sera délivré au routeur avec l'adresse 144.28.0.0. Le routeur considère ensuite la partie sous-réseau de l'identifiant d'hôte pour décider d'acheminer le paquet vers le sous-réseau 16 ou vers le sous-réseau 32.

Masques de sous-réseau

Pour qu'un sous-réseau fonctionne, le routeur doit savoir quelle partie de l'identifiant d'hôte il doit utiliser pour l'identifiant de réseau du sous-réseau. Ce petit tour de passe-passe est accompli par un autre nombre de 32 bits appelé *masque de sous-réseau*. Ces bits d'adresse IP qui représentent l'ID de réseau sont représentés par un 1 dans le masque et ceux qui représentent l'ID d'hôte par un 0. Il en résulte qu'un masque de sous-réseau est toujours formé d'une chaîne de 1 à gauche, suivie d'une chaîne de zéros.

Par exemple, le masque de sous-réseau, dans lequel l'ID de réseau est constitué des 16 bits de l'ID de réseau, auxquels s'ajoute un ID de sous-réseau supplémentaire de 4 bits, se présenterait ainsi :

```
11111111 11111111 11110000 00000000
```

En d'autres termes, les 20 premiers bits sont des 1 et les 12 bits restants des 0. Par conséquent, la longueur de l'ID de réseau complet est de 20 bits, la longueur de la véritable partie de l'ID de l'hôte de l'adresse de sous-réseau étant de 12 bits.

Pour déterminer l'identifiant de réseau d'une adresse IP, le routeur doit connaître à la fois l'adresse IP et le masque de sous-réseau. Il effectue ensuite, sur l'adresse IP, une opération au niveau des bits appelée *ET logique*, destinée à extraire l'identifiant de réseau. À cette fin, chaque bit de l'adresse IP est comparé au bit correspondant du masque de sous-réseau. Si les deux sont à 1, le bit de l'ID de réseau sera mis à 1. Si les deux bits sont à 0, le résultat est mis à 0.

Voici, par exemple, comment l'adresse de réseau est extraite d'une adresse IP à l'aide du masque de sous-réseau de 20 bits de l'exemple précédent :

	144	.	28	.	16	.	17
Adresse IP :	10010000		00011100		00100000		00001001
Masque de sous-réseau :	11111111		11111111		11110000		00000000
Identifiant de réseau :	10010000		00011100		00100000		00000000
	144	.	28	.	16	.	0

Résultat : l'ID de réseau de ce sous-réseau est 144.28.16.0.

Le masque de sous-réseau lui-même est généralement représenté en notation décimale pointée. Il en résulte que le masque de sous-réseau de 20 bits de l'exemple précédent sera représenté sous la forme 255.255.240.0 :

Masque de sous-réseau :	11111111		11111111		11110000		00000000
	255	.	255	.	240	.	0



Ne confondez pas un masque de sous-réseau avec une adresse IP. Un masque de sous-réseau ne représente aucun périphérique ou réseau sur Internet. C'est juste une manière d'indiquer quelle partie de l'adresse IP doit être utilisée pour déterminer l'identifiant de réseau. Il est facile de repérer à coup sûr un masque de sous-réseau car le premier octet est toujours à 255. Or, 255 n'est pas un premier octet valide pour une classe d'adresse IP.

Limites des sous-réseaux

Vous devez connaître les quelques restrictions que subissent les masques de sous-réseaux, notamment :

- ✓ Le nombre minimum de bits d'un identifiant de sous-réseau est 8. Par conséquent, le premier octet d'un masque de sous-réseau est toujours 255.
- ✓ Le nombre maximum de bits d'un identifiant de sous-réseau est 30. Vous devez réserver au moins deux bits de la partie de l'identifiant d'hôte, dans l'adresse, afin d'autoriser au moins deux hôtes. Si vous utilisiez tous les 32 bits pour l'ID de réseau, il n'en resterait aucun pour l'ID d'hôte. Il va de soi que cela ne fonctionnerait pas. Ne laisser qu'un seul bit pour l'ID d'hôte ne fonctionnerait pas non plus. En effet, un ID d'hôte, composé uniquement de 1, est réservé pour l'adresse de diffusion, tandis que s'il ne comporte que des 0, il se réfère au réseau lui-même. C'est pourquoi, si vous utilisiez 31 bits pour l'ID de réseau en n'en laissant qu'un seul pour l'ID d'hôte, l'ID d'hôte 1 serait attribué à l'adresse de diffusion tandis que l'ID d'hôte 0 serait le réseau lui-même, ne laissant plus de place pour de véritables hôtes. Voilà pourquoi la taille maximale de l'ID de réseau est limitée à 30 bits.
- ✓ Puisqu'un ID de réseau est toujours composé d'une succession de bits mis à 1, neuf valeurs seulement sont possibles pour chacun des octets d'un masque de sous-réseau, en comptant le 0. Ces valeurs sont représentées dans le Tableau 6.3.

Tableau 6.3 : Les neuf valeurs des octets de sous-réseau.

<i>Octet binaire</i>	<i>Décimal</i>	<i>Octet binaire</i>	<i>Décimal</i>
00000000	0	11111000	248
10000000	128	11111100	252
11000000	192	11111110	254
11100000	224	11111111	255
11110000	240		

Adresses privées et adresses publiques

Tout hôte directement connecté à Internet doit avoir une adresse IP globalement unique. Tous les hôtes ne sont cependant pas directement connectés

à Internet. Certains sont cachés derrière un pare-feu, ainsi leur connexion à Internet est indirecte.

Plusieurs blocs d'adresses IP sont mis de côté à cette fin. Ils sont destinés à être utilisés sur des réseaux privés qui ne sont pas connectés à Internet ou sur des réseaux cachés derrière un pare-feu. Il existe trois plages de telles adresses, récapitulées dans le Tableau 6.4. Dès que vous créez un réseau TCP/IP privé, vous devriez utiliser une adresse de l'une de ces plages.

Tableau 6.4 : Espaces d'adressage privé.

<i>CIDR</i>	<i>Masque de sous-réseau</i>	<i>Plage d'adressage</i>
10.0.0.0/8	255.0.0.0	10.0.0.1 à 10.255.255.254
172.16.0.0/12	255.255.240.0	172.16.1.1 à 172.31.255.254
192.168.0.0/16	255.255.0.0	192.168.0.1 à 192.168.255.254

Comprendre la traduction des adresses de réseau

De nombreux pare-feu font appel à une technique appelée *NAT* (*Network Address Translation*, traduction d'adresse de réseau) pour cacher la véritable adresse IP d'un hôte au monde extérieur. Dans ce cas de figure, le périphérique NAT doit utiliser une adresse IP globalement unique qui représente l'hôte sur Internet mais, derrière le pare-feu, l'hôte peut utiliser n'importe quelle adresse IP. Lorsqu'un paquet franchit le pare-feu, le périphérique NAT traduit l'adresse IP privée en adresse IP publique et inversement.

L'un des avantages du NAT est qu'il réduit la fréquence à laquelle l'espace d'adressage IP est assigné car un périphérique NAT ne peut utiliser qu'une seule adresse IP publique pour plus d'un hôte. Pour cela, il garde une trace des paquets sortants afin de pouvoir faire correspondre les paquets entrants avec l'hôte approprié. Pour comprendre comment tout cela fonctionne, examinons les étapes suivantes :

1. Un hôte dont d'adresse privée est 192.168.1.100 envoie une requête vers 216.239.57.99, qui est l'adresse de www.google.com. Le périphérique NAT convertit l'adresse IP source du paquet en 208.23.110.22, qui est l'adresse du pare-feu. De cette manière, Google renverra sa réponse au routeur pare-feu. Le NAT enregistre que 192.168.1.100 a envoyé une requête à 216.239.57.99.

2. À présent, un autre hôte à l'adresse 192.168.1.107 envoie une requête à 207.46.134.190 qui est l'adresse de `www.microsoft.com`. Le périphérique convertit l'adresse IP source de la requête en 208.23.110.22 afin que Microsoft puisse répondre au routeur pare-feu. Le NAT enregistre que 192.168.1.107 a envoyé une requête à 207.46.134.190.
3. Quelques secondes plus tard, le pare-feu reçoit une réponse de 216.239.57.99. Dans cette réponse, l'adresse du destinataire est 208.23.110.22, l'adresse du pare-feu. Pour déterminer à qui il doit acheminer la réponse, le pare-feu vérifie ses enregistrements afin de savoir qui attend une réponse de 216.239.57.99. Il découvre que c'est 192.168.1.100. Par conséquent, il remplace l'adresse de destination par 192.168.1.100 et transmet le paquet.

À vrai dire, le processus est un peu plus compliqué que cela car il est fort probable que plusieurs utilisateurs attendent chacun une réponse de la même adresse IP publique. Dans ce cas, le périphérique NAT a recours à d'autres techniques pour déterminer vers quel utilisateur un paquet entrant doit être acheminé.

Configurer le réseau pour le service DHCP

Sur un réseau TCP/IP, chaque hôte doit avoir une adresse IP unique et être correctement configuré afin qu'il la connaisse. Lorsqu'un nouvel hôte se connecte, il doit recevoir une adresse IP correcte (c'est-à-dire qui n'a pas encore été attribuée), comprise dans la plage d'adresses du sous-réseau. Bien qu'il soit possible d'affecter manuellement des adresses IP à chacun des ordinateurs du réseau, cette tâche devient rapidement ingérable dès que le réseau compte beaucoup de machines.

C'est là qu'intervient le service *DHCP* (Dynamic Host Configuration Protocol, protocole de configuration dynamique de l'hôte). Il configure automatiquement l'adresse IP de chaque hôte d'un réseau, garantissant ainsi que son adresse est valide et unique. Le service DHCP parvient même à configurer les adresses selon que des hôtes se connectent ou se déconnectent. Comme vous l'imaginez, le DHCP peut faire gagner à l'administrateur de précieuses heures de travail de configuration.

Dans cette section, vous apprendrez les tenants et les aboutissants du DHCP : de quoi il s'agit, comment il fonctionne et comment le configurer.

Comprendre le DHCP

Le service DHCP permet à chacun des ordinateurs d'un réseau TCP/IP d'obtenir d'un serveur ses données de configuration (notamment son adresse IP).

Le serveur DHCP conserve une trace des adresses IP déjà attribuées, de sorte que si un ordinateur en demande une, le serveur puisse lui affecter une adresse IP libre.

L'alternative au DHCP consiste à attribuer à chaque ordinateur du réseau une *adresse IP statique* :



- ✓ Les adresses IP statiques sont parfaites pour les réseaux ne comportant qu'un très petit nombre d'ordinateurs.

Dès que ce nombre augmente, cette solution n'est plus du tout adaptée. Si un administrateur pas très bien réveillé attribue la même adresse IP à deux ordinateurs, vous devrez contrôler manuellement l'adresse IP de chaque machine pour découvrir le conflit. C'est pourquoi le service DHCP est incontournable, sauf pour les très petits réseaux.

Bien que la tâche principale du DHCP consiste à attribuer des adresses IP, le service DHCP peut fournir plus d'informations à ses clients que cette adresse. Ces informations complémentaires sont appelées *options DHCP*. En voici quelques-unes :

- ✓ L'adresse du routeur, appelée aussi adresse de la passerelle par défaut.
- ✓ La durée avant expiration de l'information par défaut.
- ✓ Le nom du domaine.
- ✓ L'adresse du serveur DNS.
- ✓ L'adresse du serveur WINS.

Serveurs DHCP

Un serveur DHCP peut être un ordinateur serveur situé sur le réseau TCP/IP. Fort heureusement, tous les systèmes d'exploitation des serveurs modernes sont équipés de fonctionnalités de serveur DHCP. Pour configurer le service DHCP sur un serveur de réseau, il suffit d'activer sa fonction DHCP et de configurer ses paramètres. Dans l'une des prochaines sections intitulée « Gérer un serveur DHCP sous Windows Server 2008 », je vous montre comment configurer un serveur DHCP sous Windows Server 2008.

Il n'est pas nécessaire qu'un serveur hébergeant le service DHCP soit uniquement dédié à cette tâche, à moins que le réseau ne soit très étendu. Dans la plupart des cas, un serveur de fichiers peut aussi faire office de serveur DHCP. C'est notamment vrai lorsque les adresses IP sont fournies pour un bail à long terme (la notion de *bail* sera développée dans la section « Quelle durée de bail ? », plus loin dans ce chapitre).

Beaucoup de routeurs multifonctions sont équipés de serveurs DHCP intégrés. C'est pourquoi, si vous ne désirez pas surcharger l'un de vos serveurs de réseau en lui confiant les fonctions DHCP, vous activerez le serveur intégré au routeur. L'avantage de cette solution est qu'il est rarement nécessaire d'éteindre le routeur. En revanche, il vous arrivera parfois de devoir redémarrer un serveur de fichiers pour des raisons de maintenance, pour appliquer une mise à jour ou le dépanner.



La plupart des réseaux exigent seulement un serveur DHCP. La mise en œuvre de deux serveurs ou plus sur le même réseau exige que vous coordonniez soigneusement la plage d'adresses IP affectée à chacun des serveurs. Si vous installez accidentellement deux serveurs DHCP avec la même étendue, vous risquez d'attribuer aux machines qui se connectent des adresses en double. Pour éviter ce problème, installez un seul serveur DHCP, à moins que votre réseau soit si grand qu'un seul serveur ne puisse suffire.

Comprendre les étendues

Une *étendue* est une plage d'adresses IP pour laquelle le serveur DHCP a été configuré et qu'il peut attribuer. Dans le cas le plus élémentaire, où un seul serveur DHCP supervise la configuration IP de la totalité d'un sous-réseau, l'étendue correspond au sous-réseau. Mais si deux serveurs DHCP ont été configurés pour un sous-réseau, vous pouvez configurer chacun d'eux avec une étendue qui n'alloue qu'une partie de la plage complète des adresses IP du sous-réseau. De plus, un seul serveur DHCP peut servir plus d'une étendue.

Vous devez paramétrer l'étendue avant d'activer le serveur DHCP. Au cours de ce paramétrage, vous pouvez définir les propriétés suivantes :

- ✓ Un **nom d'étendue** qui facilite son identification et indique sa fonction.
- ✓ La **description de l'étendue** qui permet de détailler sa fonction.
- ✓ L'**adresse IP de début** de l'étendue.
- ✓ L'**adresse IP de fin** de l'étendue.
- ✓ Un **masque de sous-réseau** pour l'étendue. Il peut être spécifié en notation décimale pointée ou en notation CIDR.
- ✓ Une ou plusieurs **plages d'adresses exclues**. Ces adresses seront toujours affectées à un périphérique hôte particulier (pour plus de détails, reportez-vous à la prochaine section « Sentiment d'exclusion ? »).
- ✓ Une ou plusieurs **adresses réservées**. Ce sont des adresses qui seront toujours affectées à des périphériques hôtes particuliers (pour en savoir plus, reportez-vous à la section « Réservations recommandées », plus loin dans ce chapitre).

- ✓ La **durée du bail** qui indique la durée pendant laquelle l'hôte est autorisé à utiliser l'adresse IP. Le client tentera de renouveler le bail lorsque la moitié de sa durée sera écoulée. Par exemple, si vous définissez un bail de huit jours, le client tentera de le renouveler au bout de quatre jours. Cela laisse à l'hôte beaucoup de temps pour renouveler le bail avant que l'adresse soit réaffectée à un autre hôte.
- ✓ L'**adresse du routeur** pour le sous-réseau. Cette valeur est appelée *adresse de la passerelle par défaut*.
- ✓ Le **nom de domaine et l'adresse IP** des serveurs DNS du réseau et des serveurs WINS.

Sentiment d'exclusion ?

Nous nous sommes tous sentis exclus à un moment de notre existence (avec une femme et trois filles, j'en sais quelque chose...). Mais c'est parfois une bonne chose. Dans le cas des étendues DHCP, les exclusions peuvent vous aider à prévenir des conflits d'adresses IP et vous permettre de répartir la charge de travail DHCP d'un seul sous-réseau entre plusieurs serveurs DHCP.

Une *exclusion* est une plage d'adresses qui n'est pas comprise dans l'étendue mais qui se trouve néanmoins entre son adresse de début et celle de fin. Une plage d'exclusion est comme une enclave dans l'étendue : toutes les adresses qui s'y trouvent ne seront pas attribuées.

Voici quelques raisons justifiant l'exclusion d'adresses IP de l'étendue :

- ✓ L'**adresse IP de l'ordinateur qui régit le service DHCP doit généralement être statique**. Par conséquent, l'adresse du serveur DHCP doit toujours être listée comme une exclusion.
- ✓ **Des adresses IP ont peut-être été affectées à d'autres serveurs**. Dans ce cas, chaque adresse IP de serveur doit être listée comme une exclusion.

Les réservations sont cependant une meilleure solution à ce problème, comme nous le verrons dans la prochaine section.



Réservations recommandées

Dans certains cas, vous voudrez affecter une adresse IP spécifique à un hôte donné. Une option consiste à configurer l'hôte avec une adresse IP statique afin qu'il n'utilise pas le service DHCP pour obtenir la configuration IP. Elle présente toutefois deux inconvénients majeurs :

- ✓ **La configuration TCP/IP ne se contente pas de fournir l'adresse IP.** Si vous utilisez une configuration statique, vous devez spécifier manuellement le masque de sous-réseau, l'adresse de la passerelle par défaut, l'adresse du serveur DNS et d'autres informations requises par l'hôte. Si une information change, vous devrez non seulement la modifier au niveau du serveur DHCP mais aussi au niveau de chaque hôte dont la configuration est statique.
- ✓ **Vous devez garder en tête d'exclure l'adresse IP statique de l'étendue du serveur DHCP.** Dans le cas contraire, le serveur DHCP ne saurait pas que cette adresse est statique et pourrait l'affecter à un autre hôte, d'où un épineux problème : deux hôtes sur le réseau dont l'adresse est identique.



Un meilleur moyen d'affecter une adresse IP fixe à un hôte consiste à créer une *réserve* DHCP : dès qu'un hôte particulier demande une adresse IP au serveur DHCP, ce dernier lui fournit l'adresse spécifiée dans la réserve. L'hôte ne recevra pas l'adresse IP avant de l'avoir demandée au serveur DHCP mais quand il le fera, il recevra toujours la même adresse.

Pour créer une réserve, vous associez l'adresse IP à affecter à l'hôte à l'adresse MAC de l'hôte. Vous devez obtenir l'adresse MAC de la part de l'hôte avant de créer la réserve.

- ✓ Pour ce faire, exécutez la commande `ipconfig /all` à partir de l'invite.
- ✓ Si cette action échoue parce que le protocole TCP/IP n'a pas encore été configuré sur l'ordinateur, vous trouverez l'adresse MAC dans les informations du système.

Exécutez Démarrer/Tous les programmes/Accessoires/Outils système/Informations système.



Si vous installez plus d'un serveur DHCP, vérifiez que chaque serveur possède les mêmes réserves. Si vous oubliez de répéter une réserve sur un des serveurs, celui-ci risque de l'attribuer à une machine qui se connectera.

Quelle durée de bail ?

L'une des décisions les plus importantes que vous aurez à prendre, quand vous configurerez un serveur DHCP, est la durée que vous accorderez au bail. La valeur par défaut est de huit jours, ce qui est généralement approprié. Mais, dans certains cas, vous opterez pour une durée plus longue ou plus courte.

- ✓ Plus le réseau est stable, plus le bail peut être long. Si de nouveaux ordinateurs ne sont ajoutés au réseau que de temps en temps (parfois pour en remplacer d'autres), la durée du bail peut excéder huit jours en toute sécurité.
- ✓ Plus le réseau est instable, plus le bail doit être court. Imaginez par exemple un réseau sans fil dans une bibliothèque universitaire fréquentée par des étudiants qui apportent leurs ordinateurs portables pour ne travailler que quelques heures. Pour un réseau de ce genre, un bail d'une heure est approprié.

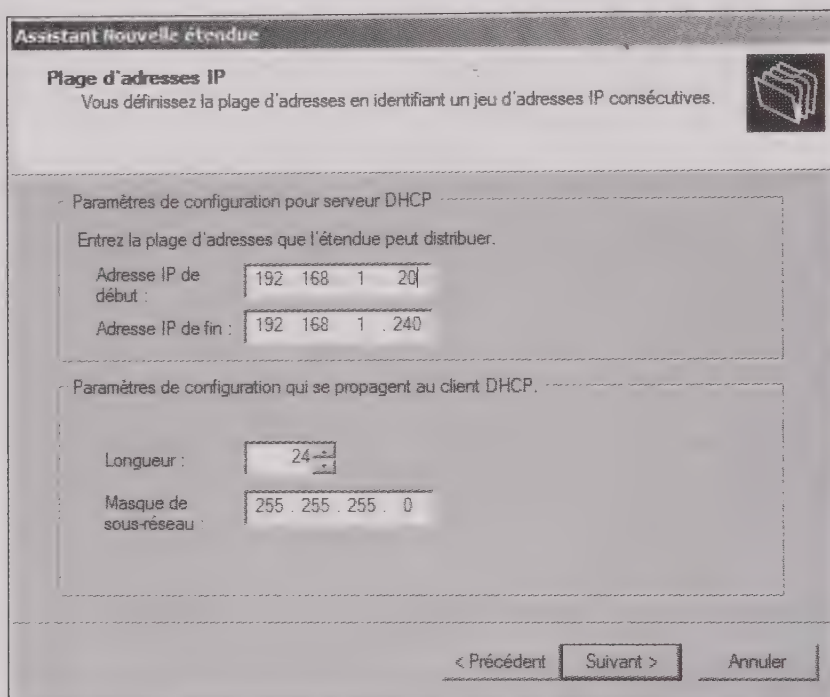


Ne configurez jamais une durée de bail illimitée. Bien que des administrateurs estiment que cette option réduit la charge de travail sur un serveur DHCP stable, aucun réseau n'est stable en permanence. Chaque fois que vous rencontrez un serveur DHCP configuré avec des baux infinis, recherchez les baux actifs : vous trouverez assurément des adresses IP attribuées à des ordinateurs qui n'existent plus.

Gérer un serveur DHCP sous Windows Server 2008

Les étapes à suivre pour configurer et gérer un serveur DHCP dépendent du système d'exploitation réseau ou du routeur utilisé. Les procédures qui suivent montrent comment travailler avec un serveur DHCP sous Windows Server 2008. Les procédures sont similaires pour les autres systèmes d'exploitation.

Si vous n'avez pas encore installé le serveur DHCP sur votre serveur, démarrez l'application Gestionnaire de serveur (sélectionnez Démarrer/Outils d'administration/Gestionnaire de serveur), cliquez sur Ajouter des rôles, sélectionnez Serveur DHCP dans la liste des rôles puis cliquez sur Suivant jusqu'à la page Ajouter ou modifier les étendues DHCP. Cliquez sur Ajouter afin de créer la première étendue du serveur DHCP. Pour ce faire, entrez le nom et la description de l'étendue ainsi que les informations d'adresse IP de base de l'étendue, dans la boîte de dialogue Ajouter une étendue, illustrée par la Figure 6.2.



Assistant Nouvelle étendue

Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début : 192.168.1.20

Adresse IP de fin : 192.168.1.240

Paramètres de configuration qui se propagent au client DHCP

Longueur : 24

Masque de sous-réseau : 255.255.255.0

< Précédent Suivant > Annuler

Figure 6.2 : Spécification de la plage d'adresses de l'étendue et du masque de sous-réseau.

Après avoir entré les adresses de début et de fin de la plage ainsi que le masque de sous-réseau, cliquez sur Suivant. L'assistant demande aussi les adresses à exclure de l'étendue, la durée du bail (6 jours, par défaut), l'adresse IP de votre routeur de passerelle, le nom de domaine du réseau et les adresses IP des serveurs DNS qui seront utilisés par les ordinateurs clients. Les tâches de l'assistant terminées, le serveur DHCP est correctement configuré. Il ne démarrera toutefois pas avant que vous l'ayez autorisé, comme je l'explique dans la prochaine section.

Pour afficher la console de gestion DHCP, exécutez Démarrer/Outils d'administration/DHCP ou cliquez sur Serveur DHCP dans le Gestionnaire de serveur. Dans les deux cas, la console de gestion DHCP représentée dans la Figure 6.3 apparaît.

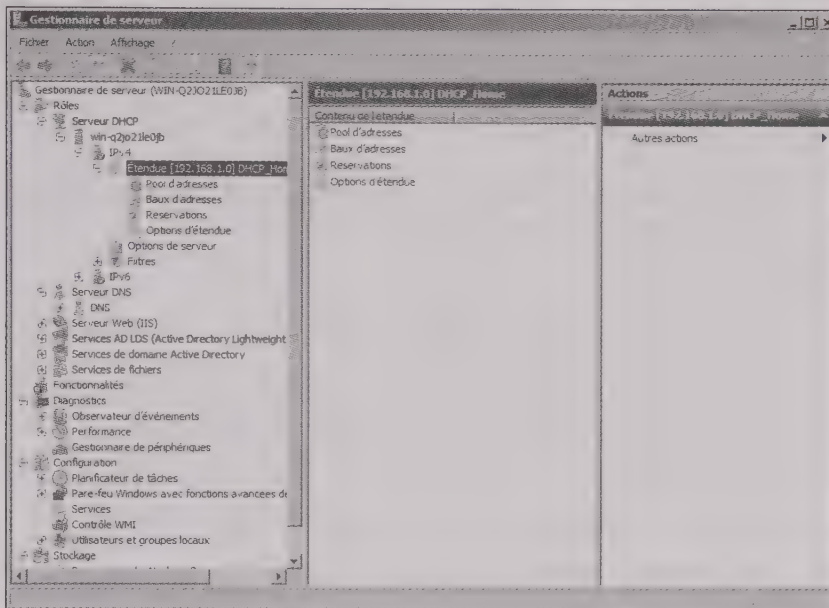


Figure 6.3 : Console de gestion DHCP.

La console de gestion DHCP octroie un contrôle complet sur la configuration et le fonctionnement du serveur DHCP. Voici quelques actions possibles grâce à la console DHCP :

- ✓ **Autoriser le serveur DHCP, soit lui permettre d'attribuer des adresses IP aux ordinateurs clients.** Pour autoriser un serveur, sélectionnez-le et choisissez Action/Gérer les serveurs autorisés/Autoriser.
- ✓ **Ajouter une nouvelle étendue.** Pour ce faire, effectuez un clic droit sur un serveur dans l'arborescence et, dans le menu contextuel, cliquez sur Nouvelle étendue. Cette action démarre l'Assistant Nouvelle étendue qui vous permettra de créer l'étendue.
- ✓ **Activer ou désactiver une étendue.** Effectuez un clic droit sur l'étendue concernée dans l'arborescence et exécutez la commande Activer ou Désactiver.
- ✓ **Modifier les paramètres d'étendue.** Effectuez un clic droit sur une étendue et sélectionnez Propriétés. La boîte de dialogue Propriétés d'Étendue qui apparaît permet de modifier les adresses de début et de fin de l'étendue, le masque de sous-réseau et la configuration DSN.
- ✓ **Modifier les exclusions d'étendue.** Cliquez sur Pool d'adresses, sous l'étendue présentée dans l'arborescence. Ainsi chaque plage d'adresses de l'étendue est affichée. Vous pouvez ajouter ou supprimer une plage. Pour ce faire, effectuez un clic droit sur la plage

et exécutez la commande Supprimer. Vous pouvez aussi ajouter une plage d'exclusion : effectuez un clic droit sur Pool d'adresses dans l'arborescence et cliquez sur Nouvelle plage d'exclusion, dans le menu contextuel.

- ✓ **Voir ou modifier des réservations.** Cliquez sur Réservations, dans l'arborescence.
- ✓ **Voir la liste des adresses actuellement attribuées.** Cliquez sur Baux d'adresses, dans l'arborescence.

Configurer un client DHCP sous Windows

Configurer un client Windows pour le service DHCP est facile. En effet, il est automatiquement inclus lorsque vous installez le protocole TCP/IP. Il ne vous reste donc plus qu'à configurer TCP/IP pour qu'il utilise le service DHCP. Pour ce faire, ouvrez la boîte de dialogue Propriétés du réseau en sélectionnant Centre Réseau et partage ou Connexions réseau dans le Panneau de configuration, en fonction de la version de Windows installée sur le client. Sélectionnez ensuite le protocole TCP/IP et cliquez sur le bouton Propriétés. La boîte de dialogue Propriétés de Protocole Internet (TCP/IP) s'ouvre, comme le montre la Figure 6.4. Pour configurer l'ordinateur de manière à ce qu'il utilise le service DHCP, activez les options Obtenir une adresse IP automatiquement et Obtenir les adresses des serveurs DNS automatiquement. Il ne vous reste plus qu'à cliquer sur OK et le tour est joué !

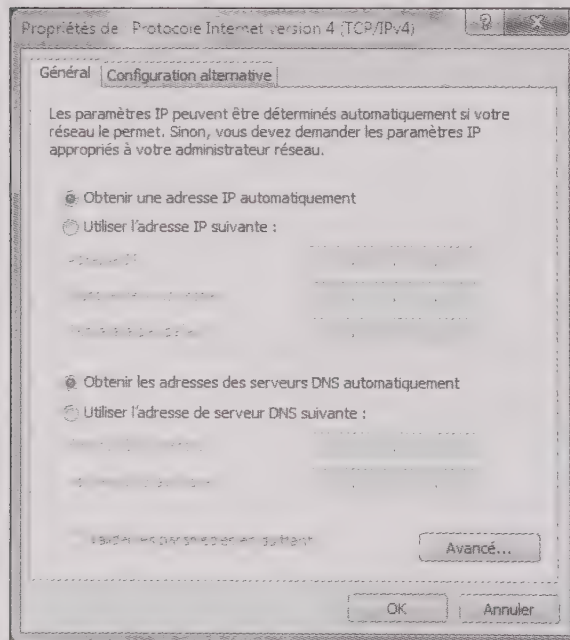


Figure 6.4 : Configuration d'un client Windows pour utiliser le service DHCP.

Utiliser le service DNS

Le service *DNS* (*Domain Name System*, système de noms de domaines) est un service TCP/IP permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine. Sans DNS, vous achèteriez des livres sur 87.238.83.167 plutôt que sur www.amazon.fr, vous vendriez vos meubles d'occasion sur 66.135.200.28 plutôt que sur www.ebay.fr et vous lanceriez des recherches sur 209.85.229.103 plutôt que sur www.google.com.

La compréhension du fonctionnement du service DNS ainsi que sa mise en œuvre sont indispensables à la mise en place et à la gestion d'un réseau TCP/IP. La suite de ce chapitre présente les bases du DNS, son fonctionnement et la technique pour installer un serveur DNS.

Domaines et noms de domaines

Pour qu'un nom DNS unique corresponde à un seul ordinateur hôte sur Internet, le service DNS emploie une technique testée et fiable : diviser pour régner. Le service DNS utilise un système de nommage structuré semblable à la structure hiérarchique des dossiers sur un ordinateur Windows. À la place des dossiers, le service DNS organise les noms en *domaines*. Chaque domaine inclut tous les noms qui dépendent directement de lui dans la structure hiérarchique.

La Figure 6.5 illustre une petite partie de la structure arborescente du DNS. Au sommet de l'arbre, se trouve le *domaine racine* (*root*), c'est le point de départ de tous les domaines. Directement en dessous, on trouve quatre domaines : edu, com, org et gov.

En réalité, il existe beaucoup plus de domaines sous la racine d'Internet. Il doit y en avoir actuellement plus de 90 millions.

Sous le domaine com de la Figure 6.5, vous pouvez voir le domaine nommé EFirst, celui de l'éditeur des *Nuls*. Pour identifier ce domaine, vous devez le combiner avec le nom de son domaine parent (dans ce cas-ci, com) pour créer le nom de domaine complet : EFirst.com. Les composants du nom de domaine sont séparés par des points. Ainsi, lorsque vous lisez ce nom de domaine, vous prononcez « efirst point com ».

Sous le nœud EFirst se trouvent quatre nœuds de serveur : production, dessin, serveur1 et imprimante1. Ces nœuds correspondent à trois ordinateurs et à une imprimante. Vous pouvez combiner le nom d'hôte avec le nom de domaine pour obtenir le nom DNS complet pour chacun des serveurs. Par exemple, `serveur1.EFirst.com` ou bien `imprimante1.EFirst.com`.

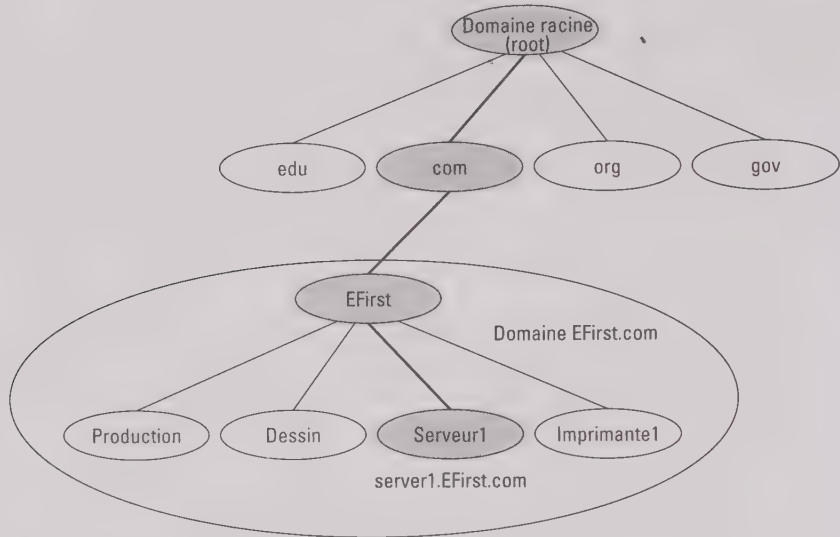


Figure 6.5 : Noms DNS.

Voici des informations supplémentaires relatives aux noms DNS :

- ✓ Les noms DNS ne font pas de distinction entre les majuscules et les minuscules. Par conséquent, EFirst, eFirst, eFIRST et efirst sont traités de la même manière. Lorsque vous utilisez un nom de domaine, vous pouvez le mettre en majuscules pour faciliter sa lecture mais le service DNS ne fera pas la distinction.
- ✓ Le nom de chaque nœud de DNS peut compter jusqu'à 63 caractères (sans compter le point) et peut inclure des lettres, des chiffres et des traits d'union. Les caractères spéciaux sont interdits.
- ✓ Un *sous-domaine* est un domaine qui se trouve sous un domaine existant. Par exemple, le domaine com est un sous-domaine du domaine racine ; de même, EFirst est un sous-domaine du domaine com.

Le service DNS est un système de nommage hiérarchique semblable au système de nommage employé par Windows pour les dossiers et sous-dossiers. Cependant, une différence cruciale existe entre le service DNS et la convention de nommage de Windows. Quand vous construisez un nom DNS complet, vous commencez à partir du bas de la structure arborescente et vous remontez jusqu'à la racine. Ainsi, production est l'élément le plus bas dans le nom production.EFirst.com. En revanche, sous Windows, la méthode de nommage est inverse : le nom commence à la racine et se déplace vers le bas : dans le chemin d'accès \Windows\System32\dns, dns est le nœud le plus bas.



- ✓ La profondeur de la structure arborescente du DNS peut aller jusqu'à 127 niveaux. Cependant, dans la pratique, elle est relativement limitée. La plupart des noms DNS n'ont que trois niveaux (sans compter la racine) et rarement plus de quatre ou cinq.
- ✓ Bien que l'arbre du DNS soit peu profond, il est très large. En d'autres termes, chacun des domaines de haut niveau a un nombre important de domaines de niveau immédiatement inférieur. Par exemple, le domaine `com` recouvre actuellement plus de deux millions de sous-domaines.

Noms de domaines complets

Si un nom de domaine se termine par un point, celui-ci représente le domaine racine et le nom de domaine est dit *absolu* ou *Fully Qualified Domain Name (FQDN)*. Un nom de domaine absolu est un nom de domaine non ambigu parce qu'il identifie les références du sous-domaine à partir de la racine. En revanche, si un nom de domaine ne se termine pas par un point, celui-ci peut être affecté à un autre domaine parent. Il s'agit alors d'un *nom relatif*.

Ce concept est semblable aux concepts de chemin relatif et de chemin absolu sous Windows. Si un chemin d'accès commence par une barre oblique inverse, par exemple `\Windows\System32\dns`, il s'agit d'un *chemin absolu*. Si le chemin d'accès ne commence pas par une barre oblique inverse, par exemple `System32\dns`, il s'agit d'un chemin relatif à partir du répertoire en cours. Si le répertoire courant est `\Windows`, `\Windows\System32\dns` et `System32\dns` renvoient au même emplacement.

Dans de nombreux cas, les noms de domaines absolus et relatifs sont interchangeables parce que le logiciel qui les interprète considère qu'ils sont des sous-domaines directs du domaine racine. C'est pourquoi, par exemple, vous pouvez saisir dans votre navigateur `www.wiley.com` (sans point final) plutôt que `www.wiley.com.` pour accéder à la page d'accueil de l'éditeur Wiley. Certaines applications, telles que les serveurs DNS, peuvent associer des noms de domaines autres que la racine à des noms relatifs.

Travailler avec un serveur DNS sous Windows

L'installation et la gestion d'un serveur DNS dépendent du système d'exploitation du serveur. Cette section décrit l'installation et l'utilisation d'un serveur DNS sous Windows 2008. La mise en œuvre sous Linux ou un

environnement Unix avec BIND est semblable mais sans l'aide d'une interface graphique utilisateur.

Pour installer le serveur DNS sur un serveur Windows 2008, exécutez la commande Démarrer/Outils d'administration/Gestionnaire de serveur. Cliquez sur Ajouter des rôles, sélectionnez Serveur DNS dans la liste des rôles puis cliquez sur Suivant pour installer le serveur DNS.

Une fois que le serveur DNS a été installé, vous pouvez l'administrer via la console de gestion DNS. Elle vous permet d'exécuter des tâches administratives communes comme ajouter des zones supplémentaires, modifier la configuration de zones ou ajouter des enregistrements A ou MX à une zone existante. La console d'administration du DNS masque les détails de commandes souvent rébarbatives et vous permet de travailler avec une interface graphique utilisateur conviviale.

Pour ajouter un nouvel hôte à une zone, effectuez un clic droit sur la zone, dans la console d'administration du DNS et cliquez sur la commande Nouvel hôte. Cette action ouvre la boîte de dialogue Nouvel hôte, illustrée par la Figure 6.6.

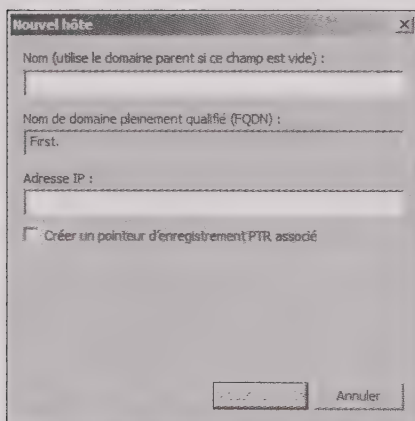


Figure 6.6 : Boîte de dialogue Nouvel hôte.

Dans la boîte de dialogue, spécifiez les informations suivantes :

- ✓ **Nom** : Le nom d'hôte pour la nouvelle machine.
- ✓ **Adresse IP** : L'adresse IP de l'hôte.
- ✓ **Créer un pointeur associé à l'enregistrement (PTR)** : Crée automatiquement un pointeur associé à l'enregistrement dans le fichier de consultation inversé. Cochez cette option si vous voulez permettre des recherches inversées pour le serveur.

- ✓ **Autoriser la mise à jour par n'importe quel utilisateur authentifié :** Cette option autorise la mise à jour par d'autres utilisateurs. En général, elle n'est pas cochée.
- ✓ **Temps de vie :** La valeur de temps de vie (*Time to live*, TTL) pour cet enregistrement.

Vous pouvez ajouter d'autres enregistrements tels que MX ou CNAME de la même manière.

Configurer un client DNS sous Windows

Les ordinateurs clients n'ont pas besoin d'une configuration très élaborée pour fonctionner correctement avec le service DNS. Le client doit avoir l'adresse d'au moins un serveur DNS. Celle-ci est généralement fournie par le serveur DHCP en même temps que son adresse.

Pour qu'un ordinateur client obtienne l'adresse du serveur DNS à partir du service DHCP, ouvrez la boîte de dialogue Propriétés du réseau en sélectionnant Centre Réseau et partage ou Connexions réseau dans le Panneau de configuration, selon la version de Windows installée sur le client. Sélectionnez le protocole TCP/IP puis cliquez sur le bouton Propriétés. S'ouvre alors la boîte de dialogue Propriétés de Protocole TCP/IP, précédemment illustrée par la Figure 6.4. Pour configurer l'ordinateur de sorte à ce qu'il utilise le service DNS, activez les options Obtenir une adresse IP automatiquement et Obtenir les adresses des serveurs DNS automatiquement. Il ne vous reste qu'à cliquer sur OK. C'est terminé !

Chapitre 7

Installer un serveur

Dans ce chapitre :

- ▶ Comprendre les fonctions d'un système d'exploitation réseau.
- ▶ Découvrir Windows Server et d'autres options serveur.
- ▶ Méthodes d'installation d'un système d'exploitation réseau.
- ▶ Prêt pour l'installation !
- ▶ Installer un système d'exploitation réseau.
- ▶ Que faire après l'installation d'un système d'exploitation réseau ?
- ▶ Configurer les rôles de serveur.

Avant d'aller plus loin, l'un des choix fondamentaux que vous devrez faire est celui du *système d'exploitation réseau (NOS)* car il est la base de votre réseau. Ce chapitre commence par décrire les principales fonctionnalités propres à tous les systèmes d'exploitation réseau. Il indique ensuite les avantages et les inconvénients des plus connus d'entre eux.

Naturellement, votre travail ne se limite pas au choix du système d'exploitation réseau. Il consiste à installer puis à mettre en service le système d'exploitation réseau. Ce chapitre fournit une vue d'ensemble sur l'installation et la configuration d'un des systèmes d'exploitation réseau les plus populaires, Windows Server 2008.

Fonctions d'un système d'exploitation réseau

Tous les systèmes d'exploitation, du plus simple au plus complexe, doivent comporter certaines fonctionnalités cruciales telles que la connexion aux autres ordinateurs du réseau, le partage des fichiers et autres ressources, la

sécurité, etc. Vous trouverez, dans les sections ci-dessous, quelques généralités sur ces fonctions.

Support réseau

Il va sans dire qu'un système d'exploitation réseau doit supporter les réseaux (parce que si, en plus, il ne supporte pas l'exploitation des ordinateurs par les ordinateurs, on n'est pas sorti de l'auberge. Il y a là matière à d'intenses cogitations !).

Cela exige les caractéristiques techniques suivantes :

- ✓ Pour qu'il réponde aux attentes de l'utilisateur, un système d'exploitation réseau doit supporter une vaste diversité de *protocoles réseau*.
Généralement, les gros réseaux relient des ordinateurs tournant sous différentes versions de Windows, des PC sous Linux et aussi des Macintosh. C'est ce qu'on appelle un réseau *hétérogène*. Le serveur devra supporter simultanément les protocoles TCP/IP, NetBIOS et AppleTalk.
- ✓ Bon nombre de serveurs sont équipés de plusieurs cartes d'interface réseau. Dans ce cas, le système d'exploitation réseau doit être capable de supporter des *connexions multiples*.
 - Idéalement, le système d'exploitation réseau doit pouvoir répartir la charge de manière égale entre ses interfaces réseau.
 - De plus, au cas où l'une des connexions échouerait, le système d'exploitation réseau doit faire en sorte qu'une autre connexion prenne le relais, sans rupture.
- ✓ La plupart des systèmes d'exploitation réseau sont capables de faire office de *routeur* reliant deux réseaux.
Les fonctions de routeur d'un système d'exploitation réseau doivent aussi comporter des fonctions de *pare-feu* interdisant l'entrée de paquets non autorisés dans le réseau local.

Services de partage de fichiers

Une des fonctions les plus importantes d'un système d'exploitation réseau est le partage des ressources entre les utilisateurs du réseau. La plus commune de ces ressources partagées est le *système de fichiers* du serveur, c'est-à-dire l'espace organisé, sur le disque dur, que le serveur doit pouvoir mettre à disposition (totalement ou partiellement) des autres utilisateurs. Ces derniers peuvent alors considérer que cet espace de stockage, sur le serveur, est une extension de l'espace disque de leur propre ordinateur.

Le système d'exploitation réseau permet à l'administrateur système de définir les parties du système de fichiers du serveur qui seront partagées.



Bien que la totalité du disque dur puisse être partagée, c'est rarement le cas. En fait, ce sont des répertoires et dossiers bien précis qui le sont. L'administrateur peut définir comment chaque utilisateur accède ou n'accède pas à chacun des dossiers partagés.

Le partage des fichiers étant la raison d'être de nombreux serveurs, un système d'exploitation réseau doit disposer de fonctions de gestion du disque dur beaucoup plus sophistiquées que celles des systèmes d'exploitation des ordinateurs de bureau. Par exemple, la plupart des systèmes d'exploitation réseau peuvent gérer plusieurs disques durs comme s'ils n'en faisaient qu'un. De plus, bon nombre d'entre eux savent créer un *miroir* d'un disque dur sur un autre disque, par sauvegardes automatiques.

Multitâche

Un ordinateur n'est utilisé que par une seule personne à la fois. En revanche, de nombreuses personnes peuvent utiliser un serveur simultanément. C'est pourquoi un système d'exploitation réseau doit fournir une prise en charge pour les multiples utilisateurs qui accèdent au serveur à distance, via le réseau.

Le cœur de ce support multiutilisateur est une fonctionnalité appelée *multitâche*. Il s'agit d'une technique qui saucissonne le traitement informatique en fines tranches de temps et jongle à la vitesse de l'éclair avec les programmes en cours. C'est ainsi que le système d'exploitation parvient à exécuter plus d'un programme (appelé *tâche* ou *processus*) à la fois. Le multitâche n'est pas sans rappeler les jongleurs du cirque de Pékin qui font tourner des assiettes sur des bâtons tout en se contorsionnant ou en pédalant sur un monocycle. Remplacez les assiettes par des logiciels et le monocycle par le gestionnaire de fichiers et vous y êtes.

Le multitâche ne fait que donner *l'impression* que plusieurs programmes s'exécutent simultanément. En réalité, un ordinateur monoprocesseur ne peut en exécuter qu'un seul. Le système d'exploitation demande au processeur de passer rapidement d'un programme à un autre pour simuler la simultanéité. Mais à un instant T, un seul programme est traité. Les autres attendent patiemment leur tour, si tant est que la patience puisse s'évaluer en millisecondes. Notez que si l'ordinateur est équipé de plusieurs processeurs, plusieurs programmes peuvent effectivement être exécutés en même temps mais c'est là une autre paire de manches.

Services d'annuaire

On trouve des annuaires partout. Vous en utilisez pour trouver un numéro de téléphone. Si vous recherchez les coordonnées d'un client, vous feuilletez l'annuaire de votre Filofax. Un annuaire n'est pas forcément sur papier : la liste des contacts de votre messagerie ou de votre PDA (assistant personnel numérique) est aussi un annuaire.

Les réseaux sont équipés d'annuaires qui recensent les ressources disponibles : utilisateurs, ordinateurs, imprimantes, dossiers partagés et fichiers. Ils jouent un rôle essentiel dans n'importe quel système d'exploitation réseau.

Dans les anciens systèmes d'exploitation réseau, comme Windows NT 3.1 et NetWare 3.x, chaque serveur maintenait sa propre *base de données de répertoire* (un fichier contenant une liste ordonnée des ressources disponibles seulement sur ce serveur). Le problème, avec cette approche, est que l'administrateur réseau devait maintenir chaque base de données séparément. Ce n'était pas problématique pour des réseaux ne comportant que quelques serveurs mais si le réseau en comptait des dizaines, voire des centaines, la tâche s'avérait quasiment impossible.

De plus, les premiers *services d'annuaire* (des programmes qui servent à exploiter les bases de données de répertoire) étaient spécifiques à telle ou telle application. Par exemple, un serveur avait un service d'annuaire pour la connexion des utilisateurs, un autre pour le partage des fichiers et un autre encore pour les adresses de la messagerie. Chaque annuaire avait ses propres outils d'ajout, de mise à jour et de suppression des entrées.

Le service d'annuaire moderne le plus populaire est *Active Directory*. Il est intégré par défaut dans les systèmes d'exploitation serveurs basés sur Windows. Active Directory fournit un annuaire simple de toutes les ressources du réseau. Il abandonne les limites imposées aux anciens noms de domaines et noms d'ordinateurs (15 caractères) utilisées avec Windows NT en faveur des noms autorisés par les DNS et Internet tels que *Marketing.MonEntreprise.com* ou *Achats.MonEntreprise.com*. La Figure 7.1 présente la console Utilisateurs et ordinateurs Active Directory, utilisée pour gérer les utilisateurs et les ordinateurs sous Windows Server 2008.

Services de sécurité

Tous les systèmes d'exploitation réseau doivent proposer des mesures de sécurité qui protègent le réseau des entrées non autorisées. Le piratage étant devenu l'un des passe-temps favoris et la plupart des ordinateurs étant connectés à Internet, n'importe qui dans le monde est susceptible d'entrer par effraction dans votre réseau.

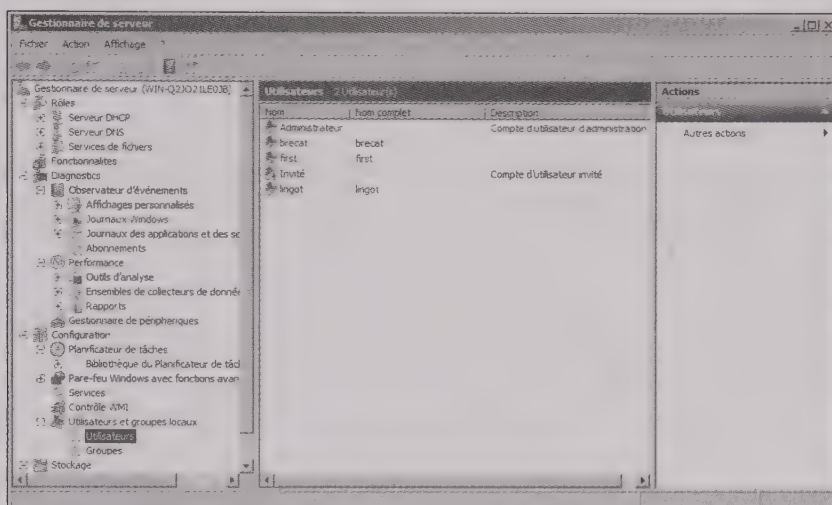


Figure 7.1 : Console Utilisateurs et ordinateurs Active Directory.

La sécurité la plus élémentaire est gérée au niveau des *comptes d'utilisateurs* qui garantissent à chacun des utilisateurs des droits d'accès aux ressources du réseau et définissent les ressources auxquelles un utilisateur a accès. Les comptes d'utilisateurs sont sécurisés par des mots de passe. C'est pourquoi une bonne politique de mots de passe est la clé de voûte de tout système de sécurité. La plupart des systèmes d'exploitation réseau proposent quelques outils de sécurité standard pour le réseau :

- ✔ **L'établissement d'une politique de mots de passe.** Elle est basée sur l'obligation de respecter une longueur minimale et de mêler des lettres et des chiffres.
- ✔ **L'expiration des mots de passe après un certain nombre de jours.** Ceci oblige les utilisateurs à changer fréquemment de mot de passe.
- ✔ **Le cryptage des données du réseau.** Le cryptage brouille les données avant de les envoyer sur le réseau ou de les enregistrer sur disque, ce qui les met à l'abri d'un usage malintentionné.

Un cryptage efficace est essentiel pour configurer un VPN (*Virtual Private Network*, réseau privé virtuel) permettant aux utilisateurs du réseau d'accéder en toute sécurité à un réseau, depuis un lieu éloigné, grâce à une connexion Internet.
- ✔ **La production de certificats numériques.** Ces codes spéciaux garantissent à l'utilisateur qu'il est bien à l'emplacement où il pense être et que les fichiers sont bien ceux qu'il croit.



Différentes versions de Windows Server 2008

Le système d'exploitation vedette de Microsoft est actuellement Windows Server 2008. En fait, Windows Server 2008 est directement inspiré de Windows Server 2003 auquel de nouvelles caractéristiques ont été ajoutées dont voici les plus importantes :

- ✓ Une version améliorée d'Active Directory, avec la possibilité de gérer les certificats numériques, un nouveau type de contrôleur de domaine appelé *contrôleur de domaine en lecture seule* et la possibilité de fermer et de redémarrer les services Active Directory sans éteindre le serveur.
- ✓ Une nouvelle interface utilisateur basée sur Windows Vista, dotée d'un nouvel outil de gestion tout-en-un appelé Gestionnaire de serveur.
- ✓ Une nouvelle version du système d'exploitation appelée *Server Core* qui ne possède pas d'interface graphique. Server Core est entièrement géré en ligne de commande ou par un ordinateur distant qui se connecte au serveur via Microsoft Management Console. Server Core fournit des serveurs de fichiers, des contrôleurs de domaine ou des serveurs DNS et DHCP performants.
- ✓ Des techniques de connexion à distance améliorées qui permettent aux ordinateurs d'établir des connexions au serveur basées sur le Web avec le protocole HTTPS sans devoir créer une connexion de réseau privé virtuel (VPN).
- ✓ Une nouvelle version d'Internet Information Services (IIS) Web server (7.0).
- ✓ Des outils de virtualisation intégrés qui vous permettent de créer et d'exécuter plus d'une instance du système d'exploitation serveur sur un même serveur.

Windows Server 2008 est décliné en plusieurs versions. Les plus courantes sont les suivantes :

- ✓ **Windows Server 2008, Standard.** C'est la version de base de Windows 2008. Cette version est celle qu'il vous faut si vous utilisez Windows Server 2008 comme serveur de fichiers ou pour fournir d'autres services réseau basiques. Elle supporte les ordinateurs multiprocesseurs (jusqu'à quatre processeurs) et jusqu'à 4 Go de RAM (32 Go sur les systèmes à 64 bits).

- ✓ **Windows Web Server 2008.** Version optimisée pour une utilisation comme serveur Web.
- ✓ **Windows Server 2008, Foundation.** Il s'agit d'une version universelle conçue pour les réseaux de petite taille.
- ✓ **Windows Server 2008, Enterprise.** Conçue pour les réseaux de grande taille, cette version supporte des ordinateurs comportant jusqu'à huit processeurs, 64 Go de RAM et des groupes de serveurs. Elle propose des fonctionnalités avancées et se caractérise par des performances élevées ainsi qu'une grande fiabilité.
- ✓ **Windows Server 2008, Datacenter.** La version la plus puissante de Windows Server 2008. Elle supporte des ordinateurs possédant jusqu'à soixante-quatre processeurs, 2 téraoctets de RAM (2,048 Go) et des groupes de serveurs. Des fonctionnalités avancées de gestion des erreurs et des tolérances en font un système de choix pour les applications les plus sophistiquées.

Autres systèmes d'exploitation réseau

Bien que Windows Server 2008 soit le système d'exploitation réseau le plus répandu, il n'est pas seul en lice. La section suivante en décrit deux autres : Linux et Macintosh OS X Server.

Linux

Linux est sans doute l'un des systèmes d'exploitation les plus intéressants. C'est un produit gratuit basé sur *UNIX*, un puissant système d'exploitation réseau souvent utilisé pour les grands réseaux. Linux a été conçu par Linus Torvalds, un étudiant finlandais qui avait développé une version d'*UNIX* pendant ses loisirs. Par la suite, des centaines de programmeurs du monde entier se portèrent volontaires pour étoffer le projet, via Internet. Aujourd'hui, Linux est une version pleinement opérationnelle d'*UNIX*. Ses adeptes le considèrent comme aussi bon, voire meilleur, que Windows. Actuellement, les utilisateurs de Linux sont aussi nombreux que les utilisateurs de Macintosh.

Linux offre les mêmes avantages de mise en réseau qu'*UNIX*. C'est un excellent choix si vous recherchez un système d'exploitation réseau performant.

Apple Mac OS X Server

Tous les systèmes d'exploitation décrits par ailleurs dans ce livre tournent sur des PC équipés de processeurs Pentium ou compatibles Pentium. Mais qu'en est-il des Macintosh ? Car, après tout, leurs utilisateurs ont aussi besoin de mettre en réseau leurs machines. À leur intention, Apple propose un système d'exploitation réseau particulier appelé Mac OS X Server. Il possède toutes les fonctionnalités nécessaires pour prendre en charge un réseau, y compris le partage de fichiers et d'imprimantes, les fonctions Internet, la messagerie, etc.

Méthodes d'installation d'un système d'exploitation réseau

Indépendamment du choix du système d'exploitation réseau, il faut aussi savoir quelle méthode d'installation vous allez choisir ; les sections suivantes présentent plusieurs solutions.

Installation complète ou mise à niveau

Vous pouvez avoir le choix entre une installation complète ou une mise à niveau du système d'exploitation en cours. Dans certains cas, il est plus simple de procéder à une installation complète même si l'ordinateur utilise une version antérieure du système d'exploitation. Voici les choix qui s'offrent à vous :

- ✓ Si vous installez le système d'exploitation réseau sur un serveur neuf, exécutez une installation complète ; le système d'exploitation sera installé et configuré avec des paramètres par défaut.
- ✓ Si vous installez le système d'exploitation réseau sur un serveur ayant déjà un système d'exploitation réseau installé, vous pouvez exécuter une mise à niveau qui remplacera le système d'exploitation mais conservera, dans la mesure du possible, les paramètres de la version antérieure.
- ✓ Vous pouvez également effectuer une installation complète sur un ordinateur qui possède déjà un système d'exploitation réseau. Dans ce cas, vous avez ces deux options :
 - *Supprimer* le système d'exploitation existant.



- Exécuter une *installation multiboot* qui installera le nouveau système d'exploitation « à côté » du système d'exploitation existant. Lorsque vous démarrerez l'ordinateur, vous aurez le choix entre les deux systèmes d'exploitation réseau.

Bien que l'installation multiboot semble être une bonne idée, elle peut être dangereuse. Je vous conseille d'éviter ce choix à moins que vous ayez une bonne raison de le faire. Pour plus d'informations sur les installations en multiboot, consultez l'encadré « Configuration multiboot ».

✓ Vous ne pouvez pas faire évoluer une version de Windows client vers une version serveur. Les choix qui s'offrent à vous sont les suivants :

- Une *installation complète* qui supprime le système d'exploitation Windows existant.
- Une *installation multiboot* qui laisse le client existant Windows intact.

Quel que soit votre choix, pensez à sauvegarder les données existantes sur l'ordinateur lorsque vous installez la version serveur.

Installation réseau

En général, le système d'exploitation réseau est installé à partir des disques de distribution sur le lecteur CD du serveur. Cependant, vous pouvez également installer le système d'exploitation à partir d'un lecteur partagé par un autre ordinateur, si le réseau est accessible. Vous pouvez aussi utiliser un disque dur réseau sur lequel vous aurez copié le contenu des disques de distribution.

Évidemment, l'ordinateur doit avoir accès au réseau ! Si le serveur possède déjà un système d'exploitation, il a probablement accès au réseau. Sinon, vous pouvez démarrer l'ordinateur à partir d'une disquette qui chargera le support de base réseau.



Si vous installez le système d'exploitation réseau sur plus d'un serveur, vous pouvez gagner du temps en copiant d'abord le CD de distribution sur un disque dur partagé. Parce que même les lecteurs de CD les plus rapides sont plus lents que le réseau. Même avec un réseau 10/100 Mbps, l'accès aux données d'un disque dur partagé est beaucoup plus rapide que l'accès à un lecteur de CD local.

Configuration multiboot

Les installations multiboot offrent plus de possibilités qu'une installation simple du système d'exploitation. Évidemment, un seul des systèmes d'exploitation peut être opérationnel à un instant T. Lorsque vous démarrez l'ordinateur, un menu apparaît et propose le choix entre les systèmes d'exploitation installés ; l'ordinateur démarre ensuite sur celui sélectionné.

Les configurations multiboot sont en général utilisées par les programmeurs ou les administrateurs réseau qui doivent s'assurer que le logiciel est compatible avec une large variété de systèmes d'exploitation. Plutôt que d'installer des ordinateurs avec différents systèmes d'exploitation, il est préférable de configurer un seul PC en multiboot avec les systèmes d'exploitation à tester. Pour des serveurs réseau en production, le choix d'une configuration multiboot n'est pas très judicieux.

Cependant, si vous estimez qu'il est indispensable qu'un serveur réseau soit configuré en multiboot, veillez à ce que chacun des systèmes d'exploitation soit installé dans sa propre partition de disque. Bien que la plupart des systèmes d'exploitation réseau acceptent une installation de deux systèmes d'exploitation (ou plus) sur une même partition, ne le faites pas ! Pour supporter deux systèmes d'exploitation sur une même partition, les systèmes d'exploitation doivent faire appel à un jeu d'interpréteur de commandes interactif qui risque d'endommager des fichiers système. Par ailleurs, si une coupure de courant intervient au moment où le système d'exploitation réseau commute les fichiers de démarrage, vous risquez de vous trouver avec un serveur qui ne pourra plus amorcer aucun des systèmes d'exploitation.

En conclusion, si vous configurez un serveur en multiboot, installez chacun des systèmes d'exploitation dans une partition séparée. Vous pourrez ensuite faire appel à un programme de gestion de boot qui démarrera dans la partition de votre choix.

Installations automatisées et à distance

Au cas où vous vous trouveriez dans l'obligation d'installer des systèmes d'exploitation réseau sur plusieurs serveurs, vous pouvez employer quelques astuces pour rationaliser le processus :

- ✓ **Installation automatisée** : Vous devez créer une séquence type d'installation qui répond à toutes les questions posées par le programme d'installation. Ensuite, vous pouvez commencer l'installation automatisée.

La mise au point de cette procédure d'installation représente un travail important, justifié uniquement si vous avez un grand nombre de serveurs à installer.





- ✓ **Les services d'installation à distance (RIS, Remote Installation Services) :** Microsoft propose un outil permettant d'installer Windows Server à partir d'un emplacement réseau distant sans avoir à se déplacer sur l'ordinateur serveur.

Ce dispositif puissant ne présente un intérêt que si vous devez installer les systèmes d'exploitation sur un nombre très important de serveurs (les services RIS permettent également d'installer des systèmes d'exploitation clients).

Inventaire des ressources nécessaires

Avant de commencer l'installation du système d'exploitation réseau, vous devez collecter tout le matériel et toutes les informations dont vous aurez besoin de sorte que vous ne soyez pas contraint de rechercher un élément ou une information au milieu de l'installation. Les sections suivantes décrivent les éléments nécessaires.

Un serveur digne de ce nom

Évidemment, vous devez avoir un ordinateur serveur sur lequel installer le système d'exploitation réseau. Chaque système d'exploitation est accompagné d'une liste de pré-requis. Le Tableau 7.1 présente les deux types de configurations requises pour Windows Server 2008 Standard :

- ✓ les pré-requis inappropriés, publiés par Microsoft ;
- ✓ les recommandations réalistes de l'auteur pour une performance correcte.

Tableau 7.2 : Configuration requise pour Windows Server 2008.

Matériel	Pré-requis Microsoft	Pré-requis de l'auteur
CPU	Processeur single-core x86 1 GHz (par ex. Intel Pentium)	Processeur dual-core x86 2 GHz (par ex. Intel Core 2 Duo)
RAM	512 Mo	4 Go
Espace disque libre	10 Go	80 Go



Actuellement, les composants de l'ordinateur sont assez bon marché. Alors, ne lésinez pas sur le matériel !

Vous devez également contrôler les composants de votre serveur avec la liste du matériel compatible éditée par le concepteur du système d'exploitation. Par exemple, Microsoft publie une liste de matériels testés et certifiés compatibles avec les serveurs Windows. Cette liste de compatibilité matérielle, ou HCL, est disponible sur www.microsoft.com/whdc/hcl/default.msp. Vous pouvez également tester la compatibilité de votre ordinateur en exécutant l'option de contrôle de la compatibilité système à partir du disque de distribution de Windows.

Un système d'exploitation serveur

Vous avez également besoin du système d'exploitation serveur à installer : soit à partir des CD de distribution, soit à partir d'un lecteur de CD ou d'un disque dur réseau. En plus des disques, vous devriez posséder les éléments suivants :



- ✓ **Les codes du produit** : Le programme d'installation requiert les codes du produit pour s'assurer que vous possédez une copie légale du logiciel.

Si vous avez les disques d'origine, le code produit se trouve sur un autocollant collé sur l'emballage.

- ✓ **Les documentations d'installation** : Si le système d'exploitation est accompagné d'une version papier des documents d'installation, conservez-la à portée de main.

- ✓ **Un disque de démarrage** : Si vous installez le logiciel sur un serveur neuf, vous avez besoin de démarrer l'ordinateur. Suivant le système d'exploitation et les caractéristiques de l'ordinateur, vous le démarrerez directement à partir du CD de distribution ou utiliserez une disquette d'amorçage.

- ✓ **Le type de licence** : Vous pouvez acheter des systèmes d'exploitation Microsoft avec des licences serveur ou des licences de site. Vous devez savoir quel a été votre choix quand vous installez le système d'exploitation réseau.



Vérifiez sur le CD de distribution s'il y a une documentation du produit et une information de dernière minute supplémentaire. Par exemple, les CD Windows possèdent un dossier \docs avec plusieurs fichiers qui contiennent des informations de configuration utiles.

D'autres logiciels

Dans la plupart des cas, le programme d'installation doit pouvoir configurer automatiquement les dispositifs matériels du serveur et installer des pilotes appropriés. Cependant, il se peut que vous deviez vous procurer les pilotes pour des dispositifs tels que des cartes d'interface réseau, des périphériques SCSI, des lecteurs de CD-ROM, des imprimantes ou des scanners.

Une connexion Internet opérationnelle

Cette condition n'est pas indispensable mais l'installation sera améliorée si vous avez une connexion Internet opérationnelle dès le début. La procédure d'installation peut utiliser cette connexion Internet pour plusieurs tâches :

- ✓ **Téléchargement des dernières mises à jour** : Cela évite d'installer un service pack lorsque la procédure d'installation du système d'exploitation réseau est terminée.
- ✓ **Localisation des pilotes pour les dispositifs non standards** : C'est indispensable si vous ne trouvez pas le disque des pilotes de votre carte SCSI.
- ✓ **Activation du produit à la fin de l'installation (pour les systèmes d'exploitation Microsoft)** : Pour plus d'informations, voir la section « Activer Windows » à la fin du chapitre.

Un bon livre

Vous passez beaucoup de temps devant l'ordinateur pendant la phase d'installation. Pour vous distraire et ne pas vous ennuyer, munissez-vous d'un bon bouquin !

Prendre les bonnes décisions

Lorsque vous installez un système d'exploitation réseau, vous êtes amené à prendre quelques décisions sur la façon dont vous voulez que le système et les serveurs soient configurés. La plupart de ces décisions ne sont pas gravées dans le marbre, aussi ne vous inquiétez pas si vous n'êtes pas sûr à 100 % de votre choix. Vous pourrez toujours y revenir et modifier la configuration. Cependant, vous pouvez gagner du temps en réfléchissant, avant la phase d'installation, à ce que vous voulez faire et aux questions qui vous seront posées par le programme.

La liste suivante présente la plupart des décisions que vous devrez prendre :



- ✓ **Le système d'exploitation actuel** : Si vous voulez conserver le système d'exploitation actuel, le programme d'installation pourra réaliser une installation en multiboot. Vous pourrez choisir le système d'exploitation démarré à chaque mise en marche de l'ordinateur.

C'est rarement une bonne idée pour des serveurs ; il est préférable de *supprimer* le système d'exploitation existant.

- ✓ **Partitionnement du disque système** : Le plus souvent, le disque du serveur conserve une partition unique. Cependant, si vous voulez diviser le disque en deux partitions ou plus, vous devrez le faire pendant l'installation (à la différence de la plupart des autres choix d'installation, il est difficile de modifier celui-ci plus tard).
- ✓ **Nom de l'ordinateur** : Pendant l'installation du système d'exploitation, vous êtes invité à fournir le nom de l'ordinateur pour identifier le serveur sur le réseau.



Si votre réseau ne possède que quelques serveurs, vous pouvez juste donner un nom tel que Server01 ou MonServeur. Si votre réseau possède un nombre important de serveurs, suivez une directive établie pour créer les noms des serveurs.

- ✓ **Mot de passe administrateur** : Vous ne devez pas entrer quelque chose d'évident comme votre prénom ou votre nom de famille. De plus, vous ne devez pas saisir quelque chose d'aléatoire que vous oublierez rapidement parce que vous serez dans une impasse si vous oubliez le mot de passe administrateur !



Inventez un mot de passe complexe se composant d'un mélange de lettres majuscules et minuscules, de chiffres et d'un ou deux caractères spéciaux. Inscrivez-le ensuite sur un papier et conservez-le dans un endroit clos où vous savez qu'il ne se perdra pas.

- ✓ **Protocoles réseau** : Vous devez presque toujours installer le protocole TCP/IP, le protocole client réseau de Microsoft et le partage de fichiers et d'imprimante. Selon la façon dont le serveur sera utilisé, vous pouvez vouloir installer d'autres protocoles.
- ✓ **Configuration TCP/IP** : Vous devez connaître l'adresse IP qui sera affectée au serveur. Même si votre réseau possède un serveur DHCP (destiné à assigner dynamiquement des adresses IP aux clients), attribuez aux serveurs des adresses IP statiques.
- ✓ **Nom de domaine** : Vous devez connaître le nom de domaine de votre réseau.

Dernières mises au point

Avant de commencer l'installation, voici quelques tâches à réaliser :

- ✓ Nettoyez le disque du serveur en désinstallant les logiciels dont vous n'avez pas besoin et en supprimant les données qui ne sont plus nécessaires. Cette étape est particulièrement importante si le futur serveur est un ancien poste client. Par exemple, sur le serveur, vous n'aurez pas besoin de Microsoft Office ni des logiciels de jeu.
- ✓ Faites une sauvegarde complète de l'ordinateur. Bien que les programmes d'installation du système d'exploitation soient stables et fiables, ce qui limite au maximum les éventuelles pertes de données au cours de l'installation, le risque n'est pas nul et vous n'êtes pas totalement à l'abri d'un incident imprévu.
- ✓ Si l'ordinateur est connecté à une alimentation secourue (onduleur) qui possède une interface série ou une connexion USB à l'ordinateur, débranchez l'interface série ou la connexion USB. Dans certains cas, cette connexion risque d'entrer en conflit avec le programme d'installation lorsqu'il tente de déterminer quels périphériques sont reliés à l'ordinateur.

Installer Windows Server 2008

Après avoir planifié votre installation et préparé votre ordinateur, vous êtes prêt à exécuter le programme d'installation. La démarche suivante décrit les étapes à respecter pour installer Windows Server 2008 sur un nouvel ordinateur équipé d'un lecteur DVD bootable.

1. Insérez le CD de distribution dans le lecteur DVD et redémarrez l'ordinateur.

Au bout d'un temps, l'Assistant Installer Windows s'ouvre.

2. Cliquez sur Installer pour démarrer l'installation.

L'assistant vous demande d'insérer le code produit qui figure sur un autocollant fixé sur le boîtier du CD.

3. Entrez le code produit de 25 caractères et cliquez sur Suivant.

Vu la longueur du code, il est possible de faire des erreurs. Si un message d'erreur vous informe que le code produit est invalide, ne paniquez pas. Recommencez !

Dès que le code produit correct est saisi, l'assistant vous demande de préciser l'édition du système d'exploitation que vous voulez installer. Les options dépendent de la version que vous avez achetée. Pour la version Standard, vous pouvez choisir d'installer l'intégralité de l'édition Standard du système d'exploitation serveur ou l'édition Core.

4. Sélectionnez l'édition que vous voulez installer et cliquez sur Suivant.

L'assistant d'installation affiche les informations d'accord de licence. Lisez-les si vous êtes fan du langage juridique.

5. Cochez J'accepte les termes du contrat de licence et cliquez sur Suivant.

L'assistant vous invite ensuite à spécifier si vous voulez effectuer une installation de mise à niveau ou une installation complète.

6. Choisissez l'option d'installation souhaitée.

Le programme d'installation affiche les informations de partition courantes de l'ordinateur. Sélectionnez la partition que vous voulez utiliser pour l'installation. Si nécessaire, vous pouvez reconfigurer vos partitions en supprimant les partitions existantes ou en en créant de nouvelles. Je suppose que vous allez créer une partition unique qui utilise tout l'espace disponible sur le disque.

7. Sélectionnez la partition sur laquelle vous voulez installer Windows et cliquez sur Suivant.

Le programme d'installation formate le disque et copie les fichiers sur le disque formaté. Cette étape peut prendre du temps. Je vous suggère de commencer à lire votre bouquin !

Une fois les fichiers copiés, le programme d'installation redémarre votre ordinateur puis il inspecte tous les périphériques de l'ordinateur et installe les pilotes nécessaires. N'hésitez pas à lire un chapitre supplémentaire de votre livre pendant cette opération !

Quand il a terminé d'installer les pilotes, le programme d'installation affiche la fenêtre Tâches de configuration initiales, illustrée par la Figure 7.2. Consultez cette fenêtre pour réaliser les tâches de configuration requises afin de rendre votre serveur opérationnel.

La fenêtre Tâches de configuration initiales vous permet d'effectuer les actions suivantes :

- Définir le fuseau horaire.
- Configurer le réseau.

- Indiquer un nom d'ordinateur et un domaine.
- Activer la mise à jour et l'envoi de rapports automatiques.
- Télécharger et installer les mises à jour.
- Ajouter des rôles et des fonctionnalités.
- Configurer le Pare-feu Windows.

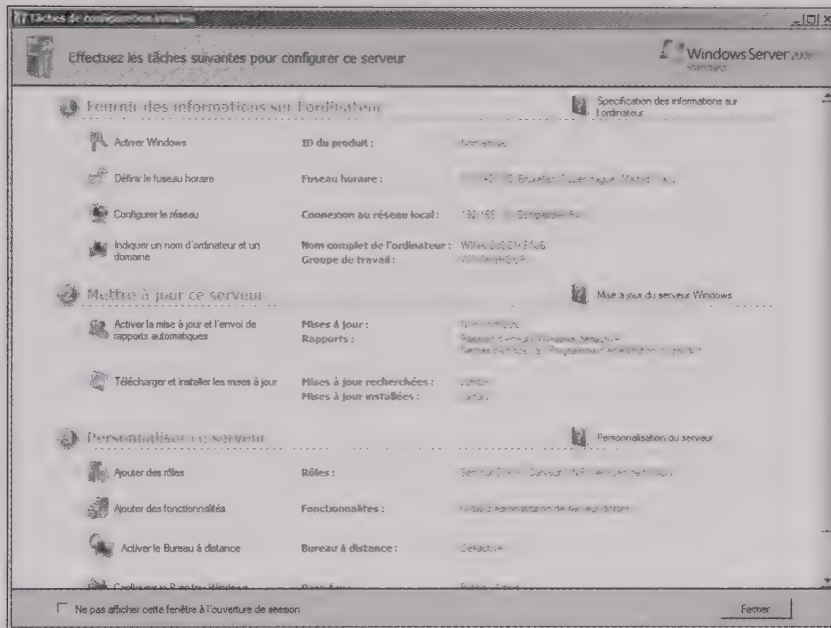


Figure 7.2 : Fenêtre Tâches de configuration initiales.

Organisez-vous comme bon vous semble pour réaliser ces différentes tâches. Les intitulés parlent d'eux-mêmes. Alors lancez-vous et laissez-vous guider par les assistants.

Après l'installation

À la fin de l'installation, vous devez encore réaliser quelques tâches pour que votre serveur soit opérationnel. Les sections suivantes décrivent les actions post-installation.

Ouvrir une session

Dès que le programme d'installation a redémarré votre ordinateur pour la dernière fois, vous devez ouvrir une session avec le compte Administrateur :

1. Appuyez sur **Ctrl+Alt+Suppr** pour ouvrir une session.
2. Entrez le mot de passe **Administrateur** que vous avez défini pendant l'installation.
3. Appuyez sur **Entrée**.

Windows ouvre la session administrateur et affiche le Bureau Windows qui vous est familier.

Activer Windows

La contrainte d'activation de Windows est assurément très ennuyeuse mais Microsoft affirme qu'elle contribue à réduire le piratage. Par conséquent, vous disposez de trente jours pour activer Windows. Si vous n'activez pas le produit durant ces 30 jours, il cesse de fonctionner, alors autant l'activer directement après l'avoir installé.

Heureusement, l'activation d'un système d'exploitation serveur Windows est une opération simple si vous avez une connexion Internet opérationnelle. Windows affiche une info-bulle de rappel de l'activation en bas à droite du Bureau. Il suffit de cliquer sur cette info-bulle pour démarrer l'Assistant Activation.

Télécharger des service packs

Les *service packs* sont les mises à jour d'un système d'exploitation. Ils contiennent des améliorations mineures et des solutions à d'éventuels problèmes. La plupart de ces solutions concernent des problèmes de sécurité qui ont été découverts après la première mise sur le marché du système d'exploitation. La méthode la plus courante pour obtenir les services packs est de les télécharger sur le site Web du fabricant du système d'exploitation.

Suivant le système d'exploitation que vous avez installé, vous devez (ou pas) installer un service pack immédiatement après son installation. Le programme d'installation de Windows Server 2008 vérifie automatiquement les mises à jour avant de commencer l'installation, ce qui vous dispense théoriquement d'installer un service pack à la fin de l'installation. Cependant, vous pouvez devoir le faire avec d'autres systèmes d'exploitation.

L'installation de *service packs* est une opération à laquelle vous n'échapperez pas au cours de la vie du serveur. Microsoft et les autres concepteurs de système d'exploitation publient périodiquement de nouveaux *service packs* pour corriger des problèmes au fur et à mesure qu'ils surgissent.

Tester l'installation

Lorsque l'installation est terminée, contrôlez votre serveur avant de le mettre en service. Voici quelques vérifications simples que vous pouvez exécuter pour vous assurer qu'il a été installé correctement :

- ✓ Consultez l'Observateur d'événements pour voir s'il contient des messages d'erreur liés à l'installation ou à la mise en route. Selon la version de Windows Server, exécutez Démarrer/Outils d'administration/Observateur d'événements ou Démarrer/Tous les programmes/Outils d'administration/Observateur d'événements (les systèmes d'exploitation serveurs autres que Windows ont des caractéristiques similaires qui permettent de visualiser les journaux d'événements).
- ✓ Vérifiez la configuration TCP/IP en exécutant la commande `ipconfig /all` à partir de l'invite de commande. Cette commande indique si le protocole TCP/IP est opérationnel et affiche le nom d'hôte, l'adresse IP et d'autres informations TCP/IP.
- ✓ Pour vous assurer que le serveur est accessible à partir du réseau, ouvrez l'invite de commande à partir d'un ordinateur du réseau et essayez d'accéder au serveur en exécutant la commande `ping nom_hôte` où `nom_hôte` est le nom d'hôte affiché par la commande `ipconfig` exécutée à partir du serveur.

Configurer les rôles du serveur

Les *rôles du serveur* sont des rôles que votre serveur peut jouer sur le réseau comme serveur de fichiers, serveur Web ou serveur DHCP ou DNS. Les fonctionnalités sont des fonctions supplémentaires du système d'exploitation Windows lui-même, comme .NET Framework ou Sauvegarde de Windows Server. En réalité, la différence entre rôles et fonctionnalités est très arbitraire. Par exemple, serveur Web est considéré comme un rôle tandis que serveur Telnet est une fonctionnalité. Allez comprendre !

La fenêtre Tâches de configuration initiales, illustrée par la Figure 7.2, vous permet d'ajouter des rôles et des fonctionnalités à votre serveur. Une fois la configuration initiale achevée, sélectionnez Démarrer/Outils d'administration/Gestionnaire de serveur pour afficher la fenêtre Gestionnaire de serveur,

représentée dans la Figure 7.3. Comme vous pouvez le voir, cette fenêtre propose un lien vous permettant d'ajouter des rôles ou des fonctionnalités.

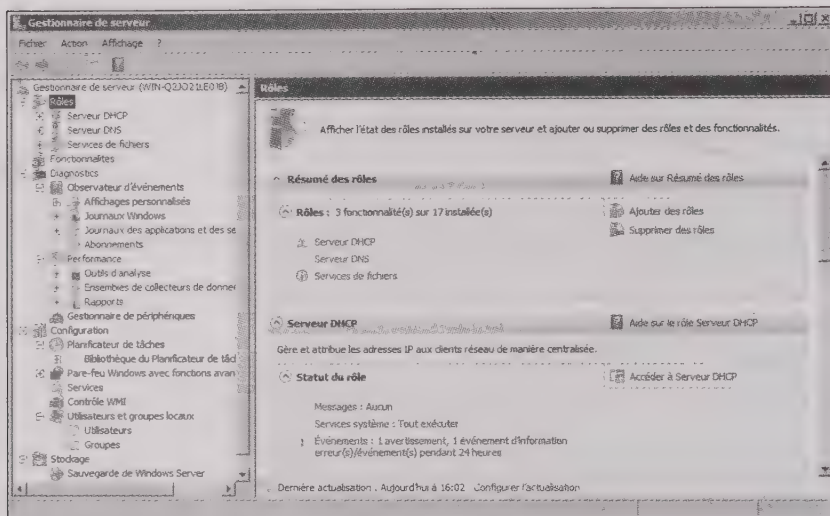


Figure 7.3 : Fenêtre Gestionnaire de serveur.

Procédez comme suit pour installer des rôles de serveur. La démarche pour installer des fonctionnalités de serveur est similaire.

1. Cliquez sur le lien **Ajouter des rôles** dans la fenêtre **Gestionnaire de serveur** ou **Tâches de configuration initiales**.

Dans les deux cas, l'assistant Ajout de rôles apparaît.

2. Cliquez sur **Suivant**.

La page Rôles de serveurs, illustrée par la Figure 7.4, s'ouvre. Elle vous invite à sélectionner un ou plusieurs rôles à ajouter au serveur.

3. Sélectionnez un ou plusieurs rôles à installer.

Dès que vous cliquez sur un rôle, une brève description s'affiche. Par exemple, si vous cliquez sur le rôle Serveur Web (IIS), le texte suivant apparaît :

Serveur Web (IIS) fournit une Infrastructure d'application Web fiable, gérable et évolutive.

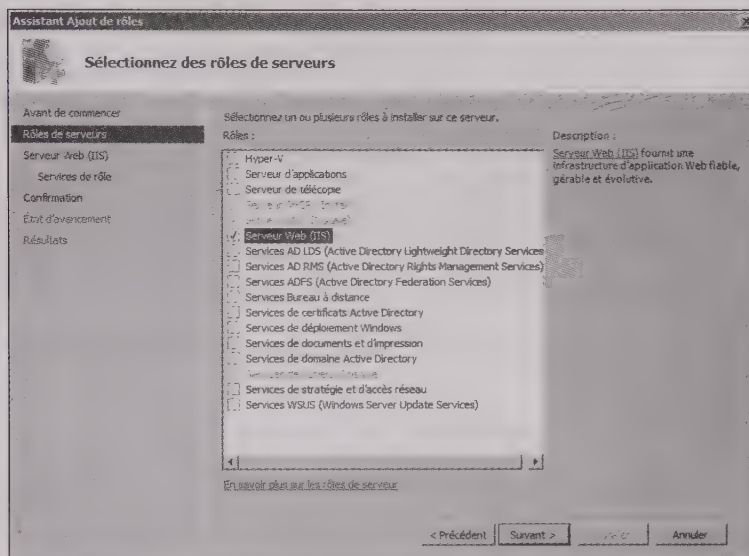


Figure 7.4 : Page Rôles de serveurs.

4. Cliquez sur Suivant.

Il se peut qu'une page supplémentaire s'affiche pour vous permettre de sélectionner les services de rôle que vous voulez installer. Tout dépend du ou des rôles sélectionnés précédemment. Par exemple, la Figure 7.5 montre la page Services de rôle du rôle Services de fichiers.

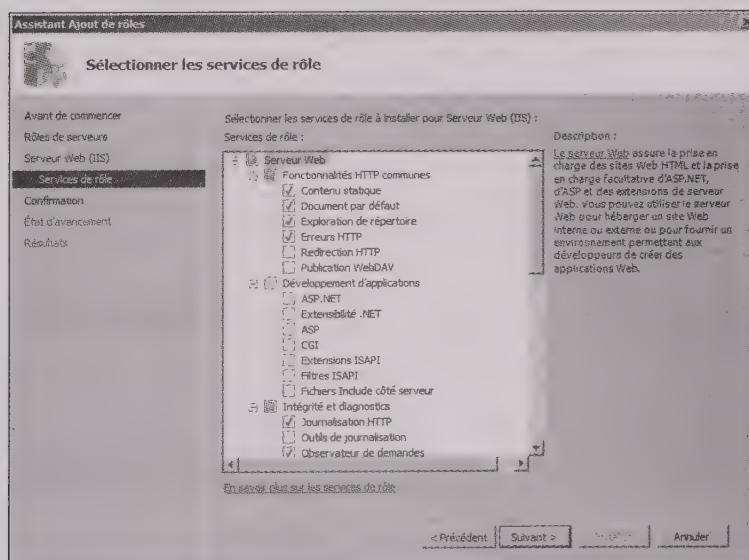


Figure 7.5 : Page Services de rôle.

5. Sélectionnez les services que vous voulez installer.

Là aussi, dès que vous cliquez sur un service, une description s'affiche. Par exemple, lorsque vous sélectionnez le service Serveur de fichiers, le texte suivant apparaît :

Le serveur de fichiers gère les dossiers partagés et permet aux utilisateurs d'accéder aux fichiers sur cet ordinateur à partir du réseau.

6. Cliquez sur Suivant.

Une page de confirmation affiche les rôles et les services que vous avez sélectionnés.

7. Cliquez sur Installer.

Windows installe le rôle de serveur et ses services. Une barre de progression défile pendant l'installation pour vous permettre de suivre l'installation. À la fin de l'installation, une page de résultats s'affiche.

8. Cliquez sur Fermer.

C'est terminé !

Chapitre 8

Configurer les clients Windows XP, Vista et 7

Dans ce chapitre :

- Configurer les connexions réseau pour les clients Windows.
- Paramétrer le nom de l'ordinateur, sa description et le groupe de travail.
- Rejoindre un domaine.
- Configurer les options de connexion.

Avant que le réseau soit opérationnel, vous devez configurer les ordinateurs clients. Il faut notamment configurer chacune de leurs cartes réseau afin qu'elles fonctionnent correctement et installer les protocoles permettant aux clients de communiquer avec les autres ordinateurs du réseau.

Fort heureusement, sous Windows, ces tâches de configuration sont un véritable jeu d'enfant. En effet, Windows reconnaît automatiquement la carte réseau au moment du démarrage de l'ordinateur. Il ne reste plus qu'à vérifier s'il a correctement installé les protocoles réseau et les logiciels clients.

À chaque nouvelle version de Windows, Microsoft a simplifié les processus de configuration du réseau. Dans ce chapitre, vous découvrirez comment configurer une mise en réseau sous Windows XP, Windows Vista et Windows 7.

Configurer des connexions réseau

Windows reconnaît automatiquement votre carte réseau quand vous démarrez votre ordinateur. Normalement, vous n'avez pas à installer manuellement les pilotes mais il se peut que vous ayez à modifier manuellement la configuration de la connexion réseau. Les sections suivantes décrivent les procédures de connexion pour Windows XP, Vista et 7.

Configurer des connexions réseau sous Windows XP

Les étapes qui suivent expliquent comment configurer votre connexion réseau sous Windows XP :

1. Choisissez Démarrer/Panneau de configuration.

Le Panneau de configuration apparaît.

2. Double-cliquez sur l'icône Connexions réseau.

La boîte de dialogue Connexions réseau s'affiche, comme le montre la Figure 8.1.

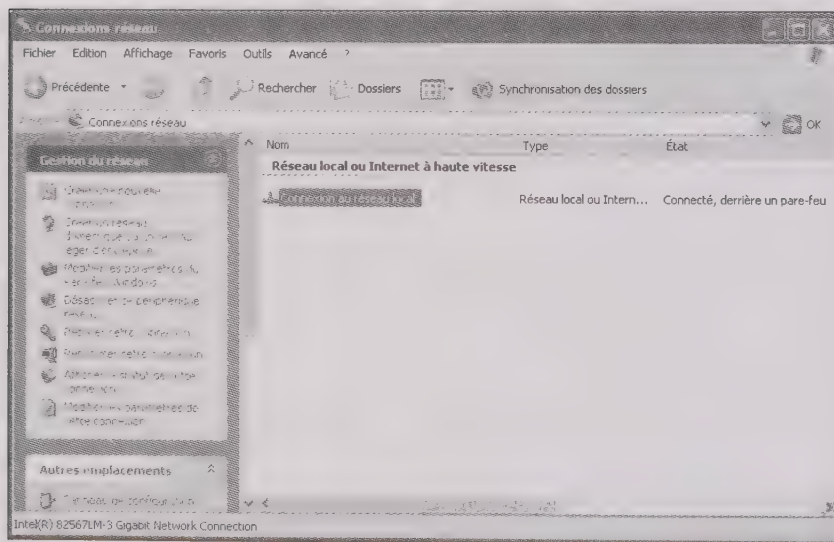


Figure 8.1 : Boîte de dialogue Connexions réseau.



3. Effectuez un clic droit sur la connexion à configurer puis, dans le menu contextuel, sélectionnez **Propriétés**.

Vous pouvez aussi sélectionner la connexion et, dans le volet des tâches, cliquer sur **Modifier les paramètres de cette connexion**. Dans les deux cas, la boîte de dialogue **Propriétés de Connexion au réseau local** apparaît (Figure 8.2).

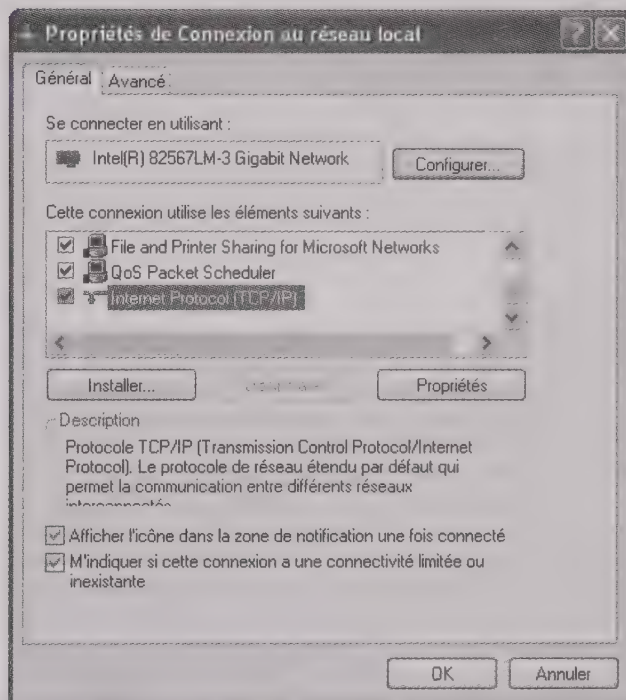


Figure 8.2 : Boîte de dialogue **Propriétés de Connexion au réseau local**.

4. Pour configurer les paramètres de la carte réseau, cliquez sur **Configurer**.

Cette action ouvre la boîte de dialogue **Propriétés de la carte réseau**, illustrée par la Figure 8.3. Elle comporte cinq onglets qui vous permettent de configurer la carte d'interface réseau :

- **Général.** Cet onglet affiche les informations de base concernant la carte réseau. Par exemple, la carte représentée dans la Figure 8.3 est une Intel® 82567LM-3 au Gigabit installée sur le connecteur PCI 0 de la carte mère.

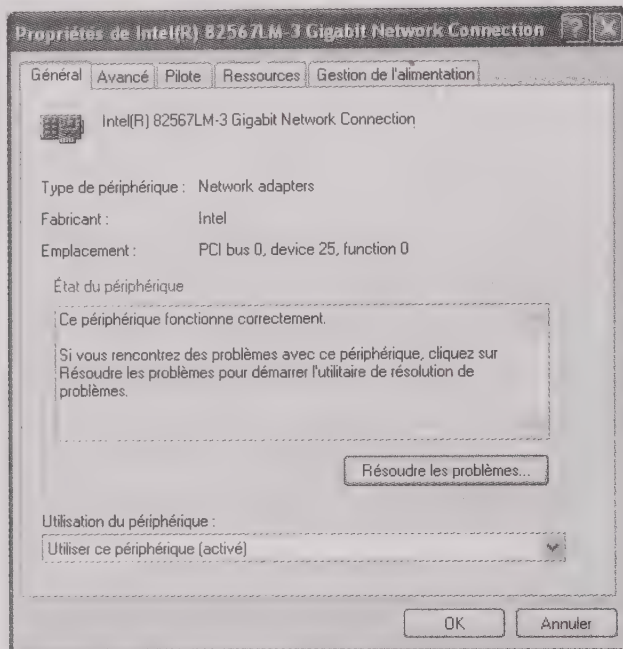


Figure 8.3 : Boîte de dialogue Propriétés d'une carte réseau.



Si vous avez des problèmes avec cette carte, cliquez sur le bouton Résoudre les problèmes. Cette action donne accès au Centre d'aide et de support. Vous pouvez aussi désactiver ce périphérique afin qu'il n'empêche pas d'autres composants de fonctionner correctement.

- **Avancé.** Cet onglet permet de configurer divers paramètres spécifiques à votre matériel dont dépend le bon fonctionnement de la carte réseau. Par exemple, certaines cartes permettent de définir le débit (classiquement, 10, 100 ou 1000 Mbps) ou le nombre de tampons alloués à la carte.

Consultez attentivement le manuel de la carte réseau avant de bidouiller ces paramètres.

- **Pilote.** Cet onglet affiche les informations concernant le pilote de la carte et permet de le mettre à jour ou bien, si la nouvelle version n'est pas satisfaisante, de revenir à la version précédente ou de désinstaller le pilote.
- **Ressources.** Dans cet onglet, vous pouvez limiter manuellement les ressources informatiques requises par la carte, notamment la plage de mémoire, la plage des entrées/sorties ainsi que l'affectation des IRQ et des canaux DMA.





À l'époque, avant l'avènement des cartes plug-and-play, vous deviez configurer ces paramètres dès que vous installiez une carte réseau, au risque de générer des conflits de ressources. Comme Windows les configure à présent automatiquement, vous aurez rarement à les modifier.

- **Gestion de l'alimentation.** Dans cet onglet, vous pouvez spécifier si la carte doit être désactivée lorsque l'ordinateur se met en veille et paramétrer un réveil périodique de l'ordinateur afin de rafraîchir l'état du réseau.



Quand vous cliquez sur OK pour valider les options de la boîte de dialogue des propriétés du réseau, cette dernière se ferme. Vous devrez cliquer sur le lien Modifier les paramètres de cette connexion pour continuer la procédure.

5. Assurez-vous que les éléments de réseau requis par l'ordinateur client sont listés dans la boîte de dialogue Propriétés de la connexion.

Les paragraphes qui suivent décrivent les éléments que vous rencontrerez le plus fréquemment. Ils ne sont pas nécessaires pour tous les réseaux :

- **Client pour les réseaux Microsoft.** Cet élément est requis si vous désirez accéder à un réseau Microsoft Windows. Il devrait toujours être présent et coché.
- **Partage de fichiers et d'imprimantes pour les réseaux Microsoft.** Cet élément permet à l'ordinateur de partager ses fichiers et les imprimantes avec les autres ordinateurs sur le réseau.



Cette option est généralement utilisée par les connexions pair-à-pair mais elle peut aussi l'être sur un réseau comportant des serveurs dédiés. Vous pouvez désactiver cet élément si vous n'avez pas l'intention de partager les fichiers et les imprimantes de l'ordinateur client.

- **Protocole Internet (TCP/IP).** Cet élément permet à l'ordinateur client de communiquer via le protocole TCP/IP.

Si tous les serveurs du réseau reconnaissent ce protocole, il devrait être le seul installé.

- **Protocole de transport compatible NWLink IPX/SPX/NetBIOS.** Ce protocole n'est requis que si le réseau se connecte à un ancien réseau NetWare utilisant le protocole IPX/SPX.

6. Si le protocole dont vous avez besoin ne figure pas dans la liste, cliquez sur le bouton **Installer** afin de l'ajouter :

Une boîte de dialogue apparaît, demandant si vous désirez ajouter un client, un service ou un protocole. Choisissez Protocole puis cliquez sur Ajouter. Une liste des protocoles disponibles s'affiche. Sélectionnez celui que vous désirez puis cliquez sur OK (il vous sera peut-être demandé d'insérer le CD de Windows).

7. Assurez-vous que le client réseau figure dans la liste des ressources du réseau.

Pour un réseau basé sur Windows, veillez que Client pour les réseaux Microsoft soit listé. Pour un réseau NetWare, assurez-vous que l'option NetWare Client de Novell apparaisse. Si votre réseau utilise les deux types de serveurs, vous pouvez choisir les deux clients.



Si vous avez des serveurs NetWare, utilisez le logiciel de client NetWare livré avec NetWare plutôt que le client fourni par Microsoft avec Windows.

8. Si le client dont vous avez besoin n'est pas listé, cliquez sur le bouton **Installer**, choisissez Client puis cliquez sur **Ajouter**. Sélectionnez ensuite le client désiré puis cliquez sur **OK**.

Le client sélectionné est ajouté à la boîte de dialogue Propriétés de la connexion réseau.

9. Pour supprimer un élément de réseau dont vous ne vous servez pas (comme Partage de fichiers et d'imprimantes pour les réseaux Microsoft), sélectionnez-le puis cliquez sur le bouton **Désinstaller**.

Pour des raisons de sécurité, vous devez supprimer tous les clients, protocoles et services que vous n'utilisez pas.

10. Pour configurer les paramètres TCP/IP, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés** pour afficher la boîte de dialogue Propriétés de Protocole Internet (TCP/IP). Configurez les paramètres puis cliquez sur **OK**.

La boîte de dialogue Propriétés de Protocole Internet (TCP/IP), représentée dans la Figure 8.4, propose les options suivantes :

- **Obtenir une adresse IP automatiquement.** Choisissez cette option si le réseau est géré par un serveur DHCP qui affecte automatiquement les adresses IP. Ce choix simplifie considérablement l'administration du protocole TCP/IP sur votre réseau (reportez-vous au Chapitre 6 pour en savoir plus sur le DHCP).

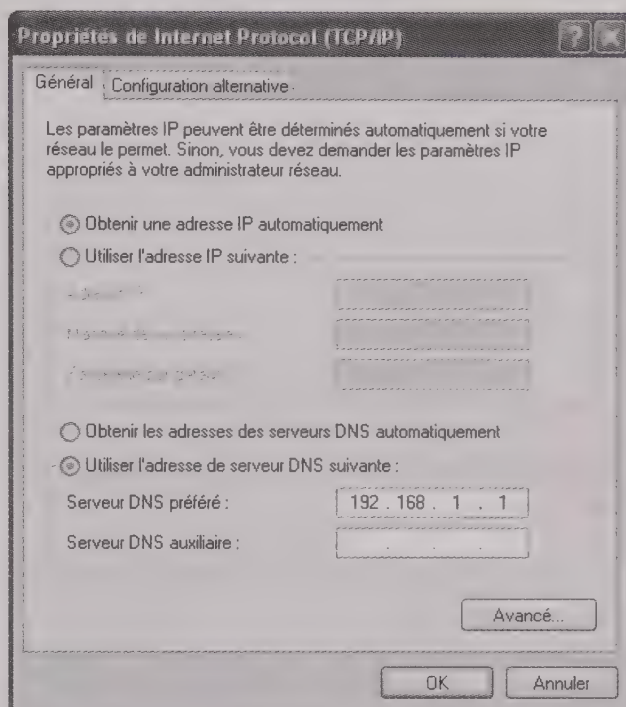


Figure 8.4 : Configuration du protocole TCP/IP.

- **Utiliser l'adresse IP suivante.** Si l'ordinateur doit avoir une adresse IP spécifique, choisissez cette option et tapez l'adresse IP de l'ordinateur, son masque de sous-réseau et l'adresse de la passerelle par défaut (reportez-vous au Chapitre 6 pour en savoir plus sur ces paramètres).
- **Obtenir les adresses des serveurs DNS automatiquement.** Le serveur DHCP peut aussi fournir l'adresse DNS (*Domain Name System*, système de nom de domaine) que l'ordinateur doit utiliser. Choisissez cette option si votre réseau est équipé d'un serveur DHCP (reportez-vous au Chapitre 6 pour en savoir plus sur le DNS).
- **Utiliser l'adresse de serveur DNS suivante.** Choisissez cette option si aucun serveur DNS n'est disponible. Tapez ensuite l'adresse IP du serveur DNS principal et celle du serveur DNS secondaire.

Configurer des connexions réseau sous Windows Vista et Windows 7

La configuration d'une connexion réseau sous Windows Vista et Windows 7 est très semblable à celle sous Windows XP. Sous Windows Vista et 7, la boîte de dialogue Propriétés de la carte réseau est légèrement plus difficile à trouver. Mais une fois que vous y êtes, les étapes de configuration sont identiques.

Procédez comme suit pour localiser les paramètres :

1. Choisissez Démarrer/Panneau de configuration.

Le Panneau de configuration apparaît.

2. Dans la catégorie Réseau et Internet, cliquez sur Afficher l'état et la gestion du réseau.

Cette étape ouvre le Centre Réseau et partage. La Figure 8.5 représente la version Windows 7 du centre Réseau et partage. Celle de Windows Vista est similaire.

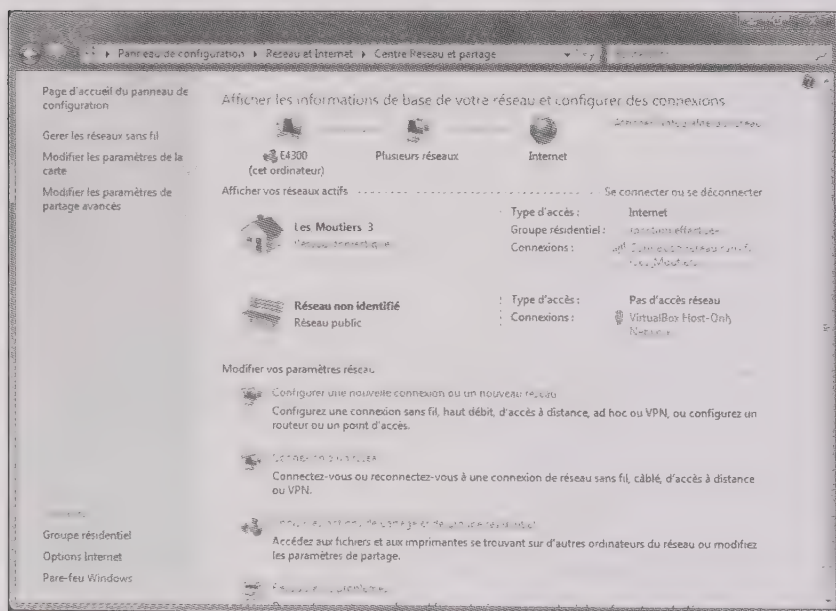


Figure 8.5 : Centre Réseau et partage (Windows 7).

3a. Sous Windows 7, cliquez sur Modifier les paramètres de la carte.

3b. Sous Windows Vista, cliquez sur Gérer les connexions réseau.

Dans les deux cas, la fenêtre Connexions réseau s'ouvre. La version Windows 7 de cette page est illustrée par la Figure 8.6.

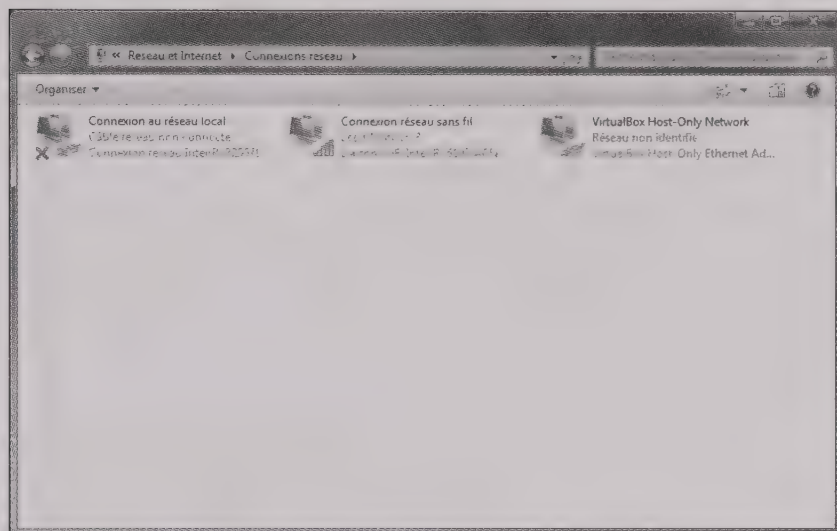


Figure 8.6 : Fenêtre Connexions réseau (Windows 7).

4. Effectuez un clic droit sur la connexion à configurer et sélectionnez Propriétés.

La boîte de dialogue Propriétés de Connexion au réseau local apparaît, comme le montre la Figure 8.7. Si vous comparez cette boîte de dialogue avec celle de la Figure 8.2, vous remarquerez qu'elles sont identiques.

5. Cliquez sur le bouton Configurer.

À partir de là, les étapes de configuration sont identiques à celles employées pour Windows XP. Par conséquent, vous pouvez continuer en revenant à l'étape 4 de la section précédente, « Configurer des connexions réseau sous Windows XP ».

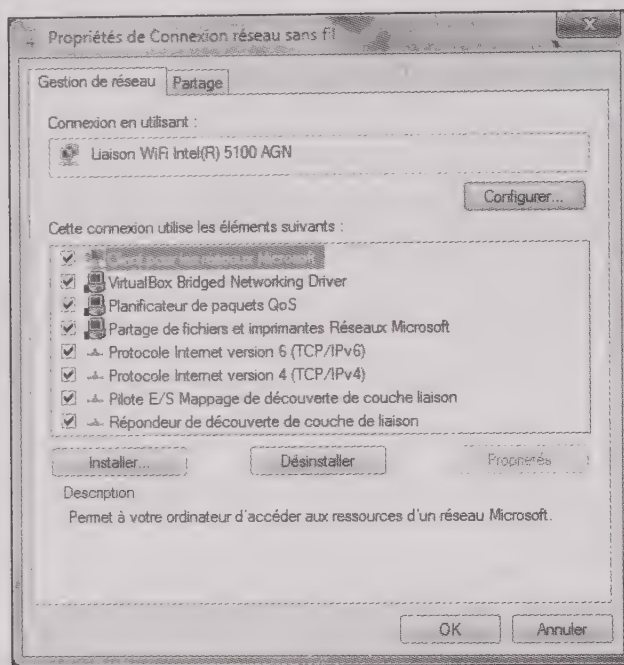


Figure 8.7 : Boîte de dialogue Propriétés de Connexion au réseau local (Windows 7).

Configurer l'identité d'un ordinateur client

Chaque ordinateur client doit s'identifier pour faire partie du réseau. Son identité est composée du nom de l'ordinateur et d'une description facultative ainsi que du nom de son groupe de travail ou du domaine auquel il appartient.

Le nom de l'ordinateur doit respecter les conventions de nommage NetBIOS : sa longueur doit être d'un à quinze caractères, il peut contenir des lettres, des chiffres ou des traits d'union mais ni espace ni point. Sur les petits réseaux, il est courant que le nom de l'ordinateur soit le même que le nom d'utilisateur. Pour des réseaux plus vastes, vous devrez développer des conventions de nommage qui indiquent l'emplacement de l'ordinateur. Par exemple, un nom comme C3051 sera affecté au premier ordinateur de la pièce 305 de l'immeuble C. Ou alors MKTG010 sera un des ordinateurs du service marketing.

Si l'ordinateur doit joindre un domaine, vous devrez pouvoir accéder, sur le domaine, à un compte Administrateur, à moins que vous ayez déjà créé un compte d'ordinateur sur ce domaine. Notez que seuls les ordinateurs

tournant sous Windows 2000, Windows XP, Windows Vista, Windows 7 et Windows Server (NT, 2000, 2003 et 2008) peuvent joindre un domaine. Les utilisateurs de Windows 95 ou 98 peuvent toutefois accéder aux ressources du domaine en s'y connectant en tant qu'utilisateurs mais des comptes d'ordinateur de domaine pour les clients Windows 9x ne sont pas requis.

Quand vous installez Windows sur un ordinateur client, le programme d'installation vous demande de définir le nom de l'ordinateur et le nom du groupe de travail ou du domaine. Ces informations peuvent être modifiées ultérieurement, si vous le désirez. La procédure varie si vous utilisez Windows XP, Windows Vista ou Windows 7.

Configurer l'identité d'un ordinateur sous Windows XP

Pour changer l'identification d'un ordinateur sous Windows XP, exécutez les étapes suivantes :

- 1. Ouvrez le Panneau de configuration puis double-cliquez sur l'icône Système pour afficher la boîte de dialogue Propriétés système.**

- 2. Cliquez sur l'onglet Nom de l'ordinateur.**

L'identité de l'ordinateur se trouve dans cet onglet.

- 3. Cliquez sur le bouton Modifier.**

La boîte de dialogue Modification du nom d'ordinateur apparaît, comme le montre la Figure 8.8.

- 4. Entrez le nouveau nom de l'ordinateur puis précisez le domaine ou le groupe de travail.**

Pour rejoindre un domaine, activez la case Domaine et saisissez le nom de domaine. Pour rejoindre un groupe de travail, activez la case correspondante et entrez le nom du groupe de travail.

- 5. Cliquez sur OK.**

- 6. Si cela vous est demandé, entrez le nom d'utilisateur et le mot de passe du compte Administrateur.**

Vous ne devrez fournir ces informations que si un compte d'ordinateur n'a pas encore été créé pour l'ordinateur client.

- 7. Dans la boîte de dialogue vous informant que vous devez redémarrer l'ordinateur, cliquez sur OK.**

C'est terminé !



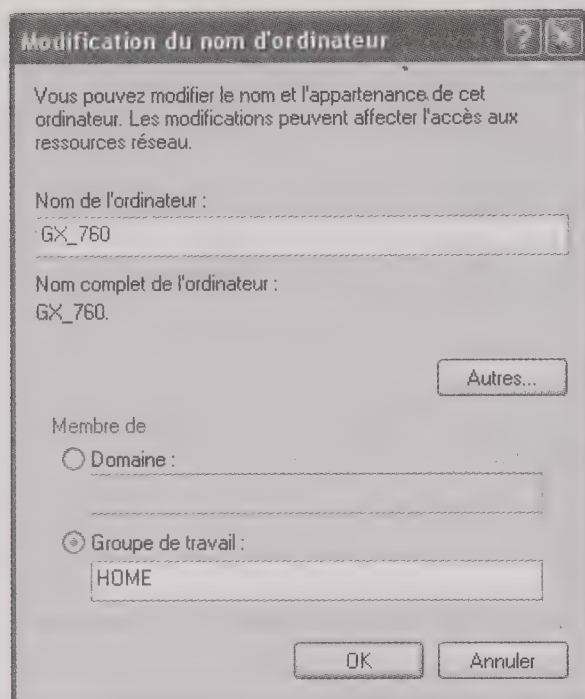


Figure 8.8 : Boîte de dialogue Modification du nom d'ordinateur (Windows XP).

Configurer l'identité d'un ordinateur sous Windows Vista et Windows 7

La méthode pour modifier l'identité d'un ordinateur est identique sous Windows Vista et Windows 7. Les figures proposées dans cette section représentent un système Windows 7. Notez qu'elles sont très similaires sous Windows Vista. Voici la démarche :

1. Cliquez sur **Démarrer** puis effectuez un clic droit sur **Ordinateur** et sélectionnez **Propriétés**.

La fenêtre **Système** apparaît, comme le montre la Figure 8.9. Localisez la section qui mentionne le nom d'ordinateur, de domaine et de groupe de travail.

2. Cliquez sur le lien **Modifier les paramètres**.

Si une boîte de dialogue s'affiche pour vous demander l'autorisation de continuer, cliquez sur **Continuer**. La boîte de dialogue **Propriétés système** s'ouvre alors (Figure 8.10).

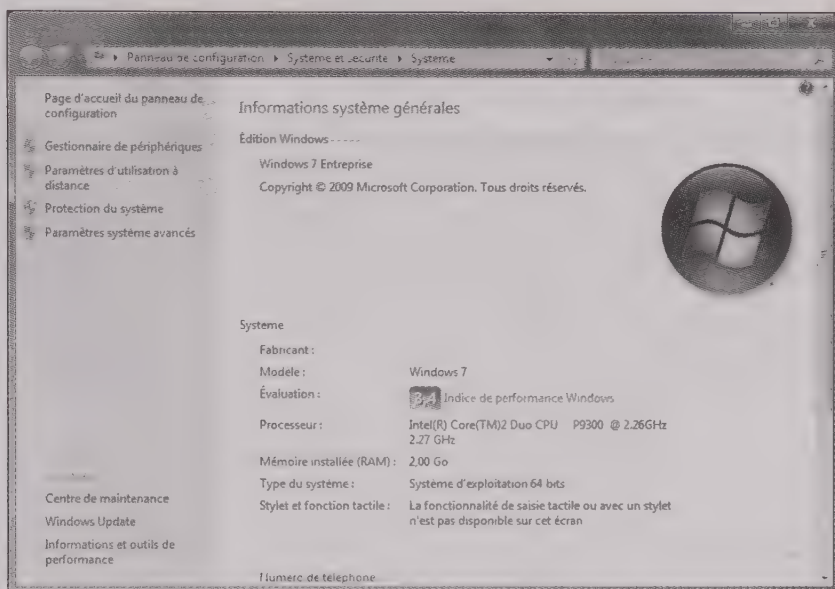


Figure 8.9 : Fenêtre Système (Windows 7).

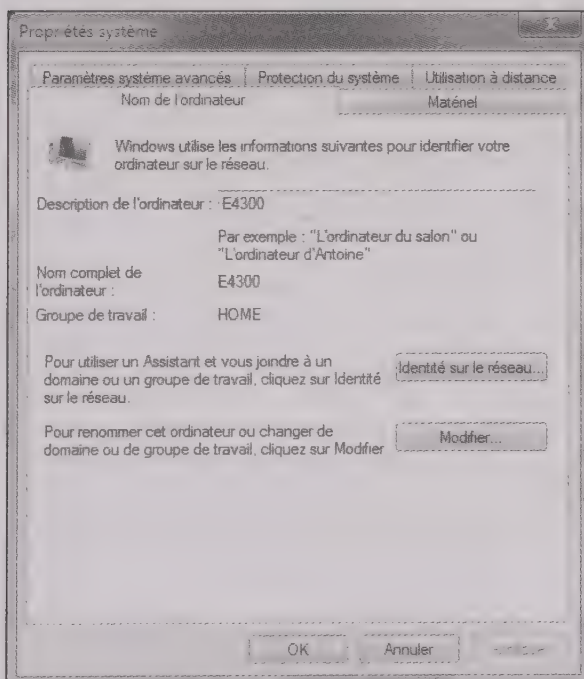


Figure 8.10 : Boîte de dialogue Propriétés système (Windows 7).

3. Cliquez sur le bouton Modifier.

La boîte de dialogue Modification du nom ou du domaine de l'ordinateur s'affiche (Figure 8.11).

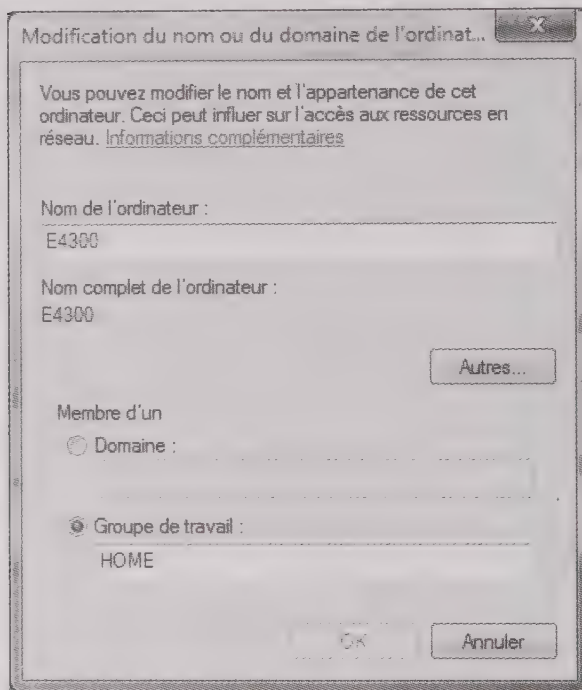


Figure 8.11 : Boîte de dialogue Modification du nom ou du domaine de l'ordinateur (Windows 7).

4. Entrez le nom de l'ordinateur puis spécifiez le domaine ou le groupe de travail.



Pour rejoindre un domaine, activez la case Domaine et entrez le nom de domaine. Pour rejoindre un groupe de travail, activez la case correspondante et entrez le nom du groupe de travail.

5. Cliquez sur OK.

6. Si cela vous est demandé, entrez le nom d'utilisateur et le mot de passe du compte Administrateur.

Vous ne devrez fournir ces informations que si un compte d'ordinateur n'a pas encore été créé pour l'ordinateur client.

7. Dans la boîte de dialogue vous informant que vous devez redémarrer l'ordinateur, cliquez sur OK.

L'ordinateur est ajouté au domaine ou au groupe de travail !

Configurer la connexion au réseau

Chaque utilisateur désireux d'accéder à un réseau basé sur un domaine doit ouvrir une session sur le domaine en faisant appel à un compte utilisateur valide. Ce dernier est créé dans le contrôleur de domaine et non dans l'ordinateur client.



Une ouverture de session au réseau n'est pas requise pour accéder aux ressources du groupe de travail. Ces ressources peuvent cependant être protégées par un mot de passe qui en restreint l'accès.

Quand vous démarrez un ordinateur tournant sous Windows qui a été configuré pour rejoindre un domaine, comme nous l'avons expliqué précédemment dans la section « Configurer l'identité d'un ordinateur client », la boîte de dialogue d'ouverture de session Windows s'affiche. L'utilisateur entre le nom d'utilisateur de domaine et le mot de passe puis il sélectionne dans une liste le domaine auquel il veut se joindre.



Il est possible de créer sous Windows des comptes d'utilisateurs locaux qui permettent aux utilisateurs d'accéder aux ressources de l'ordinateur local. Pour s'y connecter, l'utilisateur sélectionne l'option Cet ordinateur, dans la liste, et entre le nom d'utilisateur et le mot de passe d'un compte utilisateur local. Lorsqu'un utilisateur ouvre une session avec un compte local, il n'est pas connecté à un domaine de réseau. Pour ce faire, il doit sélectionner le domaine dans la liste Ouvrir une session.

Si l'ordinateur n'est pas membre d'un domaine, Windows affiche une icône pour chacun des utilisateurs locaux de l'ordinateur. L'utilisateur peut ouvrir une session en cliquant sur l'icône appropriée et en entrant un mot de passe (cette fonctionnalité n'existe pas sur les ordinateurs qui ont joint un domaine).

Notez que si l'utilisateur se connecte via un compte d'ordinateur local plutôt qu'avec un compte de domaine, il peut néanmoins accéder aux ressources du domaine. La boîte de dialogue Se connecter à apparaît dès que l'utilisateur tente d'accéder à une ressource du domaine. Il peut ensuite entrer un nom d'utilisateur de domaine et un mot de passe pour se connecter au domaine.

Chapitre 9

Réseau sans fil

Dans ce chapitre :

- ▶ S'initier aux standards des réseaux sans fil.
- ▶ Rappels de quelques notions de radio.
- ▶ Infrastructures et réseaux sans fil.
- ▶ Comprendre les points d'accès sans fil.
- ▶ Configurer Windows pour un réseau sans fil.

Avec les réseaux sans fil, plus besoin de câbles pour relier les ordinateurs car ils utilisent des ondes radio pour communiquer. Ainsi, un ordinateur peut être relié à un réseau sans fil, quel que soit l'endroit où il se trouve chez vous ou à votre bureau.



Les réseaux sans fil sont surtout utiles si vous avez des ordinateurs portables. Après tout, le principal avantage d'un portable est de pouvoir l'emporter n'importe où avec vous.

Ce chapitre présente les tenants et les aboutissants des réseaux sans fil.

Plongée dans les réseaux sans fil

Un *réseau sans fil* est un réseau qui utilise non pas des câbles mais des signaux radio pour échanger des informations.

Un ordinateur connecté à un réseau sans fil s'apparente à un téléphone portable. À l'instar des téléphones mobiles, dont vous pouvez vous servir sans être relié à une ligne téléphonique, l'ordinateur connecté à un réseau sans fil fonctionne sans câble réseau.

Les paragraphes suivants résument quelques-uns des principaux concepts et termes à connaître pour installer et utiliser un réseau sans fil basique :



- ✓ Les réseaux sans fil sont souvent appelés *WLAN* (*Wireless Local Area Network*, réseau local sans fil).

Vous trouverez aussi l'acronyme *LWAN*, pour *Local Area Wireless Network*.

Le terme *wifi* s'utilise aussi pour parler des réseaux sans fil bien qu'il désigne en fait des normes de réseau sans fil, 802.11b et 802.11g (voir la section « 802 point onze et des poussières »).

- ✓ Un réseau sans fil a un nom d'identification, le *SSID* (*Service Set Identifier*, identifiant d'ensemble de service). C'est une colle digne de *Questions pour un champion*, vous ne trouvez pas ?

Chacun des ordinateurs appartenant au même réseau sans fil doit avoir le même SSID.

- ✓ Les réseaux sans fil peuvent transmettre sur plusieurs canaux.

Pour que les ordinateurs puissent communiquer, ils doivent être configurés de façon à utiliser le même canal.

- ✓ Le type de réseau sans fil le plus élémentaire comprend plusieurs ordinateurs dotés d'une carte réseau sans fil.

Cette typologie est appelée *mode ad hoc*.

- ✓ Il existe une typologie plus complexe, le *mode infrastructure*. Plusieurs ordinateurs sans fil peuvent non seulement être connectés entre eux mais également être reliés à un réseau câblé via un appareil spécial, un *point d'accès sans fil* (*WAP*, en anglais). Je vous en dis plus sur les modes *ad hoc* et *infrastructure* plus loin dans ce chapitre.

Petite leçon d'électronique

J'étais vraiment un passionné d'électronique. J'en ai fait pendant trois ans au lycée. Le cours se trouvait juste à côté de la boutique d'accessoires auto que fréquentaient tous les copains. Je me gavais de diodes et de condensateurs tout au long de la journée tandis qu'eux achetaient des systèmes stéréo de deux gigawatts pour leur voiture.

Quelques connaissances acquises dans mes cours d'électronique me furent bien utiles pour les réseaux sans fil. Très peu, je vous rassure. Quelques notions de radio vous permettront cependant de mieux comprendre ce qu'est un réseau sans fil.

Ondes et fréquences

Une émission radio est basée sur des ondes qui traversent l'atmosphère. Elles ne sont ni visibles ni audibles mais un récepteur est capable de les convertir en sons, en images et, dans le cas des réseaux sans fil, en données informatiques.

Les ondes radio sont en fait des ondes cycliques d'énergie électromagnétique qui se répètent à une *fréquence* donnée. La Figure 9.1 montre des ondes radio à deux fréquences : l'une à un seul cycle par seconde, l'autre à deux cycles par seconde. Les ondes radio ne sont pas émises à des fréquences aussi faibles mais à des fréquences beaucoup plus élevées, comme 680 000 cycles par seconde ou 2,4 millions de cycles par seconde.



La fréquence est mesurée en *cycles par seconde*. En l'honneur de Heinrich Hertz, qui est le premier à avoir produit et capté des ondes radio (c'était en 1887), un cycle par seconde est usuellement appelé *hertz*, abrégé en *Hz*. Cette mesure est déclinée en kilohertz (KHz, mille cycles par seconde), en mégahertz (MHz, un million de cycles par seconde) et en gigahertz (GHz, un milliard de cycles par seconde). Ainsi, 2,4 MHz est correct, contrairement à 2,4 Mhz !

Les émetteurs et les récepteurs peuvent être réglés pour produire et recevoir des ondes à une fréquence bien précise, comme le savent tous ceux qui écoutent de la musique sur un poste de radio.

Longueur d'onde et antennes

La fréquence est liée à la notion de *longueur d'onde*. Les ondes radio voyagent à la vitesse de la lumière. La longueur d'onde indique la distance parcourue par le signal radio en un seul cycle. Par exemple, la vitesse de la lumière étant approximativement de 300 millions de mètres par seconde, la longueur d'une onde radio de 1 Hz est d'environ 300 millions de mètres. Celle d'un signal à 2 Hz est de 150 millions de mètres.

Comme vous le constatez, la longueur d'onde décroît lorsque la fréquence s'accroît. La longueur d'onde d'une station de radio émettant en modulation d'amplitude est de l'ordre de 580 KHz, soit 500 mètres environ. La télévision, elle, émet à 100 MHz, soit environ 3 mètres. En ce qui concerne un réseau sans fil à 2,4 GHz, la longueur d'onde n'est que de 12 centimètres.

Il en résulte que, plus la longueur d'onde est courte, plus l'antenne peut être courte. Les émissions en haute fréquence s'accommodent d'antennes de petite taille. Vous aurez remarqué que les stations de radio émettant sur les grandes ondes (GO) sont surmontées d'une haute antenne souvent placée sur un pylône, alors que les téléphones mobiles sont équipés de toutes

petites antennes. C'est tout simplement parce que ces derniers opèrent sur des fréquences beaucoup plus élevées que les stations de radio GO.

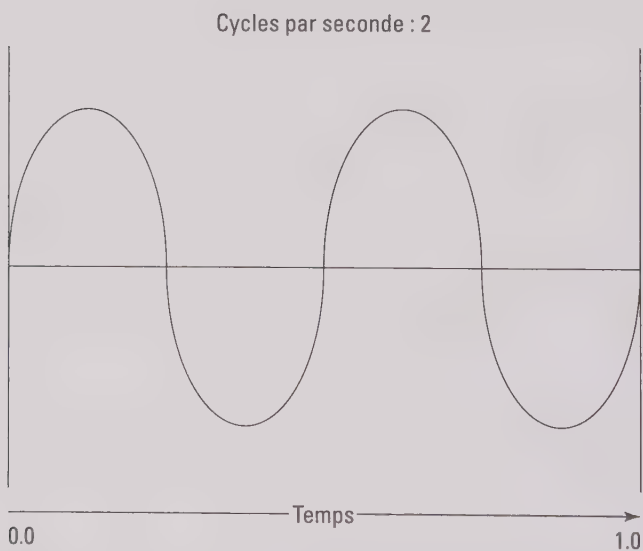
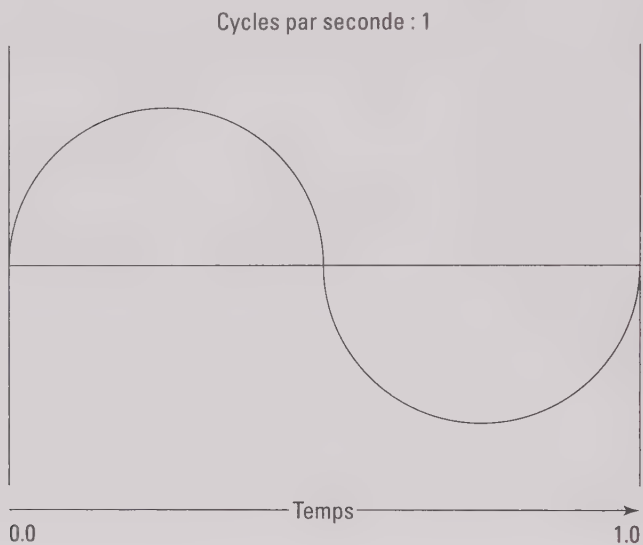


Figure 9.1 : Les ondes radio se caractérisent par leur fréquence.

Spectre et ART

Le terme *spectre* désigne une plage de fréquences. En France, l'attribution des fréquences pour la téléphonie et le wifi est décidée par l'ART (Autorité de Régulation des Télécommunications, www.art-telecom.fr).

Le Tableau 9.1 présente les bandes de fréquence les plus communément utilisées. Remarquez que certaines plages sont très vastes (la télévision UHF s'étend de 470 à 806 MHz) alors que d'autres sont confinées à des fréquences très précises. La différence entre la fréquence la plus basse et la plus élevée d'une bande est appelée *largeur de bande*.

Tableau 9.1 : Bandes radio les plus connues.

<i>Bande</i>	<i>Utilisation</i>
535 à 1700 KHz	Radio, grandes ondes (GO)
5,9 à 26,1 MHz	Radio, ondes courtes (OC)
26,96 à 27,41 MHz	CB (Citizen Band)
54 à 88 MHz	Télévision VHF (canaux 2 à 6)
88 à 108 MHz	Radio FM
174 à 220 MHz	Télévision VHF (canaux 7 à 13)
470 à 806 MHz	Télévision (canaux UHF)
806 à 890 MHz	Téléphones cellulaires
900 MHz	Téléphones sans fil
1850 à 1990 MHz	Téléphone cellulaire PCS
2,4 à 2,4835 GHz	Téléphones et réseaux sans fil (802.11b et 802.11g)
4 à 5 GHz	Télévision par satellite, grande parabole
5 GHz	Réseaux sans fil (802.11a)
11,7 à 12,7 GHz	Télévision par satellite, petite parabole

Deux des bandes du spectre sont attribuées aux réseaux sans fil : 2,4 GHz et 5 GHz. Notez que ces bandes ne sont pas réservées uniquement aux réseaux sans fil. En France, la partie basse de la fréquence à 2,4 GHz est occupée par l'armée, ce qui a posé des problèmes pour l'introduction du wifi (l'armée a

cependant cédé la bande haute de la fréquence, au-dessus de 2,4465 GHz). Certains appareils (comme les haut-parleurs sans fil, les transmetteurs TV, les téléphones sans fil, etc.) émettent parfois dans ces fréquences.

Petit retour en arrière

Voici une révélation qui va vous amuser : eh bien, le premier système Ethernet était un réseau sans fil ! Ethernet puise ses racines dans un réseau développé à l'université d'Hawaï en 1970 : l'*Alohanet*. Ce réseau transmettait les données en utilisant de petites radios. Si deux ordinateurs transmettaient des données simultanément, une collision était détectée et ils étaient contraints d'attendre pendant un laps de temps aléatoire avant de retransmettre à nouveau les données. Cette méthode constitue les fondements pour la technique de base d'Ethernet, maintenant appelée Accès multiple avec écoute de la porteuse et détection de collisions (CSMA/CD, abréviation de *Carrier Sense Multiple Access/Collision Detection*). Dans sa thèse de doctorat à Harvard en 1973, Robert Metcalfe a développé son réseau câblé, Ethernet, en s'inspirant en partie du protocole sans fil d'Alohanet.

Pendant les vingt années qui ont suivi, Ethernet n'a été qu'un puissant réseau câblé. Ce n'est que vers le milieu des années 1990 qu'Ethernet est revenu à ses racines, le « sans fil ».

802 point onze et des poussières

Les standards de réseaux sans fil les plus connus sont ceux de type IEEE 802.11. Ces standards Ethernet sans fil utilisent les mêmes techniques de transmission que les standards Ethernet câblés (en d'autres termes, 802.3). Surtout, les réseaux 802.11 utilisent la même technique CSMA/CD que l'Ethernet câblé pour éviter les collisions réseau.

Les standards 802.11 adressent les deux couches inférieures du modèle IEEE, qui en compte sept : la couche physique et la couche Media Access Control. Notez que les protocoles TCP/IP agissent sur les couches supérieures du modèle. Ainsi TCP/IP fonctionne parfaitement sur les réseaux 802.11.

Le standard original 802.11 a été adopté en 1997. Deux évolutions de ce standard, appelées 802.11a et 802.11b, ont été entérinées en 1999. Le dernier standard en date est le 802.11n.

Le Tableau 9.2 regroupe les caractéristiques des quatre variantes du standard 802.11.

Tableau 9.2 : Variantes du standard 802.11.

<i>Standard</i>	<i>Débit max.</i>	<i>Fréquence</i>	<i>Portée (intérieur)</i>
802.11a	54 Mbps	5 GHz	50 m
802.11b	11 Mbps	2,4 GHz	100 m
802.11g	54 Mbps	2,4 GHz	100 m
802.11n	144 Mbps	5 GHz	> 100 m

Actuellement, la plupart des réseaux sans fil sont basés sur le standard 802.11b ; les plus récents sur le 802.11g. Le nouveau standard 802.11n offre un meilleur débit et une portée plus étendue mais le matériel 802.11n est bien plus cher que le matériel des standards 802.11b ou 802.11g.



Les réseaux 802.11g fonctionnent sur la même fréquence radio que nombre de téléphones sans fil : 2,4 GHz. Si vous installez chez vous un réseau 802.11b ou 802.11g et que vous êtes équipé d'un téléphone sans fil à 2,4 GHz, vous n'êtes pas à l'abri d'interférences entre les deux. Le seul moyen d'éviter ces désagréments est d'acheter un téléphone à 900 MHz ou des composants réseau 802.11n, certes plus chers mais qui transmettent à 5 GHz et non à 2,4 GHz.

À portée de maison

La portée maximale d'un réseau sans fil 802.11g est d'environ 100 mètres dans les meilleures conditions. Ce peut être intéressant si vous disposez de tout un tas d'ordinateurs sans fil en réseau dont certains sont à portée de leurs congénères et d'autres non. Par exemple, imaginons que Gilbert, Lucien et Jean-Jacques aient chacun un ordinateur portable sans fil. L'ordinateur de Gilbert est situé à 70 mètres de la machine de Lucien, laquelle est à 70 mètres de celle de Jean-Jacques, dans la direction opposée (voir Figure 9.2). Avec cette configuration, Lucien est capable d'accéder à la fois aux ordinateurs de Gilbert et de Jean-Jacques mais Gilbert ne peut accéder qu'à celui de Lucien et Jean-Jacques seulement à celui de Lucien. Autrement dit, Gilbert ne pourra jamais accéder à l'ordinateur de Jean-Jacques, et inversement, car ils sont situés au-delà de la portée maximale de 100 mètres. Ça commence à ressembler à un problème de maths vicieux. Maintenant, supposons que Gilbert commence à se déplacer vers Lucien à 1,5 km/h, alors que Jean-Jacques se mette à courir vers Lucien à 10 km/h...

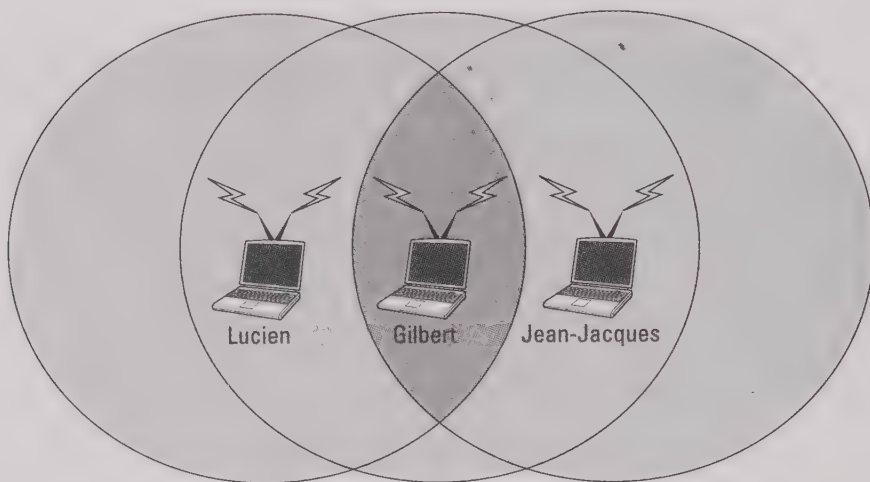


Figure 9.2 : Lucien, Gilbert et Jean-Jacques s'amuse avec leur réseau sans fil.



La portée théorique d'une carte réseau 802.11g est de 100 mètres mais dans la pratique elle peut être moins importante :

- ✓ Des obstacles, tels que les murs, le mauvais temps, les téléphones sans fil, les fours à micro-ondes, les réacteurs nucléaires d'arrière-cour, etc., peuvent se liguer pour diminuer la portée effective d'une carte réseau sans fil. En cas de problème de connexion réseau, le simple fait de réorienter les antennes peut aider.
- ✓ Les réseaux sans fil ont tendance à être plus lents lorsque la distance augmente. Les cartes réseau 802.11g sont censées fonctionner à 11 Mbps mais elles n'atteignent ce débit qu'à des portées inférieures à 30 mètres. À 100 mètres, le débit chute souvent à 1 Mbps.
- ✓ Si vous avez atteint la portée limite de la carte, vous courez davantage le risque de perdre la connexion si les conditions météorologiques sont mauvaises.

Adaptateurs ou cartes réseau sans fil

Tout ordinateur connecté à votre réseau sans fil doit être équipé d'une *carte réseau sans fil*, qui ressemble à la carte réseau utilisée pour une connexion Ethernet standard. Seule différence, la carte réseau sans fil possède une antenne et non un connecteur relié à un câble.

Il existe plusieurs types de cartes réseau sans fil. Vous les choisirez en fonction de vos besoins et du type d'ordinateur que vous possédez :



- ✓ La carte PCI sans fil s'installe à l'intérieur d'un ordinateur de bureau. Pour ce faire, il faut démonter la machine. Ne le faites que si vous avez les nerfs suffisamment solides pour plonger dans les entrailles de la bête.
- ✓ L'adaptateur USB sans fil est un boîtier séparé qui se branche sur un des ports USB de votre ordinateur. Il occupe certes de la place sur votre bureau mais, pour son installation, vous n'avez pas besoin d'ouvrir votre ordinateur.
- ✓ La carte PC sans fil (PC Card ou carte PCMCIA) se glisse dans l'emplacement approprié dont sont équipés la plupart des portables. C'est le type de carte qu'il vous faut si vous souhaitez connecter votre portable à un réseau.



Un adaptateur PCI sans fil 802.11b/g vous reviendra environ à 50 euros, alors qu'un adaptateur USB coûte approximativement 10 euros pièce.



Vous trouvez peut-être que les cartes réseau sans fil ne sont vraiment pas données. Après tout, une carte Ethernet standard ne coûte que 15 euros. Mais, rendez-vous compte, avec les solutions sans fil, vous échappez à l'achat et à l'installation de câbles. Ah ! Tout à coup, le prix du réseau sans fil devient plus acceptable, n'est-ce pas ?

Points d'accès sans fil

Contrairement à leurs homologues câblés, les réseaux sans fil ne nécessitent ni concentrateur ni commutateur. Si vous souhaitez simplement mettre en réseau un groupe d'ordinateurs sans fil, il vous suffit d'acheter un adaptateur sans fil pour chacun d'entre eux puis de placer les machines à moins de 100 mètres les unes des autres.

Que faire si vous avez déjà un réseau câblé ? Supposons, par exemple, que vous disposiez au bureau de quinze ordinateurs, tous câblés bien comme il faut et que vous vouliez ajouter deux ordinateurs portables au réseau existant. Ou supposez que vous ayez deux ordinateurs chez vous, connectés par un câble réseau mais que vous désiriez aussi relier celui de la chambre à coucher sans tirer un câble à travers le grenier. C'est là qu'entre en scène le *point d'accès sans fil* (WAP, en anglais, rien à voir avec le WAP des téléphones mobiles, qui est un protocole d'accès). Un point d'accès sans fil assure deux fonctions :

- ✓ Il agit comme point de connexion central pour tous les ordinateurs équipés d'adaptateurs de réseau sans fil.



Un point d'accès sans fil est l'équivalent d'un concentrateur ou d'un commutateur sur un réseau câblé.

- ✓ Il connecte vos ordinateurs sans fil au réseau de façon que tout ce beau monde forme une jolie petite famille bien unie.



Un *point d'accès* est un boîtier muni d'une ou deux antennes et d'un port Ethernet RJ-45. Il suffit d'y brancher le câble réseau et de relier l'autre extrémité du câble à un concentrateur ou à un commutateur et le réseau sans fil est connecté au réseau câblé.

La Figure 9.3 montre un point d'accès jouant le rôle de point de connexion central pour des ordinateurs communiquant sans fil et de pont qui les relie à un réseau câblé.

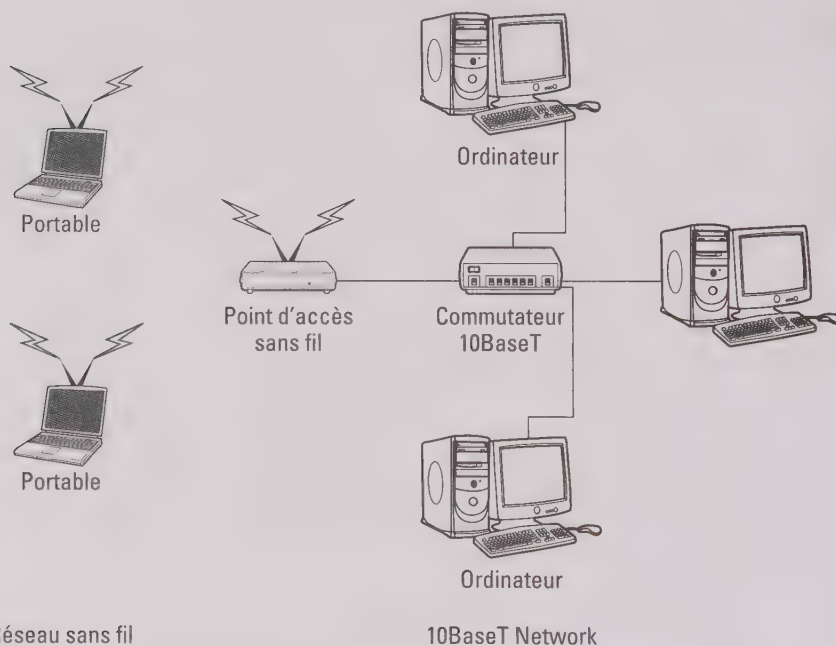


Figure 9.3 : Un point d'accès sans fil relie un réseau sans fil à un réseau câblé.

Mode infrastructure

Lorsque vous configurez un réseau sans fil équipé d'un point d'accès, vous créez un réseau en *mode infrastructure*. Il est appelé ainsi car le point d'accès fournit une infrastructure permanente au réseau. Les points d'accès sont fixés à des emplacements physiques, de sorte que les frontières du réseau sont relativement stables. Chaque fois qu'un ordinateur portable s'aventure

à portée d'un des points d'accès, il entre dans la zone d'action du réseau et peut s'y connecter.

Un point d'accès et tous les ordinateurs qui y sont reliés sont appelés BSS (*Basic Service Set*, ensemble des services de base). Chaque BSS est identifié par un SSID (*Service Set Identifier*, identifiant de l'ensemble des services). Quand vous configurez un point d'accès, vous spécifiez le SSID à utiliser. C'est souvent un nom générique, comme *réseau sans fil*, ou un nom que vous créez. Certains points d'accès utilisent l'adresse MAC du point d'accès sans fil comme SSID.

Points d'accès sans fil multifonctions



Les points d'accès sans fil offrent souvent d'autres fonctionnalités. Certains, par exemple, sont également des concentrateurs ou commutateurs Ethernet. Dans ce cas, ils sont dotés de plusieurs ports RJ-45. En outre, certains possèdent des routeurs pare-feu câble ou DSL à large bande qui permettent la connexion à Internet :

- ✓ Un point d'accès sans fil 802.11b qui m'a permis de mettre en réseau un portable et un ordinateur de bureau situé à l'autre bout de la maison car je ne voulais pas tirer des câbles à travers le grenier.
- ✓ Un commutateur 10/100 MHz quatre ports sur lequel je peux connecter jusqu'à quatre ordinateurs à l'aide de câbles à paires torsadées.
- ✓ Un routeur DSL/câble que je connecte à mon modem câblé. Cela permet à tous les ordinateurs du réseau (câblés et sans fil) d'accéder à Internet.



Un point d'accès multifonctions conçu pour servir de passerelle Internet d'un réseau domestique est parfois appelé *passerelle résidentielle*.

Itinérance (roaming)

Il est possible d'utiliser plusieurs points d'accès sans fil pour créer un grand réseau sans fil. Les utilisateurs peuvent se déplacer tout en restant connectés. Dès qu'un utilisateur sort de la zone de couverture d'un point d'accès, un autre point d'accès prend automatiquement le relais, sans que la connexion soit interrompue.

Dans cette optique, l'installation de plusieurs points d'accès sans fil nécessite que ceux-ci soient placés de telle sorte que toutes les zones du bureau ou de l'édifice figurent au moins à portée d'un des points d'accès. Ensuite, vérifiez que tous les ordinateurs et points d'accès utilisent le même SSID et le même canal.

Plusieurs points d'accès reliés pour assurer l'itinérance ainsi que les ordinateurs qui y sont connectés forment un ESS (*Extended Service Set*, ensemble de services étendus). Les points d'accès d'un ESS sont généralement connectés à un réseau câblé.



L'une des limites de l'itinérance réside dans le fait que chaque point d'accès d'un ESS doit appartenir au même sous-réseau TCP/IP. Ainsi, l'ordinateur qui passe d'un point d'accès à un autre, dans l'ESS, conserve la même adresse IP. Si les points d'accès appartenaient à des sous-réseaux différents, l'ordinateur itinérant devrait changer d'adresse IP dès qu'il passe d'un point d'accès à un autre.

Ponts sans fil

Supposons que vous ayez deux réseaux distincts à proximité l'un de l'autre dans un bâtiment mais qu'il soit difficile de les relier par câble. Dans ce cas, vous pouvez utiliser deux points d'accès sans fil pour créer un *pont sans fil* entre les deux réseaux. Connectez l'un des points d'accès sans fil au premier réseau et l'autre au second. Ensuite, attribuez le même SSID et le même nom aux deux points d'accès sans fil. Autre solution : vous pouvez utiliser un seul point d'accès sans fil doté d'une antenne plus puissante pour augmenter la portée.

Réseaux ad hoc

Un point d'accès sans fil n'est pas indispensable pour créer un réseau sans fil. En effet, quand deux périphériques sans fil sont à portée l'un de l'autre, ils peuvent se connecter et former un *réseau ad hoc*. Par exemple, si vous et quelqu'un de votre entourage possédez un ordinateur portable équipé d'un adaptateur de réseau sans fil 802.11b/g, vous pouvez vous rencontrer n'importe où, même en pleine nature et former spontanément un réseau ad hoc.

Tous les ordinateurs situés à portée les uns des autres au sein d'un réseau ad hoc forment un IBSS (*Independent Basic Service Set*, ensemble de services de base indépendant).

Configurer un point d'accès sans fil

La configuration physique d'un point d'accès sans fil est assez simple : vous extrayez la bête de sa boîte, vous la placez sur une étagère ou sur un meuble à proximité d'une prise de courant et (le cas échéant) d'une prise réseau et vous branchez le cordon d'alimentation et le câble de raccordement au réseau.

La configuration du point d'accès est un peu moins simple mais sans être compliquée. Elle s'effectue généralement au travers d'une interface Web. Pour accéder à la page de configuration du point d'accès, vous devez connaître son adresse IP. Ensuite, il suffit de la taper dans la barre d'adresse du navigateur à partir de n'importe quel ordinateur du réseau.

Les points d'accès multifonctions fournissent habituellement les services DHCP et NAT et font office de routeur. Par conséquent, ils ont typiquement une adresse IP privée située au début de la plage d'adresses IP, telle que 192.168.0.1 ou 10.0.0.1 (consultez la documentation associée au point d'accès).



Si vous utilisez un point d'accès multifonctions comme point d'accès sans fil et routeur Internet et si vous avez oublié son adresse IP, exécutez la commande `IPCONFIG` à partir de l'invite de commande de n'importe quel ordinateur du réseau. L'adresse IP de la passerelle devrait être l'adresse IP du point d'accès.

Options de configuration

La Figure 9.4 présente l'écran principal de configuration d'un routeur sans fil. J'ai accédé à cette page en indiquant dans la barre d'adresse du navigateur l'adresse IP (192.168.1.1) du routeur puis en entrant le login de l'administrateur et son mot de passe.

Cette page de configuration propose les options de configuration ci-dessous. Bien qu'elles soient propres à un certain matériel, vous les retrouverez sur la plupart des autres points d'accès :

- ✓ **Activer/désactiver** : Active ou désactive les fonctions du point d'accès sans fil.
- ✓ **SSID** : L'identifiant de l'ensemble des services sert à identifier le réseau. Celui fourni par défaut par la plupart des points d'accès est très connu.

Vous pourriez penser que votre réseau serait plus sûr en choisissant un SSID un peu plus confidentiel mais ceci ne vous protégerait que des pirates peu doués. Dès qu'ils s'y connaissent un peu plus, ils savent comment contourner un SSID. C'est pourquoi je vous recommande de conserver le SSID par défaut et d'appliquer les mesures de sécurité plus élaborées décrites dans le Chapitre 10.

- ✓ **Autoriser la diffusion du nom (SSID)** : Désactive l'émission périodique du SSID du point d'accès. Normalement, le point d'accès émet régulièrement son SSID afin que les périphériques sans fil qui arrivent à portée puissent détecter le réseau et s'y connecter.

Afin de mieux sécuriser le réseau, cette fonction peut être désactivée. Dans ce cas, un périphérique client sans fil doit connaître préalablement le SSID pour joindre le réseau.





- ✓ **Canal** : Permet la sélection de l'un des onze canaux de communication (quatre seulement en France). Tous les points d'accès et ordinateurs du réseau sans fil doivent communiquer par le même canal.

Si vous estimez que le réseau perd souvent la connexion (peut-être à cause d'interférences produites par un téléphone sans fil ou un autre appareil sans fil), testez un autre canal.

Choisir un autre canal est un moyen convivial d'éviter l'interpénétration des réseaux domestiques dans un immeuble. Vous mettre d'accord avec les voisins pour que chacun utilise un canal qui lui soit propre évite aux réseaux d'interférer les uns avec les autres. C'est aussi une mesure de sécurité qui empêche les voisins de fouiner dans votre réseau. Il existe d'autres mesures de sécurité, plus puissantes, décrites dans le Chapitre 10.

- ✓ **WEP** : Permet d'activer ou de désactiver un protocole de sécurité appelé *wired-equivalent privacy*.

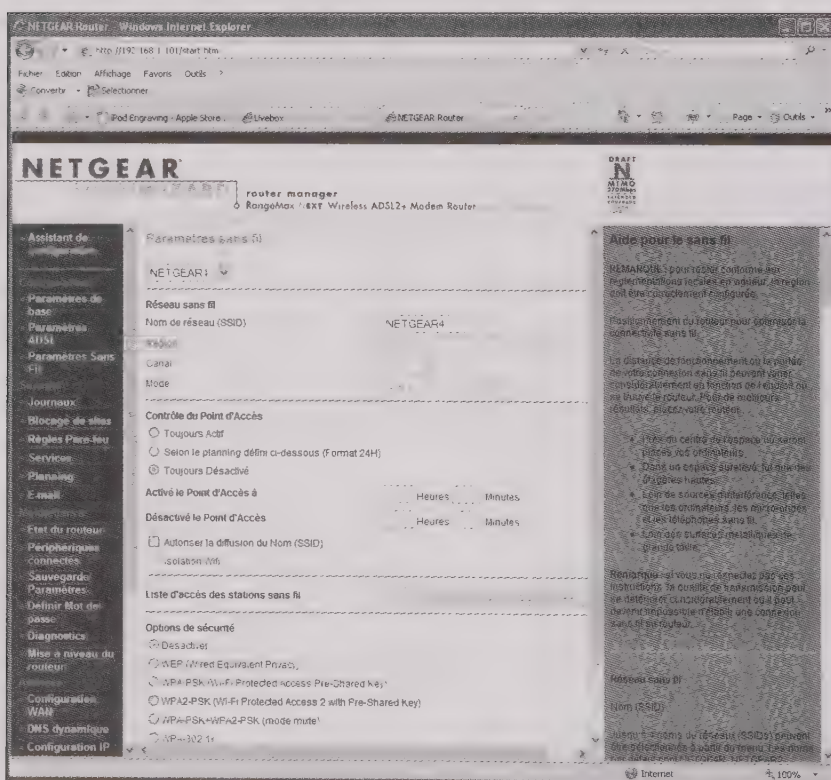


Figure 9.4 : Page principale de configuration d'un routeur sans fil.

Configurer le serveur DHCP



Vous pouvez configurer les points d'accès multifonctions pour qu'ils soient aussi des serveurs DHCP. En général, cela se fait systématiquement pour les réseaux de petite taille, dans ce cas, vous devez configurer le serveur DHCP. La Figure 9.5 affiche la page de configuration du serveur DHCP pour un routeur NetGear. Pour activer le serveur DHCP, cochez l'option adéquate et spécifiez les autres options de configuration.

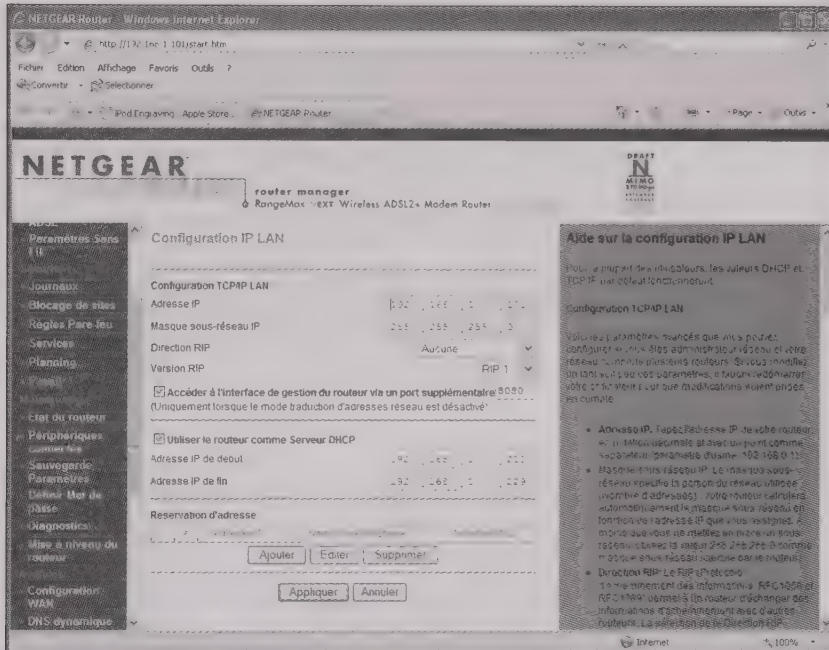


Figure 9.5 : Configuration du serveur DHCP pour un routeur NetGear.

Les réseaux plus étendus qui sont plus exigeants en ressources requièrent un serveur DHCP spécifique. Dans ce cas, vous devez désactiver la fonction de serveur DHCP sur le point d'accès.

Configurer Windows XP pour un réseau sans fil

La première étape de la configuration de Windows XP pour un réseau sans fil consiste à installer le pilote de la carte sans fil. Pour ce faire, vous avez besoin du CD d'installation qui vous a été fourni avec l'adaptateur. Suivez les instructions du programme d'installation.

Windows XP propose quelques fonctionnalités intégrées permettant de gérer l'ordinateur dans un environnement sans fil. Exécutez les étapes suivantes pour y accéder :

1. Ouvrez la fenêtre Connexions réseau.

Exécutez Démarrer/Panneau de configuration puis double-cliquez sur l'icône Connexions réseau.

2. Effectuez un clic droit sur l'icône Connexion réseau sans fil et sélectionnez Propriétés pour ouvrir la boîte de dialogue correspondante.

3. Ouvrez l'onglet Configuration réseaux sans fil.

Les options des réseaux sans fil s'affichent, comme le montre la Figure 9.6. Si votre ordinateur est équipé d'une carte réseau sans fil à laquelle est associé un logiciel d'administration, c'est ce logiciel qui sera utilisé à la place de celui de Windows.

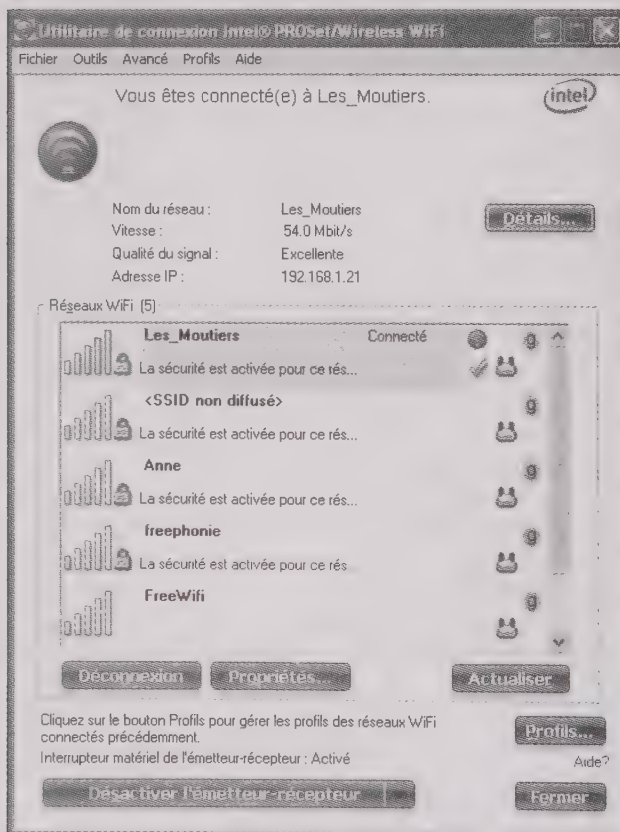


Figure 9.6 : Configuration de la connexion réseau sans fil sous Windows XP avec le pilote de la carte réseau.

Dès que vous vous connectez à un réseau sans fil, Windows XP ajoute ce réseau dans cette boîte de dialogue. Vous pouvez alors modifier l'ordre des réseaux dans la section Réseaux favoris pour indiquer celui auquel vous voulez être connecté si vous vous trouvez simultanément dans la portée de plusieurs réseaux. Utilisez les boutons Monter et Descendre pour modifier vos préférences.

Pour ajouter un réseau auquel vous ne vous êtes pas encore connecté, cliquez sur le bouton Ajouter. Cette action ouvre la boîte de dialogue illustrée par la Figure 9.7. Vous pouvez spécifier le SSID du réseau que vous voulez ajouter. Vous êtes également invité à fournir d'autres informations telles que les techniques de cryptage et d'authentification ainsi que le type de réseau (ad hoc ou infrastructure).

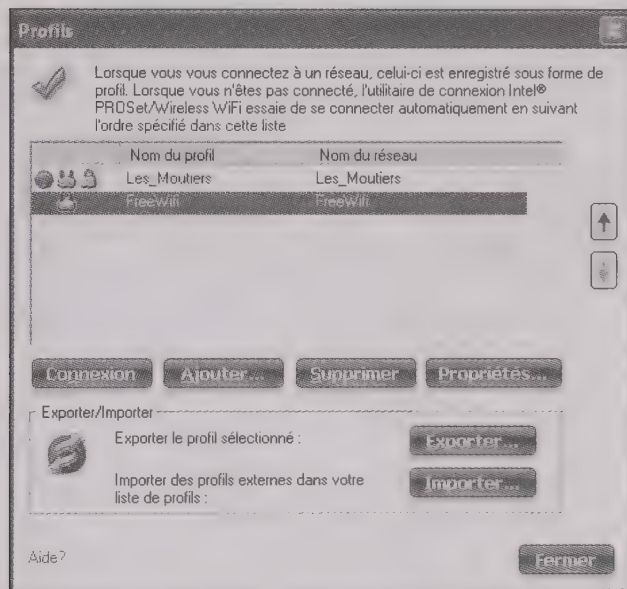


Figure 9.7 : Ajout d'un réseau sans fil sous Windows XP.

Dès que l'ordinateur arrive à portée d'un réseau sans fil, une info-bulle apparaît dans la barre des tâches, indiquant qu'un réseau est disponible. S'il s'agit d'un réseau déjà identifié pour lequel vous avez requis une connexion automatique, un clic dans l'info-bulle vous connecte automatiquement. Si Windows XP ne reconnaît pas le réseau, le clic sur l'info-bulle affiche la boîte de dialogue Connexion réseau sans fil dans laquelle vous pouvez sélectionner le réseau auquel vous souhaitez vous connecter. Pour ce faire, il suffit de cliquer sur le bouton approprié.

Se connecter à un réseau sans fil sous Windows Vista ou Windows 7

Se connecter à un réseau sans fil sous Windows Vista ou Windows 7 est plus simple que sous Windows XP. Dès que Windows Vista ou Windows 7 détecte la portée d'un réseau sans fil, une info-bulle s'ouvre et vous informe qu'un ou plusieurs réseaux sans fil sont disponibles. Double-cliquez sur cette info-bulle pour ouvrir la boîte de dialogue illustrée par la Figure 9.8. Ensuite, il ne vous reste qu'à double-cliquer sur le réseau auquel vous voulez vous connecter.

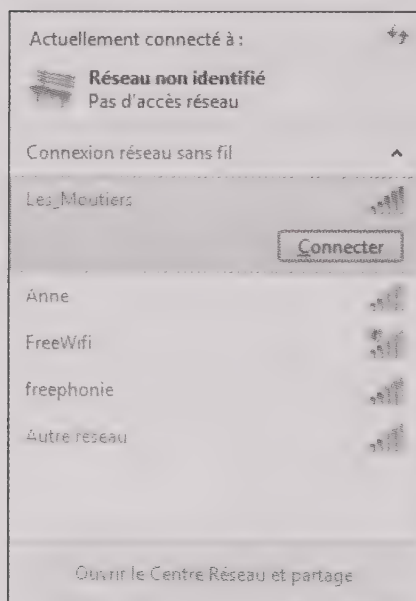
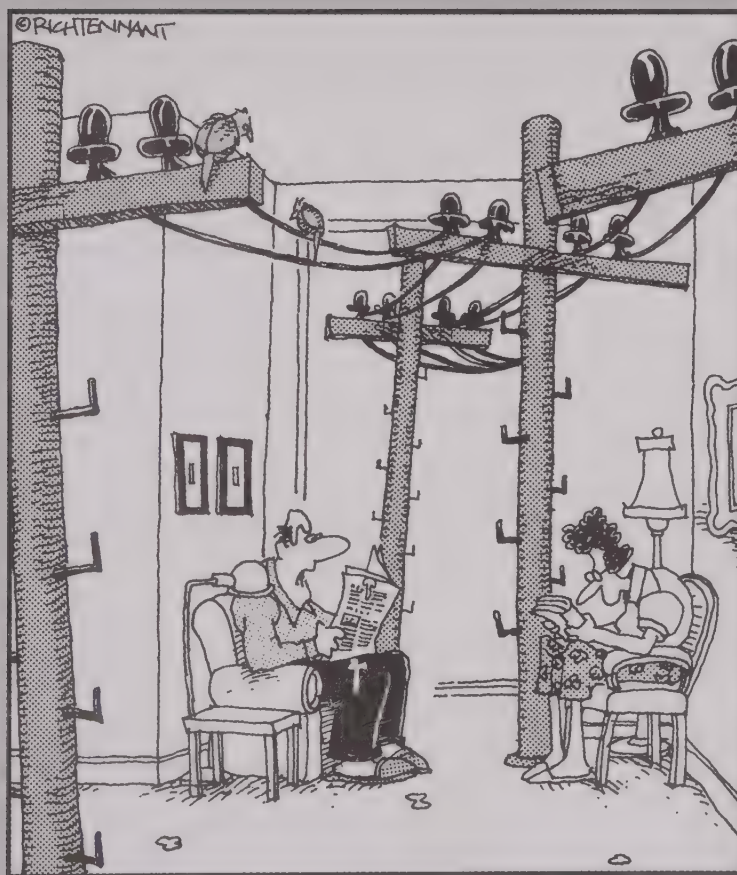


Figure 9.8 : Connexion à un réseau sans fil.

Troisième partie

Jouer dans la cour des grands



« C'est bon ! Tu vas l'avoir, ton réseau sans fil ! »

Dans cette partie...

Maintenant que votre réseau est opérationnel, vous êtes prêt à le relier au monde extérieur.

Vous apprendrez dans cette partie à connecter votre réseau à Internet, à installer et à gérer un serveur de messagerie, à créer un site intranet, à utiliser votre réseau pour les communications téléphoniques et à vous connecter à partir de votre domicile.

Chapitre 10

Connecter le réseau à Internet

Dans ce chapitre :

- ▶ Étudier les connexions ADSL et câblées.
- ▶ Comparer les connexions T1 et T3.
- ▶ Utiliser un routeur.
- ▶ Sécuriser la connexion avec un pare-feu.
- ▶ Utiliser le pare-feu de Windows.

Ainsi, vous avez décidé de connecter votre réseau à Internet ! Vous n'avez donc plus qu'à courir à la boutique de matériel informatique la plus proche, acheter un modem et le brancher, c'est bien ça ? Eh non, malheureusement, ce n'est pas suffisant pour se connecter à Internet. Pour commencer, vous devez vous assurer que la connexion par modem est la bonne solution. Il en existe d'autres, plus rapides mais plus chères. Ensuite, vous devez choisir puis installer le logiciel que vous utiliserez pour accéder à Internet. Et finalement, vous devez rester éveillé la nuit, à vous ronger d'inquiétude à l'idée que des *hackers* pourraient faire irruption dans votre réseau via la connexion Internet. Les *hackers* sont des passionnés d'informatique qui s'introduisent illégalement dans des réseaux par curiosité, jeu ou défi.

Se connecter à Internet

La connexion à Internet n'est pas gratuite. Tout d'abord, vous devez acheter le matériel nécessaire pour vous connecter. Ensuite, il vous faut obtenir une connexion auprès d'un *fournisseur d'accès à Internet* ou *FAI*. Le *FAI* vous facture un abonnement mensuel qui varie en fonction de la vitesse et de la capacité de la connexion.

Les sections suivantes décrivent les méthodes les plus courantes pour connecter les utilisateurs d'un réseau à Internet.

Se connecter par le câble ou l'ADSL

Si vos utilisateurs risquent d'employer assidûment Internet, vous avez peut-être intérêt à opter pour un des deux modes de connexion relativement récents : le câble et l'ADSL. On les appelle souvent *connexions à haut débit*.

L'accès à Internet par le câble s'effectue via les installations qui vous permettent de recevoir quarante milliards de chaînes de télévision. L'ADSL est pour sa part un service de téléphonie numérique se servant d'une ligne téléphonique classique. Ces deux solutions offrent trois avantages majeurs par rapport à la connexion par téléphone traditionnelle :

✓ **Le câble et l'ADSL sont bien plus rapides que les connexions par téléphone.**

Une connexion par câble est dix à deux cents fois plus rapide qu'une connexion par téléphone, en fonction du type de service dont vous bénéficiez. La vitesse d'une ligne ADSL est comparable à celle du câble. La connexion ADSL est une connexion dédiée tandis que les connexions par câble sont partagées par plusieurs abonnés. Le débit d'une connexion peut diminuer lorsque plusieurs abonnés sont connectés simultanément.

✓ **Avec le câble et l'ADSL, vous disposez d'une connexion permanente à Internet.**

Pas besoin de se connecter pour aller sur le Web. Plus besoin d'attendre que votre modem appelle le fournisseur d'accès et adieu sa plainte stridente lorsqu'il tente d'établir la connexion.

✓ **Le câble et l'ADSL n'immobilisent pas votre ligne téléphonique lorsque vous êtes connecté à Internet.**

Avec le câble, la connexion s'effectue à travers les installations de la télévision et non celles du téléphone. Avec l'ADSL, votre opérateur téléphonique installe une ligne spéciale pour le service ADSL, totalement indépendante de votre ligne téléphonique normale.

Malheureusement, tout se paie et la connexion ultrarapide et permanente qu'offrent le câble et l'ADSL est moins bon marché. Au début, attendez-vous à déboursier davantage par mois. Le prix du câble commence à 20 euros par mois pour les particuliers. Pour les entreprises, les tarifs sont un peu plus élevés, surtout s'il y a plusieurs utilisateurs.

Le coût du service ADSL varie selon la vitesse choisie. Les particuliers peuvent disposer d'une connexion ADSL pour 15 euros par mois. Pour des débits plus élevés ou pour les professionnels, le service ADSL est plus cher.

Mais l'accès par câble ou ADSL n'est pas possible partout. Si vous vivez dans une région non raccordée au câble ou à l'ADSL, vous pouvez malgré tout acquérir un accès à Internet très rapide grâce à une installation satellite.

Se connecter via des lignes privées haut débit T1 et T3

Si vous avez véritablement besoin d'une connexion haut débit à Internet, contactez votre compagnie de téléphone pour demander l'installation d'une liaison numérique haut débit. Ces lignes peuvent vous coûter très cher (de l'ordre de plusieurs centaines d'euros par mois), aussi sont-elles le plus souvent adaptées aux besoins des entreprises au sein desquelles plus de vingt utilisateurs doivent accéder à Internet simultanément.

La vitesse d'une ligne T1 atteint 1,544 Mbps. Une ligne T3 est plus rapide : elle transmet les données à une vitesse record de 44,184 Mbps. Bien évidemment, les lignes T3 sont considérablement plus chères que les lignes T1.

Si vous n'avez pas assez d'utilisateurs pour justifier l'installation d'une ligne T3 ou T1, vous pouvez louer une portion de ligne. Avec une *fraction de ligne T1*, vous pourrez effectuer des connexions de 128 Kbps à 768 Kbps et, avec une *fraction de ligne T3*, vous pourrez choisir entre des vitesses allant de 4,6 Mbps à 32 Mbps.

Installer une connexion T1 ou T3 à Internet est un travail de professionnel. Configurer ce type de connexion est bien plus complexe qu'installer un simple LAN.



Vous vous demandez peut-être si les lignes T1 ou T3 sont vraiment plus rapides que les connexions par câble ou ADSL. Après tout, les T1 fonctionnent à 1,544 Mbps et les T3 à 44,184 Mbps, ce qui est comparable aux vitesses annoncées pour les connexions par câble et ADSL. Il existe réellement de nombreuses différences qui justifient le coût plus élevé d'une ligne T1 ou T3. Il s'agit en particulier d'une ligne *dédiée* ; vous ne la partagez pas avec d'autres utilisateurs. La connexion est de meilleure qualité, vous bénéficiez réellement de connexions à 1,544 ou 44,184 Mbps, alors qu'avec une connexion par câble ou ADSL, le débit effectif est bien moindre que celui annoncé à cause de la qualité de la connexion.

Partager une connexion Internet

Une fois votre mode d'accès choisi (connexion commutée, ADSL, câble ou ligne T1 ou T3 à haut débit), vous pouvez vous concentrer sur la configuration, de façon à partager la connexion entre plusieurs utilisateurs de votre réseau. Le meilleur moyen consiste à recourir à un périphérique distinct appelé *routeur*. On en trouve à présent à moins de 100 euros. Les modèles conçus pour les grands réseaux sont évidemment plus onéreux.

Comme toutes les communications entre votre réseau et Internet doivent transiter par le routeur, ce dernier est l'emplacement de choix pour y installer tous les dispositifs de sécurité qui protégeront votre réseau des dangers d'Internet. C'est pourquoi un routeur intègre souvent un pare-feu, comme nous le verrons dans la section « Utiliser un pare-feu », plus loin dans ce chapitre.

Sécuriser la connexion avec un pare-feu

Si votre réseau est connecté à Internet, vous êtes confronté à une foule de problèmes de sécurité. Vous avez sans doute établi cette connexion afin que les utilisateurs du réseau bénéficient d'une fenêtre ouverte sur le monde extérieur. Malheureusement, c'est aussi par cette fenêtre qu'entrent les malfaiteurs.

Ceux qui agissent sur Internet ne s'en priveront pas. Le cyberspace est peuplé de pirates à la recherche de réseaux dans lesquels s'introduire. Ce n'est parfois que pour le plaisir de fureter dans vos affaires mais parfois aussi pour dérober des numéros de cartes bancaires ou inonder votre serveur de messagerie de milliers de courriers non sollicités. Quelles que soient les motivations, soyez assuré que votre réseau sera visité si vous ne le protégez pas.

Utiliser un pare-feu

Un *pare-feu* est un routeur sécurisé installé entre Internet et votre réseau. Sa seule tâche est de filtrer tout ce qui entre et sort. C'est une sorte de vigile entre Internet et le réseau. Tout le trafic transite par le pare-feu qui autorise ou interdit les accès.



Un pare-feu est absolument obligatoire dès lors que votre réseau accède à Internet, que ce soit par une connexion à haut débit (ADSL ou modem câble), ligne T1 ou toute autre connexion du même genre. Sans pare-feu, les pirates découvriront tôt ou tard l'existence de votre réseau non protégé, le signaleront à leurs collègues et il en subira les conséquences en quelques heures.

Un pare-feu peut être installé de deux manières :

- ✓ **Équipement pare-feu** : La manière la plus simple consiste à acheter un *équipement pare-feu*, qui est en réalité un routeur offrant des fonctionnalités de pare-feu.

La plupart sont équipés d'une interface de type Web permettant de les connecter directement depuis l'un des ordinateurs du réseau à l'aide d'un navigateur. Vous les configurez ensuite selon vos besoins.

- ✓ **Ordinateur serveur** : Vous pouvez configurer un ordinateur serveur afin qu'il fasse office d'ordinateur pare-feu.

Le serveur peut fonctionner sous n'importe quel système d'exploitation réseau. Les plus efficaces tournent cependant sous Linux.

Que vous optiez pour l'équipement pare-feu ou l'ordinateur pare-feu, ce matériel doit être placé entre le réseau et Internet, comme le montre la Figure 10.1. Le pare-feu est connecté d'une part au commutateur, qui est lui-même connecté aux autres ordinateurs du réseau, et d'autre part à Internet. Tout le trafic entre le réseau et Internet doit obligatoirement transiter par le pare-feu.

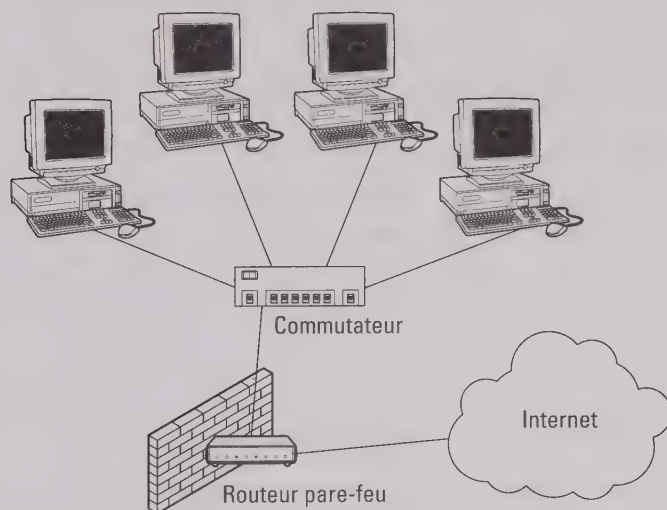


Figure 10.1 : Un routeur pare-feu sécurise le trafic entre le réseau et Internet.

Le terme *périmètre* est parfois utilisé pour décrire l'emplacement du pare-feu sur le réseau. En fait, un pare-feu est une sorte de périmètre de sécurité qui entoure votre propriété et oblige les visiteurs à s'annoncer à la porte d'entrée.



Sur les réseaux de grande taille, il est parfois difficile de savoir où se trouve le périmètre. Si le réseau bénéficie de plusieurs connexions WAN (*Wide Area Network*, réseau étendu), vérifiez que chacune d'elles est protégée par un pare-feu et n'est pas directement reliée à Internet. Cette sécurité est assurée par un pare-feu pour chaque connexion WAN ou par un seul pare-feu équipé de plusieurs ports WAN.



Certains pare-feu renforcent la protection antivirus du réseau. Reportez-vous au Chapitre 23 pour en savoir plus sur ce sujet.

Pare-feu intégré de Windows

Windows XP et Vista possèdent un pare-feu intégré qui fournit une protection de base en filtrant les données. Cependant, il est recommandé d'utiliser un routeur pare-feu qui offre de meilleures fonctionnalités de sécurité que le pare-feu Windows intégré. Celui-ci convient davantage aux réseaux domestiques ou aux réseaux d'entreprise de petite taille.

Voici comment activer le pare-feu intégré sous Windows XP ou Vista :

1. Sélectionnez Démarrer/Panneau de configuration.

Le Panneau de configuration s'ouvre.

2. Double-cliquez sur l'icône Pare-feu Windows.

La boîte de dialogue Pare-feu Windows s'affiche. La Figure 10.2 représente la version de Windows Vista.

3. Cochez l'option Activé (recommandé).

Cette option active le pare-feu.

4. Cliquez sur OK.

C'est tout.

Sous Windows 7, la démarche est légèrement différente :

1. Sélectionnez Démarrer/Panneau de configuration.

Le Panneau de configuration s'affiche.

2. Cliquez sur Système et sécurité.

La fenêtre Système et sécurité s'ouvre.

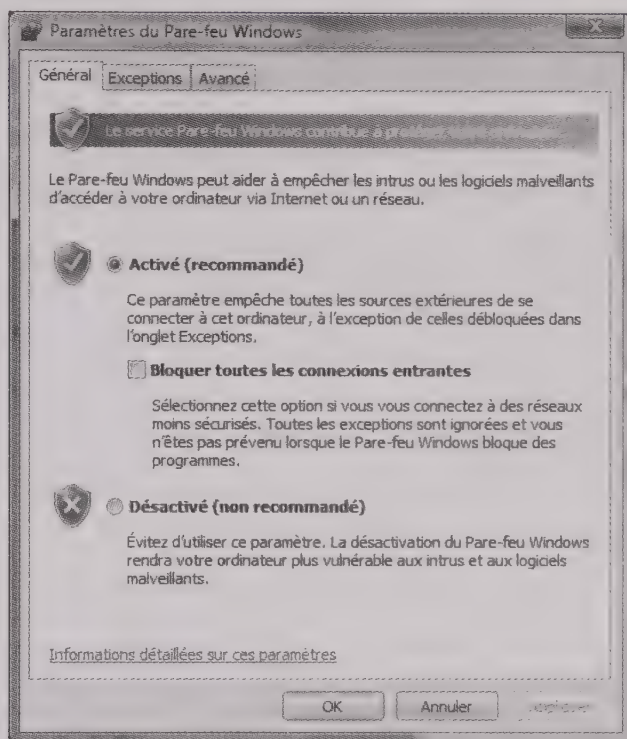


Figure 10.2 : Boîte de dialogue Pare-feu Windows sous Vista.

3. Cliquez sur Pare-feu Windows.

La fenêtre Pare-feu Windows apparaît.

4. Cliquez sur le lien Activer ou désactiver le Pare-feu Windows.

La fenêtre illustrée par la Figure 10.3 s'affiche.

5. Cochez l'option Activer le Pare-feu Windows.

Notez que vous pouvez activer ou désactiver le pare-feu indépendamment pour le réseau public (c'est-à-dire pour votre connexion à Internet) et pour votre réseau domestique ou d'entreprise (c'est-à-dire le réseau qui relie plusieurs ordinateurs à votre domicile ou au bureau). Je vous conseille d'activer ou de désactiver le pare-feu pour les deux. Désactivez le pare-feu si vous utilisez un pare-feu séparé, intégré dans le routeur qui connecte votre ordinateur ou votre réseau domestique ou d'entreprise à Internet. Activez le pare-feu si vous ne possédez pas de pare-feu séparé.

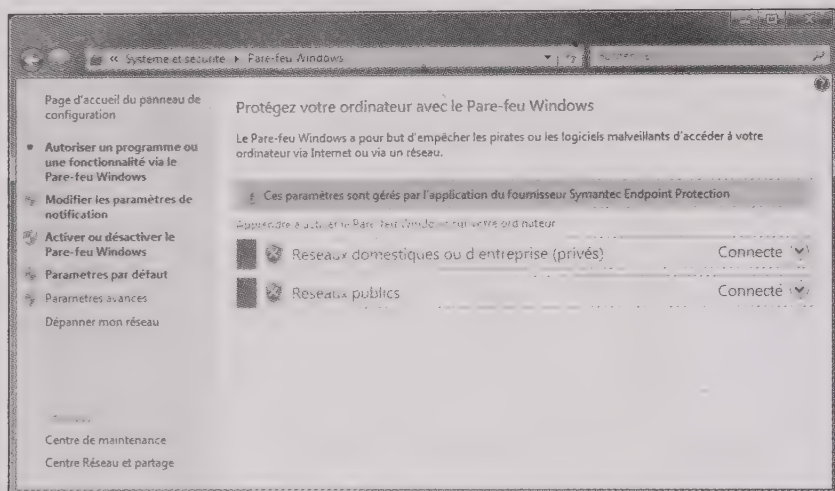


Figure 10.3 : Activation du pare-feu sous Windows 7.

Je vous conseille aussi d'activer l'option *Me prévenir lorsque le Pare-feu Windows bloque un nouveau programme* (à priori elle est activée par défaut). De cette manière, vous serez averti dès que le pare-feu bloque un programme suspect.

6. Cliquez sur OK.

Le pare-feu est activé.

Le pare-feu qui est intégré dans Windows Vista et Windows 7 propose des options supplémentaires que vous pouvez configurer. Cependant, ne vous aventurez dans cette direction que si vous maîtrisez le domaine !



N'activez pas le pare-feu de Windows si vous utilisez un routeur qui protège votre réseau. Comme les autres ordinateurs du réseau sont connectés directement au routeur et non à l'ordinateur, le pare-feu de Windows ne protégerait pas le reste du réseau. Autre effet secondaire : le réseau ne pourrait plus accéder à votre ordinateur.



Depuis le Service Pack 2 de Windows XP, le pare-feu est activé par défaut. Si votre ordinateur est déjà protégé par un pare-feu, désactivez celui de Windows.

Chapitre 11

Gérer la messagerie avec Exchange 2007

Dans ce chapitre :

- Créer des boîtes aux lettres utilisateur.
- Configurer Outlook pour travailler avec Exchange.
- Configurer une autre boîte aux lettres.

Bien qu'*Exchange Server 2007* ne fasse pas partie de Windows Server 2008, c'est le serveur de messagerie utilisé sur la plupart des réseaux Windows. Oui, je sais ! Microsoft ne considère pas Exchange Server comme un *serveur de messagerie*. C'est un *serveur de messagerie et de collaboration*. Toutefois, la raison d'être d'Exchange Server est bel et bien la messagerie.

Dans ce chapitre, vous découvrirez comment exécuter les tâches de maintenance les plus courantes sur un serveur Exchange : la création d'une nouvelle boîte aux lettres, l'accès à une boîte aux lettres supplémentaire pour un client et le problème des limites de taille des boîtes aux lettres.

Administrer des boîtes aux lettres

Lorsque vous créez un nouvel utilisateur à partir de la console Utilisateurs et ordinateurs Active Directory, une boîte aux lettres Exchange est automatiquement créée pour ce nouvel utilisateur. Vous n'avez donc pas besoin de créer de boîtes aux lettres séparément. Cependant, vous serez parfois amené à modifier la configuration Exchange d'un utilisateur.

Plusieurs onglets de la boîte de dialogue Propriétés de compte utilisateur permettent de contrôler les boîtes aux lettres. Pour accéder à cette boîte de dialogue, exécutez les commandes Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory puis double-cliquez sur le nom de l'utilisateur à modifier. S'ouvre alors la boîte de dialogue Propriétés. Les sections suivantes décrivent les onglets de cette boîte de dialogue qui sont spécifiques à Exchange.

Onglet Exchange Général

L'onglet Exchange Général, illustré dans la Figure 11.1, propose les options suivantes :

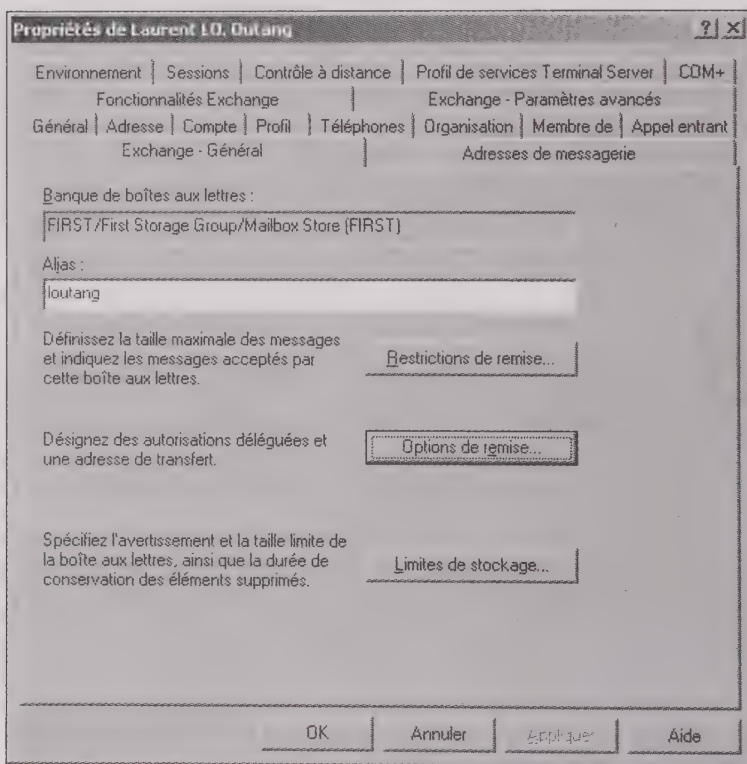


Figure 11.1 : Onglet Exchange Général.

- ✓ **Alias** : Le nom par défaut est le nom d'utilisateur. Vous pouvez le modifier si vous le souhaitez.
- ✓ **Restrictions de remise** : Ce bouton ouvre une boîte de dialogue qui vous permet de fixer une limite de taille aux messages entrants et sortants. Vous pouvez également spécifier de qui l'utilisateur peut recevoir des messages.

- ✓ **Options de remise** : Ce bouton ouvre une boîte de dialogue qui vous invite à créer une adresse de transfert et à autoriser des utilisateurs à envoyer des courriers à partir de ce compte.
- ✓ **Limites de stockage** : Permet de définir la taille de la boîte aux lettres. Vous pouvez spécifier l'envoi d'un message d'avertissement dès que la boîte aux lettres atteint une taille limite. Vous avez également la possibilité de préciser une autre taille limite qui, si elle est atteinte, interdit à l'utilisateur d'envoyer ou de recevoir du courrier.

Onolet Adresses de messagerie

L'onglet Adresses de messagerie de la boîte de dialogue Propriétés d'utilisateur (Figure 11.2) affiche les adresses de messagerie associées à un compte utilisateur. Si une adresse de messagerie est erronée, vous pouvez la corriger à partir de cette boîte de dialogue. Pour ce faire, il suffit de sélectionner l'adresse incorrecte, de cliquer sur le bouton Modifier et d'entrer la bonne adresse. Vous pouvez également ajouter ou supprimer une adresse de messagerie.

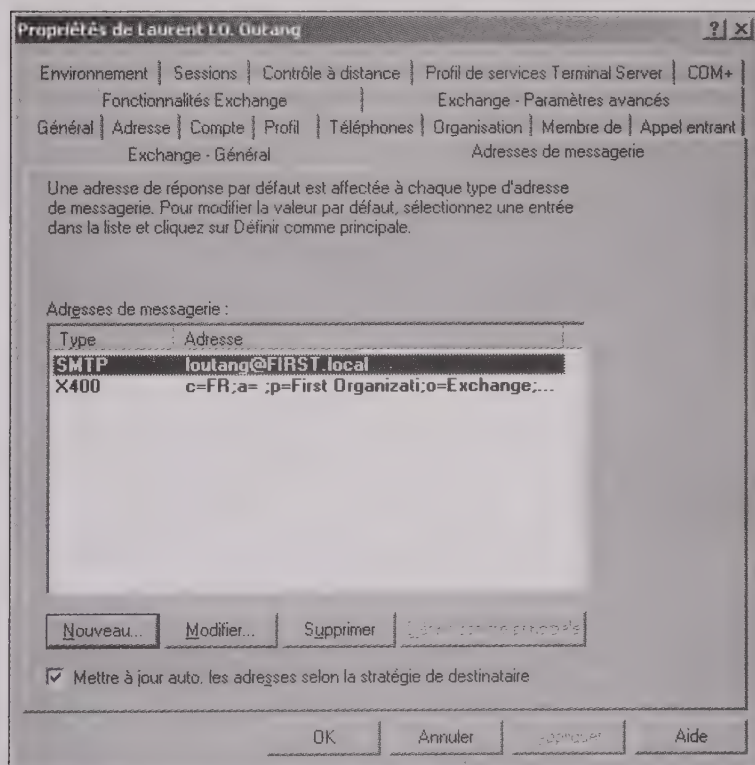


Figure 11.2 : Onolet Adresses de messagerie.

Onglet Fonctionnalités Exchange

La Figure 11.3 représente l'onglet Fonctionnalités Exchange de la boîte de dialogue Propriétés d'utilisateur qui permet de configurer les fonctionnalités d'Exchange. La liste suivante décrit ces fonctionnalités :

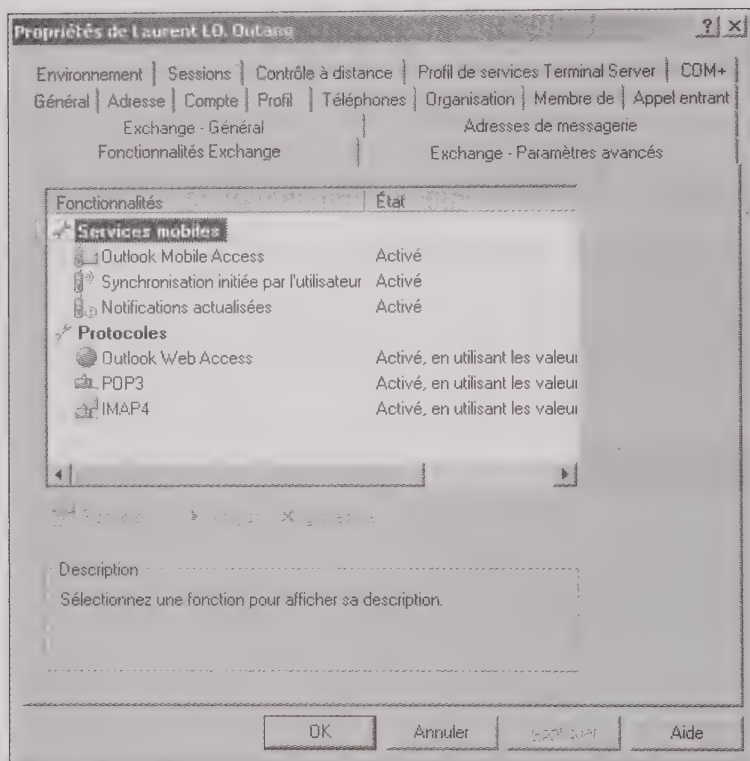


Figure 11.3 : Onglet Fonctionnalités Exchange.

- ✓ **Outlook Mobile Access** : Permet à l'utilisateur d'accéder à des données Exchange à partir d'un appareil mobile tel qu'un téléphone cellulaire ou un PDA.
- ✓ **Synchronisation initiée par utilisateur** : L'utilisateur peut déclencher lui-même la synchronisation pour mettre à jour les données de l'appareil mobile à partir du serveur Exchange.
- ✓ **Notifications actualisées** : Active les synchronisations automatiques.
- ✓ **Outlook Web Access** : Permet à l'utilisateur d'accéder à sa boîte aux lettres Exchange à partir d'un navigateur Web plutôt que d'un client Outlook. Cette configuration étant activée, l'utilisateur peut lire ces messages à partir de n'importe quel ordinateur ayant une connexion Internet.

- ✓ **POP3** : Autorise l'accès au serveur de messagerie avec le protocole POP3.
- ✓ **IMAP4** : Autorise l'accès au serveur de messagerie avec le protocole IMAP4.

Onglet *Exchange Paramètres avancés*

L'onglet Exchange Paramètres avancés (Figure 11.4) permet de définir les fonctionnalités avancées d'Exchange. La liste suivante décrit ces fonctionnalités :

- ✓ **Nom affiché simple** : Spécifie un nom d'affichage utilisable par les ordinateurs qui ne peuvent pas afficher le nom complet. Vous n'utiliserez cette fonctionnalité que pour les ordinateurs qui ne peuvent pas afficher des caractères ASCII.
- ✓ **Masquer dans la liste d'adresses Exchange** : Si la case est cochée, l'utilisateur n'apparaîtra pas dans le carnet d'adresses global. Cette option est utile pour les boîtes aux lettres confidentielles que vous ne voulez pas diffuser.
- ✓ **Déclasser la haute priorité des messageries pour X.400** : Cette option est compatible avec la norme X.400 qui a été définie en 1984. Si vous échangez du courrier avec des systèmes X.400 anciens, vous devez utiliser cette option.
- ✓ **Attributs personnalisés** : Ce bouton ouvre une boîte de dialogue qui permet de définir jusqu'à 15 attributs par utilisateur. Vous pouvez sans risque ignorer cette option.
- ✓ **Paramètres ILS** : Si vous avez installé un serveur ILS (*Internet Locator Service*), vous pouvez spécifier le serveur et le compte à partir de ce bouton. Cette fonctionnalité est utilisée par des applications telles que NetMeeting.
- ✓ **Droits de boîte aux lettres** : C'est la fonctionnalité avancée la plus utilisée. Elle permet d'accorder à d'autres utilisateurs des droits d'accès à la boîte aux lettres. Pour plus d'informations, voir la section « Configurer une autre boîte aux lettres », plus loin dans ce chapitre.

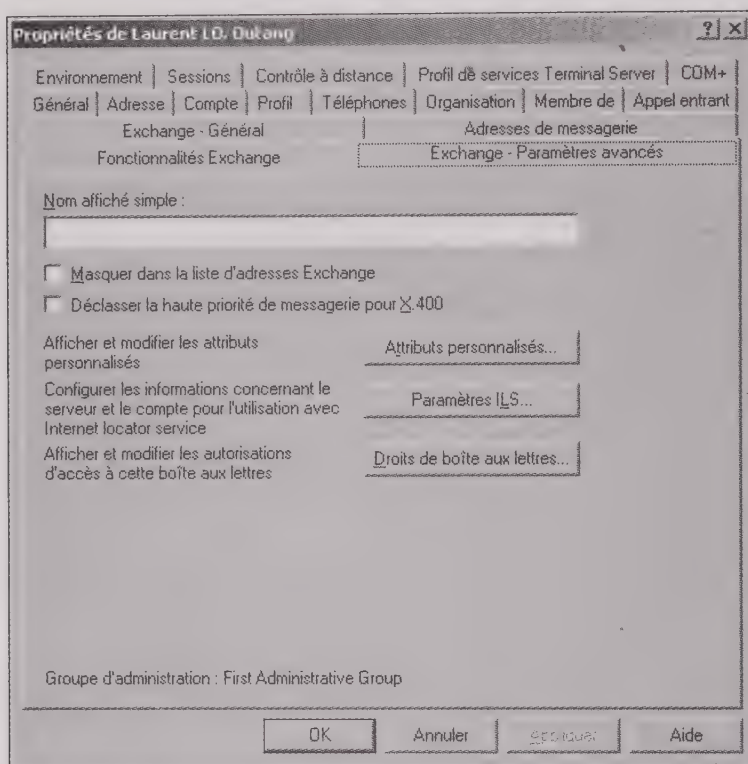


Figure 11.4 : Onglet Exchange Paramètres avancés.

Configurer Outlook pour Exchange

Lorsque vous créez un utilisateur dans Active Directory, celui-ci possède automatiquement une boîte aux lettres. Vous devez ensuite configurer le logiciel client Outlook sur le poste de l'utilisateur pour qu'il puisse accéder au serveur de messagerie. Avec Outlook 2007, la démarche est la suivante (elle est similaire pour les autres versions d'Outlook) :

1. Démarrez Outlook sur l'ordinateur de l'utilisateur.

L'icône d'Outlook est généralement située dans la partie supérieure du menu Démarrer.

2. Exécutez la commande Outils/Paramètres du compte.

La boîte de dialogue Paramètres du compte apparaît, telle qu'elle est représentée dans la Figure 11.5.

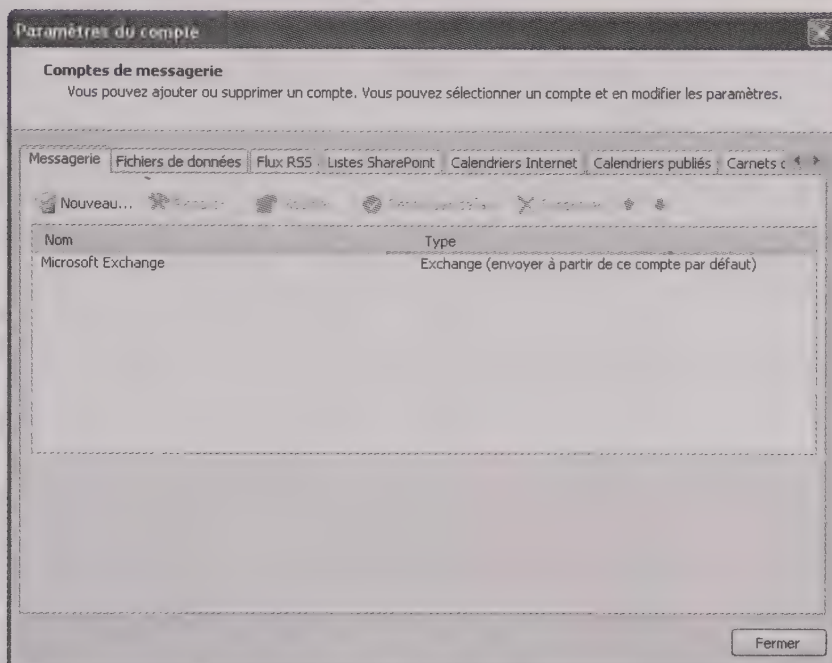


Figure 11.5 : Boîte de dialogue Paramètres du compte.

3. Cliquez sur le bouton Nouveau.

La boîte de dialogue Ajouter un nouveau compte de messagerie s'affiche. N'entrez pas votre adresse de messagerie et passez directement à l'étape 4.

4. Cochez la case Configurer manuellement les paramètres du serveur ou les types de serveurs supplémentaires et cliquez sur Suivant.

La boîte de dialogue qui s'ouvre vous demande de choisir le type de compte de messagerie que vous voulez créer. Les possibilités sont : Messagerie Internet, Microsoft Exchange et Autre.

5. Sélectionnez Microsoft Exchange et cliquez sur Suivant.

La boîte de dialogue illustrée par la Figure 11.6 apparaît.

6. Entrez le nom du serveur Exchange et le nom d'utilisateur dans les zones prévues à cet effet et cliquez sur Suivant.

Le message suivant s'affiche sur votre écran :

Pour démarrer le compte de messagerie que vous venez d'ajouter, choisissez Quitter dans le menu Fichier, puis redémarrez Microsoft Office Outlook..

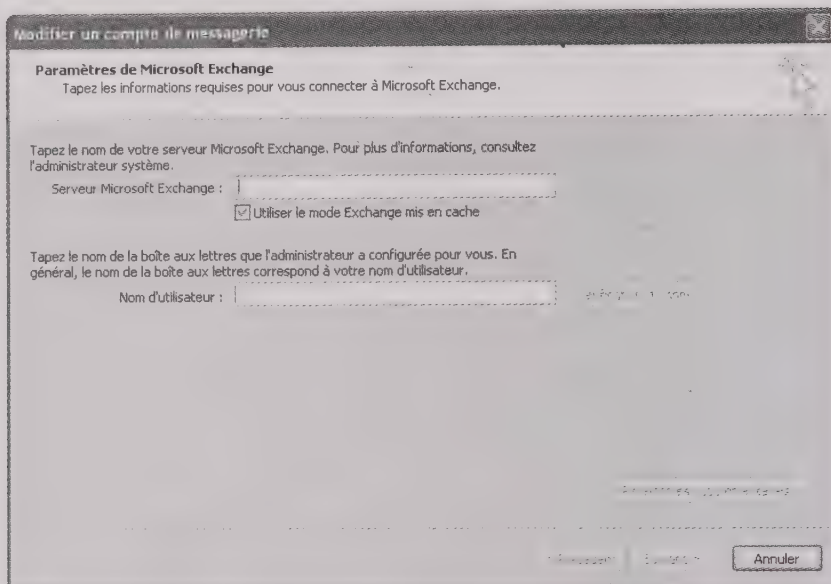


Figure 11.6 : Vous devez identifier le serveur Exchange et indiquer un nom d'utilisateur.

7. Cliquez sur OK.

Le message disparaît pour laisser place à la dernière page de l'assistant.

8. Cliquez sur le bouton Terminer.

L'assistant se ferme.

9. Cliquez sur Fichier/Quitter pour fermer Outlook et redémarrez Outlook.

La boîte aux lettres est configurée.

Configurer une autre boîte aux lettres

Il se peut qu'un utilisateur ait besoin d'accéder à sa boîte aux lettres et à la boîte aux lettres d'un autre utilisateur. Par exemple, si vous avez créé un utilisateur fonctionnel nommé Support avec lequel vos clients pourront correspondre en utilisant l'adresse de messagerie Support@VotreSociete.com pour toutes questions liées au support technique, vous devrez permettre à un ou plusieurs utilisateurs réels d'accéder à la boîte aux lettres pour pouvoir lire et expédier le courrier.

Tout d'abord, vous devez configurer la boîte aux lettres fonctionnelle pour qu'elle accorde des droits d'accès à l'utilisateur qui devra la gérer. Pour ce faire, exécutez les étapes suivantes :

1. **Sur le serveur de messagerie, exécutez la commande Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory et double-cliquez sur le compte dont la messagerie devra être partagée.**

La boîte de dialogue Propriétés apparaît.

2. **Cliquez sur l'onglet Exchange Paramètres avancés puis sur le bouton Droits de boîte aux lettres.**

La boîte de dialogue Autorisations, illustrée par la Figure 11.7, s'affiche.

3. **Cliquez sur le bouton Ajouter.**

La boîte de dialogue Sélectionnez les utilisateurs, les ordinateurs ou les groupes apparaît.

4. **Entrez le nom du ou des utilisateurs auxquels vous souhaitez accorder l'accès puis cliquez sur OK.**

Vous êtes redirigé dans la boîte de dialogue Autorisations. L'utilisateur que vous avez ajouté figure désormais dans la liste des utilisateurs qui ont accès à la boîte aux lettres.

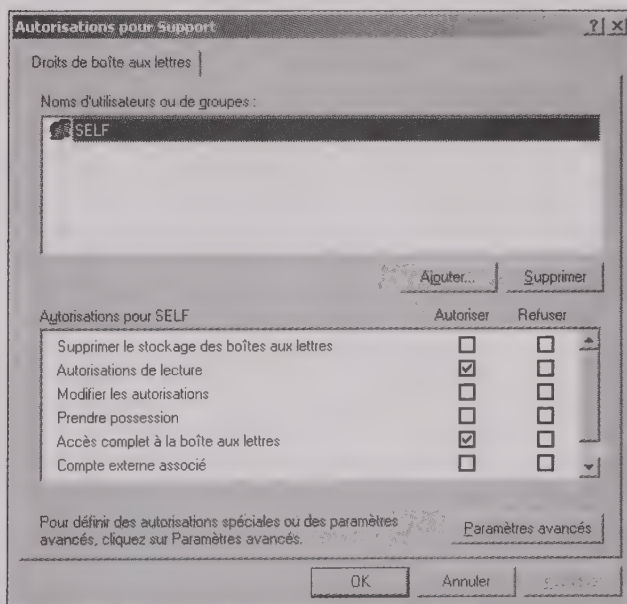


Figure 11.7 : Boîte de dialogue Autorisations.

5. Sélectionnez le nom du ou des utilisateurs auxquels accorder les droits d'accès et cochez, dans la colonne Autoriser, la case Accès complet à la boîte aux lettres puis cliquez sur OK.

La boîte de dialogue Droits de boîte aux lettres disparaît.

6. Cliquez sur OK.

La boîte de dialogue Propriétés se ferme.

À présent, vous pouvez configurer le client de messagerie Outlook de l'utilisateur pour qu'il puisse accéder à la boîte aux lettres fonctionnelle. Pour ce faire, exécutez les étapes suivantes :

1. Sur l'ordinateur de l'utilisateur, démarrez Outlook et exécutez la commande Outils/Paramètres du compte.

La boîte de dialogue Paramètres du compte s'affiche.

2. Sélectionnez votre compte principal et cliquez sur Modifier.

La boîte de dialogue Modifier un compte de messagerie apparaît. Elle est illustrée par la Figure 11.8.

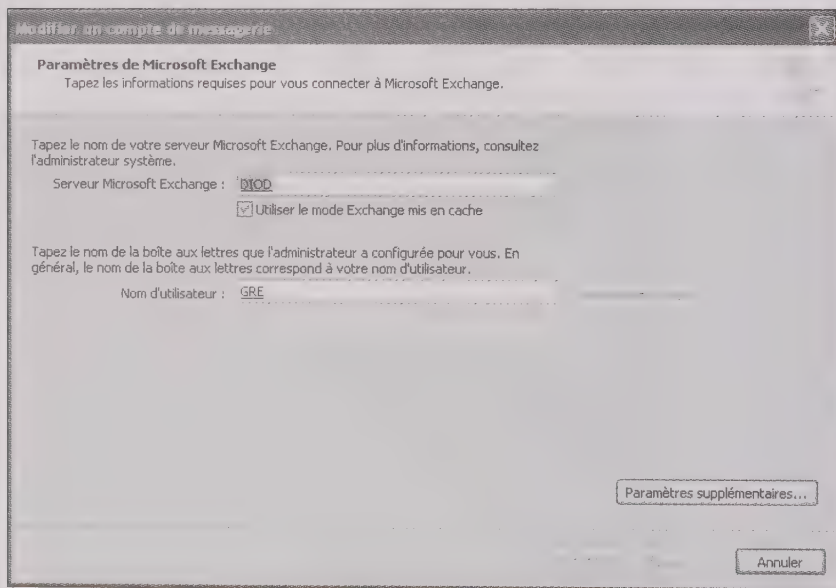


Figure 11.8 : Boîte de dialogue Modifier un compte de messagerie.

3. Cliquez sur le bouton Paramètres supplémentaires et ouvrez l'onglet Avancé.

L'onglet Avancé de la boîte de dialogue Microsoft Exchange s'ouvre. Il est représenté dans la Figure 11.9.

4. Cliquez sur le bouton Ajouter.

La boîte de dialogue qui s'affiche vous invite à indiquer le nom de la boîte aux lettres que vous voulez ajouter.

5. Entrez le nom de cette boîte aux lettres puis cliquez sur OK.

La boîte aux lettres est ajoutée à la liste de la boîte de dialogue Microsoft Exchange.

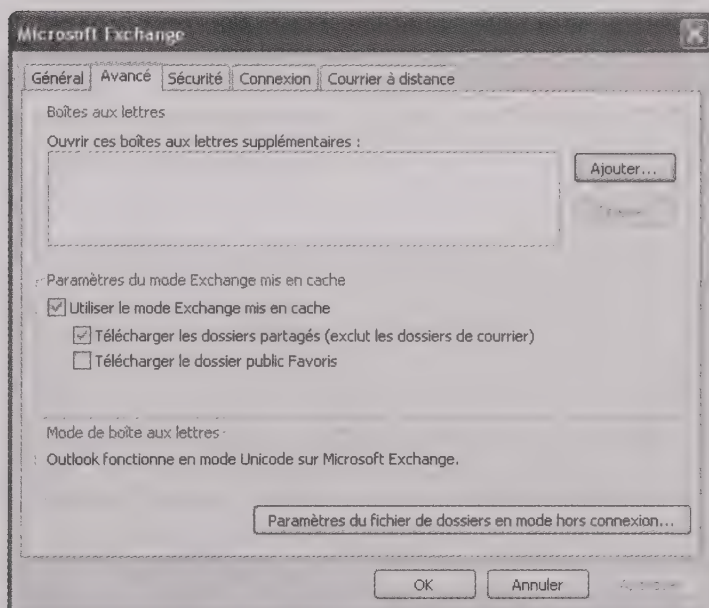


Figure 11.9 : Onglet Avancé.

6. Cliquez sur OK.

Vous basculez dans la boîte de dialogue Modifier un compte de messagerie.

7. Cliquez sur Suivant puis sur Terminer.

C'est terminé ! La boîte aux lettres fonctionnelle est accessible pour un autre utilisateur.

Pour afficher la boîte aux lettres à partir du client Outlook, exécutez la commande Atteindre/Liste des dossiers. Double-cliquez ensuite sur la boîte aux lettres fonctionnelle pour l'ouvrir.



Chapitre 12

Créer un intranet

Dans ce chapitre :

- ▶ Qu'est-ce qu'un intranet ?
- ▶ Guide des bons usages pour les intranets.
- ▶ Éléments nécessaires pour installer un intranet.
- ▶ Installer un serveur Web IIS.
- ▶ Installer un intranet de base.
- ▶ Administrer IIS.

Il ne s'agit pas d'Internet mais bien d'intranet ! Le mot *intranet* est assez récent et n'a gagné ses galons que depuis quelques années. L'intranet est semblable à l'Internet, à une différence près. Plutôt que de connecter votre ordinateur à la toile mondiale et à ses millions d'ordinateurs, un intranet limite la connexion de votre ordinateur à ceux de votre entreprise. Si vous vous demandez en quoi un intranet diffère de votre réseau, lisez la suite, vous allez comprendre !

Qu'est-ce qu'un intranet ?

Chacun sait qu'Internet, et particulièrement le World Wide Web, est devenu un phénomène auquel personne n'échappe. Des centaines de millions d'utilisateurs surfent chaque jour sur le Web.

Depuis quelque temps, les architectes réseau des grandes entreprises ont pris conscience que le Web présentait un intérêt inestimable pour la transmission d'informations au public mais qu'il était encore plus attractif pour les informations qu'il pouvait transférer au sein de l'entreprise. C'est ainsi qu'est née l'idée des intranets ! Un *intranet* est un réseau construit à partir

des mêmes outils et protocoles que ceux employés par Internet mais il est limité au réseau interne de l'entreprise.



En fait, un intranet est une petite version privée du World Wide Web. Toute personne qui peut se connecter à votre réseau local (LAN) peut accéder à votre intranet. L'intranet est consulté en utilisant un navigateur Web comme Internet Explorer ou Firefox. Les utilisateurs n'ont pas besoin d'une connexion Internet puisque les données de l'intranet sont stockées sur les serveurs de l'entreprise.

L'intranet est analogue à un système de télévision qui fonctionne en circuit fermé ; seules les personnes se trouvant dans l'entreprise peuvent le visualiser. En revanche, Internet est semblable à la télévision hertzienne, accessible par toute personne possédant un téléviseur et se trouvant à proximité d'un émetteur.

Voici deux points de vue contradictoires relatifs aux intranets :

- ✓ Quelques pandits de l'industrie informatique prétendent que les intranets sont plus populaires qu'Internet. Par exemple, de nombreuses entreprises qui vendent des outils de développement Web gagnent plus d'argent avec les logiciels utilisés pour des intranets qu'avec ceux destinés à Internet.
- ✓ D'autres pandits de l'industrie informatique pensent que l'intranet est simplement un phénomène de mode apporté par une nouvelle technologie prometteuse, et que, tel le twist ou le hula-hoop, il n'en subsistera rien d'ici quelques années. Qui vivra verra !

Pourquoi utiliser un intranet ?

Les intranets peuvent distribuer n'importe quel type d'information au sein d'une entreprise. En général, ils font appel à deux types d'applications de base :

- ✓ **Les applications de publication** : L'information est diffusée sous forme de pages que vous pouvez consulter à partir de n'importe quel ordinateur ayant un accès à l'intranet. Ce type d'application est utilisé généralement pour les bulletins de l'entreprise, des documentations diverses, des catalogues, des tarifs, etc.

Les applications de publication sont simples à mettre en place et vous pouvez le faire vous-même sans l'aide de consultants extérieurs qui risquent d'entamer fortement votre budget.



- ✓ **Les applications de transaction** : Les utilisateurs de l'intranet utilisent ce type d'application pour saisir des informations : entrées de dépenses, requêtes pour signaler un problème, inscriptions à une activité, etc.

Vous risquez de dépenser des sommes importantes en logiciels et en consultants pour mettre en œuvre ce type d'application.

Voici la différence principale entre ces deux types d'application :

- ✓ **Dans une application de publication, les flux d'informations se propagent dans une seule direction** : de l'intranet vers l'utilisateur. L'utilisateur recherche des informations et le système les lui fournit.
- ✓ **Dans une application de transaction, les flux d'informations se déplacent dans les deux directions** : non seulement l'utilisateur interroge le système mais le système attend de l'utilisateur certaines informations.



Éléments nécessaires pour installer un intranet

Voici ce dont vous avez besoin pour mettre en place un intranet :

- ✓ **Un réseau** : Un intranet n'exige pas son propre câblage, il peut utiliser un réseau existant.
- ✓ **Un serveur dédié à l'intranet** : Vous devez vous assurer que cet ordinateur a au moins 4 Go de RAM et 100 Go d'espace disque libre. Naturellement, plus la quantité d'informations et plus le nombre d'utilisateurs seront importants, plus la mémoire RAM et plus l'espace disque disponible devront être importants.
- ✓ **Windows Server ou un système d'exploitation Linux** : Les logiciels serveur Web tournent sur l'un ou l'autre.
- ✓ **Un logiciel serveur Web** : Vous devez installer un logiciel serveur Web tel qu'IIS (pour les serveurs Windows) ou Apache (pour les serveurs Linux).
- ✓ **Un programme de création de pages Web** : Si vous maîtrisez le langage HTML et si vous êtes capable de le manier comme de la prose, créez directement vos pages Web dans des fichiers texte. Dans ce cas, le seul programme dont vous avez besoin est le bloc-notes. Sinon, vous pouvez utiliser un programme spécifiquement conçu pour la création de pages Web comme Microsoft FrontPage ou Adobe Dreamweaver. Si vous envisagez de développer des applications de transaction, vous aurez besoin d'outils supplémentaires.

Installer un serveur Web IIS

Internet Information Services (ou IIS) est intégré à Windows Server 2003 et 2008 mais n'est pas activé par défaut. Après avoir installé Windows Server, vous devez ajouter le rôle Serveur Web pour activer IIS. La démarche suivante s'applique à Windows Server 2008 (elle est similaire pour Windows Server 2003) :

1. Exécutez la commande Démarrer/Outils d'administration/Gestionnaire de serveur.

Le Gestionnaire de serveur s'ouvre.

2. Cliquez sur Rôles dans le volet de navigation.

Les rôles configurés pour le serveur sont affichés.

3. Cliquez sur Ajouter des rôles.

Cette action lance la page d'accueil de l'Assistant Ajout de rôles.

4. Cliquez sur Suivant.

L'assistant affiche la page Sélectionnez des rôles de serveurs, illustrée par la Figure 12.1.

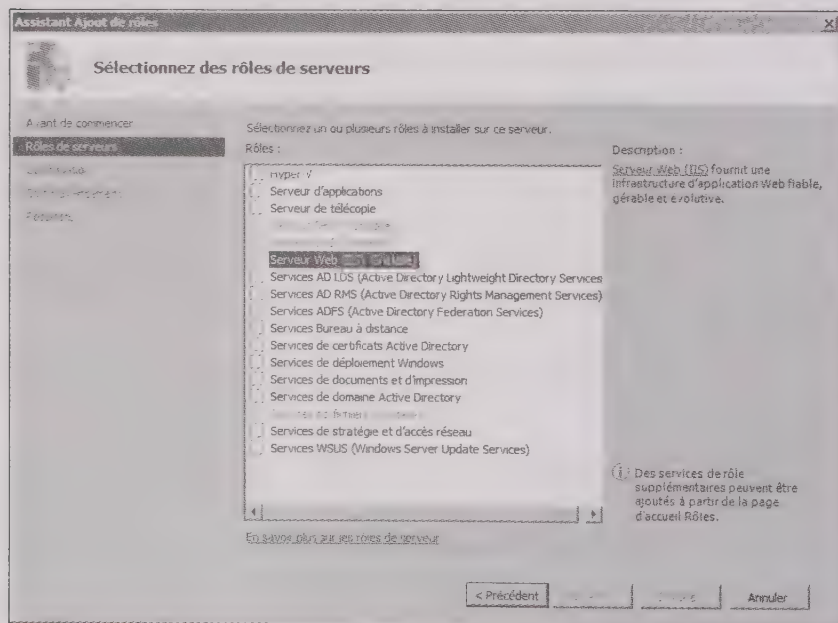


Figure 12.1 : Page Sélectionnez des rôles de serveurs de l'Assistant Ajout de rôles.

5. Cochez Serveur Web (IIS) puis cliquez sur Suivant.

La page Serveur Web (IIS) apparaît, comme le montre la Figure 12.2.

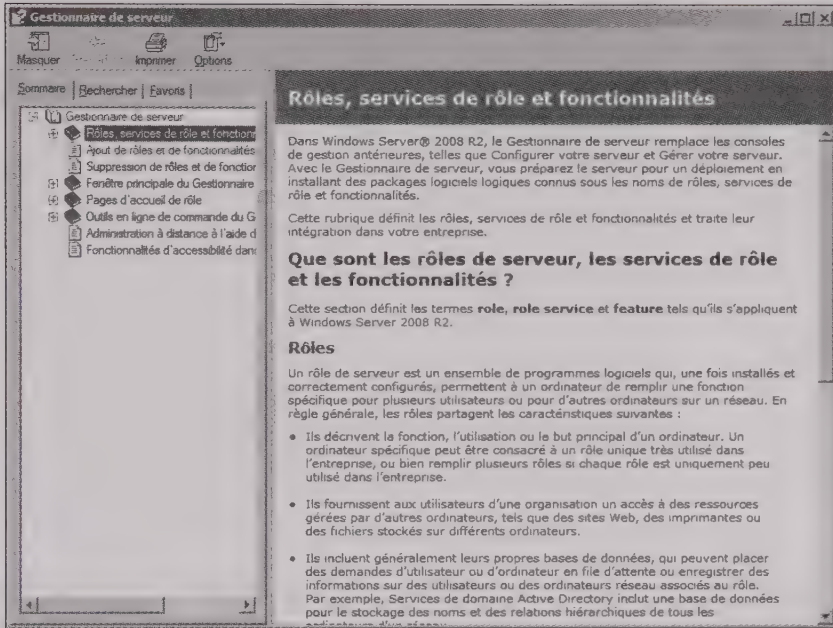


Figure 12.2 : Page Serveur Web (IIS) de l'Assistant Ajout de rôles.

6. Cliquez sur Suivant.

S'ensuit la page Sélectionner les services de rôle, illustrée par la Figure 12.3. Cette page propose plusieurs services qui peuvent être configurés pour IIS.

7. Sélectionnez les services que vous voulez configurer pour IIS.

Si vous le souhaitez, vous pouvez étudier cette liste et réfléchir aux fonctionnalités dont vous pensez avoir besoin. Vous pouvez aussi vous contenter des options sélectionnées par défaut.

Par la suite, vous pourrez, à tout moment, solliciter l'Assistant Ajout de rôles pour ajouter des fonctionnalités que vous n'avez pas installées initialement.



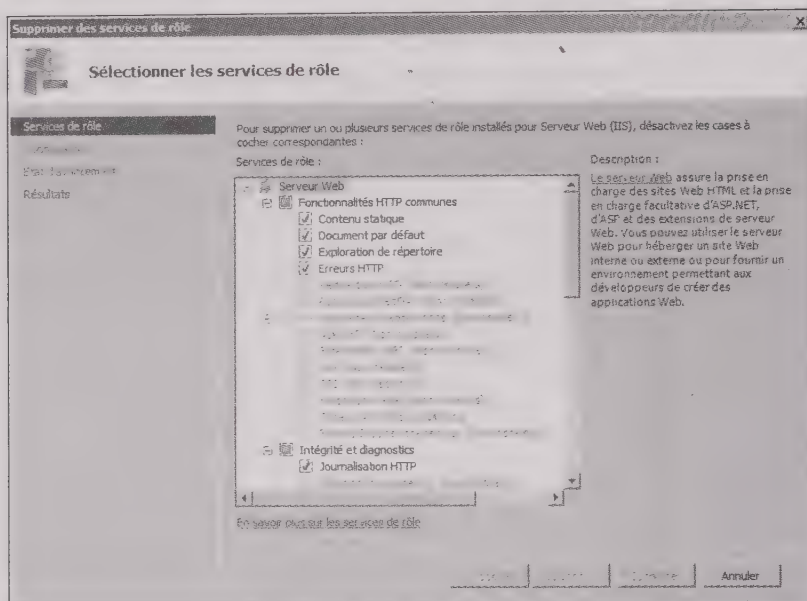


Figure 12.3 : Page Sélectionner les services de rôle de l'Assistant Ajout de rôles.

Un intranet sans serveur Web

En général, un intranet est basé sur un serveur Windows exécutant IIS ou un serveur Linux exécutant Apache ou tout autre serveur Web. Cependant, vous pouvez créer un intranet rudimentaire sans vous donner la peine d'installer de serveur Web réel. Voici comment y parvenir :

1. **Définissez un partage sur un serveur de fichiers sur lequel vous regrouperez les fichiers HTML qui composeront votre intranet.**
2. **Créez un fichier HTML pour la page d'accueil (home page) de votre intranet et sauvegardez-le dans le dossier créé à l'étape 1.**
Nommez-le `index.html`.
3. **Concevez tous les autres fichiers HTML dont votre intranet a besoin.**
Le fichier `index.html` doit contenir tous les liens vers ces pages.
4. **Indiquez à votre navigateur Web le chemin d'accès au fichier `index.html`.**
Par exemple, si le serveur est nommé `iserveur` et le partage `intranet`, entrez cette adresse dans votre navigateur : `\\iserveur\intranet\index.html`. Voilà ! C'est un intranet de base qui ne fait pas appel à un serveur Web.

Cet intranet rudimentaire fonctionne sans serveur Web parce qu'un navigateur Web peut afficher directement des fichiers HTML. Cependant, sans serveur Web, votre intranet est limité car toutes ses pages doivent être *statiques* (leur contenu est figé). Pour y insérer un contenu *dynamique*, c'est-à-dire généré en fonction du choix de l'utilisateur, vous avez besoin d'un serveur Web.

8. Cliquez sur Suivant.

L'assistant ouvre la page Confirmer les sélections pour l'installation, représentée dans la Figure 12.4.

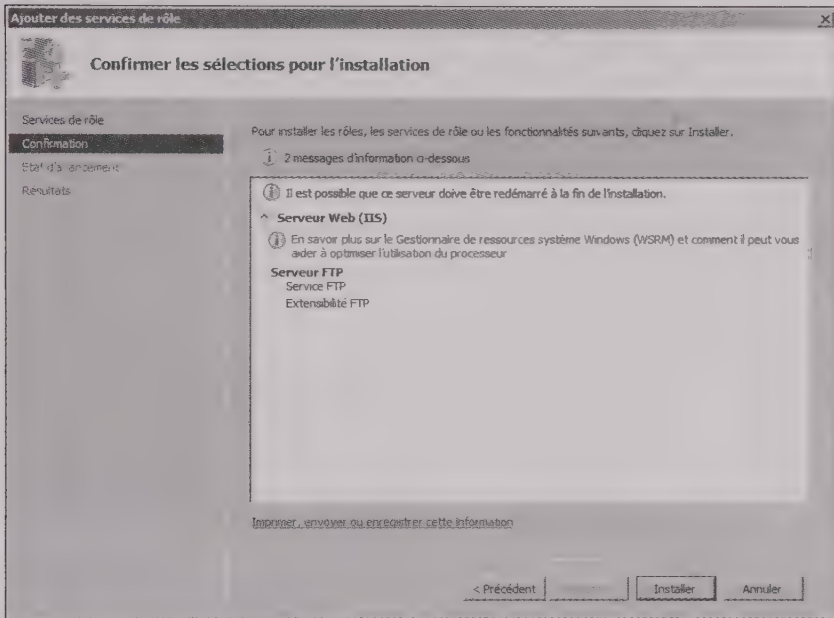


Figure 12.4 : Page Confirmer les sélections pour l'installation de l'Assistant Ajout de rôles.

9. Cliquez sur Installer.

Les fonctionnalités que vous avez sélectionnées sont installées. Cette opération peut prendre plusieurs minutes.

Lorsque l'installation est terminée, l'assistant affiche la page Résultats de l'installation, illustrée par la Figure 12.5.

10. Cliquez sur Fermer.

Le serveur IIS est installé et opérationnel !

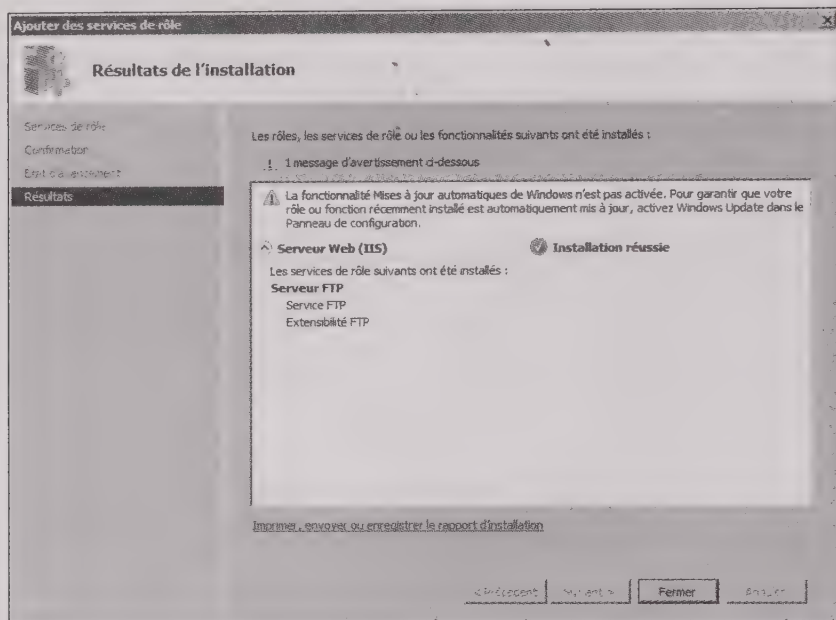


Figure 12.5 : Page Résultats de l'installation de l'Assistant Ajout de rôles.

Créer une page simple d'intranet

Au départ, le serveur IIS est configuré avec un seul site Web, appelé *site Web par défaut*. Pour vérifier si le serveur IIS est opérationnel, ouvrez la fenêtre du navigateur et tapez **localhost** dans la barre d'adresse. Autre alternative pour accéder à cette page : entrez votre nom de domaine local dans la barre d'adresse. La Figure 12.6 représente la page d'accueil standard qui s'affiche quand vous parcourez le site par défaut.

Les fichiers qui forment le site Web par défaut sont stockés sur le disque c : du serveur, dans un dossier appelé `inetpub\wwwroot`. Si vous naviguez sur le site Web par défaut sans spécifier de fichier (par exemple, en entrant simplement `localhost` dans la barre d'adresse), IIS recherche les fichiers suivants, dans cet ordre :

```
default.htm
default.asp
index.htm
index.html
iisstart.htm
default.aspx
```

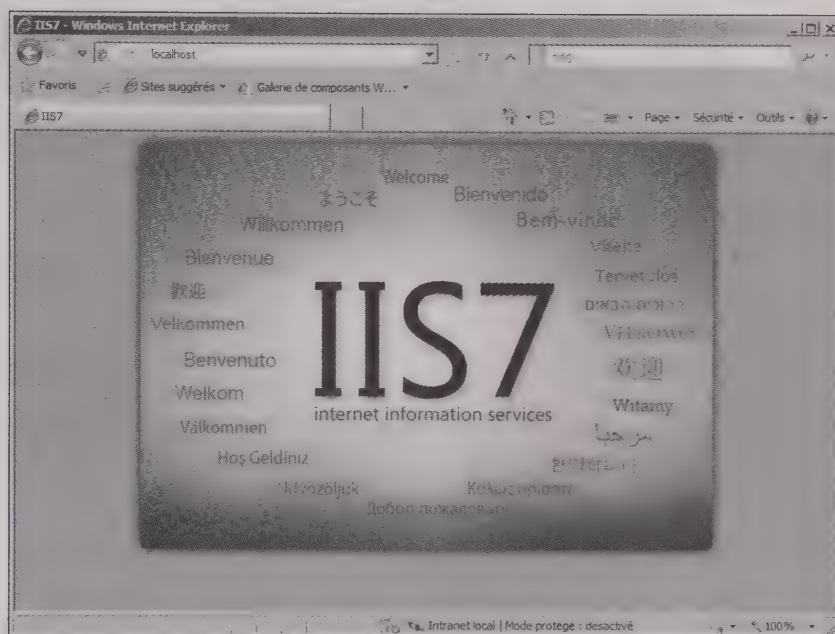


Figure 12.6 : Site Web par défaut.

Au départ, `c:\inetpub\wwwroot` contient seulement deux fichiers : `iisstart.htm` et `welcome.png`. Le fichier `iisstart.htm` correspond au fichier affiché quand vous naviguez sur le site Web. Il contient la balise HTML nécessaire pour afficher l'image contenue dans le fichier `welcome.png` qui est l'image que vous voyez sur la page.

Vous avez la possibilité de prédéfinir la page standard du site Web par défaut. Pour ce faire, vous devez fournir votre propre fichier et lui attribuer l'un des noms précités. Par exemple, vous pouvez appliquer les étapes suivantes pour créer un fichier `default.htm` simple qui affiche l'expression « Bienvenue sur l'intranet ! » sur la page de démarrage du site Web par défaut :

1. Ouvrez la fenêtre de l'Explorateur et allez dans `c:\inetpub\wwwroot`.
2. Sélectionnez Fichier/Nouveau/Document texte, tapez `default.htm` comme nom de fichier et appuyez sur Entrée.
3. Effectuez un clic droit sur le fichier `default.htm` que vous venez de créer et exécutez Ouvrir avec/Bloc-notes.
4. Saisissez le texte suivant dans la fenêtre du Bloc-notes :

```
<HTML>
<BODY>
```



```
<H1>Bienvenue sur l'intranet !</H1>
</BODY>
</HTML>
```

5. Sélectionnez **Fichier/Enregistrer** pour enregistrer le fichier puis cliquez sur **Fichier/Quitter** pour fermer le Bloc-notes.
6. Ouvrez la fenêtre du navigateur.
7. Tapez `localhost` dans la barre d'adresse et appuyez sur **Entrée**.

La page illustrée par la Figure 12.7 s'affiche.

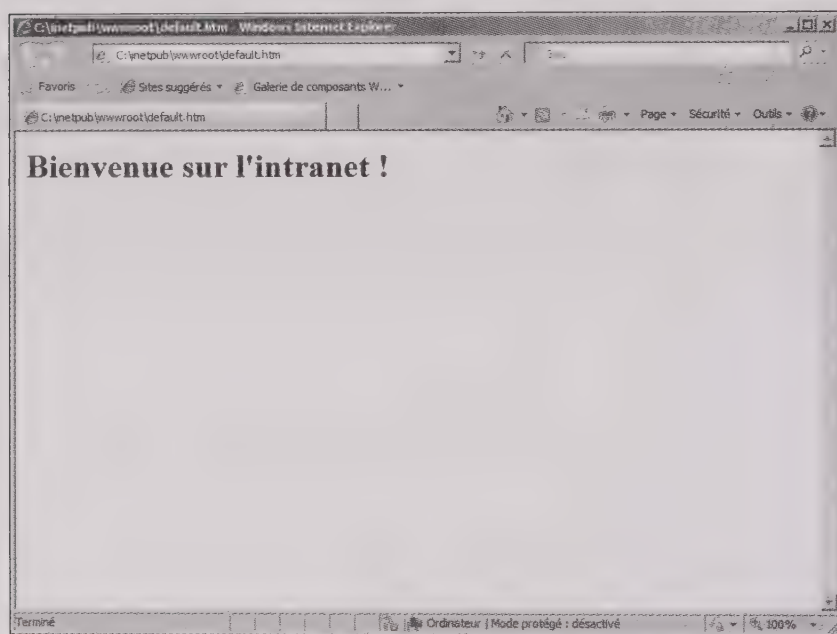


Figure 12.7 : Bienvenue sur l'intranet !

Créer un site Web

IIS peut héberger plusieurs sites Web. C'est une caractéristique très pratique pour les serveurs Web qui hébergent des sites publics mais aussi pour les serveurs Web qui hébergent des sites internes (intranet). Supposons que vous vouliez créer un site Web intranet indépendant pour les ressources humaines et lui attribuer le nom de site `rh`. Si le nom de domaine est `monentreprise.pri`, les utilisateurs peuvent naviguer sur le site Web en utilisant l'adresse `rh.monentreprise.pri`.

Procédez comme suit :

1. Dans l'Explorateur Windows, créez un dossier dans lequel vous allez stocker les fichiers pour le nouveau site Web.

Pour illustrer mon exemple, je crée un dossier nommé `c:\site-web-rh`.

2. Sélectionnez Démarrer/Outils d'administration/Gestionnaire des services Internet (IIS).

Le gestionnaire IIS s'ouvre, comme le montre la Figure 12.8.

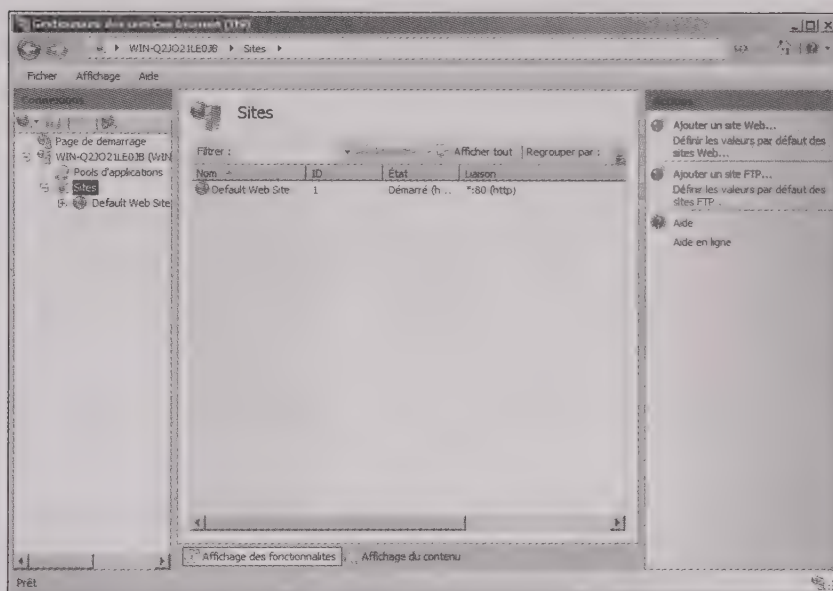


Figure 12.8 : Gestionnaire IIS.

3. Effectuez un clic droit sur Sites et sélectionnez Ajouter un site Web.

La boîte de dialogue Ajouter un site Web apparaît. Elle est illustrée par la Figure 12.9.

4. Entrez le nom du site dans la zone de texte Nom du site Web.

Par exemple, j'utilise RH puisque j'ai créé une page intranet pour le service des ressources humaines.

5. Cliquez sur le bouton ..., sélectionnez le dossier créé à l'étape 1 et cliquez sur OK.

Dans mon cas, il s'agit du dossier `c:\site-web-rh`.

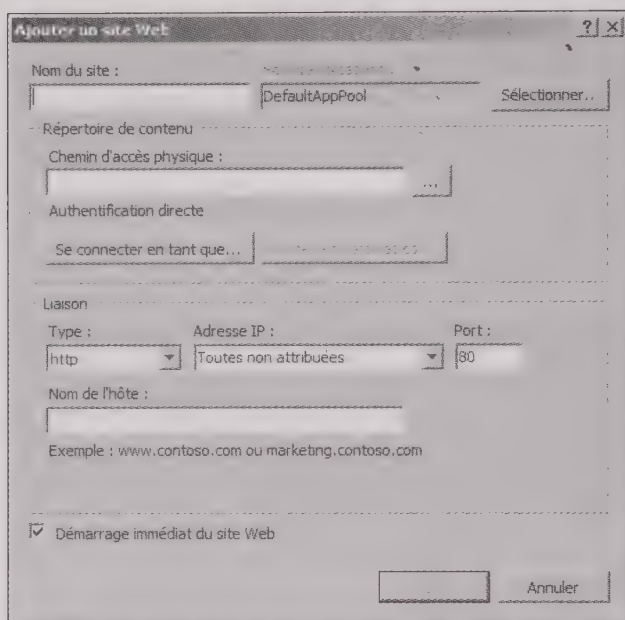


Figure 12.9 : Boîte de dialogue Ajouter un site Web.

6. Dans la zone de texte **Nom de l'hôte**, entrez le nom DNS complet que vous voulez utiliser pour le site.

Par exemple, `rh.monentreprise.pri`.

7. Cliquez sur **OK**.

Le site fraîchement créé prend place sous le nœud **Sites**, dans le **Gestionnaire IIS**, comme le montre la Figure 12.10.

8. Fermez le **Gestionnaire IIS**.

9. Créez une page Web à afficher dans le dossier que vous avez créé à l'étape 1.

Dans mon cas, j'utilise le Bloc-notes pour créer un fichier texte appelé `default.htm`, contenant le texte suivant :

```
<HTML>
<BODY>
<H1>Bienvenue sur le site Web RH !</H1>
</BODY>
</HTML>
```

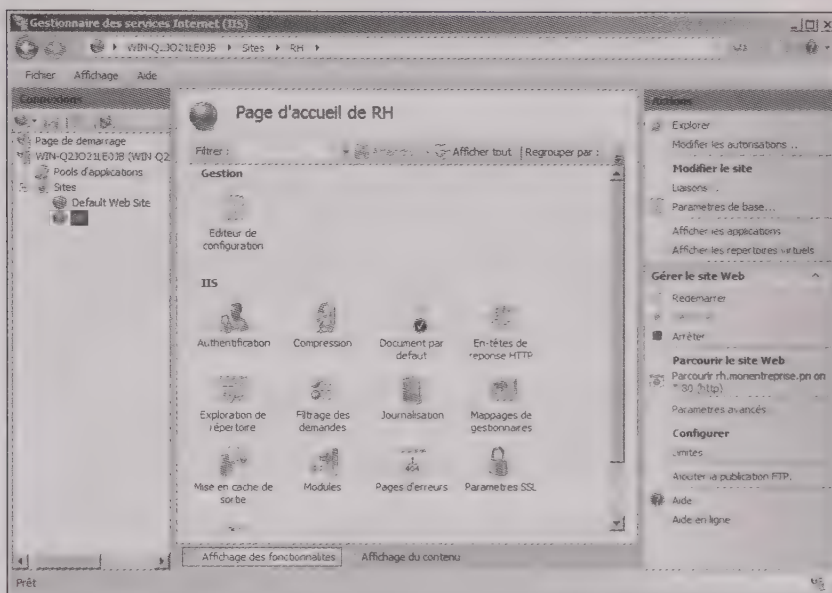


Figure 12.10 : Le site Web RH figure désormais dans le Gestionnaire IIS.

10. Exécutez la commande Démarrer/Outils d'administration/DNS.

Cette commande ouvre le Gestionnaire DNS, représenté dans la Figure 12.11.

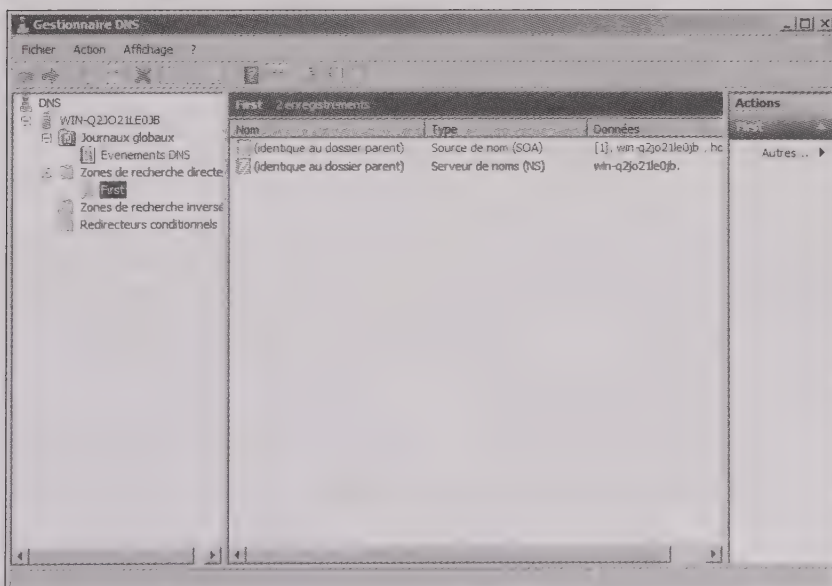


Figure 12.11 : Gestionnaire DNS.

11. Repérez le nœud de votre domaine dans le volet de navigation.

Dans l'exemple, il s'agit du nœud `monentreprise.pri`.

12. Sélectionnez Action/Nouvel alias (CNAME).

La boîte de dialogue *Nouvel enregistrement de ressource* s'affiche, comme le montre la Figure 12.12.

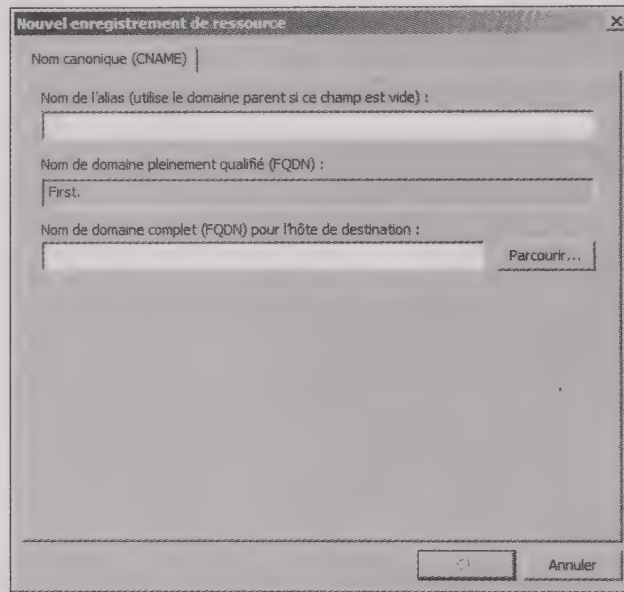


Figure 12.12 : Création d'un enregistrement CNAME.

13. Saisissez, dans la zone de texte Nom de l'alias, le nom d'alias que vous voulez utiliser.

Entrez, par exemple, `rh`.

14. Spécifiez le nom d'ordinateur de votre serveur Web dans la zone de texte Nom de domaine pleinement qualifié pour l'hôte de destination.

Entrez un nom de serveur, par exemple, `1serveur01`.

15. Cliquez sur OK.

L'alias est créé.

16. Fermez le Gestionnaire DNS.**17. Ouvrez votre navigateur.**

18. Naviguez jusqu'à l'adresse de l'alias que vous venez de créer.

Dans mon exemple, je visite la page `rh.monentreprise.pri`, illustrée par la Figure 12.13.

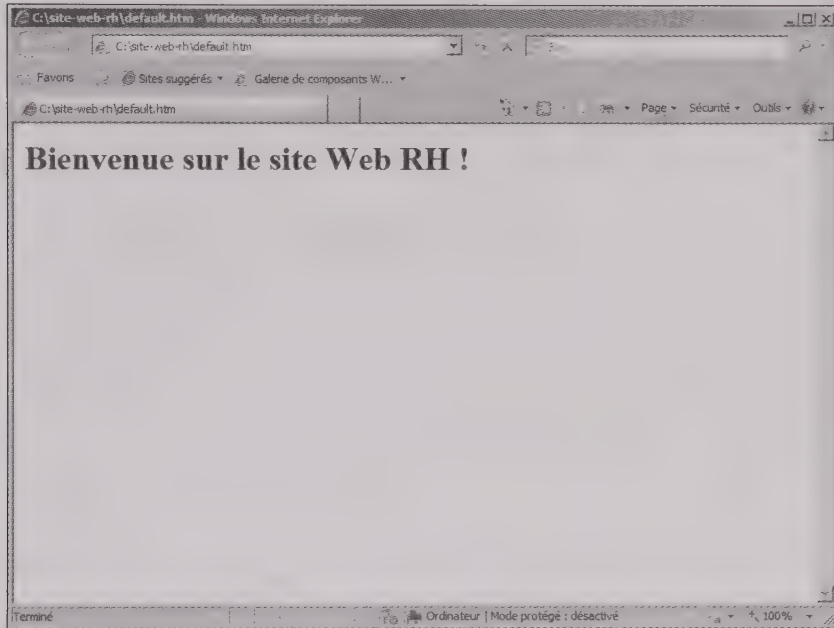


Figure 12.13 : Aperçu du site Web.

Chapitre 13

Téléphone ou ordinateur ? (ou comprendre la voix sur réseau IP !)

Dans ce chapitre :

- ▶ Comment fonctionne la VoIP ?
- ▶ Avantages de la VoIP.
- ▶ Inconvénients de la VoIP.
- ▶ Quelques fournisseurs de VoIP connus.

La convergence de deux types de réseaux semblables mais distincts, les réseaux informatiques et les réseaux téléphoniques, est l'une des nouvelles tendances dans l'univers des réseaux. Ces deux types de réseaux peuvent être câblés ou sans fil et peuvent transporter la voix et les données. En d'autres termes, la distinction entre les réseaux informatiques et les réseaux téléphoniques devient trouble.

Ce chapitre est une brève introduction à la *VoIP*, une technologie qui vous permet de transporter des signaux vocaux avec votre réseau informatique. Autrement dit, la voix sur réseau IP rend obsolètes vos câbles téléphoniques.

Ce chapitre n'est en aucun cas un guide complet sur la VoIP. Pour tout savoir sur la VoIP, je vous conseille *VoIP pour les Nuls*, signé Timothy V. Kelly et publié par Wiley.



Comprendre la VoIP

La VoIP ou *voix sur réseau IP* (Internet Protocol) fonctionne en gros comme un téléphone standard. Cependant, plutôt que d'utiliser le réseau public de téléphonie, les téléphones se connectent directement au réseau Internet. Le principal avantage est un coût réduit puisque vous utilisez le réseau Internet.

Lorsque vous utilisez un téléphone normal pour une communication, votre voix est transmise sous forme numérique par le *réseau téléphonique public commuté*. Vous êtes alors taxé par votre fournisseur en fonction de la distance et de la durée.

Lorsque vous utilisez la VoIP, votre voix est encore convertie sous forme numérique, puis, plutôt que d'être transmise par le réseau téléphonique commuté, elle est transportée sur le *réseau Internet*. Puisqu'Internet utilise le protocole IP, les données numériques qui représentent votre voix sont converties en paquets qui correspondent aux spécificités du protocole. Pour cette raison, on parle de *voix sur IP* ou de *voix sur réseau IP*.

Le transport de conversations téléphoniques sur les réseaux Internet n'est pas nouveau. La technologie existe depuis de nombreuses années. Cependant, son coût réduit est récent, c'est ce qui l'a rendue très populaire depuis peu.

Il y a deux approches de base à l'accès à la VoIP :

- ✓ **Les logiciels de VoIP** : Ils sont exécutés sur votre ordinateur et permettent de parler librement avec n'importe qui partout dans le monde, à condition que votre correspondant utilise le même logiciel que vous.

Le logiciel de VoIP le plus connu est Skype (www.skype.com). C'est un logiciel gratuit qui présente deux inconvénients majeurs :

- Vous ne pouvez l'utiliser qu'à partir d'un ordinateur. Un téléphone classique ne permet pas de composer un numéro et d'appeler par l'intermédiaire de Skype.
- Votre interlocuteur doit obligatoirement utiliser Skype. Vous ne pouvez pas appeler n'importe qui.

Skype propose désormais un système payant, SkypeOut, qui permet d'établir une communication avec un téléphone. Pour la France, l'appel est à 1,4 centime la minute vers un fixe et à 14,9 centimes vers un portable.

Notez que Skype propose des versions pour téléphone portable qui fonctionnent sur différents types de portables.



TRUC

- ✓ **Les services VoIP proposés par des fournisseurs d'accès** tels qu'Orange ou Free. Ces services n'exigent pas un ordinateur. Ils utilisent un *adaptateur de téléphone analogique* (ATA) qui connecte un téléphone normal à l'Internet. L'adaptateur permet d'utiliser la VoIP comme si vous aviez un téléphone standard. Vous prenez le téléphone et vous composez le numéro. Le fait que l'appel soit transmis sur Internet plutôt que sur le réseau téléphonique public est transparent.

Avantages de la VoIP

Le service VoIP présente plusieurs avantages importants par rapport au service de téléphonie traditionnel. En voici quelques-uns :

- ✓ **Les communications longue distance sont meilleur marché avec la VoIP** que celles proposées par les services téléphoniques traditionnels. Avec la VoIP, vous payez mensuellement quelques euros pour un usage et des distances illimités. Si votre facture téléphonique dépasse quelques dizaines d'euros, vous serez sans doute intéressé.

Si votre entreprise se trouve à un bout de la France et vos clients à l'autre bout, n'ayez aucune crainte quant au prix des appels, les communications seront au coût des communications locales, aussi bien pour vous que pour vos clients.

- ✓ **Les services de VoIP proposent des fonctionnalités** telles que la mise en attente, le transfert d'appel, l'identification de l'interlocuteur, les audioconférences à trois et plus, la messagerie, etc.
- ✓ **La qualité actuelle de la VoIP est aussi bonne** que le service téléphonique traditionnel.
- ✓ **Les services de VoIP proposent des fonctionnalités supplémentaires** que vous pouvez utiliser avec un ordinateur. Par exemple, certains services peuvent envoyer vos messages d'audiomessagerie à un compte de messagerie standard. Votre correspondant pourra ensuite y accéder avec un logiciel comme Outlook ou un autre logiciel de courrier électronique.



Inconvénients de la VoIP

Vous devez prendre en compte quelques inconvénients avant d'abandonner votre fournisseur de service téléphonique ; voici les plus importants :

- ✓ **Vous devez posséder une connexion Internet avec un haut débit fiable.** Si votre connexion Internet se dégrade, votre connexion VoIP se dégradera.
- ✓ **La VoIP a besoin de courant électrique pour fonctionner.** En conséquence, vous ne pouvez pas utiliser votre téléphone VoIP pendant une panne d'alimentation, à moins que vous possédiez un onduleur ou un groupe électrogène. Les téléphones traditionnels tirent leur puissance directement des lignes téléphoniques, c'est pourquoi ils continuent de fonctionner même pendant des pannes d'alimentation électrique.
- ✓ **La VoIP n'est pas vraiment mobile.** Ce n'est pas un portable.
- ✓ **Les appels aux numéros de secours comme le 15 ou le 18 sont problématiques** avec la VoIP. Les services de secours sont conçus pour identifier les correspondants mais la VoIP n'étant pas attachée à un emplacement particulier, ils ne pourront pas vous localiser.

Quelques fournisseurs de VoIP populaires

Si vous envisagez de passer à la VoIP, voici quelques fournisseurs :

- ✓ **Orange** : Un des fournisseurs de VoIP les plus anciens et les plus populaires. Internet plus téléphone à partir de 29,90 euros par mois : <http://www.orange.fr>.
- ✓ **Free** : Avec le service de téléphonie Freebox, profitez de la téléphonie illimitée en nombre vers les fixes de 70 destinations, dont la France, et disposez gratuitement de nombreux services optionnels. 29,99 euros par mois : <http://www.free.fr>.
- ✓ **SFR** : Appels illimités 24 h/24 et 7 j/7 en France métropolitaine et vers plus de 90 destinations si vous optez pour la neufbox de SFR. 29,90 euros par mois : <http://ads1.sfr.fr>.

Chapitre 14

Et les portables ?

Dans ce chapitre :

- Différents types de portables.
- Configurer Exchange sur des appareils sous Windows Mobile.
- BlackBerry et BlackBerry Enterprise Server (BES).
- Garantir la sécurité.

En août 2003, un consultant informatique acheta un BlackBerry d'occasion sur eBay pour 11 euros. Quand il alluma le portable après avoir changé de batterie, il découvrit qu'il contenait les adresses de messagerie et les informations de contact de cadres d'une célèbre institution financière.

Oups !

En fait, un ancien cadre de cette entreprise avait décidé de vendre son vieux BlackBerry sur eBay quelques mois après avoir quitté la société. Il pensait qu'en enlevant la batterie, il avait supprimé toutes les données contenues sur son BlackBerry.

La conclusion de cette histoire vraie est que les portables comme les BlackBerry lancent de nouveaux défis aux administrateurs réseau. Tous les administrateurs y sont confrontés, quelle que soit la taille du réseau. Par exemple, il y a quelques années, seules les grandes entreprises possédaient des BlackBerry ou d'autres portables qui intégraient la messagerie Exchange. Aujourd'hui, toutes les entreprises, même les plus petites, utilisent ce type de portables.

Ce chapitre propose une brève introduction aux portables et aux systèmes d'exploitation qu'ils exécutent. Il se concentre tout particulièrement sur Windows Mobile et les BlackBerry. Vous allez découvrir comment ces appareils interagissent avec la messagerie Exchange et comment garantir leur sécurité.

Différents types de portables

Autrefois, il y avait des téléphones portables et des PDA. Un téléphone portable était simplement un téléphone portatif qui vous accompagnait partout. Les modèles les plus performants disposaient de fonctionnalités comme un journal des appels, un carnet d'adresses voire même un jeu. Les PDA (*Personal Digital Assistants*) étaient des ordinateurs portatifs conçus pour remplacer les bons vieux agendas qui permettaient de garder un œil sur les rendez-vous et les contacts.

Tout a changé il y a quelques années quand les fournisseurs de téléphonie mobile ont offert la possibilité de transmettre des données sur leurs réseaux. Désormais les téléphones portables peuvent accéder à Internet. Cette avancée s'est illustrée par l'ajout de fonctionnalités PDA sophistiquées aux portables et de fonctions téléphoniques aux PDA au point où la distinction entre les deux est minime.

Le terme *portable* est utilisé pour désigner une vaste palette d'appareils qui tiennent dans une main et qui sont connectés via un réseau sans fil. Le terme *mobile* est également employé pour parler de tels appareils. La liste suivante décrit les appareils portables les plus courants :

- ✓ **Téléphone portable** : Un *téléphone portable* (ou *mobile*) est un appareil portable dont la fonction première est le service téléphonique. La plupart des téléphones portables possèdent des fonctionnalités telles que la messagerie textuelle, les carnets d'adresses, les agendas, les jeux. Certains peuvent aussi fournir un accès à Internet.
- ✓ **Smartphone** : Un *smartphone* est un téléphone portable doté de fonctionnalités avancées dont ne disposent pas les téléphones portables classiques. La différence entre téléphone portable et smartphone n'est pas clairement établie, si ce n'est qu'un smartphone peut fournir un accès intégré à la messagerie professionnelle. Généralement, l'écran d'un smartphone est plus grand que celui d'un portable classique, mais l'appareil ressemble tout de même à un portable avec un clavier sous l'écran.
- ✓ **PDA** : Un PDA est un appareil portatif qui sert principalement à fournir des applications PIM (Personal Information Management, gestion d'informations personnelles) comme des listes de contacts, des agendas et la messagerie. Un PDA standard possède un petit clavier et un écran relativement grand. Les PDA peuvent aussi offrir des services de téléphonie.
- ✓ **PocketPC** : Un *PocketPC* est un type de portable très particulier qui utilise des spécifications publiées par Microsoft. Les pocketPC disposent d'un écran tactile et ne possèdent généralement pas de clavier séparé. Les pocketPC utilisent la version mobile de Windows, *Windows Mobile*.

- ✓ **BlackBerry** : Les BlackBerry sont des PDA sophistiqués, développés par Research In Motion (RIM), dotés de fonctions téléphoniques. La fonctionnalité la plus marquante des BlackBerry est leur capacité à se synchroniser avec des serveurs de messagerie Exchange pour vous fournir un accès instantané à votre messagerie professionnelle. Cette synchronisation exige qu'un serveur spécifique, nommé BlackBerry Enterprise Server (BES), soit exécuté sur le réseau professionnel. Les appareils BlackBerry utilisent un système d'exploitation propriétaire développé par RIM.
- ✓ **iPhone** : L'iPhone, conçu par Apple, fonctionne avec un réseau sans fil ou un réseau de données cellulaires. Comme le BlackBerry, l'iPhone est un PDA avancé. Toutefois, l'iPhone présente deux fonctionnalités qui le distinguent des autres appareils mobiles. Premièrement, il ne possède pas de clavier mais un écran tactile qui permet la saisie. Deuxièmement, l'iPhone possède une interface très facile à utiliser, conçue par les gourous d'Apple qui semblent savoir mieux que quiconque comment créer des interfaces informatiques intuitives et faciles à utiliser.

Configurer Exchange sur un iPhone et un appareil sous Windows Mobile

Certains appareils mobiles utilisent une version de Windows nommée Windows Mobile. Windows Mobile intègre une version mobile d'Outlook, *Outlook Mobile*, qui permet une synchronisation en temps réel avec Exchange. Les fonctionnalités qui permettent cette synchronisation s'appellent *Outlook Mobile Access* et *Exchange ActiveSync*. Elles sont faciles à configurer.

L'iPhone utilise aussi Exchange ActiveSync pour se connecter à un compte de messagerie. Que vous utilisiez un appareil sous Windows Mobile ou un iPhone, vous pouvez suivre ces étapes pour activer l'accès à la messagerie :

1. **Connectez-vous au serveur Exchange avec un compte Administrateur Exchange.**
2. **Sélectionnez Démarrer/Outils d'administration/Gestionnaire système Exchange.**
3. **Dans le volet de navigation, développez le nœud Paramètres globaux.**
4. **Effectuez un clic droit sur Services mobiles et choisissez Propriétés.**

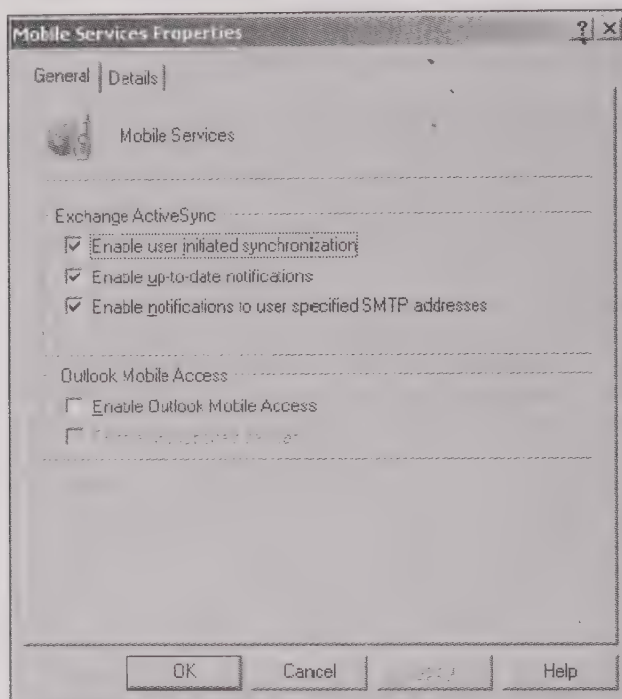


Figure 14.1 : Activation d'Outlook Mobile Access.

La boîte de dialogue illustrée par la Figure 14.1 s'affiche.

5. Activez toutes les cases à cocher de l'onglet Général.

Vous activez ainsi toutes les fonctionnalités d'Outlook Mobile Access et d'Exchange ActiveSync.

6. Cliquez sur OK.

7. Fermez le Gestionnaire système Exchange.

8. Sélectionnez Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory.

La console Utilisateurs et ordinateurs Active Directory s'ouvre.

9. Développez le domaine et localisez l'utilisateur pour lequel vous voulez activer l'accès mobile.

10. Effectuez un clic droit sur l'utilisateur et choisissez Propriétés.

11. Ouvrez l'onglet Fonctionnalités Exchange.

Les options des Fonctionnalités Exchange s'affichent, comme le montre la Figure 14.2.

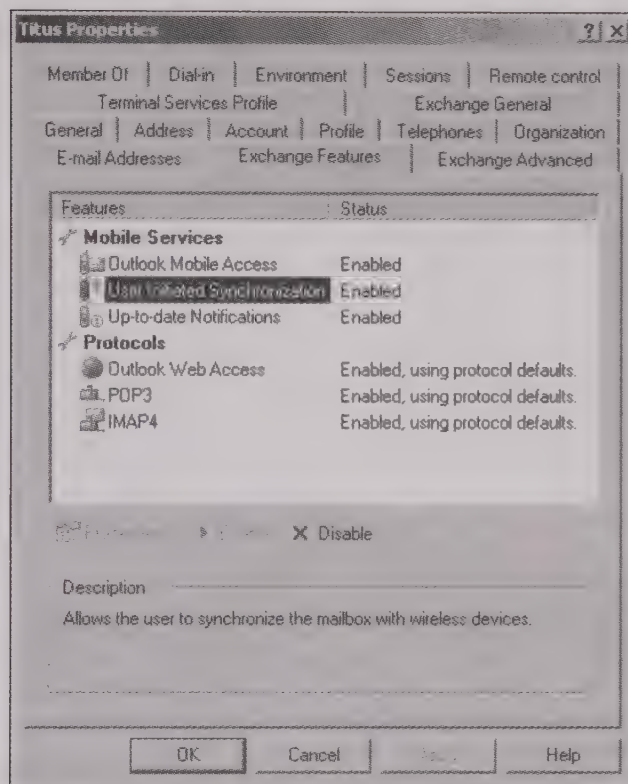


Figure 14.2 : Activation de l'accès mobile pour un utilisateur.

12. Activez les trois options proposées sous Outlook Mobile Access.

Si ces options ne sont pas encore activées, effectuez un clic sur chacune d'elles et choisissez Activer.

13. Cliquez sur OK.

14. Répétez les étapes 10 à 13 pour tous les utilisateurs pour lesquels vous voulez activer l'accès mobile.

15. Fermez la console Utilisateurs et Ordinateurs Active Directory.

C'est tout ce que vous avez à faire. Maintenant que vous avez activé ces fonctionnalités, les utilisateurs sous Windows Mobile peuvent synchroniser leur portable avec leur boîte de messagerie Exchange.

Configurer un BlackBerry

Malheureusement, la configuration d'un BlackBerry est sensiblement plus compliquée que celle d'un appareil sous Windows Mobile. Ceci s'explique de la manière suivante : Microsoft inclut une prise en charge des appareils sous Windows Mobile dans un serveur Exchange tandis que vous devez utiliser un logiciel supplémentaire pour la prise en charge d'un BlackBerry.

Si vous ne gérez que quelques utilisateurs de BlackBerry, vous pouvez synchroniser leur portable avec Exchange en utilisant un service appelé *BlackBerry Internet Service* ou *BIS*. BIS est un site Web auquel vous vous connectez pour fournir les informations de compte Exchange pour chacun de vos utilisateurs BlackBerry. BIS se charge ensuite de la synchronisation. Pour faire court, BIS agit tel un utilisateur d'Office Web Access (OWA) pour accéder aux données Exchange de l'utilisateur. Il transfère ensuite les données qu'il récupère via OWA sur le BlackBerry. Votre fournisseur de service vous indiquera l'adresse exacte du site Web BIS qui fonctionne avec votre BlackBerry.

BIS fonctionne étonnamment bien mais il n'est pas instantané. Le délai entre la réception d'un message dans la boîte Exchange et l'affichage sur le BlackBerry est d'environ 15 minutes voire plus.

Pour un accès plus rapide, vous devez installer *BlackBerry Enterprise Server* ou *BES* sur un serveur. Dans une petite structure, vous pouvez installer BES sur le même serveur physique qu'Exchange. Si vous gérez plus d'une douzaine d'utilisateurs BlackBerry, il est préférable d'utiliser un serveur séparé, dédié à BES.

Après avoir installé BES, vous pouvez l'utiliser pour administrer les utilisateurs BlackBerry. La Figure 14.3 représente le Gestionnaire BlackBerry qui sert à gérer votre administration BES. À partir de cette page, vous pouvez configurer de nouveaux utilisateurs BlackBerry, modifier ou supprimer des utilisateurs existants et réaliser d'autres tâches pour gérer votre environnement BlackBerry.

Garantir la sécurité des appareils mobiles

En tant qu'administrateur réseau, l'une de vos principales responsabilités vis-à-vis des appareils mobiles est de garantir leur sécurité. Malheureusement, c'est un défi de taille, notamment pour les raisons suivantes :

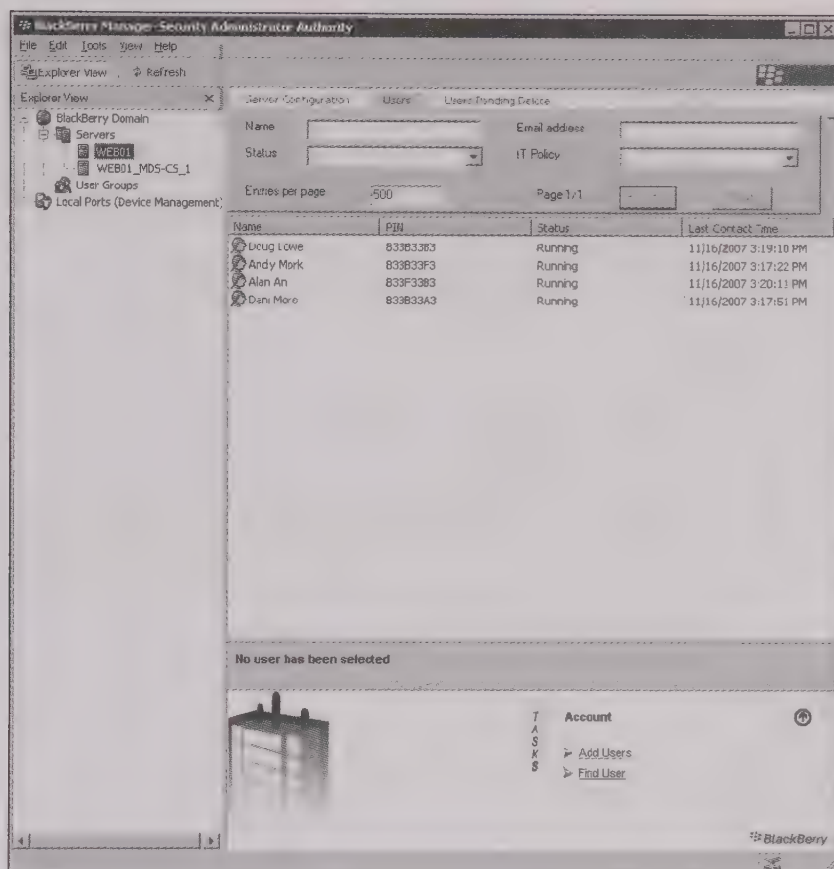


Figure 14.3 : Gestionnaire BlackBerry.

- ✓ **Les appareils mobiles se connectent à votre réseau via d'autres réseaux qui échappent à votre contrôle.** Vous pouvez faire tout votre possible pour installer des pare-feu, mettre en place un système de cryptage et définir une foule d'autres fonctions de sécurité. Quoi qu'il en soit, les portables se connectent par l'intermédiaire de réseaux publics dont les administrateurs ne sont pas forcément aussi conscients que vous.
- ✓ **Les portables se perdent facilement.** Il se peut qu'un utilisateur oublie son BlackBerry dans un restaurant ou un hôtel ou qu'il glisse de sa poche dans le métro.
- ✓ **Les mobiles utilisent des systèmes d'exploitation qui ne sont pas aussi soucieux de la sécurité que Windows.**

- ✓ Les utilisateurs qui n'osent pas installer de logiciel renégat sur leur ordinateur de bureau ne verront aucun mal à télécharger des jeux gratuits ou des sonneries de téléphone sur leur portable. Qui sait quels types de virus ou de chevaux de Troie ces téléchargements peuvent contenir ?
- ✓ Inévitablement, des personnes vont acheter leur propre portable et le connecter à votre réseau sans vous demander votre avis ni même votre permission.

Voici quelques recommandations pour renforcer la sécurité de vos appareils mobiles :

- ✓ Définissez des directives claires et cohérentes pour les appareils mobiles et appliquez-les.
- ✓ Assurez-vous que les employés comprennent qu'ils ne sont pas autorisés à se connecter à votre réseau avec leur propre portable. Permettez uniquement aux appareils de l'entreprise de se connecter.
- ✓ Informez vos utilisateurs des risques de sécurité liés à l'utilisation d'appareils mobiles.
- ✓ Implémentez une solution antivirus sur vos appareils mobiles.

Chapitre 15

Se connecter au réseau depuis son domicile

Dans ce chapitre :

- Accéder à la messagerie avec Outlook Web Access.
- Utiliser un réseau privé virtuel.

Il peut arriver qu'à la fin de la journée vous n'ayez pas terminé votre travail et que vous rapportiez un peu de boulot à la maison pour le terminer dans la soirée ou pendant le week-end. Cependant, le transfert de données entre l'ordinateur de l'entreprise et l'ordinateur familial n'est pas toujours facile.

La première solution, si vous possédez un ordinateur portable, consiste à travailler hors connexion, comme cela a été expliqué dans le Chapitre 3. Cependant, cette approche a ses inconvénients. Que se passe-t-il si quelqu'un va au bureau samedi et modifie le fichier sur lequel vous travaillez hors connexion chez vous ? Que faire si vous rentrez chez vous et que vous découvrez que le fichier dont vous avez besoin se trouve dans un dossier pour lequel vous avez oublié d'activer l'accès hors connexion ?

Qu'en est-il de la messagerie ? Un accès hors connexion ne vous permet pas d'accéder à votre compte de messagerie professionnel. Ainsi, vous ne pouvez pas vérifier si vous avez reçu des messages ni envoyer de messages depuis votre compte de messagerie professionnel.

Ce chapitre introduit deux dispositifs qui peuvent éviter ces problèmes. Le premier est l'accès, basé sur Internet, à votre messagerie par l'intermédiaire d'Outlook Web Access (OWA) dans Microsoft Exchange. La seconde est l'utilisation d'un *réseau privé virtuel* (VPN) qui vous permet de vous connecter à votre réseau d'entreprise depuis votre domicile et d'accéder à toutes les ressources du réseau comme si vous étiez connecté localement à ce réseau.

Utiliser Outlook Web Access (OWA)

La plupart des personnes qui se connectent à leur réseau d'entreprise depuis leur domicile n'ont en fait besoin que d'un accès à leur messagerie. Si c'est la seule raison d'accéder au réseau d'entreprise, OWA est une solution simple et facile à mettre en œuvre.

OWA (*Outlook Web Access*) est une fonctionnalité de Microsoft Exchange Server qui permet d'accéder à votre messagerie depuis n'importe quel ordinateur possédant une connexion Internet. L'ordinateur distant n'a besoin que d'un navigateur Web et d'une connexion Internet. Aucun VPN ou toute autre configuration spéciale n'est exigé.

Vous n'avez aucune installation particulière à réaliser pour activer OWA. Cette fonctionnalité est activée par défaut quand vous installez Microsoft Exchange. Vous pouvez bien sûr configurer différentes options pour améliorer son utilisation mais OWA est parfaitement opérationnel avec sa configuration par défaut.

Pour accéder à OWA depuis n'importe quel navigateur Web, spécifiez, dans la barre d'adresse, celle du service OWA de votre organisation. L'adresse par défaut est le nom DNS de votre serveur de messagerie suivi de /exchange. Par exemple, l'adresse OWA du serveur de messagerie smtp.messageriepro.com est smtp.messageriepro.com/exchange.

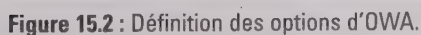
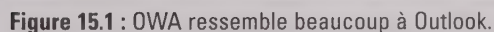


La connexion doit utiliser la version sécurisée du protocole Web HTTP. Vous devez ajouter https:// devant l'adresse OWA. L'adresse complète sera donc https://smtp.messageriepro.com/exchange.

Dès que vous accédez au serveur, vous êtes invité à entrer un nom et un mot de passe. Spécifiez le compte utilisateur et le mot de passe que vous utilisez régulièrement sur le réseau. OWA apparaîtra dans la fenêtre du navigateur, comme dans la Figure 15.1.

Si vous êtes habitué à Outlook, vous n'aurez aucune difficulté à utiliser OWA. La plupart des fonctionnalités d'Outlook sont disponibles, y compris la Boîte de réception, le Calendrier, les Contacts, les Tâches, les Rappels et même les Dossiers publics. Vous pouvez même programmer le Gestionnaire d'absences du bureau.

À la différence d'Outlook, OWA ne possède pas de barre d'outils, cependant, la plupart des fonctions qui sont proposées par la barre d'outils d'Outlook sont disponibles à d'autres endroits dans la fenêtre OWA. Si vous ne trouvez pas une fonction, ouvrez la page Options. Pour ce faire, cliquez sur le bouton Options dans la partie inférieure gauche de l'écran. La Figure 15.2 représente la page Options qui permet d'activer le Gestionnaire d'absences du bureau, de modifier la signature et de définir diverses options de la messagerie.



Utiliser un VPN (Virtual Private Networks)

Le terme *réseau privé virtuel* ou *VPN* se rapporte à plusieurs types de communications Internet sécurisées. Nous considérerons dans ce chapitre qu'un VPN est un canal sécurisé entre un ordinateur distant et un réseau local. Ce type de VPN permet d'ouvrir une session sur votre réseau d'entreprise depuis votre ordinateur familial. Vous pouvez alors accéder à n'importe quelle ressource de votre réseau d'entreprise comme si vous utilisiez l'ordinateur de votre bureau. En d'autres termes, le VPN augmente l'étendue du réseau d'entreprise pour y inclure votre ordinateur familial.



Le mécanisme de sécurité qui réalise ce travail magique est le protocole Internet connu sous le nom d'IPSec. L'étude détaillée d'IPSec dépasse le cadre de ce livre. Gardez simplement à l'esprit qu'IPSec crypte tout le trafic Internet lié au VPN. Ce chiffrement crée un tunnel crypté entre le réseau d'entreprise et votre ordinateur familial, ce qui sécurise la connexion VPN.



Bien que la connexion VPN en elle-même soit sécurisée, il se peut que *l'ordinateur* que le VPN connecte ne le soit pas. Lorsque vous utilisez le VPN avec votre ordinateur familial, c'est un peu comme si vous connectiez directement votre ordinateur au réseau de l'entreprise. S'il contient un virus, vous risquez de le transmettre à tous les ordinateurs du réseau. Par conséquent, vous devez prendre les mêmes précautions de sécurité que vous utilisiez un ordinateur de l'entreprise ou que vous vous connectiez au réseau avec votre ordinateur personnel par l'intermédiaire d'un VPN. Vous devez donc vous assurer que l'ordinateur a, au minimum, une protection antivirus et que les mises à jour de sécurité sont actives et actualisées.

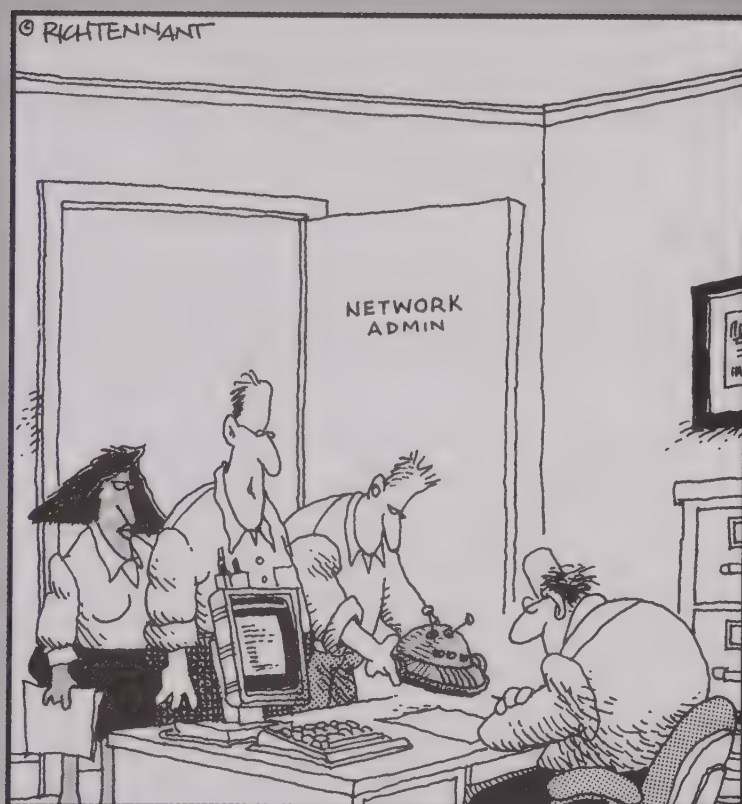
Dans la plupart des réseaux, le VPN est implémenté sur le routeur pare-feu qui connecte le réseau à Internet. Si vous prévoyez de proposer à vos utilisateurs l'accès au réseau par l'intermédiaire d'un VPN, assurez-vous que le routeur destiné à la connexion à Internet possède un support de VPN intégré.

La partie VPN du réseau est prise en charge par le routeur pare-feu et la partie VPN des ordinateurs distants est réalisée par un logiciel qui doit être installé sur ces ordinateurs. Vous devrez donc fournir une copie de ce logiciel client à chaque utilisateur qui souhaite utiliser le VPN, avec le mode d'emploi détaillé sur la façon de l'installer et de le configurer.

Une fois que l'utilisateur distant sera connecté au réseau par le VPN, il pourra accéder aux ressources partagées du réseau. Par exemple, il pourra mapper des disques réseau, accéder aux dossiers partagés, utiliser les imprimantes réseau et accéder à sa messagerie avec Outlook.

Quatrième partie

Guide de l'administration réseau pour les Nuls



« On a trouvé d'où venait la faille de sécurité dans le réseau.
Ça venait d'un autre robot aspirateur bizarroïde.
C'est le troisième ce mois-ci. Il a dû se tirer
de chez son propriétaire, comme tout le reste. »

Dans cette partie...

Vous allez découvrir qu'utiliser un réseau demande plus de travail qu'installer le matériel et le logiciel. Une fois le réseau mis en place, vous devez faire en sorte qu'il soit toujours opérationnel. C'est ce qui s'appelle l'*administration réseau*.

Les chapitres de cette partie vous montrent comment organiser la sécurité de votre réseau, en améliorer les performances et le protéger d'un désastre. Vous trouverez aussi quelques informations techniques. Eh oui, la vie de l'administrateur n'est pas toujours un long fleuve tranquille !

Chapitre 16

Bienvenue dans l'univers de l'administration réseau

Dans ce chapitre :

- Découvrir toutes les tâches de l'administrateur réseau.
- Documenter le réseau.
- Dépoussiérer, passer l'aspirateur et éponger.
- Administrer les utilisateurs du réseau.
- Choisir les bons outils.
- Étoffer sa bibliothèque.
- Obtenir les certifications.

À l'aide ! Recherchons administrateur réseau pour aider petite entreprise à reprendre le contrôle d'un réseau déchaîné. Solide sens de l'organisation et grandes qualités d'administration nécessaires. Petite expérience en informatique souhaitée. Travail à temps partiel.

Cela ressemble-t-il à une petite annonce que devrait publier votre employeur ? Tout réseau a besoin d'un administrateur, qu'il comprenne deux ou deux mille ordinateurs. Bien entendu, administrer un réseau de deux mille machines est un travail à temps plein, pas comme avec un réseau de deux machines, du moins théoriquement !

Ce chapitre vous présente le travail ennuyeux d'administrateur réseau. Oups... Vous êtes sûrement en train de lire ce chapitre parce que vous venez d'être nommé administrateur réseau alors, en d'autres termes :

Ce chapitre vous plonge dans l'univers merveilleux et passionnant de l'administration réseau ! Ça va être génial !

Tâches de l'administrateur réseau

Un administrateur réseau « administre le réseau » : il est chargé d'installer, de configurer, de développer, de protéger, de mettre à jour, d'améliorer et de réparer le réseau.

L'administrateur réseau s'occupe du matériel (câbles, concentrateurs, commutateurs, routeurs, serveurs et clients...) ainsi que des logiciels de réseau (systèmes d'exploitation, serveurs de messagerie, logiciels de sauvegarde, serveurs de bases de données et logiciels d'application). Plus important, il est en contact avec les utilisateurs du réseau, prêt à répondre à leurs questions, à écouter leurs problèmes et à proposer des solutions.

Sur un réseau de grande taille, ces responsabilités occupent un ingénieur à plein temps. Les grands réseaux sont évolutifs : les utilisateurs vont et viennent, les équipements tombent parfois en panne, des câbles se rompent. Bref, la vie sur le réseau n'est qu'une succession d'états de crise.

Un petit réseau est plus stable ; après l'avoir mis en place, il n'y a plus grand-chose à faire au niveau du matériel et des logiciels. Un incident peut occasionnellement se produire mais le nombre d'ordinateurs étant réduit, les problèmes sont rares.

Quelle que soit la taille du réseau, un administrateur réseau est impliqué dans les décisions et les tâches suivantes :

- ✓ **Il prend part aux décisions concernant l'achat d'ordinateurs, d'imprimantes et d'autres équipements.**
- ✓ **Il doit prendre note de toute modification faite au réseau, notamment la connexion de nouveaux ordinateurs.** Son travail consiste à savoir comment il faut modifier le câblage, quels noms il faut assigner aux nouveaux ordinateurs, comment intégrer les informations concernant le nouvel utilisateur dans le système de sécurité, quels droits lui seront attribués, etc.
- ✓ **Lorsqu'une nouvelle version de son système d'exploitation est disponible, l'administrateur réseau doit s'informer, décortiquer ses caractéristiques et déterminer si les améliorations apportées méritent une mise à jour.** Dans la plupart des cas, la tâche la plus ardue consiste à définir une *voie d'évolution*, c'est-à-dire un moyen d'assurer la mise à jour de la totalité du réseau en gênant le moins possible les utilisateurs. La mise à jour d'un système d'exploitation réseau est une véritable corvée. C'est pourquoi il est important d'estimer si elle en vaut la peine.



Entre deux mises à jour, les fournisseurs de logiciels ont la fâcheuse habitude de proposer des correctifs et des *service packs* qui corrigent des problèmes mineurs de leur système d'exploitation de serveurs. Pour en savoir plus, consultez le Chapitre 24.

- ✓ **L'administrateur réseau exécute quelques tâches de routine comme sauvegarder des serveurs, archiver des données anciennes, libérer de l'espace sur le ou les disques durs, etc.** La majeure partie du travail d'un administrateur réseau est de veiller à ce que tout fonctionne bien et aussi de découvrir et résoudre les problèmes avant que quelqu'un remarque un éventuel dysfonctionnement. Vu sous cet angle, le travail d'administrateur est un peu ingrat.
- ✓ **L'administrateur réseau est aussi responsable de la collecte, de l'inventaire et du suivi de la totalité des logiciels du réseau.** Autrement dit, si un problème se produit sur le vieil ordinateur du service marketing qui tourne encore sous Windows 95 et que la solution réside dans la réinstallation de cet ancien exemplaire de Lotus Approach, il faudra qu'il trouve le logiciel. Où diable le CD peut-il bien se trouver ?

Administrateur à temps partiel

Sur les réseaux de grande taille, un support technique de haut niveau est indispensable. Mais si le réseau ne compte qu'une douzaine d'ordinateurs tout au plus, son administration peut être un travail occasionnel. Dans une petite structure, l'administrateur réseau idéal est un passionné d'informatique, quelqu'un qui porte un intérêt secret aux ordinateurs sans vouloir l'admettre, quelqu'un qui emporte quelques bouquins chez lui pour les lire pendant le week-end et quelqu'un qui adore résoudre des problèmes informatiques juste pour le plaisir de les résoudre.



Le travail d'administrateur réseau requiert quelques compétences informatiques mais n'est pas un travail entièrement technique. La grosse partie du travail s'apparente à celui, routinier, d'une ménagère. L'administrateur doit dépoussiérer, passer l'aspirateur et éponger le réseau régulièrement pour éviter qu'il ne devienne un capharnaüm.

Voici quelques ressources à avoir pour être administrateur réseau :

- ✓ **Accorder le temps nécessaire à l'administration réseau.** Une à deux heures par semaine suffisent pour de petits réseaux (moins de vingt ordinateurs). Au début, il faut prévoir un peu plus de temps pour que l'heureux élu s'habitue à ses fonctions et commence à maîtriser les tenants et les aboutissants de l'administration réseau. Mais une fois qu'il sera formé, il ne devrait pas consacrer plus d'une à deux heures par semaine à l'administration réseau (bien entendu, plus le réseau est grand, plus son administration requiert du temps).

- ✓ **Faire connaître sa fonction.** Vous devez faire en sorte que chacun sache qui est l'administrateur réseau et qu'il a le pouvoir de prendre des décisions concernant le réseau, notamment accorder des droits d'accès à chaque utilisateur, déterminer les fichiers qui peuvent et ne peuvent pas être stockés sur le serveur et définir la fréquence des sauvegardes.
- ✓ **L'administrateur réseau a besoin d'une doublure,** quelqu'un qui en sait à peu près autant que lui sur les réseaux, désireux de marquer l'histoire de son empreinte et qui sourit quand on lui demande de résoudre les problèmes les plus délicats.
- ✓ **L'administrateur a une espèce de titre officiel,** comme Grand Maître du Réseau, tsar du Réseau, vice-président en charge des Opérations réseau ou Dr Réseau. Un badge, un capuchon de stylo personnalisé ou une paire d'oreilles de Spock peuvent aider à l'identifier.

Voici quelques suggestions pour sélectionner un administrateur réseau à temps partiel :



- ✓ **L'administrateur réseau doit être organisé.** Faites une inspection surprise de vos locaux et nommez administrateur réseau la personne dont le bureau est le plus propre.
Ne prévenez personne à l'avance ou tout le monde mettra un beau désordre dans son bureau la nuit précédant l'inspection.
- ✓ **L'administrateur réseau doit avoir de l'autorité** et ne pas craindre d'agacer les autres. Un administrateur réseau doit veiller au bon fonctionnement des sauvegardes *avant* la défaillance d'un disque et surveiller que tout le monde se protège correctement des virus *avant* que l'un d'eux ne supprime tout ce qui se trouve sur le réseau.
- ✓ **L'administrateur réseau doit savoir installer les logiciels.** Dans la plupart des cas, la personne qui a installé le réseau en est également l'administrateur. C'est idéal car personne ne comprend mieux un réseau que celui qui l'a conçu puis installé.

Documenter le réseau

L'une des tâches de l'administrateur réseau est de conserver à jour le *journal* du réseau, plus communément appelé *dossier d'exploitation*. Nommez ce carnet *Bible du réseau*. Voici quelques informations que l'on doit y trouver :



- ✓ **Un schéma à jour du réseau.** Il peut s'agir d'un plan d'architecte détaillé, montrant la position de chaque ordinateur, ou quelque chose de plus abstrait, dans le style Picasso. Mettez à jour le schéma à chaque fois que vous modifiez la structure du réseau. Et n'oubliez pas d'effectuer une description détaillée des modifications, la date d'application et la raison pour laquelle elles ont été apportées.

Microsoft propose un logiciel de création, entre autres, de schémas de réseaux. Il s'agit de *Visio* ; je vous le recommande vivement.

- ✓ **Un inventaire complet de votre matériel informatique.** Le Tableau 16.1 montre un exemple de formulaire que vous pouvez utiliser pour suivre votre matériel informatique à la trace.
- ✓ **Une version papier des éléments décrits dans les Informations système** pour chaque ordinateur (Démarrer/Tous les programmes/Accessoires/Outils système/Informations système).
- ✓ **Une liste détaillée des ressources réseau et des lettres de disque employées.** Ne vous contentez pas de lister le nom de chaque partage réseau. Complétez-le d'une courte description de la fonction de chaque partage.
- ✓ **Toute information que vous jugerez utile,** comme la marche à suivre pour configurer un logiciel sur le réseau, des copies de factures liées à l'ordinateur pour le cas où un élément poserait problème et que vous deviez faire fonctionner la garantie.
- ✓ **Le programme des sauvegardes.** Il faut y inclure le planning des sauvegardes des serveurs et des détails sur les rotations de bandes.



notez jamais les mots de passe !

Tableau 16.1 : Fiche signalétique d'un ordinateur.

Emplacement de l'ordinateur :

Utilisateur :

Fabricant :

Numéro de modèle :

Numéro de série :

Date d'achat :

Type de processeur et fréquence :

Mémoire :

 Taille du disque dur :

 Type de carte vidéo :

 Type d'imprimante :

 Autres équipements :

 Version du système d'exploitation :

 Logiciels et versions :

 Type de carte réseau :

 Adresse MAC :



Vous voudrez probablement utiliser un logiciel de base de données ou un tableur pour conserver sur ordinateur les informations rassemblées dans votre carnet. Cependant, assurez-vous toujours que vous disposez d'une version *imprimée*.

Si votre réseau est de grande taille, il peut être intéressant d'investir dans un logiciel d'exploration du réseau comme NetworkView (www.networkview.com) qui collecte automatiquement les informations concernant le réseau. Il analyse soigneusement le réseau à la recherche de nouveaux ordinateurs, imprimantes, routeurs et autres périphériques, en les ajoutant à une base de données. Puis il trace un joli diagramme et génère des rapports très utiles.

Réaliser les tâches de routine

La plus grande partie du travail de l'administrateur réseau est un travail de routine, comme passer l'aspirateur, dépoussiérer et éponger. Ou alors, si vous préférez, faire régulièrement les vidanges et changer les pneus quand ils sont usés.

Ces tâches sont ennuyeuses mais nécessaires :

- ✓ **L'administrateur réseau doit créer les sauvegardes.** Si un problème survient alors que les données ne sont pas sauvegardées, devinez qui sera tenu pour responsable ? D'un autre côté, s'il se produit un désastre mais que vous êtes capable de récupérer les données à partir de la sauvegarde de la veille sans trop de pertes, devinez qui sera félicité, qui recevra une prime juteuse ou gagnera un séjour aux Bahamas ? Le Chapitre 22 décrit les options de sauvegarde du réseau. Vous feriez bien de le lire rapidement.

- ✓ **L'administrateur doit s'occuper de la sécurité.** Il doit aussi protéger le réseau des menaces extérieures, qu'il s'agisse de pirates informatiques ou de virus qui tentent de s'infiltrer par la messagerie. Le Chapitre 23 décrit tout ça en détail.
- ✓ **L'administrateur doit nettoyer le serveur.** Les utilisateurs prennent le serveur pour un grenier. Ils y entreposent leurs fichiers et les oublient. L'administrateur réseau a pour mission de faire régulièrement le ménage dans le grenier. Quelle joie ! Le meilleur conseil que je puisse vous donner est de vous plaindre constamment du désordre qui règne sur le serveur et d'avertir vos utilisateurs que le nettoyage de printemps est imminent.

Administrer les utilisateurs du réseau

La gestion du matériel est la partie la plus facile de l'administration réseau. L'informatique peut sembler déroutante au premier abord mais les ordinateurs ne sont pas aussi incompréhensibles que les êtres humains. Le vrai défi de l'administrateur réseau est d'administrer les utilisateurs du réseau.

La différence entre la gestion du matériel et celle des utilisateurs est évidente : vous pouvez comprendre les ordinateurs mais pour ce qui est des êtres humains, c'est beaucoup plus dur. Ceux qui utilisent le réseau ont des comportements bien moins prévisibles que le réseau proprement dit. Voici quelques conseils pour administrer les utilisateurs :

- ✓ **La formation est une part essentielle du travail de l'administrateur réseau.** Vérifiez que tous ceux qui accèdent au réseau le connaissent et savent s'en servir. S'ils ne comprennent pas le réseau, ils peuvent involontairement faire un tas de choses étranges.
- ✓ **Ne prenez jamais vos utilisateurs pour des idiots.** Ce n'est pas de leur faute s'ils ne comprennent pas ce qu'est un réseau. Expliquez-leur. Donnez-leur un cours. Achetez-leur un exemplaire de ce livre et dites-leur de lire les six premiers chapitres. Prenez-les par la main mais ne les considérez pas comme des idiots.
- ✓ **Rédigez, sur une seule page, un document** qui contient toutes les informations que doit connaître un utilisateur. Distribuez-en un exemplaire à chacun.
- ✓ **Soyez aussi réactif que possible** quand un utilisateur se plaint d'un problème réseau. Si vous n'intervenez pas rapidement, l'utilisateur peut tenter de résoudre le problème lui-même. Cette solution est à éviter.



Plus vous comprendrez la psychologie des utilisateurs de votre réseau, mieux vous serez préparé pour corriger leurs erreurs et répondre à leurs besoins.

Choisir les bons outils logiciels

Les administrateurs réseau exigent d'avoir certains outils pour leur travail. Les administrateurs de grands réseaux complexes et coûteux ont besoin de gros outils complexes et coûteux. Les administrateurs de petits réseaux ont besoin de petits outils.

Quelques-uns de ces outils sont des outils de bricolage tels que des tournevis, des pinces à sertir et des marteaux. Mais les outils dont je veux parler sont les logiciels. Ils ont déjà été mentionnés dans ce chapitre : Visio (pour concevoir des diagrammes de réseau) est un logiciel d'exploration du réseau. En voici quelques autres :

- ✓ **Les commandes TCP/IP intégrées.** Une bonne partie des outils logiciels est livrée avec le réseau. En tant qu'administrateur réseau, vous devez lire les manuels livrés avec vos logiciels réseau pour prendre connaissance des outils disponibles. Par exemple, Windows dispose d'une commande `net diag` qui sert à vérifier que tous les utilisateurs d'un réseau peuvent communiquer entre eux (vous pouvez exécuter `net diag` à partir de l'invite MS-DOS). Pour les réseaux TCP/IP, vous pouvez utiliser les commandes de diagnostic TCP/IP résumées dans le Tableau 16.2.

Tableau 16.2 : Commandes de diagnostic TCP/IP.

Commande	Fonction
arp	Affiche les informations de résolution d'adresse utilisées par le protocole Address Resolution Protocol (ARP).
hostname	Affiche le nom d'hôte de l'ordinateur.
ipconfig	Affiche les paramètres TCP/IP courants.
nbstat	Affiche l'état de NetBIOS sur les connexions TCP/IP.
netstat	Affiche les statistiques de TCP/IP.
nslookup	Affiche l'information de DNS.

Commande	Fonction
ping	Vérifie si un ordinateur est accessible.
route	Affiche la table de routage d'un PC.
tracert	Affiche le chemin entre l'ordinateur et un hôte spécifique.

✓ **Le programme Informations système**, livré avec Windows, est nécessaire aux administrateurs réseau.

✓ **Hotfix Checker** est un outil gratuit très pratique proposé par Microsoft. Il scanne votre ordinateur et détermine les correctifs à appliquer. Pour télécharger gratuitement Hotfix Checker, rendez-vous sur le site www.microsoft.com puis recherchez **hfnetchk.exe**.

✓ **Baseline Security Analyzer**. Si vous préférez les outils avec une interface utilisateur, essayez Baseline Security Analyser, un autre outil gratuit proposé par Microsoft. Allez sur le site www.microsoft.com et faites une recherche sur **Baseline Security Analyzer**.

✓ **Un utilitaire tiers**. Je vous suggère d'acquérir l'un de ces logiciels 100 en 1 comme Norton Utilities de Symantec. Norton Utilities comprend des utilitaires indispensables pour réparer les disques endommagés, réaménager votre disque, rassembler des informations sur votre ordinateur et le matériel qu'il utilise.

N'ayez jamais recours à un utilitaire de réparation de disque ou du registre non adapté à votre version du système d'exploitation. Dès que vous installez une nouvelle version de votre système d'exploitation, veillez également à mettre à niveau vos utilitaires de réparation de disque afin qu'ils la prennent en charge.

✓ **Un analyseur de protocole**. Il s'agit d'un programme (parfois appelé *renifleur de paquets*) qui surveille et garde une trace écrite de chacun des paquets qui circulent sur le réseau. Il peut être configuré pour suivre certains types de paquets et détecter certains problèmes particuliers. Il fournit aussi des statistiques sur les paquets qu'il a capturés.

Pour la plupart des administrateurs, *Sniffer* est le meilleur outil d'analyse de protocoles (www.netscout.com). C'est hélas aussi le plus cher. Si vous préférez une solution gratuite, essayez *Ethereal*, téléchargeable sur le site www.ethereal.com.

✓ **Network Monitor**, un outil livré avec Windows 2000 et XP mais aussi avec Windows 2000 Server et Windows Server 2003. Il permet une analyse de protocole de base, souvent capable de résoudre les satanés problèmes de réseau.



Documentation technique à portée de main

L'un des grands moments de la série télévisée *Star Trek* est cette séquence où Scotty refuse de descendre à terre pour ne pas abandonner ses journaux techniques. « Tu ne te reposes jamais ?, lui demande Kirk – Mais je me repose ! », répond Scotty.

Un administrateur réseau digne de ce nom lit des ouvrages informatiques. Beaucoup d'ouvrages. Et il aime ça. Si vous êtes du genre à les emporter jusque dans votre lit ou à les lire sur la plage, vous êtes un bon administrateur réseau.

Votre bibliothèque technique doit recouvrir divers sujets. Je ne vais pas vous recommander tel ou tel titre mais plutôt vous inciter à acquérir des ouvrages approfondis sur les thèmes suivants :

- ✓ Matériel et câblage des réseaux.
- ✓ Ethernet.
- ✓ Windows Server 2003.
- ✓ Windows Server 2008.
- ✓ Windows XP Pro.
- ✓ Windows Vista.
- ✓ Windows 7.
- ✓ Exchange.
- ✓ Linux.
- ✓ TCP/IP.
- ✓ DNS et BIND.
- ✓ SendMail.
- ✓ Exchange Server.
- ✓ Sécurité informatique et piratage.
- ✓ Réseaux sans fil.

En plus de ces ouvrages, abonnez-vous à des magazines techniques pour vous tenir informé des dernières évolutions (et révolutions) techniques. Voici quelques adresses Web intéressantes :

- ✓ Le site de la presse micro : www.pressemicro.net.
- ✓ *01 Informatique* : www.01net.com.
- ✓ *IT-expert* : www.it-expertise.com.

- ✓ *Le Monde informatique* : www.lemondeinformatique.fr.
- ✓ *PC expert* : www.pcexpert.fr.
- ✓ *Réseaux & Télécoms* : www.reseaux-telecoms.net.



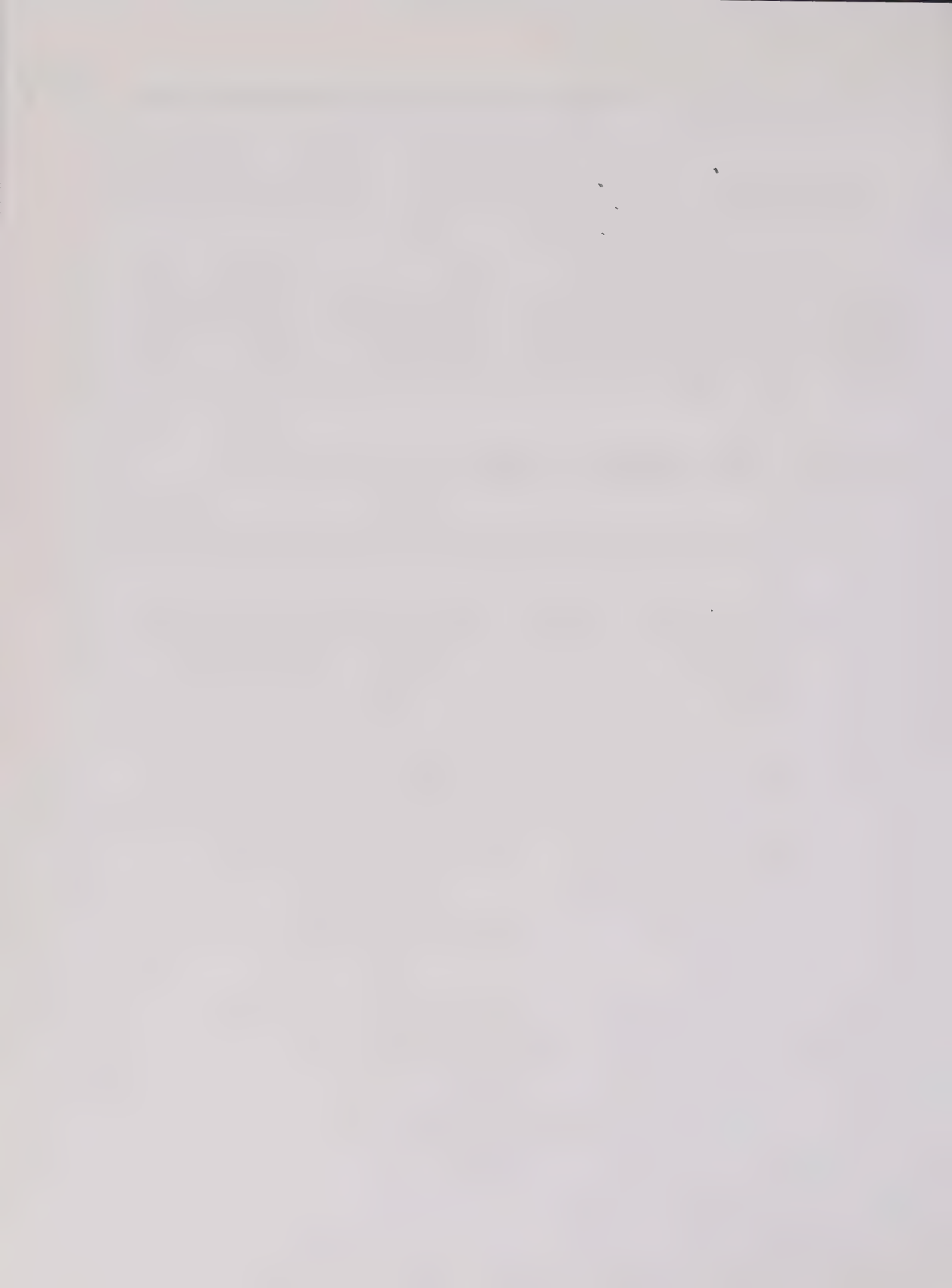
Internet est l'une des meilleures sources d'informations techniques pour les administrateurs réseau. N'hésitez pas à accumuler les favoris ou les signets dans votre navigateur. Beaucoup de sites proposent de s'abonner à leur lettre d'information, ce que je vous recommande vivement. Vous serez ainsi tenu au courant presque en temps réel.

Obtenir les certifications

À mon avis, une certification ne garantit en rien que vous serez capable d'administrer un réseau. Cette compétence naît de l'expérience, pas d'un savoir livresque et d'examens.

Néanmoins, dans un monde du travail régi par la compétitivité, la certification a pris une grande importance. Vous serez donc tenté d'être certifié, non seulement pour améliorer votre savoir-faire mais aussi pour étoffer votre CV. Pour un particulier, une certification est coûteuse, de l'ordre de plusieurs centaines d'euros par examen. De plus, selon votre niveau, vous devrez acheter des livres et prendre des cours supplémentaires.

Il existe deux types de certifications : celles proposées par un éditeur de logiciels ou un fabricant de matériel et celles qui sont indépendantes. Les grands éditeurs et fabricants comme Microsoft, Novell et Cisco proposent des certifications pour leurs propres produits. Aux États-Unis, une organisation à but non lucratif comme CompTIA propose les meilleures certifications indépendantes.



Chapitre 17

Gérer des comptes utilisateurs sous Windows

Dans ce chapitre :

- ▶ Comprendre les comptes utilisateurs.
- ▶ Créer des comptes utilisateurs.
- ▶ Configurer des comptes utilisateurs.
- ▶ Réinitialiser des mots de passe.
- ▶ Activer et désactiver des comptes.
- ▶ Supprimer des utilisateurs.
- ▶ Travailler avec des groupes.
- ▶ Créer un script d'ouverture de session.

Chaque utilisateur qui accède au réseau doit avoir un *compte utilisateur*. Les comptes utilisateurs vous permettent de contrôler l'accès au réseau, de l'autoriser ou de le refuser. Ils vous servent aussi à spécifier les ressources du réseau que chaque utilisateur peut utiliser. Sans comptes utilisateurs, les ressources seraient mises à la disposition de quiconque pénétrerait par hasard dans le réseau.

Comprendre les comptes utilisateurs sous Windows

Les comptes utilisateurs sont l'un des outils de base de la gestion d'un serveur sous Windows. En tant qu'administrateur réseau, vous leur consacrerez une grande partie de votre temps : création de nouveaux comptes utilisateurs, suppression des comptes expirés, réinitialisation des mots de passe des utilisateurs distraits, attribution de nouveaux droits d'accès et ainsi de suite. Mais, avant d'aborder les procédures spécifiques à la création et à la gestion des comptes utilisateurs, voyons d'abord de quoi il s'agit et comment ils fonctionnent.

Comptes locaux et comptes de domaine

Un *compte local* est un compte utilisateur stocké sur un ordinateur et qui ne s'applique qu'à cet ordinateur. Classiquement, chaque ordinateur du réseau a un compte local pour chaque personne qui l'utilise.

En revanche, un *compte de domaine* est un compte utilisateur stocké par Active Directory qui est accessible depuis n'importe quel ordinateur qui fait partie du domaine. La gestion des comptes de domaine est centralisée. Ce chapitre est principalement consacré à la configuration et à la maintenance des comptes de domaine.

Propriétés des comptes utilisateurs

Chaque compte utilisateur est doté d'un nombre important de *propriétés de compte* qui spécifient ses caractéristiques. Les trois propriétés de compte les plus importantes sont :

- ✓ **Le nom d'utilisateur.** C'est un nom unique qui identifie le compte. L'utilisateur doit l'entrer lorsqu'il se connecte au réseau. Le nom d'utilisateur est une information publique. Autrement dit, tous les utilisateurs du réseau peuvent (et devraient) connaître votre nom d'utilisateur.
- ✓ **Le mot de passe.** C'est un mot confidentiel qui doit être entré pour accéder au compte. Windows peut être configuré de sorte à imposer des *conventions de mots de passe* comme le nombre minimum de caractères, l'obligation d'utiliser des lettres et des chiffres et sa durée de validité.
- ✓ **Appartenance à un groupe.** Indique le ou les groupes auxquels l'utilisateur appartient. L'appartenance à un groupe est primordiale pour assurer les droits d'accès qui permettent à un utilisateur d'accéder à différentes ressources du réseau comme des imprimantes ou des fichiers partagés ou d'exécuter certaines tâches réseau telles que la création de nouveaux comptes ou la sauvegarde du serveur.

Bien d'autres propriétés de compte enregistrent des données concernant un utilisateur comme les renseignements de contact de l'utilisateur, la possibilité pour lui d'accéder au réseau à certaines heures et à partir de certains ordinateurs, etc. Je décris certaines de ces fonctions dans les prochaines sections de ce chapitre.

Créer un nouvel utilisateur

Procédez comme suit pour créer un nouveau compte utilisateur de domaine sous Windows Server 2008 :

1. Choisissez Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory.

Cette action ouvre la console d'administration Utilisateurs et ordinateurs Active Directory, illustrée par la Figure 17.1

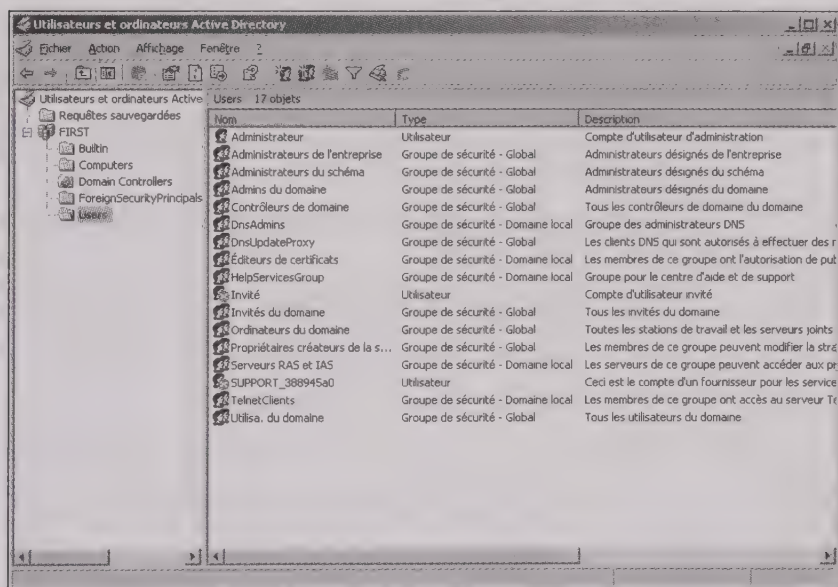


Figure 17.1 : Console d'administration Utilisateurs et ordinateurs Active Directory.

2. Effectuez un clic droit sur le domaine auquel vous désirez ajouter l'utilisateur et sélectionnez Nouveau/Utilisateur.

L'Assistant Nouvel objet - Utilisateur, représenté dans la Figure 17.2, démarre.

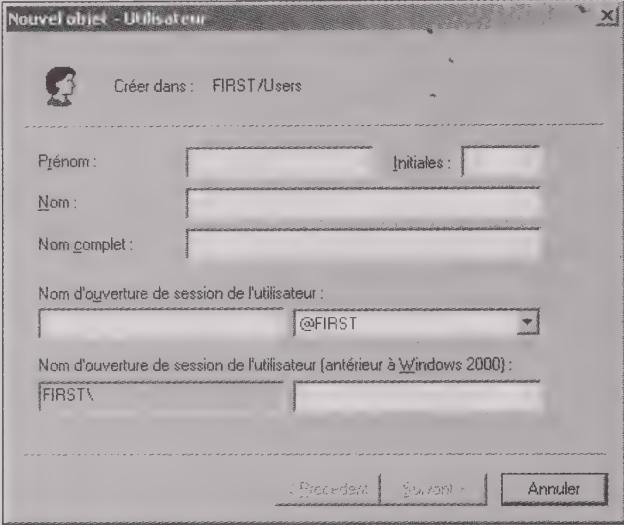


Figure 17.2 : Création d'un nouvel utilisateur.

3. Saisissez le nom, les initiales et le prénom de l'utilisateur.

Au cours de la saisie, l'assistant remplit automatiquement le champ Nom complet.

4. Modifiez le champ Nom complet, si ce qui y figure ne vous convient pas.

Vous pouvez, par exemple, permuter le nom et le prénom.

5. Entrez le nom d'ouverture de session de l'utilisateur.

Ce nom doit être unique dans le domaine.

Définissez une convention de création identique pour tous les noms d'ouverture de session : par exemple, la première lettre du prénom suivie du nom ou le nom suivi d'un point puis du prénom, ou toute autre règle à votre convenance.



6. Cliquez sur Suivant.

La deuxième page de l'assistant Nouvel objet - Utilisateur apparaît, comme le montre la Figure 17.3.

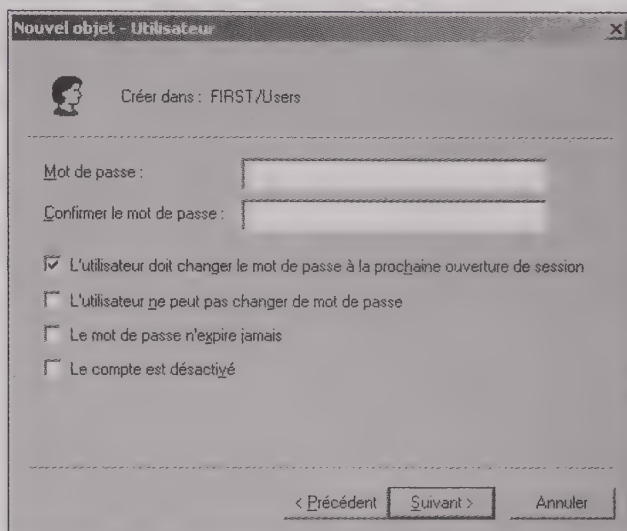


Figure 17.3 : Définition du mot de passe de l'utilisateur.

7. Saisissez le mot de passe deux fois.

Si les deux mots de passe ne sont pas identiques, cela signifie que l'un d'eux est erroné. Vous devrez alors corriger l'erreur.

8. Spécifiez les options de mot de passe à appliquer.

Les options disponibles sont :

- L'utilisateur doit changer de mot de passe à la prochaine ouverture de session.
- L'utilisateur ne peut pas changer de mot de passe.
- Le mot de passe n'expire jamais.
- Le compte est désactivé.

Pour en savoir plus sur ces options, reportez-vous à la section « Configurer les options de compte », plus loin dans ce chapitre.

9. Cliquez sur Suivant.

La dernière page de l'assistant s'ouvre. Elle est illustrée par la Figure 17.4.

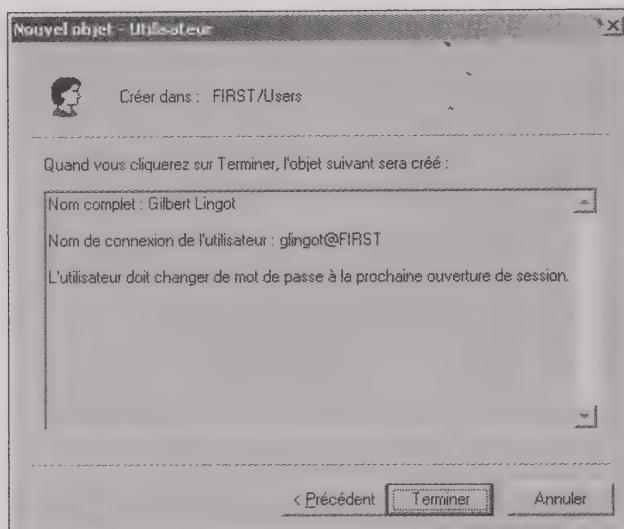


Figure 17.4 : Vérification des informations du compte utilisateur.

10. Vérifiez l'exactitude des informations puis cliquez sur Terminer pour créer le compte.

Si une information n'est pas correcte, cliquez sur le bouton Précédent et corrigez l'erreur.

C'est fait ! À présent vous pouvez personnaliser les paramètres du compte utilisateur. Vous pouvez l'ajouter à un ou plusieurs groupes, compléter les renseignements de contact ou définir d'autres options de compte.

Configurer les propriétés utilisateur

Après avoir créé un compte utilisateur, vous pouvez configurer ses propriétés. Pour ce faire, effectuez un clic droit sur le compte et sélectionnez Propriétés. Cette action affiche la boîte de dialogue Propriétés d'utilisateur qui compte de nombreux onglets que vous ouvrez pour définir différentes propriétés. La Figure 17.5 représente l'onglet Général qui contient les informations concernant l'utilisateur comme son nom, l'emplacement de son bureau, son numéro de téléphone, etc.

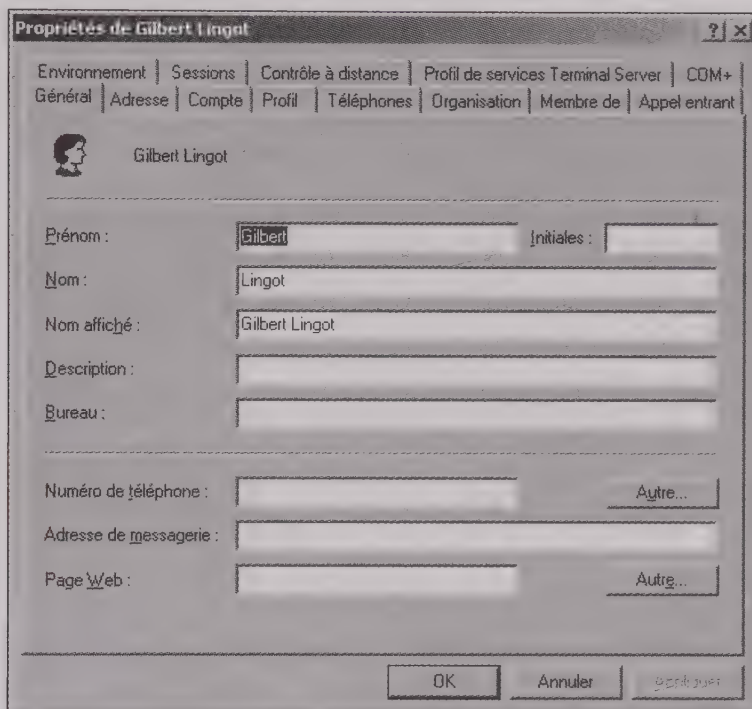


Figure 17.5 : Onglet Général.

Les sections qui suivent décrivent certaines des tâches d'administration qui peuvent être effectuées à partir de la boîte de dialogue Propriétés d'utilisateur.

Modifier les renseignements de contact de l'utilisateur

Plusieurs onglets de la boîte de dialogue Propriétés d'utilisateur contiennent des informations concernant l'utilisateur, notamment :

- ✓ **Adresse** : vous pouvez y modifier l'adresse de l'utilisateur (rue, boîte postale, ville, code postal...).
- ✓ **Téléphones** : vous y spécifiez les divers numéros de téléphone de l'utilisateur.
- ✓ **Organisation** : vous y indiquez la fonction de l'utilisateur, le nom de son gestionnaire, etc.

Configurer les options de compte

L'onglet Compte de la boîte de dialogue Propriétés d'utilisateur (Figure 17.6) comporte diverses options intéressantes. C'est là qu'il est possible de modifier le nom d'ouverture de session et les options de mot de passe définies lors de la création du compte.

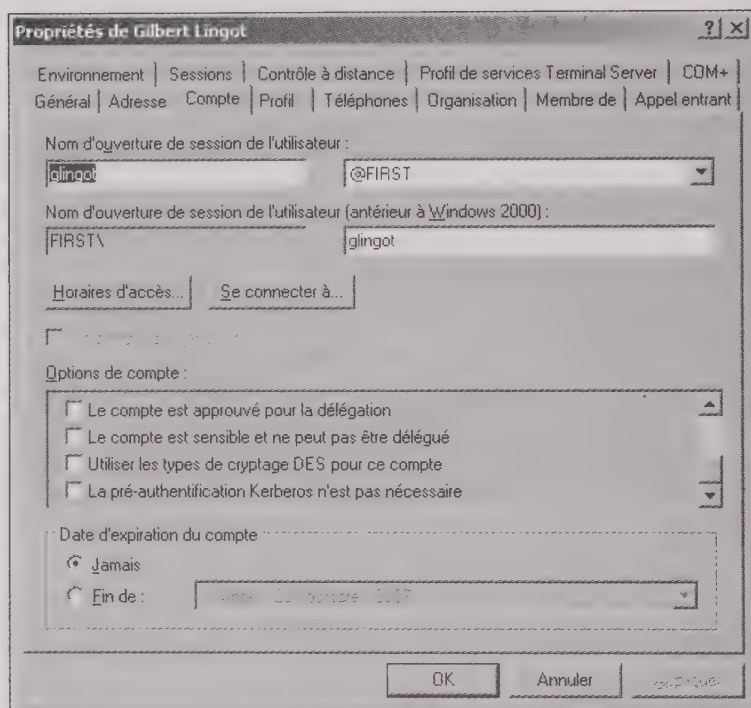


Figure 17.6 : Onglet Compte de la boîte de dialogue Propriétés d'utilisateur.

La zone Options de compte permet de spécifier les options suivantes :

- ✓ **L'utilisateur devra changer le mot de passe.** Cette option, qui est activée par défaut, impose à l'utilisateur de modifier son mot de passe à la prochaine ouverture de session. Elle permet d'attribuer à l'utilisateur un mot de passe temporaire. Ainsi, dès que l'utilisateur se connecte au réseau, il est invité à changer de mot de passe.
- ✓ **L'utilisateur ne peut pas changer de mot de passe.** Cette option interdit à l'utilisateur de changer son mot de passe (cette option n'est pas compatible avec la précédente).
- ✓ **Le mot de passe n'expire jamais.** Cette option annule la stratégie de sécurité imposée par Active Directory. Elle permet à l'utilisateur de ne jamais changer de mot de passe.

- ✓ **Enregistrer le mot de passe en utilisant un chiffrement réversible.** Cette option enregistre les mots de passe en utilisant un chiffrement que les pirates peuvent casser facilement. Évitez de cocher cette option.
- ✓ **Le compte est désactivé.** Cette option permet de préparer un compte pour une mise à disposition ultérieure. Tant que le compte est désactivé, l'utilisateur ne peut pas ouvrir de session. Consultez la section « Activer et désactiver des comptes utilisateurs », plus loin dans ce chapitre, pour plus d'informations.
- ✓ **Une carte à puce est nécessaire pour ouvrir une session interactive.** Cette option implique que l'ordinateur de l'utilisateur possède un lecteur de carte à puce.
- ✓ **Le compte est approuvé pour la délégation.** Cette option indique que le compte est digne de confiance et peut établir des délégations. Cette option est habituellement réservée au compte administrateur.
- ✓ **Le compte est sensible et ne peut pas être délégué.** Aucun utilisateur ne peut s'approprier ce compte.
- ✓ **Utiliser les types de chiffrement DES via Kerberos pour ce compte.** Cette option renforce le chiffrement pour les applications qui exigent plus de sécurité.
- ✓ **La pré-authentification Kerberos n'est pas nécessaire.** Choisissez cette option si vous utilisez une implémentation différente du protocole Kerberos.

Définir le profil utilisateur

L'onglet Profil, représenté dans la Figure 17.7, permet de configurer les paramètres de profil de l'utilisateur :

- ✓ **Chemin du profil.** Spécifie l'emplacement du profil « itinérant » de l'utilisateur. Comme les profils itinérants ne sont pas souvent utilisés, j'ai décidé de ne pas les traiter dans ce livre.
- ✓ **Script d'ouverture de session.** Définit le script de connexion : c'est un fichier de commandes qui est exécuté à chaque fois que l'utilisateur ouvre une session. Le but principal du script d'ouverture de session est de connecter automatiquement les ressources réseau dont l'utilisateur a besoin. Les scripts d'ouverture de session sont un souvenir des versions antérieures de Windows NT Server. Sous Windows Server 2008, le chargement du profil est la méthode adoptée pour configurer l'ordinateur de l'utilisateur lorsqu'il ouvre une session et qu'il doit retrouver ses ressources réseau. Cependant, de nombreux administrateurs lui préfèrent encore la simplicité des scripts d'ouverture de session. Pour plus d'informations, voir la section « Créer un script d'ouverture de session », plus loin dans ce chapitre.

- ✓ **Dossier de base.** Indique l'emplacement de stockage par défaut pour l'utilisateur.

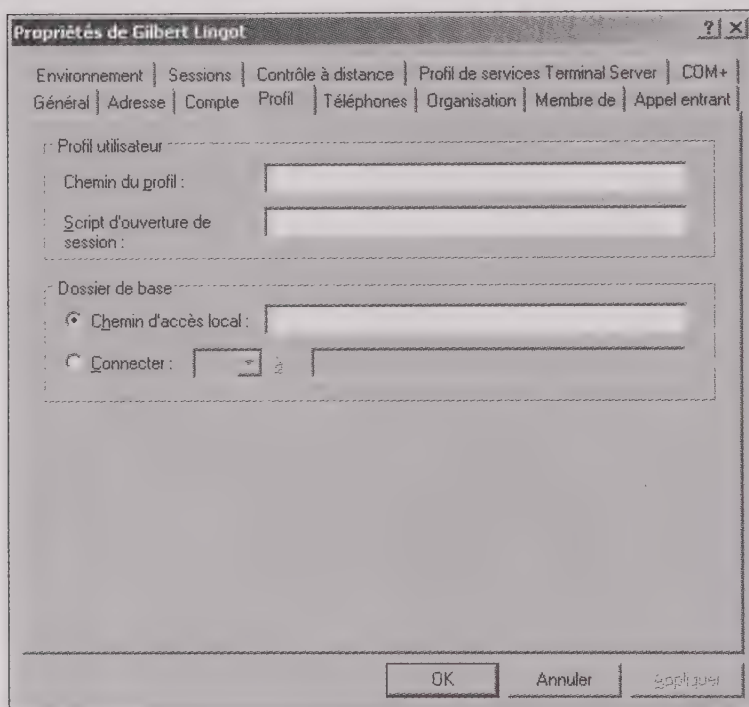


Figure 17.7 : Onglet Profil d'utilisateur.

Réinitialiser des mots de passe d'utilisateurs

D'après quelques estimations, il semblerait que la tâche d'administration qui prend le plus de temps soit la réinitialisation des mots de passe. Il est un peu facile de s'en prendre à un utilisateur lorsqu'il oublie son mot de passe mais mettez-vous à sa place : vous insistez pour qu'il choisisse un mot de passe incompréhensible, comme 94kD821eL384K, qu'il est censé changer, une semaine plus tard, par un mot tout aussi biscornu que dJUQ63DWd8131 et que bien sûr il ne doit laisser traîner nulle part ni même noter. Il y a vraiment de quoi devenir fou.

Ainsi, lorsqu'un utilisateur vous informe qu'il a oublié son mot de passe, la moindre des choses consiste à le réinitialiser. Car après tout, il a certainement déjà perdu un bon quart d'heure à tenter de retrouver ce mot de passe avant d'admettre son échec.

Voici la procédure à suivre pour réinitialiser le mot de passe d'un compte utilisateur du domaine :

1. Ouvrez une session en tant qu'administrateur.

Vous devez posséder des droits d'administrateur.

2. Choisissez Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory.

La console d'administration Utilisateurs et ordinateurs Active Directory s'affiche.

3. Dans le volet de gauche, cliquez sur Users.

4. Dans le panneau de droite, effectuez un clic droit sur l'utilisateur qui a oublié son mot de passe et sélectionnez Réinitialiser le mot de passe.

5. Saisissez le nouveau mot de passe dans les deux champs.

Vous devez l'entrer *deux fois* pour minimiser les risques de faute de frappe.

6. Si vous le souhaitez, vous pouvez activer l'option L'utilisateur doit changer de mot de page à la prochaine ouverture de session.

Si vous cochez cette case, le mot de passe que vous attribuez ne sera valable que pour une seule session. Dès que l'utilisateur tentera de se connecter, il devra changer de mot de passe

7. Cliquez sur OK.

C'est tout. Le mot de passe de l'utilisateur a été réinitialisé.

Activer et désactiver des comptes utilisateurs

Si vous souhaitez interdire temporairement l'accès au réseau à un utilisateur, vous pouvez désactiver son compte. Vous pourrez ensuite, quand vous le désirerez, le réactiver et lui redonner ainsi l'accès aux ressources du réseau. Voici comment procéder :

1. Ouvrez une session en tant qu'administrateur.

Vous devez posséder des droits d'administrateur.

2. Choisissez Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory.

La console d'administration Utilisateurs et ordinateurs Active Directory s'affiche.

3. Dans le volet de gauche, cliquez sur Users.
4. Dans le panneau de droite, effectuez un clic droit sur l'utilisateur dont vous voulez désactiver ou activer le compte et exécutez la commande Désactiver le compte ou Activer le compte.

Supprimer un utilisateur

La suppression d'un utilisateur ne présente aucune difficulté :

1. Ouvrez une session en tant qu'administrateur.

Vous devez posséder des droits d'administrateur.



2. Choisissez Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory.

La console d'administration Utilisateurs et ordinateurs Active Directory s'affiche.

3. Dans le volet de gauche, cliquez sur Users.
4. Dans le panneau de droite, effectuez un clic droit sur l'utilisateur à supprimer et choisissez Supprimer.

Windows vous demande de confirmer la suppression.

5. Cliquez sur Oui.

Le compte de l'utilisateur a été supprimé.

Travailler avec des groupes

Un *groupe* est un compte spécial qui représente un ensemble d'utilisateurs dont les besoins d'accès au réseau sont identiques. Les groupes peuvent simplifier considérablement les tâches d'attribution des droits d'accès. Plutôt que de les affecter séparément à chacun des utilisateurs, ces droits sont attribués à tout le groupe. Par la suite, ces droits sont automatiquement accordés à tout nouvel utilisateur que vous ajoutez au groupe.

Les sections suivantes décrivent certains des concepts-clés que vous devez comprendre pour utiliser des groupes ainsi que les démarches les plus courantes pour configurer des groupes pour votre serveur.

Créer un groupe

Pour créer un groupe, procédez de la manière suivante :

1. Ouvrez une session en tant qu'administrateur.

Vous devez posséder des droits d'administrateur.

2. Choisissez Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory.

La console d'administration Utilisateurs et ordinateurs Active Directory s'affiche.

3. Effectuez un clic droit sur le domaine auquel vous voulez ajouter un groupe et sélectionnez Nouveau/Groupe.

La boîte de dialogue Nouvel objet - Groupe apparaît, comme le montre la Figure 17.8.

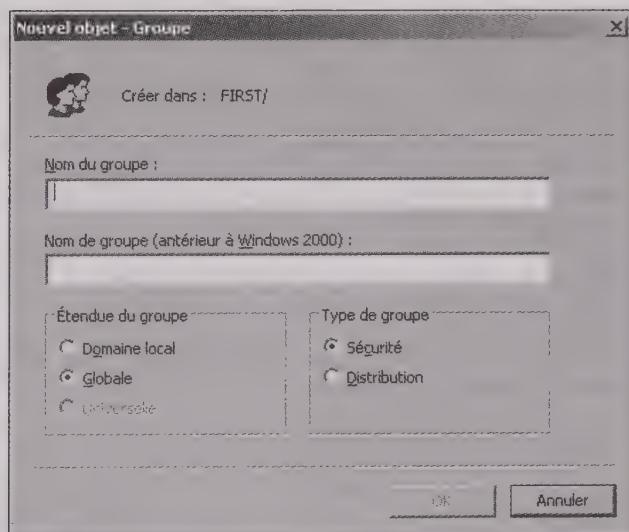


Figure 17.8 : Boîte de dialogue Nouvel objet - Groupe.

4. Entrez le nom du nouveau groupe.

Saisissez le nom dans les deux champs.

5. Choisissez l'étendue du groupe.

Les possibilités sont les suivantes : Domaine local, Globale et Universelle. Optez pour Domaine local pour les groupes qui vont posséder des droits d'accès aux ressources du réseau. Sélectionnez Globale pour les groupes auxquels vous allez ajouter des utilisateurs et des groupes de domaine local. Choisissez Universelle si vous administrez un réseau étendu avec plusieurs domaines.

6. Indiquez le type de groupe.

Les choix possibles sont Sécurité et Distribution. Dans la plupart des cas, vous choisirez Sécurité.

7. Cliquez sur OK.

Le groupe est créé.

Ajouter un membre au groupe

Les groupes sont des ensembles d'objets appelés *membres*. Les membres d'un groupe peuvent être des comptes utilisateurs ou d'autres groupes. Quand un groupe vient d'être créé, il n'a pas de membre. Un groupe ne devient utile que s'il compte au moins un membre.

Procédez comme suit pour ajouter un membre :

1. Ouvrez une session en tant qu'administrateur.

Vous devez posséder des droits d'administrateur.

2. Choisissez Démarrer/Outils d'administration/Utilisateurs et ordinateurs Active Directory.

La console d'administration Utilisateurs et ordinateurs Active Directory s'affiche.

3. Ouvrez le dossier contenant le groupe auquel vous désirez ajouter des membres. Double-cliquez ensuite sur le groupe.

La boîte de dialogue Propriétés de groupe apparaît.

4. Cliquez sur l'onglet Membres.

Les membres du groupe apparaissent.

5. Cliquez sur le bouton Ajouter et entrez le nom d'un utilisateur ou d'un autre groupe que vous désirez ajouter à ce groupe. Cliquez ensuite sur OK.

6. Répétez l'étape 5 pour chaque utilisateur ou groupe que vous voulez ajouter.

Continuez jusqu'à ce que vous ayez ajouté tout le monde !

7. Cliquez sur OK.

Ce n'est pas plus difficile que ça !



La boîte de dialogue Propriétés de groupe comporte un onglet Membre de qui liste chaque groupe dont le groupe courant est membre.

Créer un script d'ouverture de session

Un *script d'ouverture de session* est un fichier de traitement par lots qui est automatiquement démarré à chaque fois qu'un utilisateur ouvre une session sur le réseau. Un script d'ouverture de session s'utilise principalement pour mapper les partages réseau auxquels l'utilisateur veut accéder. Voici un exemple simple de script d'ouverture de session qui mappe trois partages réseau :

```
echo off
net use m: \\serveur1\partages\admin
net use n: \\serveur1\partages\marketing
net use o: \\serveur2\archives
```

Ici, deux partages de serveur1 sont mappés aux lecteurs M et N et un partage de serveur2 est mappé au lecteur O.



Les scripts d'ouverture de session sont sauvegardés au plus profond des entrailles du répertoire Windows, dans le dossier SYSVOL, à l'adresse c:\Windows\SYSVOL\Sysvol\nom_de_domaine\Scripts, où le nom_de_domaine est le nom de votre domaine. Si vous devez accéder souvent à ce dossier, créez un raccourci sur le Bureau.

Après avoir créé le script d'ouverture de session, vous pouvez l'assigner à un utilisateur en le spécifiant dans l'onglet Profil de la boîte de dialogue Propriétés d'utilisateur. Pour plus d'informations, consultez l'une des sections précédentes, intitulée « Définir le profil utilisateur ».

Chapitre 18

Gérer le stockage réseau

Dans ce chapitre :

- Comprendre le stockage réseau.
- Configurer des autorisations.
- Partager des dossiers.
- Configurer et administrer un serveur de fichiers.

L'accès partagé à l'espace disque est l'un des buts principaux des ordinateurs en réseau. Dans ce chapitre, vous découvrirez les diverses possibilités qu'un réseau peut offrir pour partager de l'espace disque. Vous apprendrez aussi à configurer Windows Server 2008 comme serveur de fichiers.

Comprendre le stockage réseau

De très nombreux serveurs réseau n'ont pour rôle essentiel que la mise à disposition d'espace disque pour les utilisateurs du réseau. Parce que les réseaux accueillent de plus en plus d'utilisateurs et que ces derniers ont besoin de plus en plus d'espace disque, les administrateurs réseau doivent trouver en permanence des moyens d'augmenter la capacité mémoire de leur réseau. Les sections suivantes présentent quelques concepts-clés pour fournir de l'espace disque sur le réseau.

Serveur de fichiers

Un *serveur de fichiers* est simplement un serveur appartenant au réseau et dont le rôle primaire est la mise à disposition de ses disques. C'est le moyen

le plus couramment utilisé pour partager des zones de stockage sur le réseau.

Un serveur de fichiers peut aussi bien être un simple ordinateur de bureau auquel on a attribué ce service qu'un serveur de fichiers dédié (dont le coût peut dépasser 25 000 euros) équipé de composants redondants, de sorte qu'il n'y ait pas d'interruption de service si un élément tombe en panne. Un serveur de fichiers peut même être équipé de baies de stockage dont les disques peuvent être remplacés en ligne sans arrêt du système.

Un des sous-systèmes de stockage disque les plus communs pour les serveurs de fichiers est le système RAID (RAID était à l'origine l'acronyme de *Redundant Array of Inexpensive Disks*, qui signifie « matrice redondante de disques bon marché ». Aujourd'hui, le mot est devenu l'acronyme de *Redundant Array of Independent Disks*, soit « matrice redondante de disques indépendants » car les disques durs sont de bien meilleure qualité qu'à l'époque). Les techniques utilisées s'assurent que si l'un des disques du système de RAID est détruit, aucune donnée n'est perdue. Le disque défectueux peut être retiré et remplacé dans la baie sans qu'un arrêt soit nécessaire et le nouveau disque est reconstruit avec les données que contenait le disque endommagé à partir d'informations stockées sur les autres disques.



La majeure partie de ce chapitre est consacrée à la configuration de Windows Server 2008 comme serveur de fichiers.

Périphérique de stockage

Un *périphérique de stockage* est un dispositif spécifiquement conçu pour fournir une zone de stockage sur le réseau. Également connu sous le nom de NAS, acronyme de *Network Attached Storage*, il désigne un périphérique de stockage relié à un réseau dont la principale fonction est le stockage de données en un gros volume centralisé pour des clients réseau. C'est une boîte « noire » préconfigurée et prête à fonctionner. Il suffit de la connecter, de la mettre sous tension et de la configurer.

Le Dell PowerVault NF500 est un NAS d'entrée de gamme typique. C'est un petit châssis pouvant être inséré dans un rack. Il supporte jusqu'à six disques durs d'une capacité totale pouvant atteindre six téraoctets (soit 6 000 Go). Le NF500 possède une carte mère biprocesseur qui peut supporter jusqu'à 8 Go de mémoire et quatre ports réseau Gigabit.

Le Dell NF500 tourne avec une version spéciale de Windows Server appelée *Windows Storage Server*. Cette version de Windows, conçue spécifiquement pour les périphériques NAS, permet de configurer la zone de stockage réseau à partir de n'importe quel ordinateur du réseau en utilisant un navigateur Web.

Notez que certains périphériques de stockage utilisent des versions personnalisées de Linux plutôt que Windows Storage Server. D'autres périphériques intègrent directement le système d'exploitation sur un disque dur externe qui peut être connecté au réseau et partagé pour les utilisateurs.

Comprendre les autorisations

Les *autorisations* sont un concept-clé de l'administration du stockage réseau. Elles permettent aux utilisateurs d'accéder aux ressources partagées du réseau. Le simple partage d'une ressource, comme l'accès à un dossier ou à une imprimante, ne garantit en rien que l'utilisateur peut y accéder. Windows demande qu'une décision soit prise pour chaque ressource. Elle repose sur des autorisations affectées aux différents groupes et à l'état de membre d'un groupe en ce qui concerne un utilisateur. Si l'utilisateur appartient à un groupe auquel des autorisations d'accès aux ressources ont été accordées, l'accès est autorisé. Sinon, il est refusé.

En théorie, tout paraît simple mais en pratique, cela peut s'avérer assez compliqué. Les paragraphes qui suivent décrivent les nuances entre le contrôle des accès et les autorisations :

- ✓ Chaque objet (c'est-à-dire chaque fichier et dossier) d'un volume NTFS bénéficie d'un ensemble d'autorisations appelé ACL (*Access Control List*, liste de contrôle d'accès).
- ✓ L'ACL identifie les utilisateurs et les groupes qui peuvent accéder à l'objet et spécifie le niveau d'accès dont bénéficie l'utilisateur ou le groupe. Par exemple, l'ACL d'un dossier spécifiera qu'un groupe d'utilisateurs peut uniquement lire les fichiers contenus dans le dossier, qu'un autre groupe peut les lire et les modifier, alors qu'un troisième groupe se verra refuser tout accès au dossier.
- ✓ Les objets conteneurs (les fichiers et les volumes) permettent à leurs ACL d'être hérités par les objets qui les contiennent. Ainsi, si vous accordez des autorisations à un dossier, ces dernières s'étendent aux fichiers et sous-dossiers qu'il contient.
- ✓ Le Tableau 18.1 décrit les six types d'autorisation qui peuvent être appliqués aux fichiers et dossiers sur un volume NTFS.

Tableau 18.1 : Autorisations applicables aux fichiers et aux dossiers.

Autorisation	Description
Contrôle total	Accorde l'accès sans restriction au fichier ou au dossier.

Autorisation	Description
Modification	Permet de lire le fichier ou le dossier, de le supprimer, d'en modifier le contenu ou d'en changer les attributs. Il est aussi possible de créer de nouveaux fichiers ou sous-dossiers dans le dossier.
Lecture et exécution	Permet de lire ou d'exécuter le fichier, d'afficher le contenu du dossier ou de lire ou exécuter les fichiers du dossier.
Affichage du contenu du dossier	S'applique uniquement aux dossiers et accorde le droit d'en visualiser le contenu.
Écriture	Permet de modifier le contenu du fichier ou de ses attributs et de créer de nouveaux fichiers ou sous-dossiers dans le dossier.
Lecture	Accorde l'autorisation de lire le fichier ou le contenu du dossier.



- ✓ Les six autorisations applicables aux fichiers et aux dossiers sont constituées d'autres *autorisations spéciales* qui définissent des permissions plus détaillées sur les fichiers et les dossiers. Le Tableau 18.2 présente ces autorisations spéciales qui s'appliquent à chacune des six autorisations applicables aux fichiers et aux dossiers.
- ✓ Il est préférable d'accorder des autorisations à des groupes plutôt qu'à chacun des utilisateurs. Par la suite, si un utilisateur a besoin d'accéder à une ressource particulière, il suffira de l'ajouter à un groupe qui a l'autorisation d'utiliser cette ressource.

Tableau 18.2 : Autorisations spéciales.

Autorisation spéciale	Contrôle total	Modification	Lecture et exécution	Affichage du contenu du dossier	Lecture	Écriture
Traverser dossier/Exécuter fichier	x	x	x	x		
Énumérer dossier/Lire les données	x	x	x	x	x	
Lire les attributs	x	x	x	x	x	

<i>Autorisation spéciale</i>	<i>Contrôle total</i>	<i>Modification</i>	<i>Lecture et exécution</i>	<i>Affichage du contenu du dossier</i>	<i>Lecture</i>	<i>Écriture</i>
Lire les attributs étendus	x	x	x	x	x	
Créer des fichiers/Écrire des données	x	x				x
Créer des dossiers/Ajouter des données	x	x				x
Écrire des attributs	x	x				x
Écrire des attributs étendus	x	x				x
Supprimer les sous-dossiers et les fichiers	x					
Supprimer	x	x				
Lire les autorisations	x	x	x	x	x	x
Modifier les autorisations		x				
Prendre possession	x					
Synchroniser	x	x	x	x	x	x

Comprendre les partages

Un *partage* est un dossier mis à la disposition de multiples utilisateurs à travers le réseau. Chaque partage se caractérise par les éléments suivants :

- ✓ **Le nom de partage** : Nom sous lequel le partage est connu sur le réseau. Pour qu'il soit compatible avec les ordinateurs anciens, il est recommandé de s'en tenir, si possible, au nom à huit caractères.
- ✓ **Le chemin** : Chemin du dossier, sur l'ordinateur local partagé, par exemple : C:\Compta.
- ✓ **La description** : Description en ligne du partage.
- ✓ **Les autorisations** : Liste d'utilisateurs ou de groupes auxquels l'accès au partage a été accordé.

Lorsque vous installez Windows et configurez les rôles du serveur, des ressources partagées particulières sont créées pour supporter ces rôles. Ne modifiez surtout pas les partages spéciaux, à moins que vous sachiez vraiment ce que vous faites. Le Tableau 18.3 présente les partages spéciaux les plus importants.

Tableau 18.3 : Partages spéciaux les plus importants.

Nom de partage	Description
drive\$	Le répertoire racine d'un disque.
ADMIN\$	Utilisé pour l'administration distante d'un ordinateur. Il pointe sur le dossier du système d'exploitation (habituellement, C: \ Windows).
IPC\$	Employé par des canaux nommés, c'est un élément de programmation qui permet aux processus de communiquer entre eux.
NETLOGON	Requis pour le fonctionnement des contrôleurs de domaine.
SYSVOL	Un partage des contrôleurs de domaine.
PRINT\$	Utilisé pour l'administration distante des imprimantes.
FAX\$	Utilisé par les clients de fax.



Quelques noms de partages spéciaux se terminent par le symbole dollar (\$) ; ce sont des *partages cachés*, invisibles pour les utilisateurs. Cependant, vous pouvez y accéder en spécifiant le nom complet du partage (avec le symbole dollar). Par exemple, le partage C\$ est créé pour permettre une connexion au répertoire racine du disque C: d'un client réseau. Les partages tels que C\$ sont protégés par des privilèges, de sorte que si un utilisateur découvre que C\$ est le répertoire racine du disque C: du serveur, il ne pourra pas y accéder.

Configurer le rôle de serveur de fichiers

Pour utiliser Windows Server 2003 ou 2008 comme serveur de fichiers, vous devez d'abord activer le rôle de serveur de fichiers. Sous Windows Server 2003, sélectionnez Démarrer/Outils d'administration/Gérer votre serveur pour ouvrir la console Gérer votre serveur. Cliquez ensuite sur Ajouter ou supprimer un rôle et sélectionnez le rôle Serveur de fichiers. Sous Windows Server 2008, sélectionnez Démarrer/Outils d'administration/Gestionnaire de serveur puis cliquez sur Rôles et activez le rôle Services de fichiers.

Administrer le serveur de fichiers

Windows Server 2008 possède une nouvelle console d'administration très pratique appelée Gestion du partage et du stockage (Figure 18.1). Cette console permet de créer de nouveaux partages, de définir des autorisations pour un partage, de supprimer un partage, etc. Pour ouvrir la console, sélectionnez Démarrer/Outils d'administration/Gestion du partage et du stockage.

Les sections suivantes décrivent quelques procédures courantes que vous serez amené à utiliser pour administrer votre serveur de fichiers.

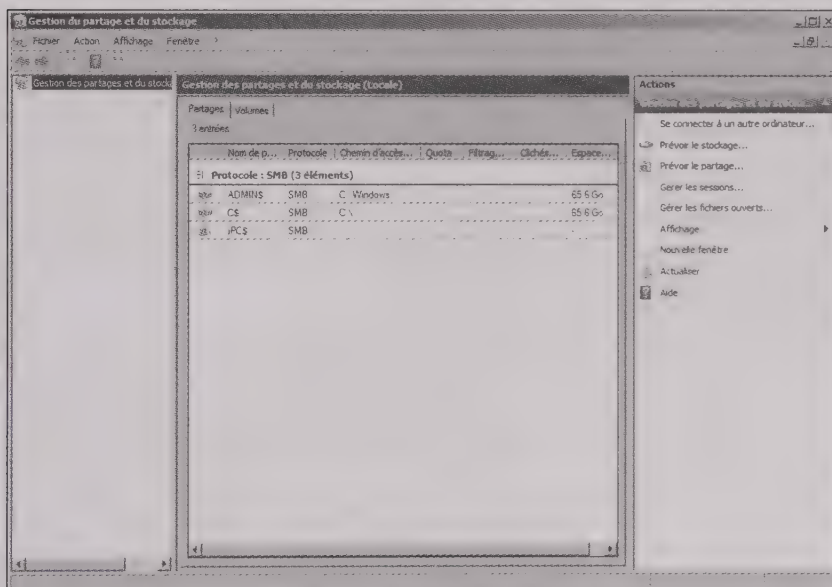


Figure 18.1 : Console Gestion du partage et du stockage.

Utiliser l'Assistant Configuration d'un dossier partagé

Pour être vraiment utile, un serveur de fichiers doit offrir plusieurs *dossiers partagés* configurés pour être accessibles de n'importe où sur le réseau. Il est possible, à partir d'un serveur de fichiers, de consulter la liste des partages actuellement disponibles en ouvrant le Gestionnaire de serveur et en cliquant sur Rôles/Services de fichiers/Gestion des partages et du stockage dans l'arborescence. La console Gestion des partages et du stockage affiche le nom de partage, la description et le chemin d'accès de chaque partage déjà créé.

Pour créer d'autres partages, utilisez l'Assistant Configuration d'un dossier partagé et suivez les étapes ci-dessous.

1. Dans la console Gestion des partages et du stockage, cliquez sur **Prévoir le partage**.

La page d'accueil de l'Assistant Configuration d'un dossier partagé s'ouvre, comme le montre la Figure 18.2. Dans un premier temps, l'assistant vous demande de préciser le dossier que vous voulez partager.

Assistant Configuration d'un dossier partagé

Emplacement du dossier partagé

Étapes :

- Emplacement du dossier partagé
- Autorisations NTFS
- Protocoles du partage
- Revoir les paramètres et créer le partage
- Confirmation

Spécifiez le dossier à partager. Sur un volume avec des caractéristiques et une quantité d'espace appropriées, sélectionnez un dossier existant ou créez-en un nouveau. S'il n'existe aucun volume approprié, cliquez sur **Prévoir le stockage** et créez-en un.

Emplacement : Parcourir...

Volumes disponibles :

Volume	Capacité	Espace libre	Type
Réservé au sy...	100 Mo	71,9 Mo	Simple
⌈)	74,4 Go	65,6 Go	Simple

Détails

Volume : Réservé au système

Clichsés instantanés : Inconnu

Indexation : Inconnu

Serveur à haut niveau de disponibilité : Le volume n'est pas mis en cluster

Prévoir le stockage...

Précédent Suivant Annuler

Figure 18.2 : L'assistant Configuration d'un dossier partagé vous demande de spécifier le dossier que vous voulez partager.

2. Entrez l'emplacement du dossier que vous voulez partager sur le réseau et cliquez sur **Suivant**.

Si vous n'êtes pas sûr de l'emplacement, cliquez sur le bouton **Parcourir**. Cette action ouvre une boîte de dialogue qui vous permet d'examiner le disque dur du serveur à la recherche du dossier à partager. Vous pouvez aussi créer un nouveau dossier à partir de cette boîte de dialogue, si le dossier que vous voulez partager n'existe pas encore. Après avoir sélectionné ou créé le dossier à partager, cliquez sur **OK** pour retourner dans l'assistant.

La boîte de dialogue, illustrée par la Figure 18.3, apparaît.

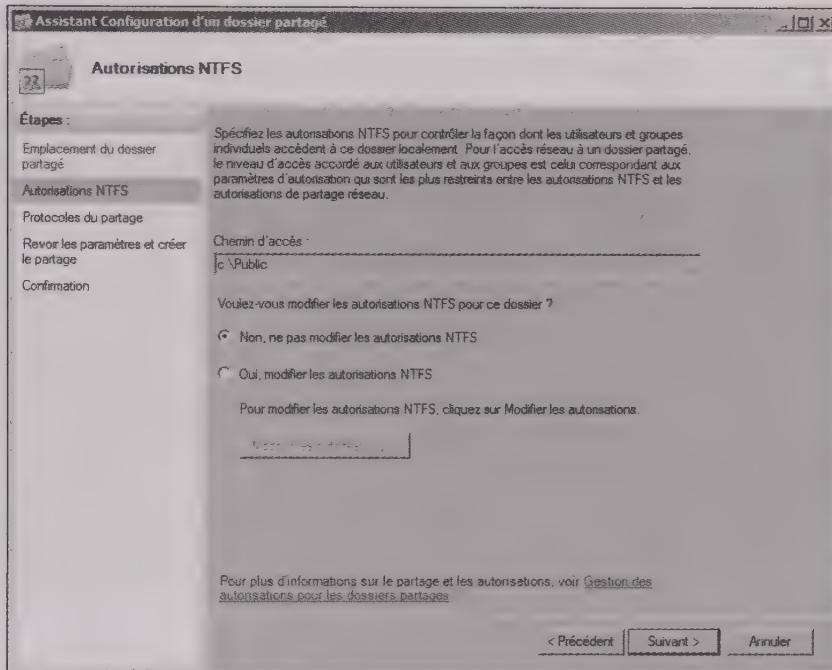


Figure 18.3 : L'assistant vous demande si vous souhaitez modifier les autorisations NTFS.

3. Modifiez les autorisations NTFS si nécessaire puis cliquez sur Suivant.

Les autorisations NTFS sont les autorisations appliquées au dossier que vous partagez et non au partage lui-même. Si vous voulez modifier les autorisations NTFS pour le dossier que vous partagez, activez la case Oui, modifier les autorisations NTFS, cliquez sur le bouton Modifier les autorisations et définissez les autorisations comme bon vous semble. Si vous ne souhaitez pas modifier les autorisations, cliquez sur Suivant pour accéder à la prochaine étape. L'assistant affiche la boîte de dialogue représentée dans la Figure 18.4 qui vous invite à nommer le partage.

4. Tapez le nom à utiliser pour le partage dans le champ Nom du partage.

Le nom par défaut est celui du dossier partagé. S'il est trop long, entrez un nom plus bref.

Windows Server 2008 offre la possibilité de partager des fichiers qui utilisent le protocole NFS. Si vous avez activé le partage NFS sur cette machine, cette boîte de dialogue vous permet aussi de partager des informations pour NFS.



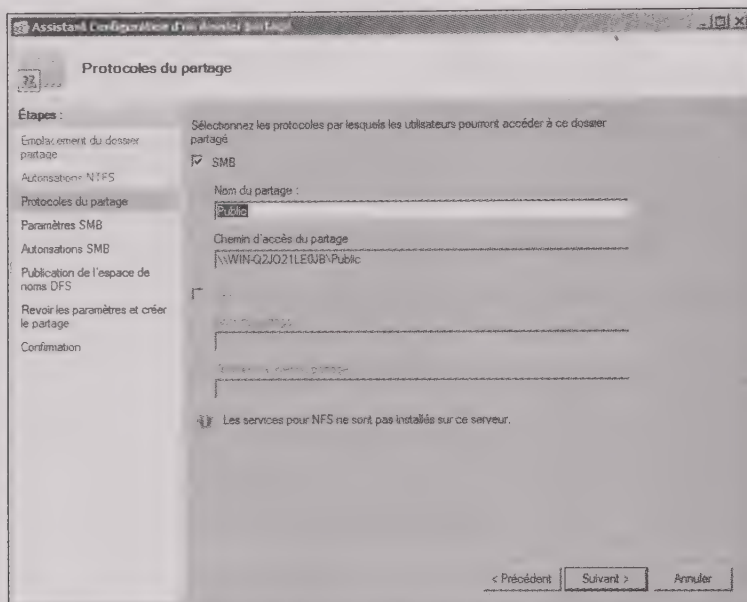


Figure 18.4 : Spécification du nom du partage.

5. Cliquez sur Suivant.

La Figure 18.5 représente la boîte de dialogue qui s'affiche.

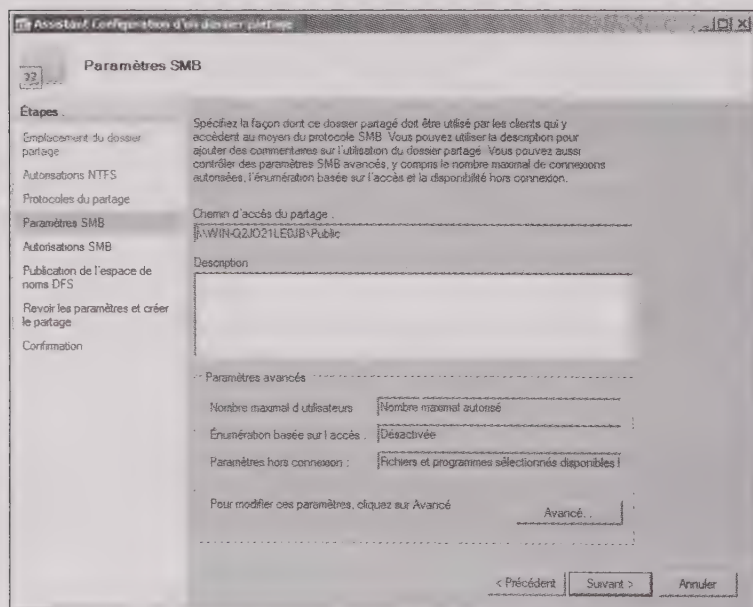


Figure 18.5 : Saisie de la description du partage.

6. Entrez la description du partage et cliquez sur Suivant.

S'ouvre alors la boîte de dialogue illustrée par la Figure 18.6.

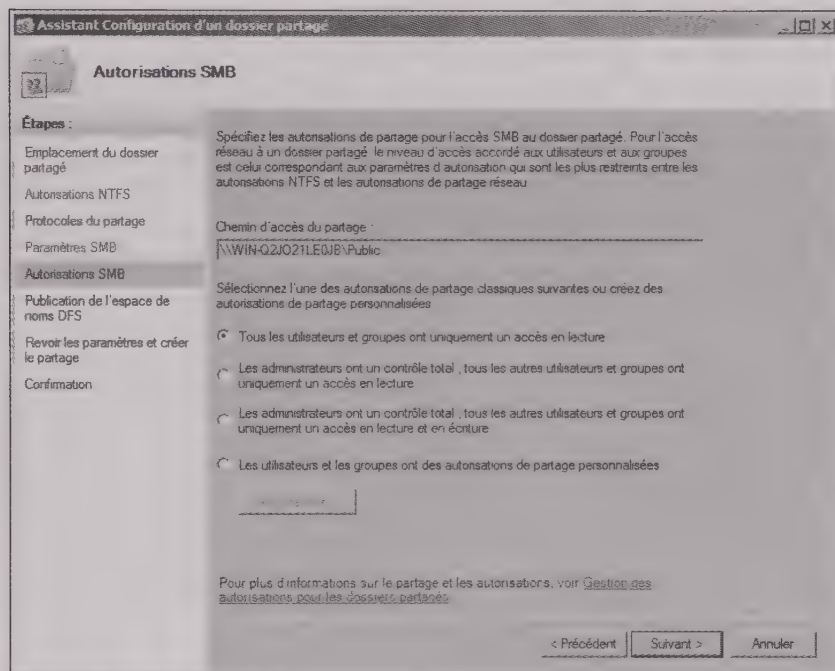


Figure 18.6 : Configuration des autorisations du partage.

7. Sélectionnez les autorisations que vous voulez imposer.

Quatre possibilités s'offrent à vous :

- *Tous les utilisateurs et groupes ont uniquement un accès en lecture.* Utilisez cette option pour partager des informations auxquelles chacun a accès mais que personne ne doit modifier.
- *Les administrateurs ont un contrôle total ; tous les autres utilisateurs et groupes ont uniquement un accès en lecture.*
- *Les administrateurs ont un contrôle total ; tous les autres utilisateurs et groupes ont uniquement un accès en lecture et en écriture.*
- *Les utilisateurs et les groupes ont des autorisations de partage personnalisées.* Si vous activez cette option, vous pouvez cliquer sur le bouton **Autorisations** pour configurer les autorisations personnalisées.

8. Cliquez sur Suivant.

La boîte de dialogue illustrée par la Figure 18.7 s'affiche.

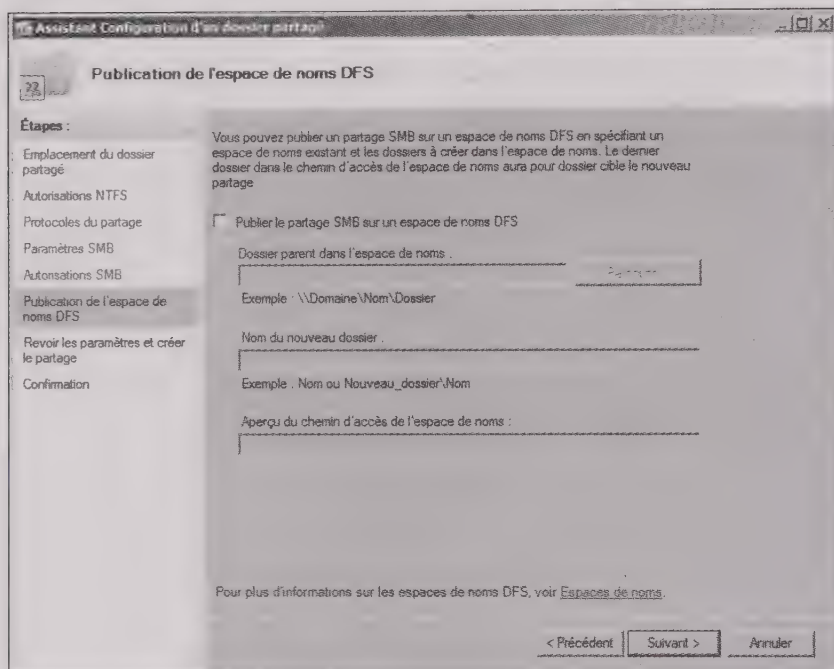


Figure 18.7 : Possibilité de joindre un réseau DFS.

9. Si vous avez défini un espace de noms DFS (Distributed File System) et que vous souhaitez y connecter ce partage, activez la case Publier le partage SMB sur un espace de noms DFS.

DFS est un système qui permet de combiner deux ou plusieurs partages de fichiers sous un seul nom. Il vise à simplifier l'administration des grands réseaux de serveurs de fichiers. Il est donc principalement utilisé sur des réseaux qui possèdent de nombreux serveurs de fichiers.

Si vous n'aviez jamais entendu parler de DFS jusqu'à présent, sautez cette étape.

10. Cliquez sur Suivant.

L'écran affiche la boîte de dialogue représentée dans la Figure 18.8.

11. Vérifiez que tous les paramètres sont corrects et cliquez sur Créer.

Le partage est créé et l'assistant affiche une dernière boîte de dialogue de confirmation, comme le montre la Figure 18.9.

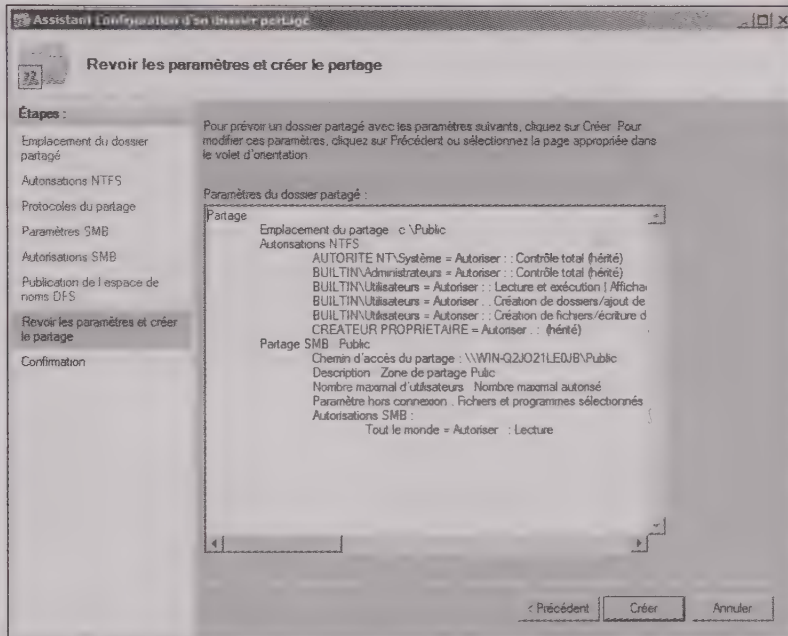


Figure 18.8 : Boîte de dialogue Revoir les paramètres et créer le partage.

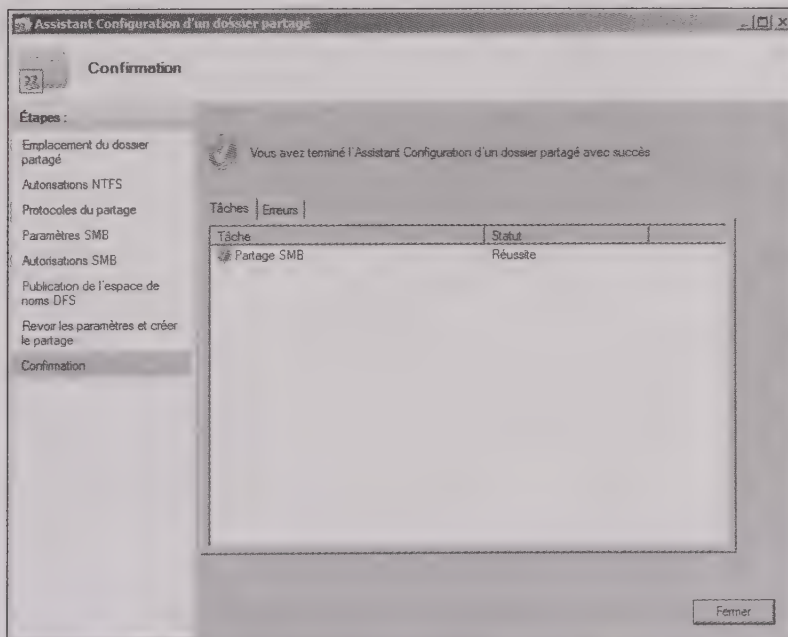


Figure 18.9 : Beau travail !

Partager un dossier sans l'assistant

Si vous pensez que les assistants devraient se contenter de faire de la magie dans *Harry Potter*, vous pouvez configurer un partage sans utiliser l'assistant. Procédez comme suit :

1. Ouvrez l'explorateur Windows et repérez le dossier que vous voulez partager.
2. Effectuez un clic droit sur le dossier et cliquez sur **Propriétés**.

Cette action ouvre la boîte de dialogue Propriétés du dossier.

3. Ouvrez l'onglet **Partage**.

L'onglet Partage s'ouvre, comme le montre la Figure 18.10.

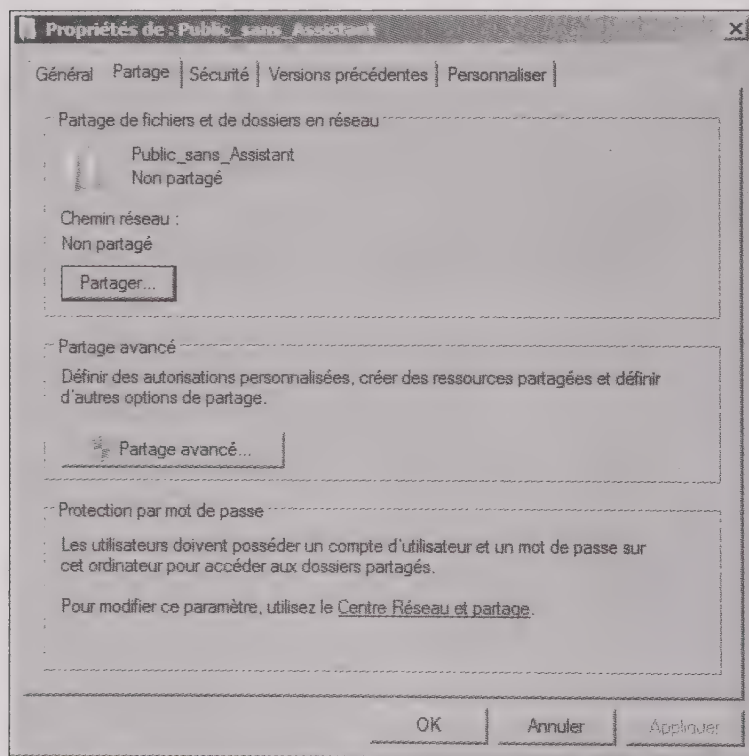


Figure 18.10 : Partage manuel d'un dossier.

4. Cliquez sur le bouton **Partage avancé**.

La Figure 18.11 représente la boîte de dialogue qui s'affiche.

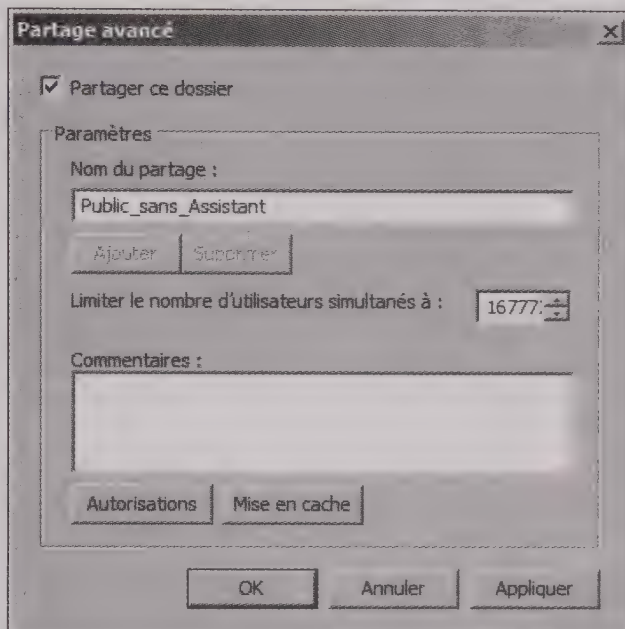


Figure 18.11 : Définition du nom du partage.

5. Cochez la case Partager ce dossier pour que le dossier soit considéré comme partagé.

Les paramètres de cette boîte de dialogue sont grisés tant que vous ne cochez pas cette case.

6. Entrez le nom du partage dans le champ Nom du partage ainsi qu'une description du partage dans la zone Commentaires.

Le nom par défaut est celui du dossier partagé. S'il est trop long, entrez un nom plus bref.

La description est facultative mais elle peut être utile pour indiquer le contenu du dossier aux utilisateurs.

7. Si vous voulez définir les autorisations, cliquez sur le bouton Autorisations.

Cette action ouvre une boîte de dialogue qui vous invite à créer des autorisations pour le partage. Pour plus d'informations, reportez-vous à la section suivante, « Définir des autorisations ».

8. Cliquez sur OK.

Le dossier est partagé.

Définir des autorisations

Quand vous venez de créer un partage de fichiers, les utilisateurs n'y accèdent d'abord qu'en lecture seule. Pour leur permettre de modifier les fichiers ou d'en ajouter de nouveaux, il faut des autorisations supplémentaires. Voici comment procéder à partir de la console Gestion du partage et du stockage :

1. Sélectionnez Démarrer/Outils d'administration/Gestion du partage et du stockage.

La console Gestion du partage et du stockage s'ouvre.

2. Effectuez un clic droit sur le partage pour lequel vous voulez définir des autorisations, cliquez sur Propriétés et ouvrez l'onglet Autorisations.

La boîte de dialogue de la Figure 18.12 apparaît. Elle vous permet de définir des autorisations pour le partage lui-même ou des autorisations NTFS pour le dossier partagé.

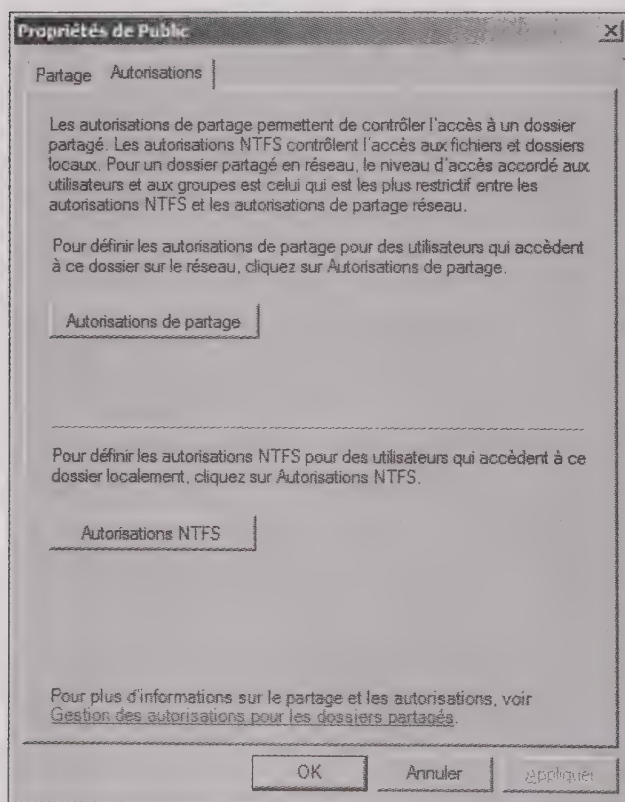


Figure 18.12 : Définition des autorisations.

3. Cliquez sur le bouton Autorisations de partage.

La boîte de dialogue illustrée par la Figure 18.13 s'ouvre. Elle propose une liste de tous les utilisateurs et groupes auxquels vous avez accordé une autorisation pour le dossier. Lorsque vous sélectionnez un utilisateur ou un groupe dans la liste, les cases à cocher au bas de la liste indiquent les autorisations spéciales que vous avez attribuées à chaque utilisateur ou groupe.

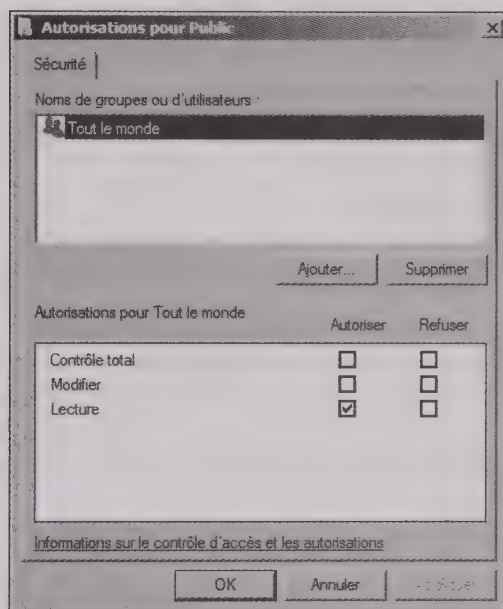


Figure 18.13 : Définition des autorisations de partage.

4. Cliquez sur Ajouter.

S'ouvre alors la boîte de dialogue illustrée par la Figure 18.14.

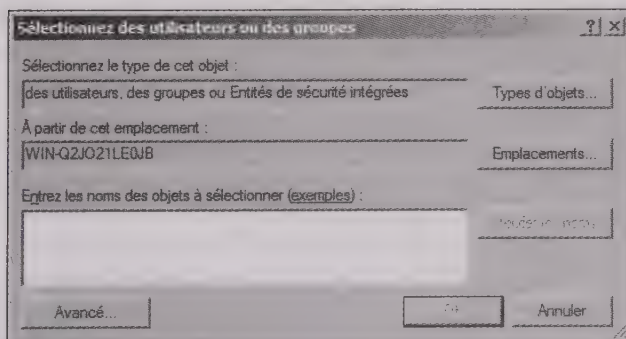


Figure 18.14 : Boîte de dialogue Sélectionnez des utilisateurs ou des groupes.

- 5. Entrez le nom de l'utilisateur ou du groupe auquel vous voulez accorder une autorisation et cliquez sur OK.**

Vous rebasculez dans l'onglet Autorisations de partage dans lequel figure désormais le nouvel utilisateur ou groupe ajouté.



Si vous n'êtes pas sûr du nom, cliquez sur Avancé. S'ouvre alors une boîte de dialogue dans laquelle vous pouvez rechercher les utilisateurs par leur nom.

- 6. Cochez les cases Autoriser ou Refuser pour indiquer les autorisations à attribuer à l'utilisateur ou au groupe.**
- 7. Répétez les étapes 3 à 6 pour toutes les autres autorisations que vous souhaitez ajouter.**
- 8. Pour finir, cliquez sur OK.**



Voici quelques remarques concernant l'ajout d'autorisations :

- ✓ Si vous désirez accorder un accès total à tous pour ce dossier, ne perdez pas de temps à définir des autorisations. Sélectionnez le groupe Tout le monde et cochez la case Autoriser pour chaque type de permission.
- ✓ Pour supprimer une autorisation, sélectionnez-la et cliquez sur Supprimer.
- ✓ Si vous ne souhaitez pas travailler avec la console Gestion du partage et du stockage, vous pouvez définir les autorisations dans Ordinateur. Effectuez un clic droit sur le dossier partagé, sélectionnez Partage et sécurité et cliquez sur Autorisations. Respectez ensuite la procédure décrite précédemment.
- ✓ Les autorisations attribuées dans cette procédure ne s'appliquent qu'au partage lui-même. Les sous-dossiers peuvent eux aussi avoir reçu des autorisations. Si c'est le cas, c'est toujours l'autorisation la plus restrictive qui l'emporte. Par exemple, si dans Autorisations de partage, vous avez opté pour l'autorisation Contrôle total mais que l'autorisation affectée au dossier ne permet que la lecture à l'utilisateur, ce dernier ne bénéficiera que d'une autorisation en lecture seule pour le dossier.



Chapitre 19

Optimiser les performances du réseau

• • • • •

Dans ce chapitre :

- ▶ Comprendre les problèmes de performances.
 - ▶ Rechercher les goulots d'étranglement.
 - ▶ Résoudre les problèmes de performances.
 - ▶ Surveiller les performances.
 - ▶ Accélérer le réseau.
- • • • •

Le terme *performances du réseau* se rapporte à l'efficacité avec laquelle le réseau répond aux besoins de l'utilisateur. Il va sans dire que tout accès à des ressources s'effectuant au travers du réseau sera plus lent que ce même accès n'impliquant pas le réseau. Par exemple, il sera plus long d'ouvrir un document Word situé quelque part sur le réseau que de l'ouvrir depuis le disque dur d'un ordinateur. La différence est *minime*, mais si elle est gênante, c'est à cause d'un problème de performances du réseau.

Ce chapitre est une introduction aux techniques d'amélioration du réseau afin qu'il fonctionne aussi efficacement que possible. Gardez à l'esprit le fait que de nombreux conseils d'optimisation sont dispersés dans ce livre. Dans ce chapitre, vous découvrirez des techniques d'analyse des performances du réseau, avec les actions à entreprendre en cas de problème et la manière de garder une trace de vos améliorations.

Pourquoi les administrateurs ont horreur des problèmes de performances

Les problèmes de performances du réseau sont parmi les plus difficiles à détecter et à résoudre. Si un utilisateur ne parvient pas à se connecter, l'administrateur ne met pas longtemps avant de trouver l'origine du problème : un câble rompu, le dysfonctionnement d'un commutateur ou d'une carte réseau, une autorisation qu'il n'a pas, etc. Après quelques recherches, le problème est rapidement identifié et corrigé et vous pouvez passer au suivant.

Il n'en va malheureusement pas de même avec les problèmes de performances, qui sont plus délicats. Voici quelques raisons pour lesquelles les administrateurs réseau en ont horreur :

- ✓ **Les problèmes de performances sont difficiles à quantifier.** Dans quelle mesure le réseau est-il plus lent qu'une semaine auparavant, un mois auparavant, voire un an auparavant ? Parfois, le réseau donne l'impression d'être lent mais il est impossible de savoir pourquoi.
- ✓ **Les problèmes de performances se développent généralement progressivement.** Il arrive qu'un réseau ralentisse soudain beaucoup. Mais le plus souvent, le ralentissement est progressif, un peu plus chaque jour, jusqu'au moment où l'utilisateur s'en rend compte.
- ✓ **Les problèmes de performances ne sont souvent pas signalés.** Ils alimentent les discussions oiseuses autour de la machine à café mais personne ne vient vous dire que le réseau semble 20 % plus lent que d'habitude. Tant que les utilisateurs parviennent à accéder au réseau, ils pensent que le problème n'est que temporaire ou que c'est subjectif.
- ✓ **Beaucoup de problèmes de performances sont intermittents.** Parfois, un utilisateur se plaint que certaines opérations traînent et, quand vous allez voir sur place ce qu'il en est, la même opération s'exécute instantanément. Il arrive parfois de découvrir un indice : le ralentissement se produit plutôt le matin que l'après-midi ou alors au moment de la sauvegarde ou quand une imprimante fonctionne. Mais parfois, vous ne trouvez rien : parfois ça rame, parfois pas.
- ✓ **La recherche des performances n'est pas une science exacte.** Elle est souvent très empirique, basée sur des suppositions. La segmentation du réseau améliorera-t-elle les performances ? Peut-être... L'augmentation du débit, le passage de 100 Mbps à 1 Gbps supprimera-t-elle les goulets d'étranglement ? Une augmentation de 4 Go pour la mémoire du serveur le fera-t-elle travailler plus vite ? Allez savoir...

- ✓ **La solution à un problème de performances est parfois difficile à faire passer.** Si l'utilisateur ne parvient pas à se connecter au réseau à cause du dysfonctionnement d'un composant, la question ne se pose pas : il faut remplacer l'élément défectueux.

Mais si vous pensez que la seule solution au ralentissement du réseau consiste à répartir la charge de travail sur deux serveurs au lieu d'un, vous aurez du mal à convaincre la direction de la nécessité d'acheter un second serveur.

Qu'est-ce qu'un goulet d'étranglement ?

Le terme *goulet d'étranglement* ne se réfère pas au physique d'un fou d'informatique (même si je pense que ce pourrait parfois être le cas). En fait, l'expression a été utilisée pour la première fois par des mordus d'informatique quand ils ont découvert que la forme de la bouteille de Coca limitait la vitesse à laquelle ils pouvaient absorber le breuvage. « Eh ! dit un jour un fondu d'informatique, l'étroitesse de ce goulet limite la vitesse à laquelle je peux consommer ce breuvage goûteux et caféiné contenu dans cette bouteille. Cela me conduit à faire une analogie évidente avec les effets qu'un seul élément d'un système informatique peut avoir sur les performances du système. »

« Fascinant », répondirent les autres fondus d'informatique qui avaient la chance d'être présents en cet instant historique.

L'expression est restée et permet aujourd'hui d'attirer l'attention sur le simple fait qu'un système informatique n'est jamais plus rapide que le plus lent de ses éléments. C'est l'équivalent informatique d'un vieux truisme qui veut qu'une chaîne ne soit jamais plus solide que le plus faible de ses anneaux.

Pour une simple démonstration de ce concept, voyons ce qui se passe quand vous imprimez un document sur une imprimante très lente. Votre traitement de texte lit les données du disque et les envoie à l'imprimante. Vous vous asseyez et attendez que le document soit imprimé.

Le document ne s'imprimerait-il pas plus vite si vous achetiez un processeur plus rapide ou ajoutiez de la mémoire ? Non. Le processeur est déjà plus rapide que l'imprimante et votre ordinateur dispose déjà de plus de mémoire qu'il n'en faut pour imprimer le document. L'imprimante est le goulet d'étranglement. Le seul moyen d'imprimer le document plus vite est donc de remplacer votre imprimante par une autre plus rapide ou d'augmenter sa mémoire.

Voici quelques autres notions sur les goulets d'étranglement :

- ✓ **Un système informatique présente toujours un goulet d'étranglement.** Prenons un exemple : vous avez découvert que sur votre serveur le goulet d'étranglement est un disque SCSI 10000 RPM particulièrement lent. Vous décidez donc de le remplacer par un disque 15000 RPM. Dorénavant, le disque n'est plus le goulet d'étranglement, il traite les informations plus rapidement que la carte contrôleur à laquelle il est relié. Cela ne signifie pas que vous avez réglé le problème, c'est la carte contrôleur qui est devenue le goulet d'étranglement à la place du disque. Quoi que vous fassiez, l'ordinateur aura toujours un élément qui ralentira l'ensemble du système.
- ✓ **Un moyen de limiter les effets d'un goulet d'étranglement est d'éviter d'attendre qu'il se présente.** Par exemple, le spooling d'impression vous permet de ne pas attendre pendant l'impression. Le spooling ne rend pas l'imprimante plus rapide mais il vous donne la possibilité de vous libérer pour un autre travail pendant que l'imprimante bosse. Dans le même ordre d'idée, la mise en mémoire cache sur disque vous évite d'attendre si vous disposez d'un disque dur lent.

Les cinq goulets d'étranglement les plus courants

Vous trouverez ici les cinq types de goulets d'étranglement qui peuvent pénaliser le réseau.

Le matériel intégré dans les serveurs

Les serveurs doivent être des ordinateurs puissants, capables de prendre en charge toutes les tâches que le réseau leur confie. Ne comptez pas sur un ordinateur bas de gamme acheté au supermarché du coin.

Voici les quatre éléments les plus importants d'un serveur :

- ✓ **Le processeur.** Il doit être puissant. Un processeur soldé à quelques centaines d'euros à la boutique d'à côté ne fera pas l'affaire. Autrement dit, évitez les processeurs destinés aux ordinateurs domestiques.
- ✓ **La mémoire.** Il n'y en a jamais trop. Son prix ayant baissé, ne lésinez pas ; un serveur ne saurait avoir moins de 4 Go de RAM.

- ✓ **Le ou les disques durs.** Pas question d'installer des disques durs IDE bon marché. Pour obtenir des performances respectables, il vous faut des disques durs SCSI. Rien de moins.
- ✓ **La carte réseau.** Les cartes réseau bon marché, à une dizaine d'euros, sont parfaites pour un réseau domestique. En revanche, n'espérez pas les utiliser efficacement sur un serveur de fichiers desservant deux cents utilisateurs. Rappelez-vous que le serveur utilise le réseau bien plus que n'importe lequel des ordinateurs clients. C'est pourquoi il doit être équipé d'une bonne carte. En fait, pour de bonnes performances, vous devrez installer plusieurs cartes réseau.

Les options de configuration du serveur

Tous les systèmes d'exploitation réseau sont équipés d'options permettant de les configurer. Certaines suffisent pour faire la différence entre un réseau qui se traîne et un réseau ultra rapide. Il n'existe malheureusement pas de règle établie pour configurer ces options. D'ailleurs, si elles existaient, on n'aurait pas besoin d'options.

Voici les principales :

- ✓ **Les options de mémoire virtuelle.** La *mémoire virtuelle* est définie par un fichier de pagination créé temporairement sur le disque dur, que le serveur utilise lorsqu'il ne dispose plus de suffisamment de mémoire vive (RAM). Comme peu de serveurs possèdent suffisamment de mémoire vive, la mémoire virtuelle joue un rôle important. Il est possible de spécifier la taille et l'emplacement du fichier de pagination utilisé comme mémoire virtuelle.

Pour de meilleures performances, la taille du fichier doit être d'au moins 1,5 fois la quantité de mémoire vive. Par exemple, si l'ordinateur est équipé de 4 Go de RAM, il faudra lui allouer au moins 6 Go de mémoire virtuelle. Au besoin, il sera possible de l'augmenter par la suite.

- ✓ **La répartition sur plusieurs disques.** Utilisez le défragmenteur pour optimiser le stockage des données sur le disque dur du serveur.

Si le serveur est équipé de plusieurs disques durs, vous pouvez créer des volumes entrelacés qui permettront aux opérations d'entrée/sortie de s'exécuter simultanément sur chacun des disques.

- ✓ **Les protocoles réseau.** Assurez-vous que les protocoles réseau sont configurés correctement et supprimez tous ceux qui ne sont pas nécessaires.
- ✓ **L'espace disque libre sur les serveurs.** Il doit toujours rester beaucoup de place sur le disque dur des serveurs.





Si cette place se réduit considérablement, le serveur est pénalisé et les opérations de lecture/écriture sur les disques commencent à s'éterniser. Quelques gigaoctets libres offrent une bonne marge de manœuvre.

Les serveurs surmenés

Une des raisons classiques de la baisse des performances d'un serveur est la surcharge des tâches. Le fait que les systèmes d'exploitation réseau modernes soient livrés avec des dizaines de services différents ne signifie pas que vous deviez les activer tous et les utiliser en même temps sur le même serveur. Si un serveur fonctionnant seul rame parce que la charge de travail est trop élevée, ajoutez-en un second qui délesterá le premier de certaines corvées. Rappelez-vous du vieil adage : « Plus on est nombreux, plus ça va vite. »

Par exemple, si le réseau a besoin de plus d'espace disque, envisagez l'ajout d'un second serveur de fichiers plutôt que d'ajouter un disque dur à un serveur qui en a déjà quatre, tous bien remplis. Ou mieux, achetez un ordinateur dont la seule tâche sera de servir des fichiers.

Le bénéfice secondaire de la répartition des tâches sur plusieurs serveurs est un réseau plus facile à administrer et plus fiable. Par exemple, si un seul serveur fait office de serveur de fichiers et de serveur de messagerie, vous perdrez momentanément ces deux services s'il tombe en panne ou si vous devez le mettre à niveau. Si chacune de ces tâches est prise en charge par un serveur dédié, un seul service sera interrompu en cas d'incident.

L'infrastructure du réseau

L'*infrastructure* est composée de tous les câbles, concentrateurs, commutateurs, routeurs et autres composants qui se trouvent entre les serveurs et les clients.

Les éléments d'infrastructure suivants peuvent ralentir le réseau :



- ✓ **Les concentrateurs.** Les commutateurs étant devenus très bon marché, vous résoudrez beaucoup de problèmes de performances en remplaçant vos vieux concentrateurs démodés par des commutateurs qui réduiront la charge globale sur le réseau.
- ✓ **La taille des segments.** Faites en sorte que sur chacun des segments du réseau le nombre d'ordinateurs et autres périphériques reste dans les limites du raisonnable, c'est-à-dire une vingtaine. Notez qu'en remplaçant les concentrateurs par des commutateurs, vous réduisez instantanément la taille de chaque segment car chaque port d'un commutateur est un segment à lui seul.

- ✓ **La vitesse du réseau.** Si votre réseau est ancien, vous découvrirez probablement que beaucoup d'utilisateurs, voire tous, sont encore connectés à 10 Mbps. La mise à niveau à 100 Mbps augmentera considérablement la vitesse du réseau, et si vous passez au gigabit (1 Gbps), ce sera encore plus rapide.
- ✓ **La vitesse de la dorsale.** Si les segments du réseau sont reliés à une dorsale, envisagez la mise à niveau de cette dernière à 1 Gbps.



Le plus difficile lors d'une recherche d'amélioration des performances du réseau est de découvrir l'emplacement des goulets d'étranglement. Avec du matériel de test sophistiqué et des années d'expérience, les spécialistes des réseaux parviennent à les localiser par déduction. Même sans équipement ni expérience, vous pouvez vous aussi vous en sortir.

Les dysfonctionnements matériels

Une carte réseau ou un autre composant qui fonctionne mal peut ralentir le réseau. Par exemple, un commutateur peut mal fonctionner par intermittence : il laisse passer des paquets de temps en temps mais en perd suffisamment pour que le réseau ralentisse. Après avoir identifié le composant fautif, son remplacement restaurera les performances du réseau.

Améliorer les performances du réseau : la méthode maniaque

Vous avez deux moyens d'améliorer les performances de votre réseau. Le premier consiste à réfléchir un peu, à penser à ce qui pourrait améliorer les performances, à faire des tests et à vérifier si le réseau fonctionne plus vite. C'est l'approche choisie par la plupart.

Il y a ensuite la méthode maniaque, idéale pour les personnes qui trient leurs chaussettes par couleur et rangent leurs placards par catégories d'aliments ou par ordre alphabétique. Cette approche ressemble à celle qui suit :

1. Élaborez une méthode pour tester objectivement les performances d'un des aspects du réseau.

Il s'agit de la méthode du *banc d'essai*. Par exemple, si vous voulez améliorer les performances de l'impression en réseau, ayez recours à un chronomètre pour mesurer le temps que prend l'impression de documents volumineux.

2. Changez une variable de la configuration de votre réseau et procédez de nouveau au test.

Par exemple, si vous pensez qu'augmenter la taille de la mémoire cache du disque peut améliorer les performances, modifiez-la, relancez le serveur et lancez la mesure des performances. Notez si les performances s'améliorent, restent les mêmes ou se détériorent.

3. Répétez l'étape 2 pour chacune des variables que vous voulez tester.

Voici quelques points importants qu'il convient de garder à l'esprit si vous voulez améliorer les performances de votre réseau avec cette méthode :

- ✓ **Si possible, testez chaque variable séparément.** Autrement dit, revenez à la configuration d'origine avant le test de la variable suivante.
- ✓ **Écrivez le résultat de chaque test** de sorte que vous disposiez d'un enregistrement précis de l'impact de chaque modification sur les performances du réseau.
- ✓ **Veillez à ne modifier qu'une option de la configuration à chaque fois que vous démarrez le banc d'essai.** Si vous effectuez plusieurs modifications, vous ne saurez pas laquelle a influencé les performances. Il se peut aussi qu'une modification ait entraîné une amélioration des performances mais qu'une autre ait eu l'effet inverse, si bien que les modifications s'annulent entre elles (comme au football, lorsque l'arbitre siffle une faute).
- ✓ **Réalisez vos tests pendant les heures de travail, quand le réseau est soumis à sa charge habituelle.**
- ✓ **Pour mesurer les performances, exécutez votre banc d'essai deux ou trois fois afin d'être sûr que les résultats obtenus sont constants.**

Surveiller les performances du réseau

Chronométrer la durée nécessaire pour accomplir une tâche sur le réseau comme ouvrir un document ou imprimer un rapport est une manière de surveiller les performances du réseau.

Une approche plus technique consiste à utiliser un programme de surveillance qui collecte en permanence des statistiques sur le fonctionnement du réseau. Tapi dans l'ordinateur, il espionne discrètement l'activité sur le réseau et enregistre tout ce qui s'y passe dans un journal des performances. Vous pouvez à tout moment consulter ce journal pour savoir comment se porte le réseau.

Si le réseau est de grande taille, vous pouvez utiliser un programme de surveillance sophistiqué qui tourne sur son propre serveur dédié. Pour des réseaux petits à moyens, vous aurez plutôt recours à un utilitaire livré avec le système d'exploitation. La Figure 19.1 représente le moniteur de fiabilité et de performances fourni avec Windows Server. D'autres systèmes d'exploitation sont équipés du même genre d'utilitaire.

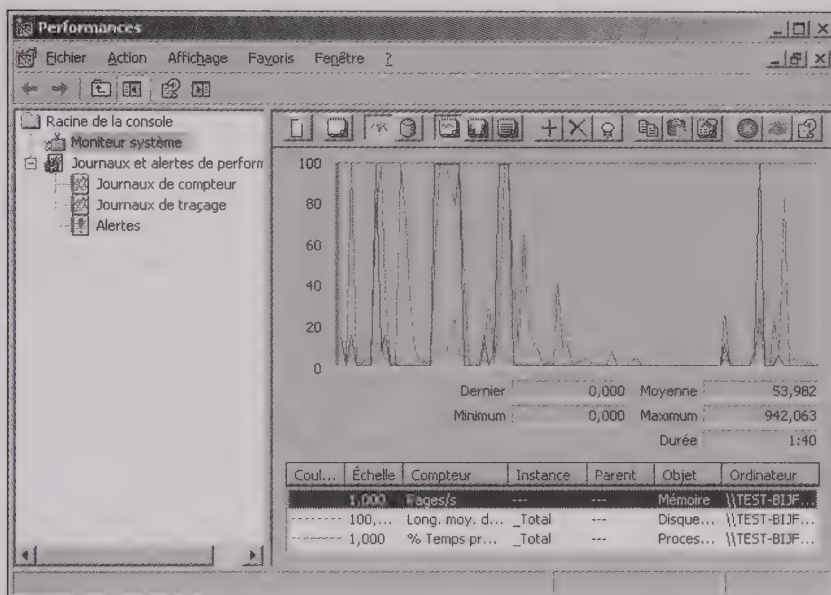


Figure 19.1 : Suivi des performances sous Windows Server.

Le moniteur de fiabilité et de performances de Windows permet de surveiller différents paramètres en même temps. Chacun de ces paramètres est défini par un compteur. Le Tableau 19.1 montre les plus communément utilisés mais il en existe des dizaines. Notez que chaque compteur se réfère à un objet du serveur comme le disque physique, la mémoire ou le processeur.

Tableau 19.1 : Compteurs de performances communément utilisés.

Objet	Compteur	Description
Disque physique	% espace libre	Pourcentage d'espace libre sur les disques physiques du serveur. Doit être d'au moins 15 %.
Disque physique	Longueur moyenne de la file d'attente	Nombre d'opérations disque en attente pendant que le disque est occupé à effectuer d'autres opérations disque. Doit être de 2 au maximum.

Objet	Compteur	Description
Mémoire	Pages par seconde	Nombre de pages extraites chaque seconde du fichier de pagination de la mémoire virtuelle. Le seuil moyen se situe à environ à 2 500 pages par seconde.
Processeur	% temps processeur	Indique le pourcentage du temps pendant lequel le processeur est occupé à des tâches au lieu d'être en attente. Doit être de 85 % au maximum.

Voici quelques autres points à prendre en considération lors du suivi des performances :

- ✓ **Le moniteur de fiabilité et de performances permet de surveiller les données en temps réel ou de voir celles qui ont été enregistrées dans un fichier du journal.** Les données en temps réel donnent un aperçu de ce qui se passe sur le réseau à un moment donné. Les informations les plus utiles sont toutefois celles consignées dans le journal.
- ✓ **Il est possible de planifier l'inscription dans le journal afin qu'elle démarre à une certaine heure, pendant un intervalle donné.** Par exemple, des données seront inscrites dans le journal toutes les quinze secondes de 9h à 9h30 puis de 15h à 15h30.
- ✓ **Même si vous n'avez pas de problème de performances, il est recommandé de consigner les performances dans le fichier journal et ce pendant quelques semaines afin de collecter des données de fonctionnement normal.** Si des problèmes surgissent par la suite, ces données vous seront extrêmement précieuses.



Ne configurez pas la journalisation non-stop. La collecte des données de performances ralentit le serveur. Consultez-les de temps en temps pour obtenir des données de base ou si vous décelez un problème au niveau des performances.

Quelques conseils supplémentaires

Voici quelques conseils de dernière minute concernant les performances :

- ✓ **Il suffit parfois d'observer les concentrateurs ou les commutateurs pendant quelques minutes pour déceler la source d'un ralentissement.** Ils sont équipés de témoins vert et rouge. Le témoin vert clignote dès que des données sont transmises. Le témoin rouge clignote à chaque fois qu'une collision de données se produit. Il est normal que la lumière rouge clignote de temps en temps mais si elle le fait tout le temps, la carte réseau est sans doute défectueuse.

- ✓ **Vérifiez les tâches planifiées comme les sauvegardes, les mises à jour de données par lots ou les rapports de tâches.** Si c'est possible, planifiez-les pour qu'elles se déroulent en dehors des heures de travail, la nuit par exemple, quand les bureaux sont déserts. Ces tâches tendent à ralentir le réseau à cause des nombreux accès aux disques durs du serveur.
- ✓ **Il arrive parfois qu'une application dégrade les performances.** Par exemple, certains logiciels produisent ce que l'on appelle de la *mémoire non allouée* : ils utilisent de la mémoire mais oublient de la libérer une fois qu'ils sont fermés. Les programmes qui quittent sans libérer la mémoire peuvent accaparer une bonne partie de la mémoire vive du serveur, qui finit par ramer lamentablement et même se bloquer. Si vous soupçonnez un programme de ne pas libérer la mémoire, contactez l'éditeur pour voir s'il n'existe pas un correctif.
- ✓ **Un spyware peut contribuer à ralentir le système.** Il s'agit d'un programme qui s'installe subrepticement dans l'ordinateur, surveille ce que vous faites et transmet périodiquement un rapport de vos activités à un autre ordinateur connecté à Internet. Heureusement, il existe de nombreux outils gratuits ou peu chers qui suppriment les spyware. Pour plus d'informations, utilisez Google ou un autre moteur de recherche pour trouver un tel outil.

Chapitre 20

Résoudre des problèmes réseau

Dans ce chapitre :

- Vérifier ce qui est évident.
- Ressusciter un ordinateur qui semble mort.
- Découvrir l'origine du problème.
- Redémarrer les serveurs et les ordinateurs clients.
- Déchiffrer les journaux d'événements.
- Conserver une trace des petites misères du réseau.

R

econnaissons-le : les réseaux ont une fâcheuse tendance à tomber en panne.

Ils comportent beaucoup trop d'éléments « qui commencent par un c » : câbles, connecteurs, commutateurs, cartes. Tous ces éléments doivent être maintenus ensemble dans un certain équilibre, sachant que l'équilibre d'un réseau est très facile à rompre. Même les réseaux informatiques les mieux conçus se comportent parfois comme s'ils étaient faits de fils de fer reliés par du chewing-gum et du ruban adhésif.

Comme si les choses n'étaient pas assez compliquées, les réseaux suscitent la suspicion. Une fois que vous avez connecté votre ordinateur au réseau, vous avez tendance à blâmer ce dernier à chaque fois que quelque chose ne va pas, que votre problème soit lié ou non au réseau. Pourquoi ces colonnes ne peuvent-elles pas s'aligner dans Word ? Ça doit être le réseau. Les totaux de vos feuilles de calcul ne tombent pas juste ? C'est encore ce #\$\$@ de réseau.

Le pire avec les problèmes de réseau c'est qu'ils peuvent affecter toute une entreprise. Ce n'est pas si grave si un seul utilisateur ne peut pas accéder à un dossier partagé sur un serveur de fichiers. En revanche, si un serveur critique tombe en panne, les utilisateurs du réseau peuvent être privés

d'accès à leurs fichiers, applications, messages électroniques et tout ce dont ils ont besoin pour travailler comme d'habitude. Quand cela se produit, ils défoncent la porte de votre bureau et vous menacent jusqu'à ce que le réseau soit de nouveau opérationnel.

Dans ce chapitre, je décris les causes les plus fréquentes, à l'origine de problèmes de réseau, et propose quelques solutions que vous pouvez utiliser quand votre réseau tombe en panne.

Quand les ordinateurs en bonne santé rencontrent des problèmes

Les conseils de dépannage suivants vous indiquent comment réagir face aux premiers signes de problème réseau. Dans la plupart des cas (voire tous), les solutions proposées peuvent relancer votre réseau :

1. Vérifiez que votre ordinateur et tous ses périphériques sont bien branchés.

Les férus d'informatique sont pliés quand un utilisateur les appelle à l'aide et qu'ils doivent lui expliquer que l'ordinateur n'était pas branché. Ils l'écrivent dans leur journal pour pouvoir le raconter plus tard à leurs amis. Ils peuvent même demander à vous prendre en photo pour pouvoir vous montrer à leurs amis geek.

2. Vérifiez que votre ordinateur est correctement connecté au réseau.

3. Notez tous les messages d'erreur qui s'affichent sur l'écran.

4. Contrôlez l'espace disque libre sur votre ordinateur et sur le serveur.

Quand un ordinateur n'a plus ou peu d'espace disque, des choses bizarres peuvent se produire. Un message d'erreur s'affiche parfois pour vous tenir au courant de la situation, mais pas toujours. Quelquefois l'ordinateur marque une pause : les opérations qui prenaient quelques secondes durent désormais plusieurs minutes.

5. Faites quelques essais pour vérifier si le problème vient du réseau ou de votre ordinateur.

La section « Expérimenter, en désespoir de cause » de ce chapitre vous indique quelques astuces simples pour identifier l'origine du problème.

6. Essayez de redémarrer votre ordinateur.

Un nombre incroyable de problèmes sont résolus par un simple redémarrage. Bien sûr, dans bien des cas, le problème se manifestera de

nouveau, mais comme il a montré le bout de son nez, vous pourrez en identifier la cause et le résoudre. Quelques problèmes ne sont qu'occasionnels ; un simple redémarrage est alors suffisant.

7. Essayez de redémarrer le serveur du réseau.

Reportez-vous à la section « Redémarrer un serveur », plus loin dans ce chapitre.

Ressusciter un ordinateur qui semble mort

Si votre ordinateur semble mort, vérifiez les points suivants :

- ✓ **Prise électrique.** Est-il branché ?
- ✓ **Protection électrique.** Si votre ordinateur est connecté à une prise multiple ou à une barrette d'écrtage, assurez-vous que la prise ou la barrette est branchée et allumée. Si la prise multiple ou la barrette d'écrtage est équipée d'un témoin lumineux, celui-ci devrait briller.
- ✓ **Interrupteur.** Vérifiez que le bouton On/Off de votre ordinateur est bien positionné. Cela semble idiot à dire mais beaucoup d'ordinateurs sont configurés de telle manière que l'interrupteur de courant est toujours positionné sur « On ». L'ordinateur s'allume ou s'éteint avec l'interrupteur de la prise multiple ou de la barrette d'écrtage. Nombreux sont les utilisateurs qui découvrent avec surprise l'existence d'un interrupteur On/Off à l'arrière de leur machine.

Pour compliquer les choses, les ordinateurs récents sont capables de dormir. Ils semblent éteints mais en fait pas du tout. Pour les réveiller, il suffit de bouger la souris. Il est facile de penser que l'ordinateur est éteint : on appuie sur le bouton Marche, on se demande pourquoi il ne se passe rien puis on appuie une nouvelle fois sur le bouton Marche, en maintenant le doigt dessus, en pensant que ça va... marcher. Mais si vous maintenez le doigt appuyé sur le bouton Marche/Arrêt assez longtemps, l'ordinateur s'éteint et, lorsque vous le rallumez, vous voyez apparaître un message disant qu'il n'a pas été éteint correctement. Moralité : si vous avez l'impression que l'ordinateur est endormi, bougez la souris.

- ✓ **Ventilateur.** Si vous pensez que votre ordinateur n'est pas branché, bien qu'il semble l'être, écoutez le bruit du ventilateur. Si celui-ci fonctionne, l'ordinateur est alimenté en électricité et le problème est donc plus sérieux qu'un simple câble mal branché (si l'ordinateur est branché, que le ventilateur ne fonctionne pas et que son interrupteur est sur « On », c'est qu'il est peut-être sorti déjeuner).



TRUC



- ✓ **Prise sans électricité.** Si l'ordinateur est branché, allumé mais ne fonctionne pas, branchez une lampe sur la prise pour vérifier que le courant arrive bien. Peut-être devrez-vous alors réenclencher un disjoncteur ou remplacer une barrette d'écrtage défectueuse. Ou encore il vous faudra appeler EDF.

Les barrettes d'écrtage ont une durée de vie limitée. Après quelques années d'utilisation, elles continuent d'alimenter votre ordinateur mais elles ne le protègent plus contre les surtensions. Si la vôtre a plus de deux ou trois ans, remplacez-la.

- ✓ **Moniteur.** Le moniteur dispose de son propre interrupteur et de sa propre prise. Vérifiez qu'il est bien branché et allumé. Deux câbles doivent être connectés au moniteur. L'un va de l'arrière de l'ordinateur à l'arrière du moniteur, l'autre est un cordon d'alimentation qui part de l'arrière du moniteur et doit être connecté à une prise de courant.
- ✓ **Câbles.** Votre clavier, votre souris, votre moniteur et votre imprimante sont tous connectés à l'arrière de l'ordinateur par des câbles.
Assurez-vous que ces câbles sont bien branchés. Vérifiez que les autres extrémités des câbles du moniteur et de l'imprimante sont, elles aussi, bien connectées.
- ✓ **Réglages du moniteur.** La plupart des moniteurs sont équipés de boutons qui permettent d'ajuster le contraste et la luminosité de l'affichage. Essayez de tourner ces boutons si votre ordinateur fonctionne mais que l'affichage est sombre. Il se peut qu'ils soient réglés au minimum.
- ✓ **Composants internes.** Si vous êtes compétent et audacieux, arrêtez l'ordinateur, débranchez-le, ouvrez la tour puis retirez et réinsérez soigneusement les composants tels que la mémoire et les cartes vidéo. S'ils sont mal fixés, ces composants sortent de leur logement. Les retirer puis les réinsérer peut parfois faire revivre un ordinateur qui semblait mort.

Tester la connexion réseau

Les câbles qui connectent des ordinateurs clients au reste du réseau sont fragiles. Ils peuvent se casser. N'entendez pas par là qu'ils se cassent physiquement en deux. Bien sûr, un problème de câble est parfois l'œuvre du fouineur de service et de ses cisailles. Mais généralement ce type de problème n'est pas visible à l'œil nu.



Si votre réseau utilise du câble à paires torsadées, vous pouvez rapidement dire si la connexion au réseau est bonne en regardant à l'arrière de votre ordinateur. Une petite lumière se trouve à côté de l'endroit où se branche le

câble. Si cette lumière brille, le câble est bon. Si la lumière est éteinte ou si elle scintille de manière intermittente, vous avez un problème de câble.

Si la lumière ne brille pas, essayez de déconnecter le câble de votre ordinateur puis de l'y reconnecter. Cela peut résoudre un problème de mauvaise connexion.

- ✓ Certains réseaux sont câblés de telle sorte que votre ordinateur est connecté au réseau via un câble très court (environ deux mètres). Une extrémité de ce câble est reliée à votre ordinateur tandis que l'autre est connectée à une prise murale. Essayez de débrancher puis de rebrancher rapidement ce câble. Si cela ne produit aucun résultat, trouvez un câble de rechange que vous pouvez utiliser.
- ✓ Le commutateur est souvent sujet à des problèmes, notamment les commutateurs qui sont câblés d'une manière si « professionnelle » qu'ils sont noyés dans un sac de nœuds. Ne touchez pas au sac de nœuds. Laissez ce problème au marin de service, c'est-à-dire au spécialiste réseau.

Perdu dans une nuée de messages d'erreur !

Avez-vous remarqué des messages d'erreur sur l'écran de votre ordinateur quand vous l'avez démarré ? Si oui, notez-les. Ce sont de précieux indices qui peuvent aider le gourou du réseau à résoudre le problème.



Si vous voyez des messages d'erreur quand vous démarrez votre ordinateur, gardez à l'esprit ce qui suit :

- ✓ Ne paniquez pas si vous voyez beaucoup de messages d'erreur défiler. Un problème simple à résoudre peut parfois générer une pléthore de messages d'erreur quand vous démarrez votre ordinateur. Les messages peuvent laisser penser que votre ordinateur part en morceaux mais la solution est peut-être toute simple.
- ✓ Si les messages défilent si vite que vous ne pouvez pas les noter, appuyez sur la touche Pause. Votre ordinateur s'arrête dans un crissement de pneus, ce qui vous donne une chance de pouvoir lire les messages. Quand vous en avez lu assez, appuyez à nouveau sur la touche Pause pour que les choses reprennent leur cours. La touche Pause est nommée « Arrêt Defil » sur certains ordinateurs. Utilisez la combinaison Ctrl+Verr Num ou Ctrl+S sur les ordinateurs qui n'ont pas de touche Pause.
- ✓ Si vous avez manqué les messages d'erreur la première fois, redémarrez votre ordinateur et regardez plus attentivement.

- ✓ Mieux, appuyez sur la touche F8 dès que vous voyez le message Démarrage de Windows à l'écran. Cette opération ordonne au système d'exploitation de traiter les lignes de CONFIG.SYS une par une, avant que la commande suivante ne soit exécutée.

Revérifier les paramètres du réseau

Je soupçonne des petits hommes verts de s'introduire dans le bureau la nuit, d'allumer les ordinateurs et de mettre la pagaille dans les configurations TCP/IP rien que pour rigoler.

Bizarrement, il arrive que les paramètres de configuration réseau d'un ordinateur soient modifiés sans que personne n'y ait touché. Résultat : un ordinateur qui moulinait sans histoire dans son coin depuis des mois ou des années est tout à coup incapable d'accéder au réseau. L'une des premières choses à faire, après avoir vérifié que l'ordinateur est allumé et que les câbles sont en bon état, est d'examiner attentivement ses paramètres réseau. Vérifiez les points suivants :

- ✓ **Paramètres TCP/IP** : À l'invite de commande MS-DOS, démarrez ipconfig afin de vous assurer que le protocole TCP/IP est actif sur l'ordinateur et que l'adresse IP, les paramètres de masques de sous-réseau et de passerelle sont valables.
- ✓ **Protocoles** : Ouvrez la boîte de dialogue Propriétés de Connexions réseau et assurez-vous que les protocoles requis sont correctement installés.
- ✓ **Nom de l'ordinateur** : Ouvrez la boîte de dialogue Propriétés système (double-cliquez sur l'icône Système du Panneau de configuration) et vérifiez les paramètres de l'onglet Nom de l'ordinateur. Assurez-vous que le nom de l'ordinateur est unique et que le nom du groupe de travail ou du domaine est correctement orthographié.
- ✓ **Autorisations** : Vérifiez (plutôt deux fois qu'une) le compte utilisateur afin de vous assurer qu'il a l'autorisation d'accéder aux ressources dont il a besoin.

Expérimenter, en désespoir de cause

Si vous ne parvenez pas à trouver d'explications évidentes (comme un ordinateur débranché) à vos problèmes, vous devrez vous livrer à quelques expériences pour restreindre le champ des possibilités. Ayez vos expé-

riences autour d'une question de base : est-ce un problème de réseau ou un problème lié à l'ordinateur ?

Voici quelques suggestions pour restreindre le champ des hypothèses possibles :

- ✓ **Essayez d'effectuer la même opération sur un autre ordinateur.** Si personne sur le réseau ne peut accéder à un disque ou à une imprimante réseau, quelque chose cloche peut-être avec le réseau. En revanche, si vous êtes le seul à rencontrer ce problème, il ne peut provenir que de votre ordinateur. Ce dernier dialogue peut-être mal avec le réseau ou n'est pas bien configuré. Le problème peut aussi ne pas être lié au réseau.
- ✓ **Si vous arrivez sans problème à effectuer la même opération sur l'ordinateur de quelqu'un d'autre, essayez de vous connecter au réseau avec votre ID utilisateur depuis cet ordinateur.** Voyez alors si vous pouvez répéter l'opération sans rencontrer d'erreur. Si vous le pouvez, le problème provient probablement de votre ordinateur plutôt que de l'ordinateur serveur. Si vous n'y parvenez pas, le problème est peut-être dû à la configuration de votre compte utilisateur.
- ✓ **Si vous ne pouvez pas vous connecter depuis un autre ordinateur, attendez quelques instants.** Votre compte est peut-être temporairement bloqué, pour diverses raisons, dont la plus courante est plusieurs tentatives successives de connexion avec un mot de passe erroné. Si au bout d'une heure le problème persiste, appelez l'administrateur réseau et offrez-lui un biscuit.

On commence par qui ?

Quand il s'agit de résoudre un problème de réseau, il est souvent utile de savoir qui est actuellement connecté au serveur. Par exemple, si un utilisateur est incapable d'accéder à un fichier présent sur le serveur, commencez par vérifier s'il est connecté. Si oui, vous saurez que le compte de l'utilisateur est valide mais que cet utilisateur n'a peut-être pas l'autorisation d'accéder au fichier ou au dossier en question. Par ailleurs, si l'utilisateur n'est pas connecté, le problème est probablement dû au compte lui-même ou à la manière dont l'utilisateur tente de se connecter au serveur.

Il est aussi utile de savoir qui est connecté, au cas où vous pourriez avoir besoin de redémarrer le serveur. Pour plus d'informations sur cette opération, reportez-vous à la section « Redémarrer un serveur », plus loin dans ce chapitre.



Pour savoir qui est connecté à un serveur Windows Server 2008, exécutez les étapes suivantes :

1. Exécutez **Démarrer/Outils d'administration/Gestion de l'ordinateur** pour ouvrir la fenêtre **Gestion de l'ordinateur**.
2. Dans la liste de gauche, développez **Outils système**, **Dossiers partagés** puis **Sessions**.

La liste des utilisateurs ayant ouvert une session apparaît.

Vous pouvez sélectionner **Fichiers ouverts** pour voir quels sont les fichiers utilisés par les utilisateurs du réseau.

Redémarrer un ordinateur client

Il arrive qu'un problème bloque l'ordinateur à un point tel que la seule solution consiste à le redémarrer. Dans certains cas, l'ordinateur se met soudain à se comporter étrangement. Des caractères bizarres apparaissent à l'écran ou Windows s'embrouille et ne vous permet pas de quitter un programme. Votre ordinateur est parfois si déboussolé qu'il ne peut plus rien faire. Il reste planté là, comme une borne kilométrique. Il ne veut pas bouger, même si vous appuyez sur la touche Echap ou Entrée. Vous avez beau déplacer la souris dans tous les sens ou même la jeter à travers la pièce, son pointeur reste parfaitement immobile sur l'écran.

Quand un ordinateur commence à se comporter de la sorte, vous devez le redémarrer. Si vous êtes contraint de le redémarrer, faites-le aussi proprement que possible. Je sais que cette procédure va vous sembler élémentaire mais il n'est jamais vain de répéter la technique permettant de redémarrer un ordinateur client en toute sécurité, même si elle est simplissime :

1. **Essayez de sauvegarder votre travail, si vous le pouvez.**

Si cela vous est possible, utilisez la commande **Fichier/Enregistrer** pour sauvegarder les documents ou fichiers sur lesquels vous étiez en train de travailler quand les choses ont commencé à aller de travers. Si vous ne pouvez pas accéder aux menus, essayez de cliquer sur le bouton **Enregistrer** de la barre d'outils. Si ça ne marche pas, essayez d'utiliser la combinaison de touches **Ctrl+S**, le raccourci clavier standard pour la commande **Enregistrer**.

2. **Fermez les programmes en cours, si vous le pouvez.**

Exécutez la commande **Fichier/Quitter** ou cliquez sur le bouton **Fermer** dans l'angle supérieur droit de la fenêtre du programme. Autre alternative : appuyez sur **Alt+F4**.

3. Arrêtez l'ordinateur.

Sous Windows XP, choisissez Démarrer/Arrêter l'ordinateur. Sous Windows Vista ou Windows 7, cliquez sur le bouton Démarrer puis sur la flèche à droite du cadenas, et choisissez Arrêter.

La boîte de dialogue Arrêter l'ordinateur apparaît.

4. Sélectionnez l'option Redémarrer et cliquez sur OK.

Votre ordinateur redémarre.

Si redémarrer votre ordinateur ne résout pas le problème, vous pouvez tenter de l'éteindre complètement puis de le rallumer. Pour ce faire, suivez les étapes 1 à 3 de la procédure ci-dessus. Choisissez l'option Arrêter plutôt que l'option Redémarrer et cliquez sur OK. Selon le type d'ordinateur, Windows l'éteindra automatiquement ou affichera un message vous invitant à le faire. Si Windows n'éteint pas tout seul l'ordinateur, basculez l'interrupteur On/Off de votre ordinateur sur Off. Attendez quelques secondes puis rallumez-le.



La plupart des ordinateurs récents ne s'éteignent pas immédiatement lorsque vous appuyez sur le bouton Arrêt. Vous devez maintenir ce dernier enfoncé quelques instants. Il s'agit d'une précaution destinée à vous empêcher d'éteindre accidentellement votre ordinateur.

Voici quelques actions que vous pourriez tenter si vous rencontrez des problèmes pour redémarrer votre ordinateur :

- ✓ Si votre ordinateur refuse de répondre à la commande Démarrer/Arrêter, essayez d'appuyer sur les touches Ctrl, Alt et Suppr simultanément.
Quand vous appuyez sur Ctrl+Alt+Suppr, Windows 9x et les versions ultérieures affichent une boîte de dialogue qui vous permet de fermer n'importe quel programme en cours d'exécution ou d'éteindre tout simplement votre ordinateur. Malheureusement, Windows 9x est parfois tellement perturbé qu'il n'est pas en mesure d'afficher la boîte de dialogue de redémarrage. Dans ce cas, appuyer sur Ctrl+Alt+Suppr peut redémarrer votre ordinateur.
- ✓ Si Ctrl+Alt+Suppr ne fonctionne pas, vous n'avez plus d'autres solutions que d'appuyer sur le bouton de réinitialisation (*Reset*) de votre ordinateur.
- ✓ Appuyer sur le bouton de réinitialisation est un moyen radical auquel vous ne devez avoir recours que si votre ordinateur ne répond plus du tout. Tout le travail que vous n'aurez pas encore sauvegardé sur le disque sera perdu. Si votre ordinateur ne dispose pas d'un bouton de réinitialisation, éteignez-le, attendez quelques minutes puis rallumez-le.





- ✓ Si possible, sauvegardez votre travail avant de redémarrer votre ordinateur. Tout travail non sauvegardé sera irrémédiablement perdu. Malheureusement, si votre ordinateur est dans un état irrécupérable, vous ne pourrez rien faire. Pour limiter les dégâts, pensez à sauvegarder votre travail régulièrement.

Redémarrer des services du réseau

De temps en temps, le service du système d'exploitation réseau, qui gère la tâche à l'origine d'un problème, s'arrête ou se bloque. Si l'utilisateur ne peut pas accéder au serveur, c'est probablement parce qu'un service clé vient de se bloquer.

L'état des services peut être consulté à l'aide de l'outil Services, illustré dans la Figure 20.1. Pour l'afficher, cliquez sur Outils d'administration/Services. Parcourez la liste et assurez-vous que tous les services clés sont démarrés. Si l'un d'eux est en pause ou arrêté, redémarrez-le.

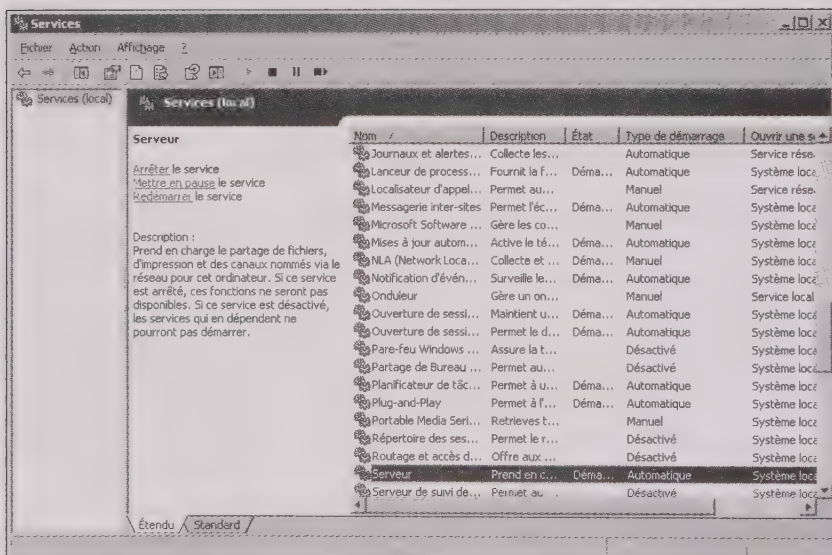


Figure 20.1 : Outil d'administration Services.

Le service que nous qualifions de « clé » dépend du rôle que vous lui avez défini sur le serveur. Le Tableau 20.1 répertorie les services les plus courants dans les systèmes d'exploitation réseau Windows. Cependant, beaucoup de serveurs exigent, outre ceux-ci, des services supplémentaires.

Tableau 20.1 : Services clés de Windows.

Service	Description
Explorateur d'ordinateur	Gère la liste des ordinateurs accessibles sur le réseau. Si ce service est désactivé, les ordinateurs ne pourront pas utiliser les services d'exploration, comme les Favoris réseaux ou l'Explorateur de réseau.
Client DHCP	Permet à l'ordinateur d'obtenir son adresse IP d'un serveur DHCP. Si ce service est désactivé, les adresses IP des ordinateurs ne seront pas correctement configurées.
Client DNS	Permet à l'ordinateur d'accéder au serveur DNS afin de résoudre les noms DNS. Si ce service est désactivé, l'ordinateur n'est plus capable de déchiffrer les noms DNS, notamment ceux des adresses Internet et d'Active Directory.
Serveur	Fournit au serveur un service de partage de fichiers et d'imprimantes de base. Si ce service est désactivé, les clients ne pourront pas se connecter au serveur pour accéder aux fichiers ou aux imprimantes.
Station de travail	Permet à l'ordinateur d'établir des connexions clients avec d'autres serveurs. Si ce service est désactivé, l'ordinateur ne pourra pas se connecter à d'autres serveurs.



Généralement, les services clés ont une bonne raison de s'arrêter. C'est pour quoi se contenter de redémarrer un service ne résoudra probablement pas le problème de réseau ou pas durablement. Vous devez examiner le journal Système à la recherche de tout message d'erreur qui expliquerait l'arrêt du service.

Si vous utilisez Windows 2000 Server, Windows Server 2003 ou Windows Server 2008, vous pouvez double-cliquer sur un service pour afficher une boîte de dialogue qui le décrit. C'est bien pratique lorsque vous vous interrogez sur la signification de l'un d'eux.

Redémarrer un serveur

Si vous pensez que le réseau est à l'origine du problème, vous pouvez redémarrer le serveur pour voir si cela met fin à vos ennuis.



Redémarrer un serveur est une solution de dernier recours. Les systèmes d'exploitation réseau sont conçus pour fonctionner des mois ou des années sans jamais redémarrer. Le redémarrage d'un serveur entraîne inévitablement un arrêt temporaire du réseau. Si vous devez vraiment redémarrer un serveur, faites-le si possible pendant les heures creuses.



Avant de redémarrer un serveur, vérifiez si un service requis n'est pas en pause ou arrêté. Peut-être suffit-il simplement de redémarrer un service plutôt que la totalité du serveur. Pour en savoir plus, reportez-vous à la section précédente « Redémarrer des services du réseau ».

Voici la démarche à suivre pour redémarrer un serveur :

1. Assurez-vous que personne n'est connecté au réseau.

Le plus sûr est de redémarrer le serveur après les heures de travail, quand tout le monde est parti. Ainsi, vous ne risquez pas de pénaliser quelqu'un qui serait resté sur le réseau.

Pour vérifier si des utilisateurs sont encore connectés, reportez-vous à la section « On commence par qui ? », plus haut dans ce chapitre.

2. Une fois que vous êtes certain que plus aucun utilisateur n'est connecté au réseau, éteignez le serveur.

Comportez-vous en citoyen responsable et faites les choses proprement. Pour les serveurs Windows, exécutez la commande Démarrer/Arrêter.



Windows Server ne vous laissera pas éteindre le serveur sans lui donner une bonne raison de le faire. Quand vous appuyez sur Ctrl+Alt+Suppr, une boîte de dialogue s'affiche et vous demande de fournir une raison.

3. Redémarrez l'ordinateur serveur ou éteignez-le puis rallumez-le.

Observez le serveur quand il redémarre pour vérifier qu'aucun message d'erreur ne s'affiche.

4. Demandez à tous les utilisateurs de se reconnecter et vérifiez que tous peuvent maintenant accéder au réseau.

Avant de redémarrer un serveur, souvenez-vous des règles suivantes :



- ✓ Il est bien plus radical de redémarrer un serveur que de redémarrer un ordinateur client. Vérifiez auparavant que chaque utilisateur a sauvegardé son travail et s'est déconnecté du réseau ! Vous pouvez provoquer de graves problèmes si vous éteignez le serveur tandis que des utilisateurs y sont connectés.
- ✓ Bien sûr, le fait de redémarrer un serveur peut perturber tous les utilisateurs du réseau. C'est pourquoi il est préférable de le faire en dehors des heures de travail.

Consulter les journaux d'événements

L'une des techniques les plus efficaces pour diagnostiquer les problèmes de réseau et les dépanner est de consulter les journaux d'événements. Ils contiennent des informations intéressantes concernant tous les dysfonctionnements qui auraient pu se produire, au jour le jour, lors des opérations sur le réseau. Ordinairement, ces journaux travaillent en tâche de fond, consignnant tranquillement ce qui se passe sur le réseau. Si quelque chose ne va pas, vous pouvez consulter les journaux pour voir si le problème a généré un événement significatif. Dans bien des cas, les journaux d'événements contiennent une entrée qui met en évidence la cause exacte du problème et suggère une solution.

Pour afficher les journaux d'événements d'un serveur Windows, utilisez l'Observateur d'événements, disponible dans les Outils d'administration. La Figure 20.2 représente l'Observateur d'événements d'un système Windows Server 2008. Le volet de gauche liste six catégories d'événements qui font l'objet d'un suivi : Application, Sécurité, Système, Service d'annuaire, Serveur DNS et Service de réplication de fichiers. Sélectionnez l'une de ces options afin d'accéder au journal qui vous intéresse. Pour obtenir des détails sur un événement spécifique, double-cliquez sur cet événement. S'ouvre alors une boîte de dialogue contenant des informations détaillées sur l'événement.

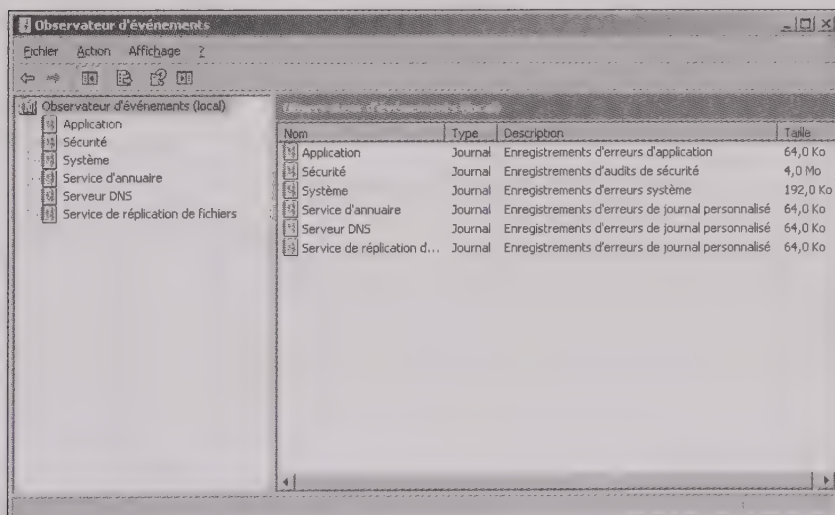


Figure 20.2 : Observateur d'événements.

Documenter les interventions sur le réseau

Pour un réseau de grande taille, vous investirez sans doute dans un logiciel de résolution des problèmes de gestion, capable de suivre l'évolution d'un problème, de son signalement initial à sa résolution finale. Pour des réseaux de taille petite ou moyenne, quelques classeurs à spirale et des formulaires seront suffisants. Ou alors vous pouvez consigner les incidents dans un document Word ou une feuille Excel.

Quelle que soit votre manière de gérer les problèmes du réseau, le journal de suivi doit contenir les informations suivantes :

- ✓ Le nom réel et le nom d'utilisateur de la personne qui signale le problème.
- ✓ La date du premier signalement du problème.
- ✓ Une évaluation de la gravité du problème. S'agit-il d'un simple inconvénient ou d'un incident qui empêche un utilisateur de travailler ? Existe-t-il une solution provisoire ?
- ✓ Le nom de la personne chargée de résoudre le problème.
- ✓ Une description du problème.
- ✓ Une liste des logiciels impliqués, y compris leur version.
- ✓ Une description des diverses étapes mises en œuvre pour résoudre le problème.
- ✓ Une description de chacune des étapes intermédiaires, y compris l'annulation de celles qui n'ont servi à rien pour résoudre le problème.
- ✓ La date à laquelle le problème a été résolu.

Chapitre 21

Conserver la maîtrise du réseau et maintenir les utilisateurs à distance

Dans ce chapitre :

- ▶ Former les utilisateurs.
- ▶ Constituer une bibliothèque.
- ▶ Trouver des sources d'aide.
- ▶ Présenter des excuses.

Les administrateurs réseau n'ont pas la tâche facile. Les utilisateurs viennent les voir au moindre problème, lié ou non au réseau. Ils frappent à la porte s'ils n'arrivent pas à se connecter, s'ils ont perdu un fichier ou s'ils ne se rappellent plus comment on utilise le four à micro-ondes.

Ce chapitre passe en revue quelques petites astuces qui vous permettront de rendre votre vie d'administrateur réseau plus facile.

Former les utilisateurs

Une fois votre réseau opérationnel, invitez vos utilisateurs à l'École du réseau, pour leur apprendre comment se comporter sur le réseau. Montrez-leur de quelle façon se connecter, vérifiez qu'ils comprennent bien comment partager un fichier et expliquez-leur les règles.

Comme excellente entrée en matière, demandez-leur de lire les six premiers chapitres de ce livre. Souvenez-vous, ces chapitres ont été écrits à l'intention d'utilisateurs réseau, si bien qu'il n'y est question que de choses élémentaires. Si vos utilisateurs lisent d'abord ces chapitres, ils seront plus à même de poser des questions pertinentes.

Voici quelques moyens supplémentaires pour rendre la formation moins difficile pour vos utilisateurs et vous-même :

- ✓ **Écrivez un court résumé (une page environ) des connaissances de base en matière de réseau que doivent avoir vos utilisateurs.** Faites-y figurer l'ID de chacun, le nom des serveurs, les lettres des lecteurs, les imprimantes réseau et la procédure à suivre pour se connecter. Assurez-vous que chacun a bien reçu une copie de ce guide d'utilisation du réseau.
- ✓ **Insistez sur l'étiquette de la vie en réseau.** Vérifiez que chacun a bien compris que tout l'espace disque disponible sur le lecteur réseau n'était pas son espace personnel. Expliquez combien il convient de traiter les fichiers des autres avec respect. Suggérez-leur de toujours avertir les collègues avant de lancer un travail d'impression de trois heures.
- ✓ **Ce n'est pas parce que vous êtes administrateur du réseau qu'il faut avoir la grosse tête.** Si vous n'êtes pas un génie de l'informatique, ne prétendez pas l'être sous prétexte que vous en savez un peu plus que les autres. Soyez honnête avec vos utilisateurs, dites-leur que vous êtes tous dans le même sac et que vous ferez tout votre possible pour résoudre les problèmes qui pourraient survenir.

Constituer une bibliothèque

L'un des aspects les plus détestables de la fonction d'administrateur réseau est la propension des utilisateurs à vous prendre pour un expert connaissant parfaitement tous les programmes informatiques qu'ils utilisent. C'est parfaitement possible quand vous n'avez que deux utilisateurs travaillant uniquement avec Microsoft Word. Mais, si vous avez un véritable troupeau d'utilisateurs qui se sert d'une foule de programmes différents, il est presque impossible d'être expert en tout.

Le seul moyen de résoudre ce dilemme est de mettre en place une bibliothèque informatique bien fournie qui contienne les informations indispensables pour faire face à tous les problèmes se présentant. Quand un utilisateur vient vous ennuyer au sujet d'un problème inédit, vous pouvez lui répondre d'un ton rassurant : « Je vais régler cela dans quelques instants. »

Votre bibliothèque doit comprendre :

- ✓ **Un exemplaire de votre carnet de notes.** Il doit indiquer toutes les informations relatives à la configuration du réseau. Ne mettez pas l'original dans la bibliothèque ; conservez-le sous clé dans votre bureau.
- ✓ **Un exemplaire des manuels de chaque programme mis à disposition sur le réseau.** La plupart des utilisateurs ne se servent jamais de ces manuels, ils ne vous tiendront donc pas rigueur de cet « emprunt » pour votre bibliothèque. Si un utilisateur ne veut pas se séparer d'un manuel, notez où il se trouve.
- ✓ **Un exemplaire du Kit de ressources Windows pour chaque version de Windows utilisée sur le réseau.** Vous pouvez trouver le *Kit de ressources Windows* dans une librairie disposant d'un rayon informatique bien fourni.
- ✓ **Un exemplaire du ou des manuels du logiciel réseau.**
- ✓ **Au moins vingt exemplaires de ce livre.** Plus sérieusement, votre bibliothèque doit contenir des livres adaptés au niveau de votre expertise. Bien entendu, il existe des livres... *pour les Nuls* sur presque tous les sujets informatiques. C'est une bonne idée que de réserver une étagère entière à ces livres jaunes et noirs.

Rester informé de l'état de l'art

L'industrie informatique évolue rapidement et vos utilisateurs attendent probablement de vous que vous soyez au courant des dernières tendances et développements.

« Eh, Lucien, disent-ils, que pensez-vous de la dernière version de SkyWriter ? Devrions-nous l'installer ou conserver la version 23 ? »

« Nous voulons construire un site Web intranet. Quel est le meilleur éditeur de pages Web à moins de 150 euros ? »

« Mon fils veut acheter une carte son. Laquelle est la meilleure, la VideoPro ou la MovieMaker ? »

Le seul moyen de répondre à peu près intelligemment à ce genre de questions est de s'informer. Achetez les magazines informatiques qui vous conviennent. Voici quelques conseils pour être à la page :

- ✓ **Abonnez-vous à au moins un magazine informatique généraliste et à une revue spécialement destinée aux utilisateurs de réseaux.** De cette manière, vous vous tiendrez au courant des grandes tendances et vous vous documenterez sur des sujets plus spécifiques aux réseaux.

- ✓ **Abonnez-vous à des lettres d'information sur les systèmes que vous utilisez.**
- ✓ **Recherchez les magazines qui proposent à la fois de bons articles pédagogiques et des bancs d'essai sur les nouveaux produits.**
- ✓ **Ne sous-estimez pas la valeur des publicités dans les grands magazines informatiques.** Certaines personnes (dont moi) s'abonnent à ces magazines pour lire non seulement les articles mais aussi les publicités.
- ✓ **Gardez à l'esprit que presque tous les magazines informatiques sont très techniques.** Essayez de trouver des magazines adaptés à votre niveau. Après un an ou deux, il se pourrait que votre magazine ne vous fasse plus progresser et que vous deviez opter pour un autre, plus technique.

Le spécialiste a besoin d'un maître

Quel que soit votre niveau en informatique, nombreux sont ceux qui en savent plus que vous. La règle semble pouvoir s'appliquer à chaque barreau de l'échelle de l'expérience informatique. Je suis certain qu'un ultime barreau existe quelque part, occupé par le meilleur spécialiste informatique du monde. Mais je ne suis pas assis sur ce barreau et vous n'y êtes pas non plus. Bill Gates non plus d'ailleurs car, en fait, s'il en est arrivé là c'est parce qu'il a embauché des personnes occupant les barreaux du haut de l'échelle.

En tant que spécialiste informatique local, votre bien le plus précieux est cet ami qui est un cran ou deux au-dessus de vous sur l'échelle des gourous informatiques. Si vous êtes vraiment bloqué, vous pouvez l'appeler au secours. Voici quelques conseils pour prendre soin de votre « maître » :

- ✓ **N'oubliez pas la Règle d'or des gourous informatiques : « Fais appel à ton spécialiste comme tu voudrais que tes utilisateurs fassent appel à toi. »** Ne l'ennuyez pas avec des problèmes élémentaires auxquels vous n'avez tout simplement pas assez réfléchi. Mais, si vous avez retourné le problème dans tous les sens sans parvenir à trouver une solution, appelez votre maître. La plupart des experts informatiques aiment être confrontés à un problème informatique inhabituel. C'est génétique.
- ✓ **Si vous ne connaissez pas quelqu'un qui en sait plus que vous en informatique, rejoignez votre groupe local d'utilisateurs de PC.** Le groupe peut avoir un sous-groupe spécialisé dans les logiciels réseau ou peut tout simplement n'être formé que de personnes qui utilisent les mêmes logiciels que vous. Vous êtes certain de vous faire un ou deux amis lors d'une réunion du groupe.



Vous pouvez probablement convaincre votre patron de payer les frais d'inscription au groupe.

- ✔ **Si vous ne pouvez pas trouver un spécialiste en chair et en os, essayez d'en trouver un en ligne.** Explorez les divers groupes de discussion qui traitent de l'informatique sur Internet. Et abonnez-vous à des bulletins en ligne qui vous seront envoyés automatiquement par courrier électronique.

Excuses de l'administrateur réseau

En tant qu'administrateur réseau, vous ne serez parfois pas capable de résoudre un problème ou du moins pas immédiatement. Dans ce cas, vous avez deux solutions.

La première est d'expliquer que le problème est particulièrement difficile et que vous allez tenter de trouver la solution aussi vite que possible.

La seconde est de mentir. Voici quelques-unes de mes excuses favorites et autres explications bidon :



- ✔ C'est toujours la faute à la *version* du logiciel (peu importe lequel) que vous utilisez.
- ✔ C'est la faute à cette mémoire pas chère importée d'on ne sait où.
- ✔ C'est la faute à la droite. Ou à la gauche. Ou à l'extrême centre. Peu importe.
- ✔ J'espère que le problème n'a pas été causé par une décharge d'électricité statique. Cette cause de dysfonctionnement est très difficile à établir. Les utilisateurs qui ne se déchargent pas de leur électricité statique avant de se servir de leur ordinateur peuvent causer des problèmes.
- ✔ Votre ordinateur a besoin de plus de mémoire.
- ✔ Votre ordinateur a besoin d'un disque dur plus gros.
- ✔ Vous avez besoin d'un ordinateur multiprocesseur pour faire cela.
- ✔ C'est la faute à Jar Jar Binks.
- ✔ Vous devez migrer vers Windows 7.
- ✔ Vous n'utilisez pas Windows 7. Je me trompe ?
- ✔ Ça ressemble à un virus.
- ✔ Ou à des taches solaires.
- ✔ Ça ira mieux demain.

Cinquième partie

Protéger le réseau



« Oh, Arthur est très soucieux de la sécurité sur le Web.
Il ne se connecte jamais dans la même pièce deux jours consécutifs. »

Dans cette partie...

La protection du réseau est l'une des tâches principales de l'administrateur. En effet, le monde est plein de personnages étranges qui tirent gloire de s'introduire dans un réseau informatique et de réussir à le mettre à genoux.

Les chapitres de cette partie décrivent les actions les plus importantes que l'administrateur réseau doit mettre en œuvre pour garantir la sécurité de son réseau. Vous apprendrez à sauvegarder les données sensibles, à protéger le réseau contre les virus et autres menaces et à surveiller votre connexion Internet pour vous préserver des intrus.

Chapitre 22

Sauvegarder les données

Dans ce chapitre :

- ▶ Comprendre l'utilité des sauvegardes.
- ▶ Travailler avec des lecteurs de bandes et d'autres supports de sauvegarde.
- ▶ Comprendre les différents types de sauvegarde.
- ▶ Définir le nombre de sauvegardes à conserver.
- ▶ Maîtriser la rotation des bandes.
- ▶ Nettoyer les têtes de lecture.
- ▶ Sauvegarder en toute sécurité.

Si vous êtes administrateur réseau, pas de chance, la sauvegarde des données du réseau vous incombe ! Vous êtes payé pour vous faire un sang d'encre, à ne pas pouvoir en dormir la nuit. Vos données seront-elles toujours là demain ? Sinon, serez-vous en mesure de les récupérer ? Et (plus important) si vous n'y parvenez pas, serez-vous encore là vous-même ?

Ce chapitre traite de la conduite à adopter pour être un bon administrateur réseau, responsable et digne de confiance. Personne ne vous donnera de médaille pour ce travail et c'est dommage.

Sauvegarder les données

Des sauvegardes effectuées régulièrement sont un rempart efficace contre tout désastre informatique. Sans elles, une simple défaillance du disque dur peut renvoyer votre entreprise des jours ou des semaines en arrière, sans que vous ayez la garantie de pouvoir reconstituer les données manquantes. En fait, sans sauvegarde, l'existence même de votre société est livrée au hasard.



Le principal objectif des sauvegardes est simple : vous assurer que, quoi qu'il puisse se produire, vous ne perdrez jamais plus d'une journée de travail. Même si la Bourse s'effondre, vous ne perdrez jamais plus d'une journée de travail si vous veillez à toujours bien effectuer vos sauvegardes.

Pour cela, il faut bien sûr que les données soient sauvegardées quotidiennement. Sur bon nombre de réseaux, cette opération est effectuée chaque nuit pour chacun des disques durs. Mais, si des sauvegardes nocturnes ne sont pas envisageables, vous adopterez néanmoins des techniques qui garantissent qu'aucune copie de sauvegarde d'un fichier n'ait plus d'un jour.

Tout sur les bandes et les lecteurs de bandes

Vous aurez besoin d'un support si vous projetez de sauvegarder les données stockées sur les disques de votre serveur. Vous pourriez copier les données sur des CD mais il en faudrait 750 pour sauvegarder le contenu d'un disque de 500 Go ; vous pourriez aussi utiliser des DVD, il en faudrait alors une bonne centaine et passer une heure pour chacun d'eux.



Étant donné la capacité limitée des CD et des DVD, les administrateurs réseau utilisent des bandes magnétiques pour leurs sauvegardes. Selon la marque et le modèle de bande, vous pouvez stocker au moins 800 Go sur chacune d'elles.

La sauvegarde sur bande ne requiert pas la présence de l'administrateur. Elle peut être programmée et s'exécuter automatiquement, en particulier pendant les heures creuses, celles où aucun utilisateur n'est connecté. Pour que les sauvegardes puissent s'exécuter automatiquement, vous devez vous assurer que la capacité des bandes est suffisante et qu'il n'y aura pas besoin de les permuter. Si les données des disques réseau représentent quelques centaines de gigaoctets, elles tiendront sans problème sur une seule bande. Si elles représentent plusieurs téraoctets (1 téraoctet = 1 000 Go), il faudra investir dans un robot de sauvegarde équipé d'un magasin de bandes.

Voici quelques informations supplémentaires sur les sauvegardes sur bande :

- ✓ Pour les petits réseaux, les lecteurs Travan sont le type de bandes le plus répandu. Il en existe plusieurs modèles, dont la capacité va de 20 Go à 40 Go. Vous pouvez acheter un lecteur de 20 Go pour environ 200 euros.
- ✓ Pour de plus grands réseaux, vous pouvez utiliser un lecteur plus rapide et de plus grande capacité que les lecteurs Travan. Les lecteurs DAT (*Digital Audio Tape*, bande audionumérique) peuvent sauvegarder jusqu'à 80 Go sur une seule bande et les lecteurs DLT (*Digital Linear Tape*, bande linéaire numérique), jusqu'à 200 Go. Vous trouverez des lecteurs DAT et DLT à partir de 1 000 euros.

- ✓ Si vous devez sauvegarder des centaines de gigaoctets, vous pouvez acquérir des robots de sauvegarde qui vont chercher les cartouches dans une bibliothèque et les chargent automatiquement dans le lecteur. Ils vous permettent d'effectuer des sauvegardes complètes sans avoir à manipuler les bandes. Les plus petits, avec une bibliothèque pouvant contenir huit cartouches et une capacité de sauvegarde supérieure à 5 000 Go, sont vendus à partir de 4 000 euros.

Logiciels de sauvegarde

Toutes les versions de Windows possèdent un programme de sauvegarde intégré. En outre, la plupart des lecteurs de bandes sont livrés avec des programmes de sauvegarde plus souples que celui de Windows.

Vous pouvez également acheter des programmes de sauvegarde sophistiqués, particulièrement conçus pour les réseaux et les serveurs multiples. Pour un serveur de fichiers sous Windows, vous pouvez utiliser le programme de sauvegarde livré avec Windows Server. Les sauvegardes peuvent être planifiées, après quoi le programme s'occupe de tout.

Les programmes de sauvegarde font bien plus que de copier les données de votre disque dur sur des bandes. Ils utilisent une technique de compression particulière qui permet de stocker davantage de données sur moins de bandes. Des facteurs de compression 2:1 sont courants. Ainsi, vous pouvez stocker 100 Go sur une bande qui ne peut contenir que 50 Go de données non compressées. Les fabricants de lecteurs de bandes tendent à exprimer la capacité de leurs lecteurs compression comprise. Avec un facteur de 2:1, un lecteur de 200 Go a donc une capacité de 100 Go sans la compression.

L'obtention d'un facteur de compactage de 2:1 dépend de la nature des données que vous sauvegardez :



- ✓ Si les données à sauvegarder sont essentiellement constituées de documents Office tels que Word et Excel, vous obtiendrez probablement plus qu'un compactage de 2:1.
- ✓ Si les données à sauvegarder sont essentiellement constituées de fichiers images et graphiques, vous n'obtiendrez probablement qu'un très faible compactage. En effet, la plupart des formats images sont déjà compressés et les méthodes de compression des logiciels de sauvegarde n'ont pratiquement aucun effet.

Les programmes de sauvegarde vous aident également à distinguer les données sauvegardées des données non sauvegardées. En outre, ils offrent des options de sauvegarde incrémentielle et différentielle qui peuvent simplifier les procédures. La section suivante vous en dit plus sur le sujet.



Si votre réseau comporte plusieurs serveurs, n'hésitez pas à investir dans un bon logiciel de sauvegarde. Yosemite est l'un des plus populaires. Pour plus d'informations, consultez le site de son fournisseur, BarracudaWare : www.barracudaware.com. Outre la sauvegarde de serveurs multiples, la possibilité de sauvegarder les données d'un serveur Microsoft Exchange à chaud (c'est-à-dire sans devoir interrompre le service) est l'un des principaux avantages des logiciels de sauvegarde tels que Yosemite.

Types de sauvegarde

Il existe cinq types de sauvegarde. Quelques administrateurs exécutent quotidiennement une sauvegarde complète mais, pour certains réseaux, il est plus commode d'adopter une démarche mettant en œuvre plusieurs types de sauvegarde.

La différence entre ces cinq types de sauvegarde repose sur un petit détail technique connu sous le nom de *bit d'archive*. Il indique si un fichier a été modifié depuis la dernière sauvegarde. Le bit d'archive est un petit drapeau stocké avec le nom de fichier, sa date de création, l'entrée de répertoire et d'autres informations. Lorsqu'un programme modifie le fichier, le bit d'archive est mis à 1 (état actif). Le logiciel d'archivage sait ainsi que le fichier a été modifié et qu'il doit être sauvegardé.

La différence entre les divers types de sauvegarde dépend de la manière dont ils exploitent le bit d'archive pour savoir si un fichier doit être sauvegardé et la façon dont ils basculent ensuite le bit à la valeur 0 (état inactif). Ces différences sont récapitulées dans le Tableau 22.1 et expliquées dans les prochaines sections.



Un programme de sauvegarde permet de sélectionner n'importe quel agencement de lecteurs et de dossiers à archiver. C'est pourquoi il est possible de personnaliser la sélection des fichiers à prendre en compte. Par exemple, une sauvegarde pourra être paramétrée afin d'archiver tous les dossiers partagés ainsi que le contenu des serveurs de courrier, en omettant les dossiers dont le contenu change rarement (c'est le cas des fichiers du système d'exploitation qui peuvent être sauvegardés moins fréquemment). Les lecteurs et dossiers sélectionnés pour la sauvegarde sont globalement appelés *sélection de sauvegarde*.

Tableau 22.1 : Utilisation du bit d'archive selon les types de sauvegarde.

Type de sauvegarde	Sélection des fichiers en fonction de l'état du bit d'archive ?	Désactivation du bit d'archive après la sauvegarde ?
Normal	Non	Oui
Copie	Non	Non
Quotidien	Non*	Non
Incrémentiel	Oui	Oui
Différentiel	Oui	Non

*Sélection des fichiers selon la date de la dernière modification.



S'il avait été connu à l'époque, le bit d'archive aurait pu inspirer Laurel et Hardy : « Bien, je veux savoir qui a modifié le bit d'archive – Quoi ? – Qui ? – Non, quoi ? – Attends un peu... Dis-moi juste quel est le type qui a modifié le bit d'archive ! – OK. »

Sauvegardes normales

Une *sauvegarde normale*, appelée aussi *sauvegarde complète* ou encore *sauvegarde totale*, est le type d'archivage le plus élémentaire. Lors d'une sauvegarde normale, tous les fichiers de la sélection de sauvegarde sont archivés, quel que soit l'état de leur bit d'archive. Autrement dit, les fichiers sont sauvegardés même s'ils n'ont pas été modifiés depuis la dernière sauvegarde. Au cours de l'opération d'archivage, le bit est réinitialisé à zéro (état inactif). Ainsi, toute sauvegarde qui sélectionnerait les fichiers selon l'état du bit d'archivage n'archiverait pas ces fichiers.

À la fin d'une sauvegarde normale, plus aucun des fichiers de la sélection de sauvegarde n'a son bit d'archive à l'état actif. De ce fait, si vous démarrez aussitôt une sauvegarde de type incrémentiel ou différentiel, aucun fichier ne sera pris en compte car leur bit d'archive est inactif.

Ce type de sauvegarde gagne à être planifié chaque nuit. Au besoin, vous pourrez restaurer des fichiers à partir de la ou des bandes. La restauration des fichiers est plus compliquée lorsque d'autres types de sauvegarde sont impliqués.



Par conséquent, je vous recommande de procéder à des sauvegardes normales chaque nuit si la capacité des bandes magnétiques permet de les laisser sans surveillance, c'est-à-dire sans devoir les changer lorsqu'elles sont pleines. Si ce n'est pas possible, faute de capacité de stockage suffisante, vous opterez pour un autre type de sauvegarde, combiné à la sauvegarde normale.



Si une seule bande est insuffisante pour une sauvegarde normale et si vous n'avez pas les moyens de vous offrir un second lecteur de bande, examinez de près les données incluses dans la sélection de sauvegarde. Il m'est récemment arrivé de rencontrer des problèmes pour sauvegarder un réseau sur une seule bande. Après avoir examiné les données, j'ai découvert près de 5 Go de données statiques qui étaient essentiellement des archives en ligne de projets anciens. Ces données étaient indispensables car les utilisateurs du réseau en avaient besoin pour leurs recherches mais elles étaient en lecture seule. Bien qu'elles ne puissent pas être modifiées, elles n'en étaient pas moins sauvegardées chaque nuit, d'où la nécessité de recourir à deux bandes. Après les avoir retirées de la sauvegarde nocturne, une bande s'est avérée suffisante pour l'archivage.

Si vous retirez des données statiques d'une sauvegarde, assurez-vous qu'elles ont été enregistrées sur une autre bande, un CD ou tout autre support.

Copies de sauvegarde

Une *copie de sauvegarde* est identique à une sauvegarde normale, sauf que le bit d'archive des fichiers n'est pas remis à zéro. Par conséquent, les copies de sauvegarde n'interrompent pas le cycle des sauvegardes normales, incrémentielles ou différentielles.

Les copies de sauvegarde ne sont généralement pas incorporées à des sauvegardes normales planifiées. Elles sont, au contraire, utilisées pour des sauvegardes ponctuelles. Par exemple, si vous êtes sur le point de mettre le système d'exploitation à jour, vous devrez sauvegarder le contenu du serveur. Si vous effectuez une sauvegarde complète, tous les bits d'archives seront remis à zéro et vos sauvegardes habituelles seront faussées. Mais, si vous effectuez une copie de sauvegarde, les bits d'archives des fichiers modifiés restent inchangés. Par la suite, la sauvegarde normale, incrémentielle ou différentielle n'en pâtira pas.

Si vous n'incorporez pas de sauvegarde incrémentielle ou différentielle dans vos routines d'archivage, la différence entre une sauvegarde normale et une copie de sauvegarde est discutable.

Sauvegardes journalières

Une *sauvegarde journalière* ou *sauvegarde du jour* ne concerne que les fichiers modifiés le jour où la sauvegarde est effectuée. Une sauvegarde du jour examine la date de modification stockée dans l'entrée de répertoire de chaque fichier et en déduit si le fichier doit être sauvegardé ou non. Les sauvegardes du jour ne remettent pas le bit d'archive à zéro.

Je ne suis pas fan de cette option car le risque que des fichiers passent entre les mailles est très faible. Si quelqu'un travaille tard le soir et modifie un fichier après la sauvegarde de la nuit mais avant minuit, ce fichier échappera à la sauvegarde car le lendemain il ne sera plus « du jour ». Les sauvegardes incrémentielles ou différentielles, qui se basent sur l'état du bit d'archive plutôt que sur la date de modification, sont plus fiables.

Sauvegardes incrémentielles

Une *sauvegarde incrémentielle* n'archive que les fichiers modifiés depuis la dernière sauvegarde. Ce type de sauvegarde est beaucoup plus rapide qu'une sauvegarde complète car les utilisateurs du réseau ne modifient sans doute quotidiennement qu'assez peu de fichiers du serveur. Par conséquent, si une sauvegarde complète exige trois bandes, une sauvegarde incrémentielle parviendra sans doute à faire tenir les sauvegardes de toute la semaine sur une seule bande.

Lors d'une sauvegarde incrémentielle, les bits d'archives des fichiers sont remis à zéro. De cette manière, un fichier n'est sauvegardé avant la prochaine sauvegarde normale que s'il est de nouveau modifié par un utilisateur.

Voici quelques remarques concernant les sauvegardes incrémentielles :



- ✓ Le moyen le plus facile de procéder à des sauvegardes incrémentielles consiste à effectuer :
 - une sauvegarde *normale* tous les lundis ;
 - Si la sauvegarde totale dure plus de 12 heures, vous pouvez la commencer le vendredi de sorte qu'elle puisse déborder sur le week-end.
 - puis des sauvegardes *incrémentielles* le mardi, le mercredi, le jeudi et le vendredi.
- ✓ Quand vous faites des sauvegardes incrémentielles, la sauvegarde complète est constituée de la totalité des bandes auxquelles s'ajoutent les sauvegardes incrémentielles effectuées depuis la sauvegarde complète.

Si le disque dur tombe en panne et que vous devez restaurer les données sur un nouveau disque, vous restaurerez d'abord la sauvegarde normale du lundi puis toutes les sauvegardes incrémentielles réalisées depuis.
- ✓ Les sauvegardes incrémentielles compliquent la tâche de restauration de tel ou tel fichier car la copie la plus récente peut se trouver dans la bande de la sauvegarde complète ou dans n'importe quelle sauvegarde incrémentielle.



Fort heureusement, les logiciels de sauvegarde savent où se trouve la version la plus récente de chaque fichier, ce qui simplifie les choses.

✓ Lors des sauvegardes incrémentielles, vous avez le choix entre :

- Le **stockage** de chaque sauvegarde incrémentielle sur sa propre bande.
- L'**ajout** de chaque sauvegarde à la suite d'une autre.

Dans bien des cas, une seule bande est suffisante pour la totalité des sauvegardes incrémentielles de la semaine.

Sauvegardes différentielles

Une *sauvegarde différentielle* est identique à une sauvegarde incrémentielle, sauf qu'elle ne remet pas à zéro le bit d'archive des fichiers sauvegardés. De ce fait, chaque sauvegarde différentielle correspond à la différence entre la dernière sauvegarde normale et l'état courant du disque dur.

Pour procéder à une restauration à partir d'une sauvegarde différentielle, vous devez d'abord restaurer la dernière sauvegarde normale puis la sauvegarde différentielle la plus récente.

Par exemple, supposons que vous effectuiez une sauvegarde normale le lundi et des sauvegardes différentielles le mardi, le mercredi et le jeudi, et que votre disque dur tombe en panne le vendredi matin. Le vendredi après-midi, vous installez le nouveau disque dur. Pour récupérer les données, vous restaurez d'abord la sauvegarde normale du lundi puis la sauvegarde différentielle du jeudi. Celles du mardi et du mercredi ne sont pas nécessaires.

La principale différence entre les sauvegardes incrémentielles et différentielles réside dans le fait que :

- ✓ Les **sauvegardes incrémentielles** produisent des sauvegardes moins nombreuses et plus rapides.
- ✓ Les **sauvegardes différentielles** sont plus faciles à restaurer.

Si les utilisateurs vous demandent fréquemment de restaurer des *fichiers isolés*, vous choisirez plutôt la sauvegarde différentielle.



Sauvegardes locales ou sauvegardes sur le réseau ?

Lorsque vous sauvegardez des données du réseau, le logiciel de sauvegarde vous propose deux choix : effectuer une *sauvegarde locale*, au cours de laquelle le logiciel de sauvegarde situé sur le serveur enregistre les données sur une bande reliée au serveur ou une *sauvegarde sur le réseau*, au cours de laquelle un des ordinateurs du réseau se charge de sauvegarder les données d'un autre ordinateur. Dans ce cas, les données doivent voyager sur le réseau entre les deux ordinateurs.

Si la sauvegarde est régie par le serveur de fichiers, vous accaparez le serveur au cours de l'opération. Les utilisateurs se plaindront de la lenteur des accès au serveur. Par ailleurs, si la sauvegarde est faite sur le réseau, d'un ordinateur client ou d'un serveur d'archivage dédié, vous inonderez le réseau avec les gigaoctets de données en train d'être sauvegardés. Là, c'est de la lenteur de tout le réseau que se plaindront les utilisateurs.

Le maintien des performances du réseau justifie les sauvegardes en dehors des heures de travail, lorsque le réseau est peu fréquenté. Autre avantage : les sauvegardes peuvent être plus minutieuses. En effet, lorsqu'une sauvegarde est en cours alors que des utilisateurs accèdent à des fichiers, ces derniers risquent d'être ignorés et donc exclus de l'archivage. Paradoxalement, les fichiers les plus utilisés et modifiés échapperont à la sauvegarde.

Voici quelques remarques supplémentaires au sujet des sauvegardes depuis le serveur :

- ✓ Vous pourriez penser que sauvegarder directement sur le serveur plutôt que depuis un client est plus rapide car les données n'ont pas à circuler sur le réseau. Ce n'est pas toujours le cas car la plupart des réseaux sont plus rapides que les lecteurs de bandes. Le réseau ne ralentira probablement pas les sauvegardes, à moins que vous ne sauvegardiez à l'heure de pointe, quand des hordes d'utilisateurs déboulent par les portes du réseau.
- ✓ Afin d'accélérer les sauvegardes et de réduire leurs effets sur le reste du réseau, connectez le serveur au client de reprise à l'aide d'un commutateur à 1 000 Mbps plutôt qu'un commutateur à 100 Mbps. De cette manière, le trafic entre le serveur et le client de reprise ne ralentira pas le réseau.
- ✓ Tout fichier ouvert au moment de la création des sauvegardes ne sera pas sauvegardé. Cela ne pose généralement pas de problème car les sauvegardes sont effectuées en dehors des heures de travail, lorsque tout le monde a déserté les bureaux. Cependant, si quelqu'un a laissé



son ordinateur allumé, avec un document Word ouvert, ce dernier ne sera pas sauvegardé. Pour remédier à cela, il existe une solution : programmer le serveur pour qu'il déconnecte automatiquement tous les utilisateurs du réseau avant l'exécution des sauvegardes.

- ✓ Certains logiciels de sauvegarde sont dotés de fonctions spéciales qui leur permettent de sauvegarder des fichiers ouverts. Par exemple, Windows Server 2003 le fait en créant un instantané du volume au début de la sauvegarde, générant ainsi des copies temporaires de tous les fichiers modifiés pendant la sauvegarde. La sauvegarde archive ces copies temporaires plutôt que les versions modifiées. La sauvegarde terminée, les copies temporaires sont supprimées.

Combien de jeux de sauvegardes faut-il conserver ?

Ne cherchez pas à faire des économies en achetant une seule bande et en la réutilisant chaque jour. Que se passera-t-il si vous supprimez accidentellement un fichier important un mardi et que vous ne réalisiez votre erreur que le jeudi ? Le fichier n'existant plus le mercredi, il ne sera donc pas présent sur la sauvegarde du mercredi. Vous avez intérêt à être plutôt chanceux si vous ne disposez que d'une bande réutilisée tous les jours.

Il est plus sûr de prendre une nouvelle bande chaque jour et de garder toutes vos vieilles bandes dans une cave. Il se peut que très bientôt votre cave commence à ressembler à l'entrepôt où est stockée l'Arche d'alliance à la fin des *Aventuriers de l'Arche perdue*.



La plupart des administrateurs choisissent une solution intermédiaire : ils se servent de plusieurs bandes et les font tourner. De cette manière, vous pouvez toujours chercher sur plusieurs bandes précédentes au cas où un fichier dont vous auriez besoin ne serait pas disponible sur la sauvegarde la plus récente. Cette technique est nommée *rotation des bandes* et il en existe plusieurs variantes :

- ✓ L'approche la plus simple consiste à acheter trois bandes et à les étiqueter A, B et C. Vous utilisez ces bandes quotidiennement selon la séquence suivante : A, B, C, A, B, C, et ainsi de suite. Vous aurez chaque jour trois générations de bandes : aujourd'hui, hier et avant-hier. Les experts informatiques aiment appeler ces bandes *grand-père*, *père* et *fils*.
- ✓ Une autre approche triviale consiste à acheter cinq bandes et à en choisir une pour chaque jour de la semaine.

- ✓ Une variante de cette méthode consiste à acheter huit bandes. Prenez-en quatre et écrivez *lundi* sur l'une, *mardi* sur une autre, *mercredi* sur la troisième et *jeudi* sur la quatrième. Sur les quatre autres bandes, écrivez *vendredi 1*, *vendredi 2*, *vendredi 3* et *vendredi 4*. Accrochez maintenant un calendrier sur le mur, à côté de l'ordinateur et numérotez tous les vendredis de l'année : 1, 2, 3, 4, 1, 2, 3, 4, et ainsi de suite.

Du lundi au jeudi, vous vous servez de la bande qui porte le nom du jour. Quand vous devez effectuer la sauvegarde du vendredi, consultez le calendrier pour identifier la bande à utiliser. Vous pourrez ainsi conserver quatre bandes contenant les sauvegardes de quatre vendredis, en plus des bandes de sauvegarde des cinq derniers jours.

- ✓ Si des données comptables figurent sur le réseau, il est conseillé de faire une copie de sauvegarde de tous vos fichiers (ou au moins des fichiers comptables), avant de clore l'exercice mensuel et de conserver ces sauvegardes mensuelles durant toute l'année. Cela signifie-t-il que vous devez acheter douze autres bandes ? Pas nécessairement. Si vous ne sauvegardez que vos fichiers comptables, vous pourrez sans doute faire tenir les douze mois sur une seule bande. Vérifiez simplement que vous sélectionnez bien l'option « ajouter à la bande » et non « effacer la bande » afin que les données de la dernière version ne soient pas détruites. Cette sauvegarde des données comptables doit être complètement indépendante de votre sauvegarde quotidienne.

Vous devriez aussi conserver au moins la plus récente des sauvegardes à un autre endroit. De cette manière, si votre bureau est victime d'un missile Scud égaré ou d'un astéroïde, vous pourrez récupérer les données de la bande que vous aurez conservée en lieu sûr.

Un mot sur la fiabilité des bandes

Je parle en connaissance de cause. Bien que les lecteurs de bandes soient très fiables, j'ai remarqué qu'ils perdent parfois la tête, sans vous prévenir. Un lecteur de bandes (et plus particulièrement les lecteurs Travan les moins chers) peut tourner pendant de longues heures sans sauvegarder vos données. Autrement dit, un lecteur de bandes peut vous tromper et vous risquez de découvrir que les bandes sont inutilisables seulement à la suite d'un désastre.

Ne paniquez pas ! Vous n'avez qu'à vous assurer par vous-même que votre lecteur de bandes fonctionne bien. Activez tout simplement l'option Comparer après la sauvegarde de votre logiciel de sauvegarde. Aussitôt que le programme aura fini de sauvegarder vos données, il rembobinera la bande,



lira chaque fichier sauvegardé et le comparera avec la version originale sur le disque. Si toutes les comparaisons sont validées, vous saurez que vos sauvegardes sont dignes de confiance.

Voici quelques notes supplémentaires sur la fiabilité des bandes :

- ✓ La fonction de comparaison double le temps nécessaire pour effectuer une sauvegarde, ce qui a peu d'incidence si une seule bande vous suffit car vous pouvez simplement laisser tourner le lecteur après les heures de travail. Peu importe que cela prenne une heure ou dix heures, du moment que la sauvegarde est terminée le lendemain matin quand vous revenez au bureau.
- ✓ Si vos sauvegardes tiennent sur plusieurs bandes, vous n'activerez peut-être pas l'option de comparaison à chaque fois. Cependant, utilisez-la périodiquement pour vérifier que votre lecteur fonctionne bien.
- ✓ Si votre programme de sauvegarde vous signale une erreur, jetez la bande et prenez-en une nouvelle.
- ✓ À vrai dire, à propos du dernier point, vous ne devriez même pas attendre que le logiciel de sauvegarde signale une erreur et mettre la bande au rebut bien avant. Selon la plupart des experts, une bande ne devrait être utilisée que vingt fois. Si vous l'utilisez quotidiennement, remplacez-la chaque mois. Si vous avez une bande pour chaque jour de la semaine, remplacez-les deux fois par an. Si vous avez un grand nombre de bandes, essayez de déterminer des cycles de vingt utilisations et pensez aussi à nettoyer les têtes de lecture.

Nettoyer les têtes de lecture

Eh oui, la fiabilité des sauvegardes repose aussi sur un bon entretien des lecteurs de bandes. Chaque fois que vous procédez à une sauvegarde, de microscopiques fragments de bande sont attirés par les têtes de lecture et d'écriture. S'ils sont trop nombreux, ils peuvent compromettre la lecture et l'écriture des données.

C'est pourquoi vous devez entretenir régulièrement les têtes. Le meilleur moyen consiste à utiliser une cartouche de nettoyage que vous insérez dans le lecteur. Le lecteur reconnaît qu'il s'agit d'une cartouche de nettoyage et exécute aussitôt une routine spéciale qui fait aller et venir la bande contre des tampons. Le nettoyage terminé, la bande est éjectée. La procédure complète ne dure qu'une trentaine de secondes.

Comme les exigences d'entretien varient d'un équipement à un autre, reportez-vous au manuel pour savoir comment le nettoyer (l'équipement, pas le manuel !). En règle générale, un lecteur doit être nettoyé chaque semaine.

Le seul ennui, avec les cartouches de nettoyage, est leur durée de vie très limitée. Même si la cartouche est encrassée, le lecteur ne refusera jamais de l'utiliser. C'est pourquoi il est recommandé de noter le nombre de fois qu'elle est utilisée puis de la jeter lorsque vous avez dépassé le nombre d'utilisations préconisé par le fabricant.

Sécurité des sauvegardes

Les sauvegardes soulèvent des problèmes de sécurité qui sont souvent mésestimés. Quel que soit le soin avec lequel vous configurez les comptes utilisateurs et renforcez les conventions de mots de passe, si un utilisateur (y compris un visiteur) est capable d'exécuter une sauvegarde sur le système, il peut aussi exécuter une sauvegarde non autorisée. De plus, les bandes et les lecteurs amovibles sont exposés au vol. Vous devez donc prendre les mesures suivantes :

- ✓ Définissez un compte utilisateur pour les utilisateurs qui effectuent des sauvegardes. Comme ce compte bénéficiera d'une autorisation de sauvegarde de la totalité du serveur, le mot de passe doit être soigneusement protégé. Car quiconque connaît le nom d'utilisateur et le mot de passe pourra ouvrir une session et outrepasser toutes les restrictions sécuritaires.
- ✓ Vous pouvez contrer les problèmes de sécurité en restreignant l'identifiant (ID) de l'utilisateur qui fait les sauvegardes à un certain ordinateur client et à des moments précis de la journée. Si vous y tenez, il est même possible de faire en sorte que le seul programme que cet utilisateur puisse exécuter soit le programme de sauvegarde.
- ✓ Cryptez les sauvegardes enregistrées sur les bandes.
- ✓ Rangez les bandes en lieu sûr, dans un coffre par exemple.

Chapitre 23

Sécuriser le réseau

Dans ce chapitre :

- ▶ Évaluer le niveau de sécurité requis.
- ▶ Définir la sécurité de base.
- ▶ Protéger physiquement l'équipement du réseau.
- ▶ Sécuriser les comptes utilisateurs.
- ▶ Autres techniques de sécurisation du réseau.
- ▶ Garantir la sécurité des utilisateurs.

Avant le réseau, la sécurité informatique était une question simple. Vous n'aviez qu'à fermer votre porte quand vous quittiez le travail en fin de journée. Vous pouviez dormir tranquille, sachant que les malfaiteurs devaient fracturer votre porte pour accéder à votre ordinateur.

Le réseau a tout changé. Maintenant, n'importe qui peut accéder à un ordinateur du réseau et voler *vos* fichiers. Vous devez non seulement fermer votre porte mais également vous assurer que les autres en font autant.

Heureusement, presque tous les systèmes d'exploitation réseau disposent de fonctionnalités de sécurité intégrées. Cette situation rend plus difficile le vol de vos fichiers même si l'on fracture votre porte. Ces mesures de sécurité sont plus qu'appropriées pour tous les utilisateurs, exception faite des paranoïaques.

Quand je dis *plus* qu'appropriées, je veux dire presque trop. Ne sécurisez pas votre système au point que même les personnes autorisées ne puissent plus accéder à leurs travaux !





Si des ordinateurs de votre réseau sont connectés à Internet, vous devrez prendre en considération une nouvelle dimension de la sécurité. Reportez-vous au Chapitre 24 pour plus d'informations sur la sécurité Internet. En outre, si votre réseau comprend du matériel sans fil, vous devez prendre en compte des problèmes spécifiques de sécurité. Pour en savoir plus sur la sécurité des réseaux sans fil, lisez le Chapitre 9.

Besoin de sécurité ?

La plupart des petits réseaux se trouvent dans de petites structures où tout le monde se connaît et se fait confiance. Personne ne verrouille son bureau pour aller prendre un café et bien que chacun sache où se trouve la caisse, l'argent ne disparaît jamais.

Sécuriser le réseau ne semble pas nécessaire dans une situation aussi idyllique, n'est-ce pas ? Erreur ! Voici pourquoi le réseau doit être configuré en respectant un minimum de sécurité :

- ✓ Même dans le plus convivial des environnements de travail, il y a toujours une information qui doit rester confidentielle. Si cette information est stockée sur le réseau, elle doit être placée dans un répertoire auquel seuls les utilisateurs autorisés ont accès.
- ✓ Les atteintes à la sécurité ne sont pas toutes malveillantes. Un utilisateur du réseau peut être machinalement en train de passer en revue ses fichiers et tomber sur un fichier dont le nom ne lui est pas familier. Il peut alors rapatrier le fichier sur son disque et découvrir qu'il contient une information personnelle et confidentielle, un gros ragot de bureau ou votre CV. La curiosité, plus que la volonté délibérée de nuire, est souvent à l'origine des atteintes à la sécurité.
- ✓ Bien entendu, tous vos collègues de bureau sont aujourd'hui dignes de confiance. Mais que se passe-t-il si quelqu'un est mécontent, « pète les plombs » et décide de détruire les fichiers du réseau avant de donner sa démission ? Et si la même personne décide plutôt d'imprimer plusieurs chèques de 1 000 euros avant de faire ses bagages pour Tahiti ?
- ✓ Pour certaines personnes, la tentation de voler ou de frauder est parfois trop forte pour résister. Donnez accès au fichier des feuilles de paie à tout le monde et il se pourrait que le personnel décide de s'accorder une augmentation quand personne ne regarde.
- ✓ Si vous estimez que votre réseau ne contient aucune donnée qui puisse intéresser quelqu'un, pensez-y à deux fois. Vos données personnelles contiennent sans doute suffisamment d'informations pour permettre une usurpation d'identité : votre nom, votre adresse, vos numéros de téléphone, de sécurité sociale, voire celui de votre carte bancaire.

- ✓ Les intrus qui pénètrent par effraction dans votre réseau peuvent installer sur le serveur un *cheval de Troie*, qui leur permet ensuite d'en disposer à leur guise. Par exemple, ils pourront utiliser votre serveur pour envoyer par messagerie des milliers, voire des millions de messages. Il sera impossible de faire un lien entre ce spam et les intrus. C'est vous qui endosserez toute la responsabilité.
- ✓ Pour finir, rappelez-vous que beaucoup d'utilisateurs n'en savent pas assez long sur le fonctionnement de Windows et du réseau pour qu'il soit raisonnable de leur accorder des accès complets à vos disques réseau. Un clic de souris malheureux peut faire disparaître un répertoire entier du réseau. L'une des meilleures raisons pour activer la sécurité réseau, c'est de protéger les utilisateurs contre des erreurs commises par d'autres utilisateurs qui ne savent pas ce qu'ils font.

Deux approches de la sécurité

Quand vous envisagez l'implémentation de mesures de sécurité dans votre réseau, vous devez d'abord considérer laquelle de ces deux approches vous adopterez :

- ✓ Une sécurité de type **porte ouverte**, dans laquelle, par défaut, tout le monde accède à tout, après quoi vous placez des restrictions aux ressources dont l'accès doit être limité.
- ✓ Une sécurité de type **porte fermée** où vous commencez par refuser l'accès à tout, après quoi vous accordez des accès aux ressources au coup par coup, à des utilisateurs spécifiques. Dans la plupart des cas, le système « porte ouverte » est le plus facile à mettre en œuvre. Classiquement, seule une petite partie des données qui circulent sur le réseau (fiches signalétiques des employés, formule de l'extrait de base du Coca-Cola...) nécessite d'être sécurisée. Les autres informations peuvent circuler au vu et au su de tout le monde.

Si vous choisissez l'approche « porte fermée », vous commencez par faire en sorte qu'aucun utilisateur n'ait accès à quoi que ce soit. Ensuite, au fil des demandes, vous accordez l'accès aux fichiers et aux dossiers dont chacun a besoin.

L'approche « porte fermée » est plus sûre mais les utilisateurs peuvent se plaindre qu'ils n'ont jamais accès aux informations dont ils ont besoin. Vous passerez donc votre temps à distribuer des droits d'accès. N'optez pour cette approche que si le réseau contient énormément d'informations très sensibles et si vous êtes d'accord pour investir beaucoup de votre temps dans l'administration de la sécurité du réseau.



L'approche « porte ouverte » peut être considérée comme un droit acquis, dans lequel vous partez du principe que tout le monde est autorisé à accéder à tous les recoins du réseau, tandis que l'approche « porte fermée », à base de permissions, est fondée sur l'idée que nul ne peut accéder à quoi que ce soit s'il n'y a pas été autorisé.

Sécurité physique : fermer la porte

Le premier niveau de toute sécurité informatique est la sécurité physique. Je suis toujours étonné de voir que dans le hall de réception d'un cabinet de comptabilité des ordinateurs sont laissés sans surveillance. Trop souvent, le réceptionniste s'est connecté au système puis a quitté son poste un moment, laissant l'ordinateur seul.

La sécurité physique est certes primordiale pour les stations de travail mais elle est vitale pour les serveurs. S'il bénéficie d'un accès physique à un serveur, n'importe quel pirate ou personne malintentionnée peut outrepasser les mesures de sécurité les plus drastiques. Pour protéger un serveur :

- ✓ Fermez à clé la pièce où il se trouve.
- ✓ Ne confiez la clé qu'à des personnes sûres.
- ✓ Notez le nom des personnes qui ont la clé.
- ✓ Montez les serveurs dans des boîtiers ou des racks qui peuvent être verrouillés.
- ✓ Désactivez le lecteur de disquette et le lecteur de CD-DVD du serveur.
Une technique de piratage très courante consiste à démarrer le serveur à partir d'une disquette ou d'un CD, ce qui outrepasser les fonctions de sécurité du système d'exploitation réseau.
- ✓ Installez un pitbull affamé à proximité du serveur.



Il y a une grande différence entre une porte fermée à clé et une porte avec une serrure : si la clé n'est pas utilisée, la serrure ne sert à rien.

Les ordinateurs clients doivent aussi être physiquement sécurisés :

- ✓ Exigez du personnel qu'il ne laisse jamais un ordinateur sans surveillance lorsqu'il est connecté au réseau.
- ✓ Dans les lieux de passage (comme un hall de réception), les ordinateurs doivent pouvoir être verrouillés.
- ✓ Les bureaux doivent être fermés à clé lorsque plus personne ne s'y trouve.



Voici quelques autres risques dont vous devez vous méfier :

- ✓ L'équipe de nettoyage de nuit a très certainement accès à l'installation informatique. Qui vous dit que parmi les personnes chargées de l'entretien ne se trouve pas quelqu'un qui travaille pour la concurrence ou dont le passe-temps favori consiste à pirater des ordinateurs ? Si vous ne connaissez pas personnellement l'équipe, vous devez la considérer comme une menace potentielle.
- ✓ Et la corbeille à papier ? Les déchiqueteuses à papier ne sont pas uniquement destinées aux comptables véreux de chez Enron. Une corbeille peut contenir toutes sortes d'informations intéressantes : des rapports d'activité, des journaux de sécurité, des exemplaires imprimés du règlement de sécurité de la société voire des mots de passe griffonnés sur des bouts de papier. Pour plus de sécurité, tout papier qui quitte l'immeuble via la corbeille doit passer par la déchiqueteuse.
- ✓ Où stockez-vous les bandes de sauvegarde ? Ne vous contentez pas de les empiler à proximité du serveur. Non seulement elles sont faciles à voler mais ce comportement va aussi à l'encontre d'une des règles élémentaires de la sécurité : la sécurité physique contre des risques comme l'incendie. Si le feu se déclare dans la salle informatique et que les sauvegardes s'y trouvent, votre société ne s'en remettra pas et vous perdrez certainement votre gagne-pain. Stockez les sauvegardes dans un coffre ignifugé et conservez des copies dans un local éloigné.
- ✓ J'ai déjà vu des réseaux dont les serveurs se trouvaient dans une salle informatique fermée à clé mais dont les concentrateurs et les commutateurs étaient dans un local non sécurisé. Rappelez-vous que tout concentrateur ou commutateur est une porte d'entrée au réseau. Ces périphériques doivent être en lieu sûr au même titre que les serveurs.

Sécuriser les comptes utilisateurs

Après la sécurité physique, l'une des principales mesures de sécurité réseau est la création de *comptes utilisateurs* qui ne permettent qu'aux utilisateurs accrédités d'accéder au réseau. Sans compte, l'utilisateur d'un ordinateur ne peut pas se connecter et ne peut donc pas utiliser le réseau. Les sections suivantes proposent quelques conseils que vous pouvez mettre en œuvre pour renforcer la sécurité relative aux comptes utilisateurs.

Brouiller les noms d'utilisateurs

La plupart des administrateurs réseau affectent des noms d'utilisateurs formés par une combinaison des nom et prénom de chaque utilisateur, comme DupontJ ou jDupont. Un pirate peut cependant facilement découvrir ce genre d'identifiant pour peu qu'il connaisse le nom d'au moins un employé. Une fois qu'il l'a obtenu, il peut se consacrer à la découverte du mot de passe.

Pour ralentir les recherches d'un pirate, utilisez des noms obscurs. Voici quelques suggestions :

- ✓ Ajoutez un nombre à trois chiffres après le nom. Exemples : DupontJ320 ou jDupont320.
- ✓ Placez des chiffres au milieu du nom. Exemples : Du3pontJ ou jDu2pont5.
- ✓ Assurez-vous que les noms d'utilisateurs sont différents de ceux de l'adresse électronique. Par exemple, si l'adresse électronique d'un utilisateur est xMartin@mondomaine.com, n'utilisez pas xMartin comme nom d'utilisateur. Choisissez un nom plus obscur.



Ne comptez pas sur le brouillage pour tenir les gens à l'écart du réseau. Il ne procure aucune sécurité. Un pirate déterminé peut découvrir un nom d'utilisateur aussi obscur soit-il. Le brouillage ne sert qu'à ralentir les intrus, pas à les arrêter. En les gênant, vous avez plus de chances de découvrir leurs tentatives de forcer le réseau et de les contrecarrer avant qu'ils y parviennent.

Utiliser des mots de passe efficaces

Un des aspects essentiels de la sécurité d'un réseau est l'emploi de mots de passe.



Les identifiants ou « ID utilisateurs » ne sont généralement pas tenus secrets. Même s'ils sont obscurs, un pirate moyennement doué parviendra à les deviner.

En revanche, les mots de passe sont secrets. Votre mot de passe réseau est la barrière qui empêche un imposteur de se connecter au réseau avec votre ID utilisateur et donc de se voir conférer les mêmes droits que vous. *Alors, veuillez bien sur votre mot de passe !*

Voici quelques conseils pour créer de bons mots de passe :



- ✓ Ne prenez pas des mots de passe évidents comme votre prénom, le nom de votre enfant ou celui de votre chien.
- ✓ Ne choisissez pas un mot de passe en vous inspirant de vos passe-temps. Un de mes amis est passionné de bateaux. Eh bien, son mot de passe est le nom de son bateau. Qui le connaît peut deviner son mot de passe en quelques essais. Cinq coups de fouet si vous choisissez le nom de votre bateau !

- ✓ Gardez votre mot de passe dans votre tête et non sur un papier.
À éviter : écrire son mot de passe sur un billet autocollant et le coller sur le moniteur de l'ordinateur.

- ✓ La plupart des systèmes d'exploitation réseau vous permettent de fixer la date d'expiration d'un mot de passe. Par exemple, vous pouvez spécifier que les mots de passe doivent changer tous les trente jours. Passé ce délai, l'utilisateur doit modifier son mot de passe. Vos utilisateurs peuvent trouver ce procédé pénible mais il permet de limiter le risque de voir quelqu'un voler un mot de passe puis tenter de s'introduire ultérieurement dans votre système informatique.

- ✓ Il est également possible de configurer les comptes utilisateurs de sorte qu'au moment où l'utilisateur change de mot de passe, il ne puisse pas réutiliser un mot de passe *récent*. Par exemple, vous pouvez indiquer qu'un nouveau mot de passe ne peut être identique aux trois derniers choisis par l'utilisateur.

- ✓ Vous pouvez également définir une politique de sécurité et faire en sorte que les mots de passe comportent un mélange de lettres majuscules et minuscules, des chiffres et des symboles spéciaux. Ainsi, des mots de passe comme DIMWIT ou DUFUS seraient interdits tandis que 87dIM@wif ou duF39&US seraient autorisés.



- ✓ Certains administrateurs réseau s'opposent à l'utilisation de mots de passe car ils considèrent que la sécurité n'est pas essentielle pour leur réseau. Ou alors ils choisissent des mots de passe évidents, attribuent le même à tous les utilisateurs ou les inscrivent sur de grandes pancartes qu'ils accrochent dans tout le bâtiment. Je pense que, même sur les petits réseaux, les mesures de sécurité élémentaires à base de mots de passe sont importantes. Vous pouvez vous en passer uniquement si votre réseau est très petit (disons deux ou trois ordinateurs), si aucune donnée sensible n'est conservée sur le serveur de fichiers ou si le principal objectif du réseau est de permettre le partage de l'imprimante et non le partage de fichiers. Même sans avoir recours aux mots de passe, il reste possible de mettre en place des mesures de sécurité permettant notamment de limiter l'accès à certains répertoires. Rappelez-vous simplement que sans mot de passe rien ne vous empêche de vous connecter avec l'ID d'un autre utilisateur.

Générer des mots de passe pour les Nuls

Comment trouver des mots de passe que personne ne pourra deviner mais dont vous vous souviendrez ? La plupart des experts en sécurité disent que les meilleurs mots de passe ne correspondent à aucun mot du langage naturel mais sont des séquences de lettres, de chiffres et de caractères spéciaux. Comment diable pouvez-vous retenir un mot de passe tel que DKS4%DJ2 ? Et plus particulièrement si vous devez le remplacer dans trois semaines par 3PQ&X(D8.



Voici une solution de compromis qui vous permet de créer des mots de passe formés de deux mots de quatre lettres juxtaposés. Prenez votre livre favori (vous venez de gagner une vie si c'est ce livre) et choisissez une page au hasard. Recherchez le premier mot de quatre lettres dans cette page. Supposons que ce soit VOUS. Répétez le processus pour trouver un autre mot de quatre lettres ; supposons que ce soit PLUS. Combinez maintenant les mots pour former votre mot de passe : VOUSPLUS. Je pense que vous serez d'accord sur le fait que VOUSPLUS est plus facile à retenir que 3PQ&X(D8 et qu'il est tout aussi difficile à deviner. Je ne pense pas que les gars des services secrets se servent un jour de cette méthode mais elle est assez fiable pour la plupart d'entre nous.

Voici quelques précisions supplémentaires sur la façon de choisir des mots de passe à partir de votre livre favori :

- ✓ Si les mots sélectionnés se trouvent être les mêmes, choisissez un autre mot et prenez des mots dont la combinaison ne semble pas trop commune.
- ✓ Variante intéressante : sélectionnez un mot de quatre lettres et un mot de trois lettres puis choisissez au hasard un des caractères spéciaux du clavier (comme *, & ou >) pour séparer ces deux mots. Vous obtiendrez ainsi des mots de passe tels que MOT!PAGE, EST#GARS ou ELLE*VIE.
- ✓ Pour semer encore plus le trouble chez vos amis et vos ennemis, préférez des mots médiévaux extraits de *Gargantua*, de Rabelais. Rabelais est une excellente source de mots de passe car il vivait bien avant que ne soient inventés le traitement de texte et la correction automatique. Il écrivait mousches au lieu de mouches, beaux à la place de beaux, senestre plutôt que gauche. Et surtout, il employait beaucoup de mots de huit lettres pouvant servir de mot de passe : soubdain (soudain), traicter (traiter), boullietz (boulets).
- ✓ Ne venez pas vous plaindre si vous utilisez l'un de ces systèmes de génération de mots de passe et que quelqu'un réussit à prendre le contrôle de votre compte. Qui est le feignant qui n'a pas voulu retenir D#SC\$H4% ?



- ✓ Si vous décidez d'opter pour des mots de passe du genre KdI22UR3xdkL, vous trouverez des générateurs sur Internet. Il suffit d'utiliser un moteur tel que Google (www.google.fr) et de lancer une recherche sur l'expression « générateur de mots de passe ». Vous trouverez des pages Web qui vous permettront de générer des mots de passe aléatoires à partir de critères que vous aurez précisés (longueur, emploi de lettres, chiffres, signes de ponctuation, minuscules, majuscules, etc.).

Sécuriser le compte administrateur

Il va de soi qu'un utilisateur du réseau doit pouvoir l'utiliser sans aucune des restrictions imposées aux autres. Cet utilisateur est appelé *administrateur*. Il est responsable de la configuration du système de sécurité du réseau. À ce titre, il doit être exempté de toutes les restrictions.



Beaucoup de réseaux créent automatiquement un compte administrateur lorsque vous installez le logiciel de réseau. Le nom d'utilisateur de cet administrateur initial se trouve dans la documentation du réseau et il est le même pour tous les réseaux basés sur le même système d'exploitation. L'une des premières choses à faire, juste après avoir créé le réseau, est de *modifier le mot de passe de ce compte d'administrateur standard*. Sinon, toutes les mesures de sécurité élaborées par la suite, aussi sophistiquées soient-elles, seraient faites en pure perte. Quiconque connaissant le nom d'utilisateur attribué par défaut à l'administrateur pourrait accéder au système avec tous les droits et privilèges, ce qui lui permettrait d'outrepasser toutes les sécurités.



N'oubliez jamais le mot de passe du compte administrateur ! Si un utilisateur oublie son mot de passe, vous pouvez vous connecter comme superviseur et changer son mot de passe. Mais si vous oubliez le mot de passe d'administrateur, vous êtes planté !

Gérer la sécurité des utilisateurs

La sécurité au niveau des utilisateurs est le pilier de l'ensemble de la sécurité informatique. Grâce à des comptes utilisateurs, vous pouvez savoir qui accède au réseau et définir les ressources auxquelles tel ou tel utilisateur peut accéder. Vous pouvez restreindre l'accès à tels ordinateurs et à telle plage horaire. De plus, il vous est possible de verrouiller l'accès au réseau pour les utilisateurs qui n'ont pas ou plus de raison de s'y connecter. Les sections qui suivent décrivent les principes de base de la sécurité du réseau.

Comptes utilisateurs

Chaque utilisateur accédant au réseau doit avoir un compte utilisateur. Il permet à l'administrateur du réseau de déterminer qui peut accéder au réseau et de quelles ressources il peut disposer. De plus, un compte utilisateur peut être personnalisé afin de fournir diverses commodités comme un menu Démarrer personnalisé ou l'affichage des documents récemment utilisés.

À chaque compte utilisateur est associé un *nom d'utilisateur*, souvent appelé *ID utilisateur*, que l'utilisateur doit entrer lorsqu'il se connecte au réseau. À chaque compte sont aussi liées les informations suivantes :

- ✓ **Le mot de passe de l'utilisateur.** Cette information comprend aussi les conventions de mot de passe, notamment la fréquence à laquelle il doit être changé, la complexité du mot de passe, etc.
- ✓ **Les coordonnées du contact.** Son nom complet, son numéro de téléphone, son adresse postale et son adresse électronique ainsi que d'autres informations utiles.
- ✓ **Les restrictions de compte.** Ce sont notamment les heures auxquelles un utilisateur peut se connecter. Par exemple, il sera impossible à un utilisateur de s'introduire dans le réseau en dehors des heures de travail. Cette fonction est appréciable car elle décourage les heures supplémentaires. Vous pouvez aussi n'autoriser l'accès qu'à certains ordinateurs.
- ✓ **L'état du compte.** Un compte utilisateur peut être temporairement désactivé, empêchant l'utilisateur de se connecter.
- ✓ **Le répertoire d'accueil.** C'est un dossier partagé dans lequel l'utilisateur peut stocker ses documents.
- ✓ **Les autorisations de connexion distante.** Elles permettent à l'utilisateur d'accéder au réseau à distance, via une connexion par modem.
- ✓ **L'appartenance à un groupe.** Elle garantit à l'utilisateur certains droits selon le groupe auquel il appartient.

Pour plus d'informations, reportez-vous à la section « Thérapie de groupe », plus loin dans ce chapitre.



Comptes intégrés

La plupart des systèmes d'exploitation sont préconfigurés avec deux comptes : Administrateur et Invité. De plus, certains services, comme les serveurs Web ou de bases de données, créent leurs propres comptes utilisateurs. Voici les caractéristiques des différents comptes :



- ✓ **Le compte Administrateur.** Le compte Administrateur est le seigneur et maître du réseau. Il ne connaît aucune des restrictions imposées au commun des mortels. Quand vous êtes connecté en tant qu'administrateur, vous avez tous les pouvoirs. C'est pourquoi ce compte ne doit pas être attribué à n'importe qui. Ne le proposez que si c'est vraiment nécessaire.

Étant donné qu'un compte d'administrateur procure un accès illimité au réseau, il est impératif que vous le sécurisiez immédiatement après son attribution. Lorsque le programme de configuration du système d'exploitation réseau demande le mot de passe du compte Administrateur, choisissez un mélange aléatoire de caractères majuscules et minuscules, de chiffres et de symboles. Ne choisissez pas un mot facile à mémoriser en vous promettant de le changer plus tard. Si vous oubliez de le faire et que quelqu'un l'utilise, rien ne l'empêchera de formater le disque C: du serveur ou de s'approprier des numéros de cartes bancaires.

- ✓ **Le compte Invité.** Autre compte communément créé par défaut, le compte *Invité* est configuré avec un mot de passe vide et, le cas échéant, des droits d'accès. Ce compte permet à quiconque de se connecter au réseau, sans qu'il puisse y faire grand-chose. Je n'en vois pas tellement l'intérêt ; c'est pourquoi je vous suggère de le désactiver.
- ✓ **Les comptes de service.** Certains utilisateurs du réseau ne sont pas des personnes en chair et en os mais des processus logiciels qui demandent un accès à des ressources sécurisées et qui, de ce fait, nécessitent un compte utilisateur. Ces comptes sont généralement créés automatiquement lorsque vous installez ou configurez un serveur.

Par exemple, lorsque vous installez le serveur Web de Microsoft (IIS), un compte utilisateur nommé IUSR est créé. Le nom complet de ce compte est IUSR_<nomDuServeur>. Par conséquent, si un serveur est nommé WEB1 et son compte IUSR_WEB1, ISS se servira de ce compte pour permettre à des utilisateurs Internet anonymes d'accéder aux fichiers présents sur le site Web.



En règle générale, vous ne devriez pas toucher aux comptes utilisateurs si vous ne savez pas exactement ce que vous faites. Par exemple, si vous supprimez ou renommez le compte IUSR, vous devrez reconfigurer ISS afin qu'il prenne la modification en compte. Sinon ISS refusera l'accès à quiconque tentera d'atteindre votre site. Notez qu'à condition de savoir ce que vous faites, renommer ces comptes peut augmenter la sécurité du réseau mais ne faites rien tant que vous ne connaissez pas ce sujet à fond.

Droits d'utilisateur Les comptes utilisateurs et les mots de passe ne constituent que la première ligne de défense du réseau. Une fois qu'un utilisateur

a réussi à accéder au réseau en tapant son ID et son mot de passe, une seconde ligne de défense entre en jeu : les *droits*.

Dans la dure réalité de la vie du réseau, tous les utilisateurs sont égaux mais certains le sont plus que d'autres. Le préambule de la Déclaration d'indépendance du réseau stipule que « nous tenons les vérités suivantes pour évidentes : *quelques* utilisateurs sont dotés par l'administrateur réseau de certains droits inaliénables... »

Les droits spécifiques que vous pouvez accorder aux utilisateurs dépendent de votre système d'exploitation réseau. Voici une liste partielle des droits disponibles sous Windows Server :

- ✓ **Se connecter localement** : L'utilisateur peut se connecter directement à l'ordinateur serveur depuis le clavier de ce dernier.
- ✓ **Changer l'heure système** : L'utilisateur peut changer l'heure et la date que gère le serveur.
- ✓ **Arrêter le système** : L'utilisateur peut purement et simplement arrêter le serveur.
- ✓ **Sauvegarder des fichiers et des répertoires** : L'utilisateur peut effectuer la sauvegarde des fichiers et répertoires du serveur.
- ✓ **Récupérer des fichiers et des répertoires** : L'utilisateur peut restaurer des fichiers sauvegardés.
- ✓ **Devenir propriétaire de fichiers et autres objets** : L'utilisateur peut prendre le contrôle de fichiers et de ressources réseau qui appartiennent à d'autres utilisateurs.

NetWare propose plus ou moins les mêmes droits d'utilisateurs.

Droits du système de fichiers (qui peut faire quoi)

Les droits utilisateurs déterminent ce que ces derniers peuvent faire sur l'ensemble du réseau. Les droits du système de fichiers vous permettent d'affiner votre sécurité réseau en contrôlant certaines opérations de fichiers spécifiques pour des utilisateurs donnés. Par exemple, vous pouvez configurer les droits du système de fichiers de sorte que les utilisateurs du service comptabilité puissent accéder aux fichiers stockés dans le répertoire \COMPT. Ces droits peuvent aussi autoriser des utilisateurs à lire des fichiers précis sans toutefois pouvoir les modifier ou les supprimer.

Chaque système d'exploitation réseau gère les droits du système de fichiers selon des principes qui lui sont propres. Mais, dans tous les cas, il en résulte

que vous pouvez donner à chaque utilisateur la permission d'accéder de diverses manières à certains fichiers, dossiers ou lecteurs. Par exemple, vous pouvez attribuer à un utilisateur un accès total à quelques fichiers et lui allouer uniquement un accès en lecture seule à d'autres fichiers.



Tous les droits du système de fichiers que vous octroyez à un dossier s'appliquent automatiquement à tous ses sous-dossiers, à moins que vous n'ayez explicitement accordé des droits différents pour ces sous-dossiers.



Vous ne pouvez appliquer les autorisations de Windows qu'aux fichiers et dossiers créés sur des lecteurs formatés en NTFS. Si le système de fichiers des lecteurs partagés est au format FAT ou FAT32, vous ne pourrez pas protéger tel ou tel de leurs fichiers ou dossiers. C'est une des raisons principales qui justifient l'utilisation du format NTFS sur les serveurs Windows.

Thérapie de groupe

Un *compte de groupe* est un compte qui ne représente pas un utilisateur individuel mais un ensemble d'utilisateurs qui utilisent le réseau de la même manière. Au lieu d'octroyer des droits à chacun d'eux séparément, vous pouvez les octroyer au groupe et affecter également des utilisateurs individuels à ce groupe. Dans ce cas, le nouveau venu hérite des droits spécifiques au groupe.

Droits réseau à étudier pour l'avenir

Les droits réseau accordés par la plupart des systèmes d'exploitation réseau sont plutôt ennuyeux. En voici quelques-uns dont je voudrais bien disposer :

- ✔ **Tricher** : Vous permet de voir les cartes des autres joueurs quand vous jouez à la « Dame de pique ».
- ✔ **Espionner** : Surveiller clandestinement les accès Internet des utilisateurs afin de connaître les sites Web auxquels ils se connectent.
- ✔ **Se plaindre** : Envoi automatique d'un courrier électronique aux autres utilisateurs pour leur expliquer combien vous êtes occupé, fatigué ou énervé.
- ✔ **Modifier la feuille de paie** : Vous donne des droits d'accès spéciaux au système de calcul de la paie pour que vous puissiez vous accorder une augmentation.
- ✔ **Porter plainte** : Aux États-Unis, chacun a le droit de porter plainte. Ce droit devrait donc être automatiquement donné à tous les utilisateurs.
- ✔ **Mettre le feu** : Ne serait-il pas agréable de pouvoir mettre le feu à vos collègues devenus insupportables ?

Supposons, par exemple, que vous ayez créé un groupe nommé Comptabilité pour le service comptable et que vous autorisiez tous les membres de ce groupe à accéder aux fichiers et applications de la comptabilité. Au lieu d'octroyer ces droits à chacun des employés du service, vous faites de chacun d'eux un membre du groupe Comptabilité.

Voici quelques détails supplémentaires concernant les groupes :

- ✓ Les groupes facilitent considérablement la gestion du réseau. Vous devriez éviter autant que possible de gérer individuellement les utilisateurs du réseau. Intégrez-les plutôt à des groupes. Quand cinquante utilisateurs du service Comptabilité doivent pouvoir accéder à un nouveau dossier partagé, il est plus rapide de mettre un groupe à jour que chacun des cinquante comptables.
- ✓ Un utilisateur peut faire partie de plusieurs groupes. Il hérite alors des droits de chacun de ces groupes. Par exemple, si vous avez configuré des groupes nommés Comptabilité, Ventes, Marketing et Finances, un utilisateur qui doit accéder aux données comptables et financières deviendra membre des groupes Comptabilité et Finances. De même, un utilisateur qui doit accéder aux données des ventes et du marketing fera partie des groupes Ventes et Marketing.
- ✓ Vous pouvez octroyer des droits spécifiques à tel ou tel utilisateur ou restreindre ses droits. Par exemple, vous pourriez attribuer quelques autorisations spéciales au directeur du service comptable et imposer des restrictions à certains utilisateurs.

Profils d'utilisateurs

Les *profils d'utilisateurs* sont une fonctionnalité Windows conservant la trace des préférences individuelles des utilisateurs en ce qui concerne la configuration de Windows. Les profils d'utilisateurs permettent à deux utilisateurs (ou plus) d'employer un même ordinateur quand ce dernier n'est pas relié au réseau, chaque utilisateur spécifiant ses propres paramètres de Bureau dont l'arrière-plan, les couleurs, les options du menu Démarrer, etc.

Le véritable intérêt des profils d'utilisateurs ne se révèle que sur un réseau. Le profil d'un utilisateur peut être stocké sur l'ordinateur serveur et utilisé dès que cet utilisateur se connecte au réseau depuis n'importe quel ordinateur Windows du réseau.

Voici quelques-unes des fonctionnalités de Windows contrôlées par les paramètres d'un profil d'utilisateur :

- ✓ Les paramètres du Bureau de la boîte de dialogue Propriétés d'affichage, dont l'arrière-plan, les économiseurs d'écran et les couleurs.

- ✓ Les programmes du menu Démarrer et les options de la barre d'outils de Windows.
- ✓ Les favoris, qui permettent d'accéder facilement aux fichiers et aux dossiers fréquemment utilisés.
- ✓ Les paramètres du réseau dont les lecteurs associés à des disques réseau, les imprimantes réseau et les emplacements du réseau récemment visités.
- ✓ Les paramètres d'applications comme ceux de Microsoft Word.
- ✓ Le dossier Mes documents.

Scripts d'ouverture de session

Un *script d'ouverture de session* est un fichier de traitement par lots qui est automatiquement démarré lorsqu'un utilisateur ouvre une session sur le réseau. Un script d'ouverture de session peut effectuer plusieurs tâches importantes comme mapper des lecteurs réseau, démarrer des applications, synchroniser les horloges des ordinateurs clients, etc. Les scripts d'ouverture de session résident sur le serveur. Chaque compte utilisateur peut spécifier si un script d'ouverture de session doit être démarré et si oui lequel.

Voici un exemple de script d'ouverture de session qui mappe quelques lecteurs réseau et les synchronise :

```
net use m: \\MONSERVEUR\Compta
net use n: \\MONSERVEUR\Admin
net use o: \\MONSERVEUR\R&D
net time \\MONSERVEUR /set /yes
```

Les scripts d'ouverture de session sont quelque peu tombés en désuétude car la plupart de leurs actions peuvent être effectuées par des profils d'utilisateurs. Cependant, beaucoup d'administrateurs apprécient la simplicité des scripts d'ouverture de session, de sorte qu'ils sont encore utilisés, même sous Windows Server 2003.

Sécuriser les utilisateurs

Les techniques de sécurisation (comme la sécurité physique, la sécurité des comptes utilisateurs et des serveurs, le verrouillage de l'accès aux serveurs) sont un jeu d'enfant par rapport à la tâche la plus ardue qui vous attend : la sensibilisation des utilisateurs du réseau à la sécurité. Vos mesures de sécurité les plus élaborées seront vaines si les utilisateurs laissent traîner leur mot de passe sur un Post-It collé sur l'ordinateur.

La règle de base de toute sécurité au niveau de l'utilisateur consiste à imprimer un règlement de sécurité affiché au vu et au su de tout le monde. Organisez une réunion afin de vous assurer que chacun a bien pris conscience des enjeux et compris le règlement. N'hésitez pas à prévoir des sanctions dissuasives en cas de manquement.

Voici quelques règles qui pourraient figurer dans le règlement sur la sécurité informatique :

- ✓ N'écrivez jamais votre mot de passe sur papier et ne le communiquez à personne.
- ✓ Ne partagez pas vos comptes. N'utilisez jamais le compte de quelqu'un d'autre pour accéder à des ressources qui vous sont interdites. Si ces ressources vous sont indispensables, vous devez en demander officiellement l'accès sous votre propre compte.
- ✓ De même, ne communiquez jamais vos informations de compte à un collègue désireux d'accéder à des ressources auxquelles il n'a pas droit. Ce collègue doit demander un accès à ces ressources sous son propre compte.
- ✓ N'installez aucun logiciel ou matériel sans avoir préalablement obtenu l'autorisation. Ceci concerne notamment les périphériques d'accès sans fil ou les modems.
- ✓ N'activez jamais le partage de fichiers et d'imprimantes sur une station de travail sans en avoir obtenu l'autorisation.
- ✓ Ne tentez jamais de désactiver ou d'outrepasser les fonctions de sécurité du réseau.

Chapitre 24

Renforcer la sécurité du réseau

Dans ce chapitre :

- Comprendre le rôle des pare-feu.
- Comparer les différents types de pare-feu.
- Utiliser le pare-feu Windows intégré.
- Étudier la protection contre les virus.
- Mettre les ordinateurs à niveau.

Si votre réseau est connecté à Internet, vous êtes confronté à une foule de problèmes de sécurité. Vous avez sans doute établi cette connexion afin que les utilisateurs du réseau bénéficient d'une fenêtre ouverte sur le monde extérieur. Malheureusement, c'est aussi par cette fenêtre qu'entrent les malfaiteurs.

Ceux qui agissent sur Internet ne s'en priveront pas. Le cyberspace est peuplé de pirates à la recherche de réseaux dans lesquels s'introduire. Ce n'est parfois que pour le plaisir de fureter dans vos affaires mais parfois aussi pour dérober des numéros de cartes bancaires ou inonder votre serveur de messagerie de milliers de courriers non sollicités. Quelles que soient les motivations, soyez assuré que votre réseau sera visité si vous ne le protégez pas.

Ce chapitre présente une vue d'ensemble de trois techniques de base pour renforcer la sécurité de votre réseau vis-à-vis d'Internet : contrôle d'accès par l'intermédiaire d'un pare-feu, détection des virus avec un logiciel antivirus et correction des failles de sécurité avec les mises à niveau de sécurité.

Pare-feu

Un *pare-feu* est un routeur sécurisé interposé entre Internet et votre réseau. Sa seule tâche est de filtrer tout ce qui entre et sort. C'est une sorte de vigile entre Internet et le réseau. Tout le trafic transite par le pare-feu qui autorise ou interdit les accès.



Un pare-feu est absolument obligatoire dès lors que votre réseau accède à Internet, que ce soit par une connexion à haut débit (DSL ou modem câble), ligne T1 ou toute autre connexion haut débit. Sans pare-feu, les pirates découvriront tôt ou tard l'existence de votre réseau non protégé, le signaleront à leurs collègues et il en subira les conséquences en quelques heures.

Un pare-feu peut être installé de deux manières. La plus simple consiste à acheter un *équipement pare-feu*, qui est en réalité un routeur offrant des fonctionnalités de pare-feu. La plupart sont équipés d'une interface de type Web permettant de les connecter directement depuis l'un des ordinateurs du réseau à l'aide d'un navigateur. Vous les configurez ensuite selon vos besoins.

Autre solution : vous pouvez configurer un ordinateur serveur afin qu'il fasse office d'ordinateur pare-feu. Le serveur peut fonctionner sous n'importe quel système d'exploitation réseau. Les plus efficaces tournent cependant sous Linux.

Que vous optiez pour l'équipement pare-feu ou l'ordinateur pare-feu, ce matériel doit être placé entre le réseau et Internet, comme le montre la Figure 24.1. Le pare-feu est connecté d'une part au commutateur, qui est lui-même connecté aux autres ordinateurs du réseau, et d'autre part à Internet. Tout le trafic échangé entre le réseau et Internet doit obligatoirement transiter par le pare-feu.

Le terme *périmètre* est parfois utilisé pour décrire l'emplacement du pare-feu sur le réseau. Un pare-feu est en effet une sorte de périmètre de sécurité qui entoure votre propriété et oblige les visiteurs à s'annoncer à la porte d'entrée.



Sur les réseaux de grande taille, il est parfois difficile de savoir où se trouve le périmètre. Si le réseau bénéficie de plusieurs connexions WAN (*Wide Area Network*, réseau étendu), vérifiez que chacune d'elles est protégée par un pare-feu et n'est pas directement reliée à Internet. Cette sécurité est assurée par un pare-feu pour chaque connexion WAN ou par un seul pare-feu équipé de plusieurs ports WAN.

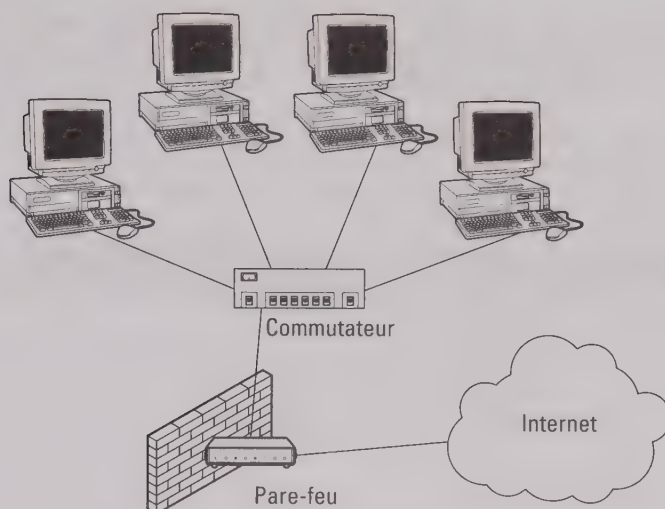


Figure 24.1 : Un routeur pare-feu sécurise le trafic entre le réseau et Internet.

Types de pare-feu

Les pare-feu utilisent quatre techniques de base pour protéger les réseaux. Elles sont décrites dans les sections suivantes.

Filtrer les paquets

Un pare-feu utilisant le *filtrage de paquets* examine chaque paquet qui transite par le pare-feu et le teste selon un ensemble de règles qui ont été définies. Si le paquet subit un test positif, il peut passer. Si le test est négatif, il est rejeté.

Les pare-feu utilisant le filtrage de paquets sont les moins chers. Par conséquent, ils sont très courants. Cependant, le filtrage de paquets conserve un certain nombre d'imperfections que les pirates bien informés peuvent exploiter. En fait, les pare-feu par filtrage de paquets ne sont pas les plus puissants.

Le filtrage de paquets consiste à examiner les adresses IP des sources et des destinations et les numéros de ports contenus dans chaque paquet TCP/IP. Les *ports TCP/IP* sont des nombres assignés aux services spécifiques qui aident à identifier à quel service chaque paquet est destiné. Par exemple, le numéro de port du protocole HTTP est 80. Ainsi, tous les paquets entrants destinés à un serveur HTTP spécifieront le port 80 comme port de destination.

Les numéros de ports sont souvent spécifiés avec des doubles points après l'adresse IP. Par exemple, le service HTTP sur un serveur dont l'adresse IP est 192.168.10.133 sera 192.168.10.133:80.

Des milliers de ports sont utilisés. Le Tableau 24.1 présente quelques-uns des ports les plus connus.

Tableau 24.1 : Ports TCP/IP les plus utilisés.

<i>Port</i>	<i>Description</i>
20	File Transfer Protocol (FTP)
21	File Transfer Protocol (FTP)
22	Secure Shell Protocol (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Server (DNS)
80	World Wide Web (HTTP)
110	Post Office Protocol (POP3)
119	Network News Transfer Protocol (NNTP)
137	Service de noms NetBIOS
138	Service de datagramme NetBIOS
139	Service de session NetBIOS
143	Protocole de messagerie IMAP (IMAP)
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
389	Protocole LDAP (LDAP)
396	NetWare sur IP
443	HTTP sur TLS/SSL (HTTPS)

Les règles que vous définissez pour le filtrage des paquets autorisent ou bloquent ces derniers en fonction de l'adresse IP ou du numéro de port. Par exemple, vous pouvez laisser passer les paquets qui sont destinés à votre serveur de messagerie ou à votre serveur Web et refuser tous les autres.

Vous pouvez aussi configurer une règle qui refuse spécifiquement tous les paquets qui sont destinés aux ports NetBIOS. Cette règle empêche des intrus d'Internet d'accéder à des ressources NetBIOS telles que des fichiers ou des imprimantes.

Une des plus grandes faiblesses du filtrage de paquets est qu'il considère que les adresses d'origine et les adresses de destination des paquets sont vraies. Les pirates exploitent cette faiblesse en utilisant la technique d'*usurpation d'adresse IP (IP spoofing)*, dans laquelle ils spécifient des adresses IP d'origine fausses dans les paquets qu'ils envoient sur votre réseau.

Une autre faiblesse importante du filtrage de paquets est l'examen isolé de chaque paquet, sans tenir compte des paquets précédents et suivants. En d'autres termes, le filtrage des paquets est *sans état*. Soyez sûr que les pirates savent comment exploiter la nature sans état du filtrage de paquets pour tromper les pare-feu.

Malgré ces faiblesses, les pare-feu par filtrage de paquets présentent plusieurs avantages qui expliquent pourquoi ils sont si souvent utilisés :

- ✓ **Les filtres de paquets sont très efficaces.** Ils ne mettent que quelques millisecondes pour analyser dans les paquets la destination, les ports et les adresses de la source. Les adresses d'origine, de destination et les numéros de ports sont déterminés, les règles sont appliquées et, en fonction du résultat, le paquet est transmis ou rejeté. La plupart des autres techniques de filtrage requièrent un temps de traitement plus important.
- ✓ **Les filtres de paquets sont pratiquement transparents pour les utilisateurs.** Le seul cas où un utilisateur se rend compte qu'un pare-feu avec filtrage de paquets est utilisé, c'est lorsque les paquets sont rejetés. Les autres techniques de pare-feu exigent que les clients et/ou les serveurs soient spécialement configurés pour pouvoir travailler.
- ✓ **Le filtrage de paquets est très bon marché.** La plupart des routeurs proposent le filtrage de paquets intégré.

Inspection dynamique des paquets (SPI)

L'*inspection dynamique des paquets*, également connue sous le nom de *SPI*, est une évolution du filtrage de paquets. Un pare-feu avec inspection dynamique des paquets traite des groupes de paquets plutôt que des paquets individuels. Il maintient les paquets dans le pare-feu, ce qui permet la détection des accès non autorisés. Dans certains cas, le pare-feu bloque les paquets jusqu'à ce qu'il ait recueilli suffisamment d'informations pour décider s'ils doivent être transmis ou rejetés.



Jusqu'à présent, l'inspection dynamique des paquets ne se trouvait que sur les routeurs haut de gamme et les routeurs utilisés dans les entreprises. À présent, les pare-feu avec inspection dynamique des paquets sont plus abordables et on les utilise fréquemment dans les réseaux de petite taille ou de taille moyenne.

Passerelle de niveau circuit (circuit-level gateway) Une *passerelle de niveau circuit* contrôle les connexions entre les clients et les serveurs en se basant sur les adresses TCP/IP et les numéros de ports. Une fois que la connexion a été établie, la passerelle de niveau circuit n'interfère pas sur les paquets qui circulent entre les systèmes.

Par exemple, vous pouvez utiliser une telle passerelle pour permettre les connexions Telnet (port 23) à un serveur particulier et pour interdire tout autre type de connexion à ce serveur. Une fois que la connexion est établie, la passerelle laisse les paquets circuler librement entre les machines connectées. Par conséquent, la passerelle de niveau circuit ne peut pas empêcher un utilisateur Telnet de lancer des programmes spécifiques ou d'utiliser des commandes spécifiques.

Passerelle applicative

Une *passerelle applicative* est un système de pare-feu qui est plus intelligent qu'un filtrage de paquets, une inspection dynamique des paquets ou une passerelle de niveau circuit. Les filtrages de paquets traitent tous les paquets TCP/IP de la même manière tandis que les passerelles applicatives sont informées sur la nature des paquets en fonction des applications auxquelles ils sont destinés ou desquelles ils proviennent. Par exemple, une passerelle applicative Web a une connaissance détaillée des paquets HTTP. Ainsi, elle peut analyser plus que la source, les adresses et les ports de destination pour déterminer si les paquets sont autorisés à traverser le pare-feu.

Par ailleurs, les passerelles applicatives fonctionnent comme *serveurs mandataires* ou *proxy*. Un *serveur mandataire* est un serveur interposé entre l'ordinateur client et le serveur réel. Il intercepte les paquets destinés au serveur et les traite. Il peut ensuite décider de les transmettre au serveur ou de les rejeter. Le serveur mandataire peut aussi répondre lui-même à un client sans impliquer le serveur.

Par exemple, les serveurs mandataires enregistrent en mémoire des copies des pages Web au fur et à mesure de leur consultation sur le serveur. Ensuite, lorsqu'un client souhaite accéder à une page Web du serveur, le serveur mandataire intercepte la demande et s'il possède une copie de la page en mémoire, il la transmet directement au client ; sinon, il transfère la requête au serveur.

Les passerelles applicatives analysent en détail la manière dont les serveurs manipulent les séquences de paquets TCP/IP. Elles peuvent ainsi décider si un paquet entrant est légitime ou s'il constitue une attaque. Pour cette raison, les passerelles applicatives sont beaucoup plus sûres que les pare-feu utilisant le filtrage de paquets qui ne peuvent traiter qu'un seul paquet à la fois.

Cependant, le niveau de sécurité apporté par les passerelles applicatives a un prix. Ces dernières sont beaucoup plus chères que les systèmes à filtres de paquets, en termes de prix d'achat et de coûts de configuration et de maintenance. De plus, les passerelles applicatives diminuent les performances du réseau parce qu'elles contrôlent de manière plus détaillée les paquets avant de leur permettre de passer.

Pare-feu intégré de Windows

Depuis Windows XP, toutes les versions de Windows possèdent un pare-feu par filtrage de paquets intégré. Si vous ne possédez pas de pare-feu sur votre routeur, vous pouvez activer celui de Windows. Il procure une protection de base en filtrant les données. Reportez-vous au Chapitre 10 pour savoir comment configurer le pare-feu Windows.



N'activez pas le pare-feu de Windows si vous utilisez un routeur qui assure déjà cette fonction. Comme les autres ordinateurs du réseau sont connectés directement au routeur et non à l'ordinateur, le pare-feu de Windows ne protégerait pas le reste du réseau. Autre effet secondaire : le reste du réseau ne pourrait plus accéder à votre ordinateur.

Se protéger contre les virus

De nos jours, les virus sont l'un des phénomènes informatiques les moins bien compris. Qu'est-ce qu'un virus ? Comment fonctionne-t-il ? Comment se répand-il d'ordinateur en ordinateur ? Je suis heureux que vous posiez la question.

Qu'est-ce qu'un virus ?

Ne vous méprenez pas, les virus sont bien réels. Avec l'explosion du nombre d'internautes, les virus prolifèrent. Chaque utilisateur d'un ordinateur peut être victime d'un virus informatique et l'utilisation d'un réseau ne fait qu'augmenter cette vulnérabilité car il court le risque d'être infecté par un virus qui réside sur la machine d'un autre utilisateur du réseau.

Les virus n'apparaissent pas spontanément de nulle part. Ce sont des programmes informatiques créés par des programmeurs détraqués et malintentionnés qui devraient être internés.

Un virus se caractérise par sa capacité à se reproduire afin de se répandre sur les autres ordinateurs. Ces copies font à leur tour encore plus de copies qui se répandent sur d'autres ordinateurs et ainsi de suite, à l'infini.

Ensuite, le virus attend patiemment d'être activé, quand vous taperez une commande particulière, appuierez sur une touche précise ou lorsqu'une date donnée sera atteinte, selon le but que s'est fixé le créateur du virus. Alors, le virus frappe de différentes manières, toujours en fonction de l'objectif de son géniteur, quelquefois en affichant un message inoffensif comme « je vous ai bien eu » ou bien en détruisant toutes les données de votre disque dur. Ouïe !

Il y a quelques années, les virus se déplaçaient d'ordinateur en ordinateur, accrochés à des disquettes. Si vous empruntiez une disquette à un copain, vous risquiez de contaminer votre ordinateur à cause d'un virus embarqué clandestinement sur ce support.

Aujourd'hui, les créateurs de virus ont constaté que le courrier électronique était un vecteur bien plus efficace. Généralement, le virus se fait passer pour une pièce jointe très intéressante : instructions pour gagner une fortune sans rien faire, photos de célébrités nues ou message de votre amour perdu pour la Saint-Valentin. Lorsqu'un utilisateur curieux mais pas méfiant double-clique sur le fichier joint, le virus sort de sa coquille, se copie sur l'ordinateur de la victime puis, parfois, envoie son clone à toutes les personnes figurant dans le carnet d'adresses de l'utilisateur.

Une fois que le virus a pénétré dans un ordinateur du réseau, il peut ensuite attaquer tous les ordinateurs du réseau.

Voici quelques informations précieuses sur la façon de protéger un réseau contre des attaques de virus :

- ✓ Le terme *virus* est souvent employé pour désigner non seulement de vrais programmes virus (qui sont capables de se reproduire) mais aussi un autre type de programme conçu pour faire des dégâts sur votre ordinateur. Le cheval de Troie est l'un de ces programmes qui ressemblent généralement à des jeux mais sont en fait des formateurs de disques durs.
- ✓ Un *ver* ressemble à un virus, à la différence qu'il n'infecte pas les autres fichiers. En fait, il se contente de se copier dans tous les ordinateurs du réseau. Ensuite, il peut faire n'importe quoi. Par exemple, un ver peut analyser le contenu de votre disque dur à la recherche d'informations intéressantes, comme un mot de passe ou des numéros de cartes bancaires et les transmettre à son créateur par courrier électronique.

- ✓ Les experts en virus informatiques ont identifié plusieurs milliers de « variétés » de virus. La plupart d'entre eux ont des noms hauts en couleur tels que I Love You, Stoned et Michelangelo.
- ✓ Les programmes antivirus peuvent identifier les virus connus et les supprimer de votre système. Ils sont également capables de détecter les signes révélateurs de la présence de virus inconnus. Malheureusement, les imbéciles qui écrivent les virus ne sont pas des idiots (au sens intellectuel du terme), si bien qu'ils développent sans cesse de nouvelles techniques pour tromper les programmes antivirus. De nouveaux virus sont fréquemment découverts et les programmes antivirus sont donc régulièrement mis à jour pour les détecter et les supprimer.

Programmes antivirus

Le meilleur moyen de protéger votre réseau contre l'attaque de virus est d'avoir recours à un programme antivirus. Ces programmes recensent des milliers de virus connus qu'ils peuvent détecter et supprimer. De plus, ils peuvent repérer les modifications que les virus apportent aux fichiers de votre ordinateur, augmentant la probabilité de débusquer des virus inconnus.

Il serait agréable que Windows soit livré avec des fonctions antivirus mais ce n'est hélas pas le cas. Vous devez donc acheter un logiciel antivirus à part. Les plus connus sont Norton Antivirus, édité par Symantec, VirusScan de McAfee et OfficeScan signé Trend Micro.

Les éditeurs de programmes antivirus proposent, sur leur site Web, des mises à jour qui permettent aux programmes de détecter les virus récemment découverts. Consultez la documentation livrée avec votre programme antivirus pour savoir comment obtenir ces mises à jour.

Voici quelques conseils pour protéger votre réseau contre les virus :

- ✓ Installez un logiciel antivirus sur chacun des ordinateurs du réseau. Cette technique n'est efficace que si vous avez la certitude que chaque utilisateur effectuera régulièrement les mises à jour (le téléchargement des nouvelles définitions de virus est souvent automatisé). En cas de doute, il existe des solutions plus sûres.
- ✓ Configurez un service antivirus qui place des logiciels antivirus sur chaque ordinateur client du réseau, la mise à jour étant assurée par le serveur.
- ✓ Les antivirus serveur protègent les serveurs du réseau contre les virus. Par exemple, vous pouvez en installer un dans le serveur de messagerie afin qu'il analyse tous les courriers entrants et supprime les virus s'il en trouve, sans même que les utilisateurs s'en aperçoivent.

- ✓ Certains pare-feu sont équipés de fonctions antivirus qui interdisent aux utilisateurs d'accéder à Internet si leur logiciel antivirus n'est pas à jour. Ce type de pare-feu fournit la protection la plus efficace contre les virus.

Travailler en toute sécurité

En dehors de l'utilisation d'un programme antivirus, il existe quelques précautions à prendre pour éviter les infections « virales ». Si vous n'avez pas enseigné à vos enfants les précautions à prendre en matière de sécurité informatique, il est temps de le faire.

- ✓ Sauvegardez régulièrement vos données. Si vous êtes frappé par un virus, vous aurez peut-être besoin de récupérer des données. Assurez-vous que votre sauvegarde date d'avant l'attaque !
- ✓ Si vous achetez un logiciel et si vous découvrez que l'emballage a déjà été ouvert, rappelez le logiciel. N'essayez surtout pas de l'installer sur votre ordinateur. Il se peut qu'il ne corresponde pas à la version d'origine et qu'il contienne un virus.
- ✓ Utilisez votre programme antivirus pour vérifier si votre disque n'est pas infecté lors d'une éventuelle réparation dans un magasin ou dans le cas où un consultant l'aurait manipulé. Ces personnes ne vous veulent pas de mal mais ils répandent parfois des virus accidentellement, tout simplement parce qu'ils sont amenés à travailler sur des ordinateurs parfois étranges.
- ✓ N'ouvrez pas les pièces jointes envoyées par des inconnus ou celles que vous n'attendiez pas.
- ✓ Utilisez votre antivirus pour scanner un CD ou une clé USB qui ne vous appartient pas avant d'ouvrir les fichiers qu'il/elle contient.

Installer des correctifs

L'installation de correctifs (*patches*, en anglais) sur le système d'exploitation ou les autres logiciels du réseau est l'une des opérations pénibles auxquelles tout administrateur réseau est confronté. Un *correctif* est une mise à jour mineure de logiciel destinée à résoudre les petits pépins qui surviennent de temps à autre comme des baisses de performances ou des problèmes de sécurité. Ces pépins ne sont pas assez sérieux pour entraîner la sortie d'une nouvelle version du logiciel, tout en méritant d'être résolus. La plupart des correctifs remédient aux failles de sécurité dans lesquelles les pirates

informatiques (*hackers*, en anglais) se sont récemment engouffrés, avec la volonté de prouver qu'ils sont plus calés que les programmeurs de Microsoft ou Novell.

Périodiquement, tous les correctifs récemment sortis sont regroupés dans des *service packs*. Les administrateurs réseau consciencieux installent les correctifs dès leur sortie mais nombreux sont ceux qui attendent les *service packs*.

- ✓ Pour toutes les versions de Windows, vous pouvez aller sur le site Windows Update afin de mettre à jour votre système d'exploitation et vos logiciels Microsoft à l'aide de ces correctifs. Windows Update scanne votre disque automatiquement, repère les logiciels installés sur votre ordinateur et crée une liste de correctifs et d'autres composants que vous pouvez ensuite télécharger puis installer.

- Cliquez sur Windows Update dans le menu Démarrer.
- À partir d'Internet Explorer, accédez au site <http://windowsupdate.microsoft.com>.

Windows Update peut également être configuré de façon à vous avertir automatiquement de l'existence de nouvelles mises à jour. Ainsi, vous n'avez pas besoin d'aller vérifier vous-même.

- ✓ Novell propose régulièrement des correctifs et des mises à jour pour NetWare sur son site Internet de support produits (support.novell.com).

Vous pouvez vous abonner à un service de notification par courrier électronique qui vous informe automatiquement des nouveaux correctifs et mises à jour disponibles.



Maintenir à jour un grand réseau peut être l'un des défis majeurs de l'administrateur réseau. Si vous avez quelques douzaines d'ordinateurs sur votre réseau, investissez dans un logiciel de mise à jour comme Lumension (www.lumension.com). C'est un programme qui rassemble les correctifs logiciels d'une série de constructeurs et vous permet de créer les distributions qui sont automatiquement attribuées aux ordinateurs clients. Avec un logiciel comme Lumension, vous n'aurez plus à vous appuyer sur les utilisateurs pour télécharger et installer les mises à jour et vous n'aurez plus à vous connecter sur chaque ordinateur pour les installer.

Sixième partie

Au-delà de Windows



« Le comble, c'est qu'il est sorti pour rechercher un "hotspot". »

Dans cette partie...

Bien que Bill Gates soit peu disposé à l'admettre, Windows n'est pas le seul système d'exploitation des PC. Les deux chapitres de cette partie présentent les bases de la gestion réseau avec les deux alternatives à Windows les plus populaires : Linux et Macintosh.

Chapitre 25

Mettre en œuvre un serveur Linux

Dans ce chapitre :

- ▶ Découvrir Linux et le comparer avec Windows.
- ▶ Choisir une distribution Linux pour le serveur.
- ▶ Installer Linux, configurer les paramètres réseau et les comptes utilisateurs.
- ▶ Utiliser Samba pour créer un serveur de fichiers.

Linux, le système d'exploitation gratuit basé sur UNIX, est une alternative très appréciée à Windows Server, notamment pour des applications spécifiques telles que des serveurs Web ou de messagerie. Linux s'utilise aussi comme pare-feu ou comme serveur de fichiers et d'impression sur votre réseau local.

C'est en 1991 que Linus Torvalds, alors étudiant en licence à l'université d'Helsinki, a commencé à concevoir Linux. Il venait d'acheter un PC et pensait qu'il serait amusant de construire entièrement son système d'exploitation, à partir d'UNIX. Dix ans après, Linux est devenu un système d'exploitation très complet, rapide et fiable.

Dans ce chapitre, vous apprendrez à installer un serveur Linux sur votre réseau et à l'employer comme serveur de fichiers, serveur Web pour Internet ou un intranet, serveur de messagerie, ou comme routeur et pare-feu pour vous aider à connecter votre réseau à Internet.



Linux est un système d'exploitation complexe. Apprendre à s'en servir peut s'avérer assez décourageant, surtout si votre expérience en informatique se limite au seul Windows. Par chance, il existe plusieurs livres sur Linux aux éditions First Interactive qui faciliteront votre apprentissage : *Linux pour les Nuls*, *Linux Poche pour les Nuls*.

Linux versus Windows

Si vos connaissances en informatique ne concernent que Windows, la découverte de Linux s'apparentera pour vous à une longue et difficile ascension. Linux et Windows sont radicalement différents sur certains points. Voici les divergences les plus flagrantes :



- ✓ **Linux est un système d'exploitation multiutilisateur.** Cela signifie que plusieurs utilisateurs peuvent se connecter et se servir d'un ordinateur sous Linux en même temps :
 - Deux utilisateurs ou plus peuvent se connecter à partir du même clavier et moniteur grâce à des consoles virtuelles qui permettent de passer d'une session à une autre grâce à une simple combinaison de touches.
 - Les utilisateurs peuvent également se connecter à un ordinateur sous Linux à partir d'une fenêtre terminale ouverte sur une autre machine du réseau.

En revanche, la plupart des versions Windows sont mono-utilisateurs. Seul un utilisateur peut se connecter à un ordinateur doté de Windows et exécuter des commandes. Il est possible de configurer Windows 2003 en multiutilisateur avec des services de terminaux.

- ✓ **Contrairement à Windows, Linux ne possède pas d'interface utilisateur graphique intégrée (GUI, en anglais).** À la place, Linux dispose d'un composant optionnel, *X Window System*. Vous pouvez utiliser Linux sans X Window, auquel cas vous communiquez avec le système d'exploitation en tapant des commandes. Si vous préférez une GUI, vous devez installer et exécuter X Window.

X Window est divisé en deux parties :

- Un composant serveur, *serveur X*, en charge des principales corvées de gestion multifenêtre, qui s'occupe de tout ce qui est graphique pour les applications.
- Une interface utilisateur, le *gestionnaire de fenêtres*, qui fournit menus, boutons, barres d'outils, barre des tâches, etc.

Il existe plusieurs gestionnaires de fenêtres ayant chacun leur cachet. Sous Windows, vous êtes obligé d'utiliser l'interface conçue par Microsoft alors qu'avec Linux vous avez le choix entre plusieurs interfaces.

- ✓ **Linux ne permet pas d'exécuter des programmes Windows.** Cela signifie que vous ne pouvez pas utiliser Office sur un système Linux et devez donc trouver un logiciel spécialement conçu pour Linux. Linux est souvent livré avec une suite bureautique nommée *StarOffice* qui propose un tableur, des programmes de traitement de texte, de présentation, de bases de données, de messagerie et de gestion d'agendas. Des milliers d'autres logiciels fonctionnent sous Linux.



Il existe des émulateurs Windows, dont le plus connu est Wine, qui permettent d'employer certains programmes Windows sous Linux. Mais tous les logiciels Windows ne sont pas concernés et tournent plus lentement sous Linux que sous Windows.

- ✓ **Contrairement à Windows, Linux ne gère pas le plug-and-play.** Bien que Linux soit souvent distribué avec des programmes qui détectent et configurent automatiquement les matériels les plus courants, il ne dispose pas d'un support intégré permettant la gestion des périphériques plug-and-play. Vous risquez donc de rencontrer plus de problèmes de configuration avec Linux qu'avec Windows.
- ✓ **Le système de fichiers Linux est différent de celui de Windows.** Pour découvrir le fonctionnement du système de fichiers de Linux, reportez-vous à l'encadré « Où est passé mon disque C ? »
- ✓ **Linux fonctionne mieux sur les vieux ordinateurs que les différentes versions de Windows.** Linux est le système d'exploitation idéal pour un vieux Pentium doté d'au moins 32 Mo de RAM et d'un disque dur de 2 Go.

Avec un brin d'astuce, vous pouvez même parvenir à faire tourner Linux sur un 486, modestement équipé de 4 Mo de RAM et de quelques centaines de Mo d'espace disque.



Choisir une distribution Linux

Le noyau (c'est-à-dire les fonctions de base) du système d'exploitation Linux étant libre, plusieurs sociétés ont créé leurs propres *distributions* Linux, qui comprennent le système d'exploitation Linux et tout un tas d'accessoires tels que des outils d'administration, des serveurs Web et d'autres utilitaires précieux ainsi que de la documentation papier. Ces distributions sont bon marché, entre 25 et 100 euros et d'un excellent rapport qualité/prix.

Voici les distributions Linux les plus connues :

- ✓ **Fedora** est de loin la distribution Linux qui a le plus de succès. Auparavant, Fedora était une distribution proposée par Red Hat. Depuis quelques années, la société a changé sa stratégie de distribution, en faisant de cette distribution un projet de communauté. La distribution Fedora peut être téléchargée gratuitement à l'adresse www.fedora-fr.org. Vous pouvez également vous la procurer en achetant un livre contenant la distribution Fedora sur DVD ou sur CD-ROM.
Tous les exemples de ce livre sont basés sur Fedora 12.
- ✓ **Ubuntu**, un projet Linux réparti à travers le monde ; il est conçu pour de nombreuses langues. Consultez le site www.ubuntu-fr.org pour plus d'informations.

- ✓ **Linux Mandriva**, autre distribution populaire de Linux, est souvent conseillée aux débutants pour sa facilité d'installation. Consultez le site www.mandriva.com pour plus d'informations.
- ✓ **SuSE** comprend plus de 1 500 programmes et utilitaires Linux répartis sur six CD-ROM pour monter un réseau, un serveur Web, une messagerie ou un serveur de commerce électronique. Pour plus de précisions, visitez le site www.novel.com/linux.
- ✓ **Slackware**, l'une des distributions Linux les plus anciennes, a encore du succès, surtout auprès des utilisateurs Linux de la première heure. L'installation complète de Slackware vous permet de disposer des outils nécessaires pour monter un serveur réseau ou Internet. Pour plus d'informations, consultez le site www.slackware.com.

Où est passé mon disque C ?

Linux et Windows gèrent d'une manière totalement différente les disques et partitions. Les utilisateurs expérimentés de Windows peuvent éprouver pas mal de difficultés à s'habituer au système employé par Linux.

Windows se sert d'une lettre différente pour chaque disque et partition. Par exemple, si vous disposez d'un seul disque dur comprenant trois partitions, Windows considère celles-ci comme les disques C, D et E. Chacun de ces disques a son propre répertoire racine, qui peut lui aussi contenir des répertoires. Pour Windows, C, D et E sont des disques indépendants, même s'il s'agit en fait de trois partitions d'un seul disque.

Linux n'a pas recours à des lettres pour les disques. Tous les disques et partitions sont regroupés dans un seul répertoire. Une des partitions est considérée comme la partition racine (*root*). La racine correspond en gros au disque C sous Windows. Ensuite, les autres partitions sont montées sur la racine et considérées comme des répertoires. Par exemple, vous pouvez désigner la première racine comme la partition racine, nommer la deuxième `/utilisateur` puis la troisième `/var`. Ainsi, les fichiers stockés dans le répertoire `/utilisateur` seront en fait placés dans la deuxième partition et ceux du répertoire `/var` dans la troisième.

Le répertoire vers lequel le disque monte s'appelle le *point de montage* (*mount point*).

Notez que Linux utilise des barres obliques (/) pour séparer les noms dans les répertoires alors que Windows emploie des barres obliques inversées (\). Les personnes qui découvrent Linux font souvent l'erreur de taper des \ à la place des /.

Dans le même domaine, Linux fonctionne avec une convention de nommage de fichiers différente de celle de Windows. Sous Windows, les noms de fichiers se terminent par une extension de trois lettres, séparée du corps du nom par un point. Cette extension sert à indiquer le type de fichier. Par exemple, les fichiers se terminant par `.exe` sont des programmes et les `.doc` des documents de traitement de texte.

Linux n'utilise pas d'extension mais des points pour séparer les différentes parties, la dernière indiquant la plupart du temps le type de fichier. Par exemple, `ldap.conf` et `pine.conf` sont tous deux des fichiers de configuration.

Toutes les distributions de Linux comprennent les mêmes composants de base : le noyau Linux, un serveur X, des gestionnaires de fenêtres très connus tels que GNOME et KDE, des compilateurs, des logiciels Internet tels qu'Apache, Sendmail, etc. Cependant, toutes les distributions ne sont pas équivalentes. Chaque fabricant crée ses propres programmes d'installation et de configuration de Linux.

Le programme d'installation est le juge de paix de toutes les distributions. Celles évoquées dans cette section ont chacune des programmes d'installation faciles d'emploi qui détectent automatiquement le matériel de votre ordinateur et configurent Linux en fonction de ce matériel, vous évitant ainsi pratiquement toutes les corvées d'une configuration manuelle. Le programme d'installation vous laisse également le choix des outils et vous permet de configurer un ou plusieurs comptes utilisateurs en plus du compte root (le compte d'administration).

Installer Linux

Toutes les distributions décrites dans la section « Choisir une distribution Linux » contiennent un programme d'installation qui vous simplifie la vie. Ce dernier vous pose une série de questions sur votre matériel, les composants Linux que vous souhaitez installer et la configuration retenue pour certaines fonctionnalités. Puis, il copie les fichiers nécessaires sur votre disque dur et configure Linux.



Si l'idée d'installer Linux vous effraie, vous pouvez acheter un ordinateur avec Linux préinstallé, bien que cela soit plus difficile à trouver qu'un ordinateur avec Windows déjà installé.

Voici les étapes de planification à réaliser avant de démarrer l'installation :

- ✓ Dressez une liste des *composants matériels* de votre ordinateur et de leur *configuration*.
Soyez le plus précis possible : inscrivez pour chaque composant le nom du fabricant, le numéro de série ainsi que, le cas échéant, les données sur leur configuration, les IRQ et l'adresse d'E/S par exemple.
- ✓ Définissez les partitions à créer sur votre disque dur.
Alors que Windows s'installe généralement sur une seule partition, Linux requiert pour sa part au minimum *trois* partitions :
 - **Une partition d'amorçage.** Elle doit être petite ; 16 Mo conseillés. Elle contient le noyau du système d'exploitation et sert à démarrer Linux correctement sur certaines machines.

- **Une partition de swap.** Sa taille doit être équivalente au double de la quantité de RAM dont dispose votre ordinateur. Par exemple, si l'ordinateur est doté de 2 Go de RAM, 4 Go doivent être réservés à la partition de swap. Linux utilise cette partition comme de la RAM supplémentaire.
- **Une partition racine (root).** Elle occupe généralement l'espace disque libre restant. La partition racine contient tous les fichiers et données employés par Linux.

Vous pouvez créer d'autres partitions si vous le souhaitez. Le programme d'installation comprend une fonctionnalité de partitionnement de disques qui vous permet de définir les partitions et de fixer le point de montage pour chacune d'elles. Pour plus d'informations sur les partitions, lisez l'encadré « Où est passé mon disque C ? » plus haut dans ce chapitre.

Linux est ravi de partager votre disque dur avec un autre système d'exploitation tel que Windows. Cependant, vous devrez peut-être partitionner de nouveau votre disque afin d'installer Linux sans supprimer votre système d'exploitation existant. Je vous conseille alors de vous procurer un exemplaire de PartitionMagic ou un programme de partitionnement équivalent. Cela vous permettra de jongler avec vos partitions sans perdre votre système d'exploitation actuel.

- ✓ Vous devrez également choisir les *options Linux* à installer avec le noyau Linux :
 - Si vous disposez de suffisamment d'espace disque, installez l'intégralité des outils fournis dans votre distribution. De cette manière, si plus tard vous avez besoin d'un de ces produits, vous n'aurez pas à chercher comment l'installer en dehors du programme d'installation.
 - Si vous manquez d'espace disque, veillez à installer au moins les produits réseau et Internet qui comprennent Apache, Sendmail, FTP et Samba.
- ✓ Définissez le mot de passe du compte root.
- ✓ Dans la plupart des distributions, vous aurez à décider de créer ou non un ou plusieurs *comptes utilisateurs*.

Créez au moins un compte utilisateur pendant l'installation pour que vous puissiez vous connecter à Linux en tant qu'utilisateur plutôt qu'à partir du compte root. Ainsi, vous pouvez vous entraîner à taper des commandes Linux sans craindre de supprimer ou d'endommager un fichier système important.



Ouvrir et fermer une session

Tout utilisateur qui accède à un système Linux, que ce soit localement ou sur un réseau, doit être authentifié par un compte utilisateur valide. Les sections qui suivent expliquent le pourquoi du comment de l'ouverture et de la fermeture d'une session Linux et la façon d'arrêter le système.



Se connecter et se déconnecter équivaut respectivement à ouvrir et fermer une session. Les termes sont équivalents et vous pouvez les utiliser indifféremment.

Ouvrir une session

Au démarrage, Linux affiche une série de messages vous informant de l'activation des divers services du système d'exploitation. Si vous avez opté pour X Server lors de l'installation de Linux, vous serez probablement salué par un écran d'ouverture de session, représenté dans la Figure 25.1. Pour vous connecter à Linux, entrez votre ID d'utilisateur, saisissez votre mot de passe quand vous y êtes invité et appuyez sur Entrée.



Au cours du processus d'installation, un agent de configuration a créé un compte pour vous. Chaque fois que c'est possible, vous devez utiliser ce compte plutôt que le compte utilisateur root. N'utilisez ce dernier que si vous modifiez considérablement la configuration du système. Si vous effectuez un travail de routine, ouvrez une session en tant qu'utilisateur ordinaire pour éviter de corrompre le système.

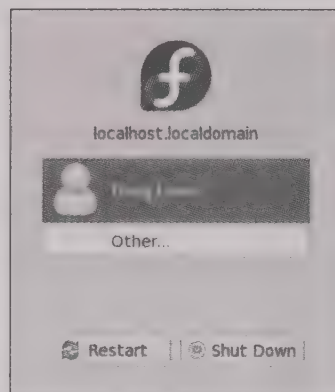


Figure 25.1 : Connexion à Linux.

Quand vous ouvrez une session, Linux mouline un moment puis il affiche le bureau GNOME décrit ultérieurement dans ce chapitre.

Si vous n'avez pas installé X Server, vous verrez apparaître une invite login de ce genre :

```
Fedora release 10 (Cambridge)
Kernel 2.6.27.5-117.fc10.o686 on an i686
LSERVER login:
```

L'invite login affiche la version de Linux (Fedora release 10), la version du noyau sur laquelle elle est basée (2.6.27...), l'architecture du processeur (i686) ainsi que le nom d'hôte du serveur (LSERVER). Pour ouvrir une session, tapez votre ID d'utilisateur, appuyez sur Entrée, entrez le mot de passe et appuyez de nouveau sur Entrée.

Si la connexion a réussi, vous êtes gratifié d'une invite telle que celle-ci :

```
Last login: Sun Jul 5 20:00:56 on :0  
[doug@LSERVER doug]$
```

Dans l'interpréteur de commandes standard de Linux, le caractère d'invite standard est le signe « dollar » (\$) plutôt que le signe « supérieur à » (>) de MS-DOS ou de Windows. Remarquez aussi que l'invite indique les noms d'utilisateur et de serveur (doug@LSERVER) ainsi que le nom du répertoire courant (doug).

Fermer la session

Une fois que vous avez ouvert une session, il faut savoir comment la fermer ! Si vous vous êtes connecté sous GNOME, cliquez sur le menu Système et exécutez la commande Fermer la session. Une boîte de dialogue vous demande si vous voulez vraiment fermer la session. Cliquez sur OK.

L'interpréteur de commandes permet de fermer une session de trois manières :

- ✓ En entrant la commande `logout`.
- ✓ En tapant la commande `exit`.
- ✓ En appuyant sur Ctrl+D.

Éteindre

Comme pour tout système d'exploitation, vous ne devez jamais éteindre un serveur Linux sans l'avoir d'abord quitté proprement. Un système Linux peut être fermé de trois manières :

- ✓ Appuyez sur Ctrl+Alt+Suppr.
- ✓ À partir de GNOME, cliquez sur le menu Système et sélectionnez Éteindre. À l'affichage de la boîte de dialogue de confirmation, optez pour Éteindre ou Redémarrer.
- ✓ Entrez `halt` dans l'interpréteur de commandes.

Utiliser GNOME

Bien que toutes les tâches de configuration de Linux puissent être effectuées par des lignes de commandes, la distribution Fedora comporte un certain nombre d'outils de configuration basés sur GNOME. Même s'il est possible de configurer Linux presque entièrement à partir de GNOME, il vous faudra de temps en temps recourir à une ligne de commandes.

La Figure 25.2 représente un bureau GNOME type dans lequel l'application Éditeur de texte est ouverte. Comme vous le constatez, le bureau GNOME ressemble beaucoup à celui de Microsoft Windows. En fait, bon nombre des manipulations de Windows comme le déplacement et le redimensionnement des fenêtres, leur réduction ou leur agrandissement et le glisser-déposer des éléments d'une fenêtre à une autre, sont identiques dans GNOME. Vous ne devriez pas être dépaycé.

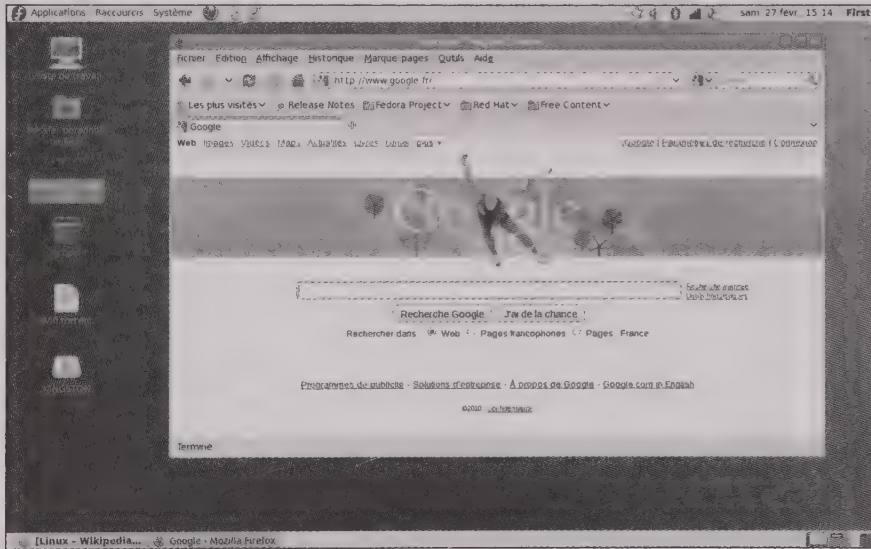


Figure 25.2 : Bureau GNOME type.

Voici quelques-unes des fonctionnalités importantes du bureau GNOME :

- ✓ Sur le **bureau** lui-même, plusieurs icônes permettent d'accéder aux fonctions les plus courantes. L'icône Dossier personnel conduit au répertoire de départ. L'icône Poste de travail est similaire à l'icône Ordinateur de Windows. De même, l'icône Corbeille est identique à celle de Windows.

- ✓ Le **tableau de bord** situé dans la partie supérieure du bureau contient plusieurs menus et icônes. Le menu Applications regroupe les applications que vous pouvez exécuter tandis que le menu Raccourcis comprend les actions que vous pouvez effectuer.
- ✓ Vous avez dit **espaces de travail** ? Un *espace de travail* est comme un bureau séparé où vous pouvez garder des fenêtres ouvertes pour réduire l'encombrement de votre écran. Le tableau de bord situé au bas du bureau propose un outil (Sélecteur de fenêtres) qui vous permet d'alterner entre les espaces de travail actifs en cliquant sur l'un des rectangles.

Utiliser l'interpréteur de commandes

Si vous devez exécuter directement des commandes dans Linux, sachez qu'il existe deux manières d'accéder à l'*interpréteur de commandes*, le programme dans lequel vous tapez vos lignes de commandes :

- ✓ La première consiste à appuyer sur Ctrl+Alt+Fx (une des touches de fonction) pour afficher l'une des consoles virtuelles. Vous pouvez ensuite ouvrir une session et exécuter toutes les commandes que vous voulez. Appuyez sur Ctrl+Alt+F7 pour revenir dans l'environnement graphique de GNOME.
- ✓ Vous pouvez aussi ouvrir l'interpréteur de commandes directement dans GNOME en choisissant Applications/Accessoires/Terminal. Cette action ouvre l'interpréteur de commandes. Il apparaît dans une fenêtre située sur le bureau GNOME, comme le montre la Figure 25.3. Comme l'interpréteur fonctionne à l'intérieur du compte utilisateur, vous n'avez pas à ouvrir de session. Vous pouvez aussitôt taper vos commandes. Pour fermer la fenêtre, tapez **Exit**.

Gérer les comptes utilisateurs

L'une des principales tâches d'un administrateur réseau est la création des comptes utilisateurs. Le programme d'installation en a créé un pour vous d'office mais vous devrez probablement en définir d'autres. Chaque compte utilisateur Linux contient les informations suivantes :

- ✓ **Nom d'utilisateur.** Le nom que l'utilisateur saisit pour se connecter au système Linux.

- ✓ **Nom complet.** Le nom complet de l'utilisateur.
- ✓ **Répertoire home.** Le répertoire dans lequel l'utilisateur est placé lorsqu'il se connecte. Dans Fedora Linux, le répertoire par défaut est /home/nom. Par exemple, si le nom de l'utilisateur est Dupont, le répertoire d'accueil sera /home/dupont.
- ✓ **Shell.** Le programme qui traite les commandes Linux. Il existe plusieurs programmes Shell. Dans la plupart des distributions, le shell par défaut est /bin/bash.
- ✓ **Groupe.** Vous pouvez créer des comptes de groupes, ce qui permet d'accorder facilement les mêmes droits à des groupes d'utilisateurs.
- ✓ **ID utilisateur.** L'identifiant interne de l'utilisateur.

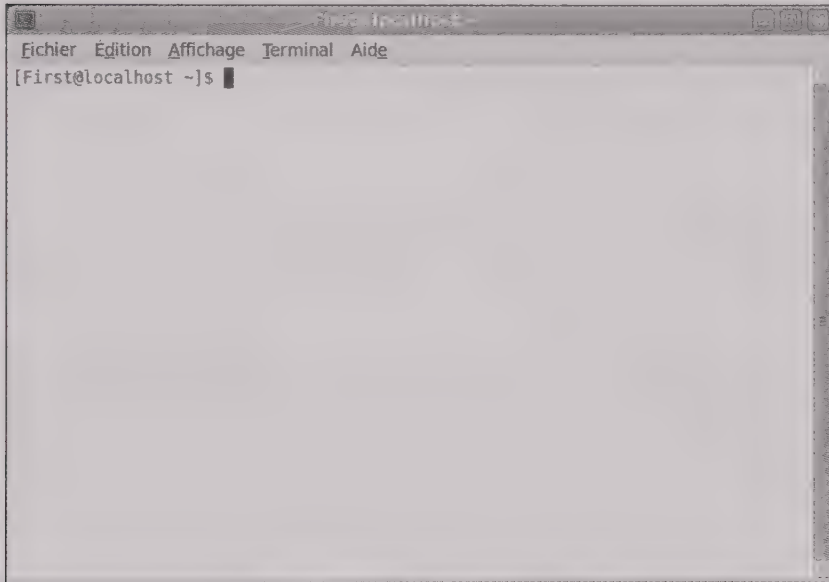


Figure 25.3 : Utilisation d'une fenêtre Terminal pour exécuter des commandes Linux.

La commande `useradd` permet d'ajouter de nouveaux utilisateurs. Par exemple, pour créer un compte utilisateur nommé `coq` et lui attribuer les valeurs par défaut pour les autres informations du compte, ouvrez une fenêtre Terminal (ou basculez dans une console virtuelle) et tapez la commande suivante :

```
# useradd coq
```

La commande `useradd` comprend de nombreux paramètres facultatifs qui servent à définir des informations sur le compte, comme le répertoire home et le shell de l'utilisateur.

Heureusement, la plupart des distributions comprennent des programmes spéciaux qui simplifient les tâches courantes d'administration du système. La distribution Fedora ne fait pas exception ; elle est livrée avec un programme nommé Gestionnaire d'utilisateurs, illustré dans la Figure 25.4. Pour démarrer ce programme, exécutez la commande Système/Administration/Utilisateurs et groupes.

Pour créer un compte utilisateur avec le Gestionnaire d'utilisateurs, cliquez sur le bouton Ajouter un utilisateur. Cette action affiche une boîte de dialogue qui demande le nom de l'utilisateur, le mot de passe et d'autres informations. Remplissez les champs puis cliquez sur Valider.

Le Gestionnaire d'utilisateurs permet aussi de créer des groupes. Vous vous simplifierez les tâches d'administration en accordant des autorisations à des groupes plutôt qu'à des utilisateurs isolés. Ensuite, si un utilisateur a besoin d'accéder à une ressource, vous l'ajouterez au groupe y ayant accès.

Pour créer un groupe, cliquez sur le bouton Ajouter un groupe. Une boîte de dialogue demande de le nommer ; entrez le nom que vous voulez puis cliquez sur Valider.

Pour ajouter un utilisateur à un groupe, ouvrez l'onglet Groupes, dans le Gestionnaire d'utilisateurs. Double-cliquez ensuite sur le nom du groupe auquel vous désirez ajouter des utilisateurs. La boîte de dialogue Propriétés du groupe apparaît. Cliquez sur l'onglet Utilisateurs du groupe puis cochez les utilisateurs qui doivent en faire partie.

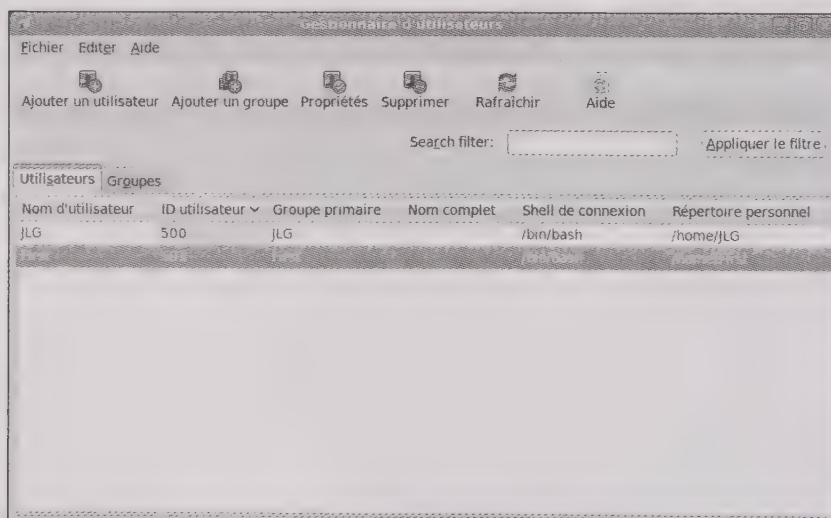


Figure 25.4 : Gestionnaire d'utilisateurs.

Configurer le réseau

Le plus souvent, la configuration d'un serveur Linux pour la mise en réseau s'effectue sans problème. Lorsque vous installez Linux, le programme d'installation détecte automatiquement les adaptateurs réseau et installe les pilotes appropriés. Il vous est ensuite demandé d'entrer les informations de base comme l'adresse IP de l'ordinateur, son nom d'hôte, etc.

Il vous arrivera parfois de devoir modifier manuellement les paramètres de réseau après l'installation. Ou bien vous devrez configurer des fonctions de réseau avancées qui ne l'avaient pas été au cours de l'installation. Dans les sections qui suivent, vous découvrirez les procédures de base pour la configuration des services de réseau Linux. Utiliser le programme de configuration réseau Fedora

Avant de pouvoir utiliser une interface de réseau, vous devez configurer ses options TCP/IP de base comme l'adresse IP, le nom d'hôte, les serveurs DNS, etc. Dans cette section, nous verrons comment le faire avec l'outil de configuration réseau Fedora. Pour y accéder, exécutez la commande `Système/Administration/Réseau`.



La plupart des distributions Linux proposent un programme similaire.

Le programme Configuration réseau vous permet de configurer les paramètres TCP/IP basiques pour une interface réseau. La Figure 25.5 représente le programme en action.

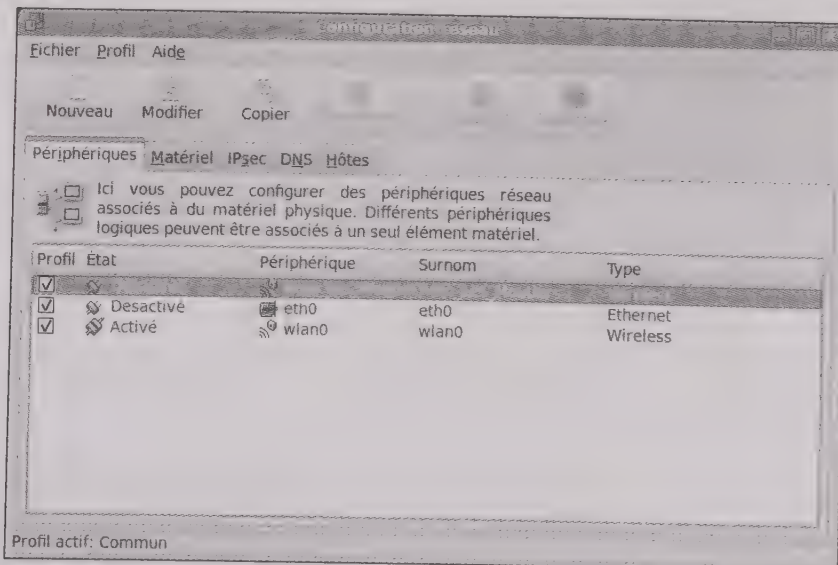


Figure 25.5 : Programme Configuration réseau.

La fenêtre principale du programme Configuration réseau affiche toutes les interfaces réseau installées dans l'ordinateur. Vous pouvez sélectionner n'importe laquelle et cliquer sur Modifier pour ouvrir une boîte de dialogue semblable à celle de la Figure 25.6. C'est là que vous définissez les options de configuration pour l'interface réseau comme l'adresse IP et d'autres informations TCP/IP.

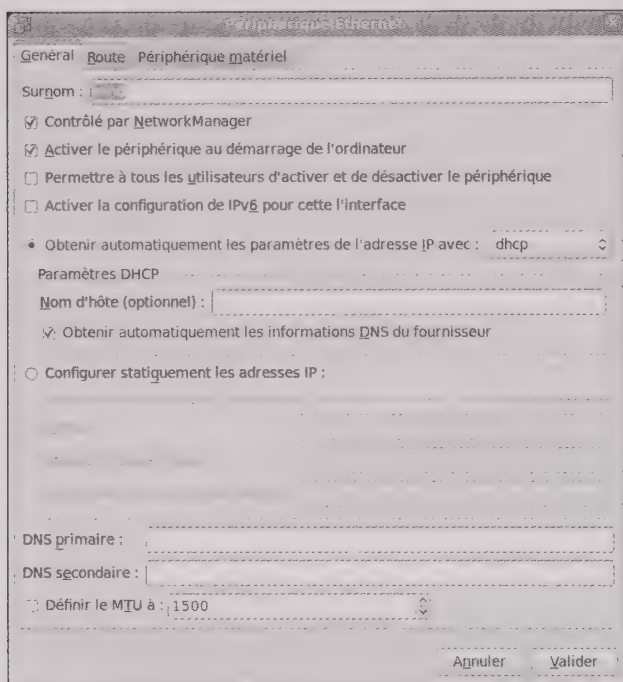


Figure 25.6 : La boîte de dialogue Périphérique Ethernet vous invite à configurer les paramètres TCP/IP de base.

Redémarrer le réseau

Dès que vous modifiez la configuration du réseau, vous devez redémarrer les services de réseau de Linux afin que les changements soient appliqués. Cette obligation vous paraîtra peut-être ennuyeuse mais estimez-vous heureux de ne pas avoir à redémarrer l'ordinateur. Il suffit simplement de redémarrer les services du réseau.

Les services de réseau d'un bureau GNOME peuvent être redémarrés en procédant comme suit :

1. Sur le bureau, exécutez la commande **Système/Administration / Services**.

La fenêtre de configuration des services apparaît, comme le montre la Figure 25.7.

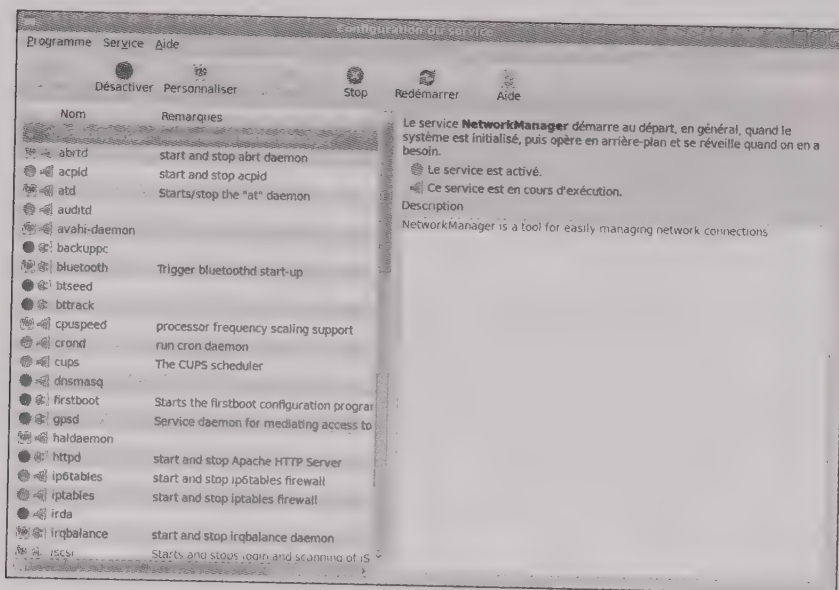


Figure 25.7 : Boîte de dialogue Configuration du service.

2. Sélectionnez le service Réseau.

Vous devrez faire défiler la liste des services pour le trouver.

3. Cliquez sur le bouton Redémarrer.

Le service est arrêté puis il est redémarré. Une petite boîte de dialogue affiche un message indiquant que le redémarrage du réseau a réussi.

4. Cliquez sur Valider.

Vous êtes rebasculé dans le programme Configuration du service.

5. Fermez le programme Configuration du service.

Si vous préférez travailler à partir de l'interpréteur de commandes, vous pourrez redémarrer le réseau en entrant la commande `service network restart`. Procéder de la sorte affiche un message semblable à celui-ci :

```
Shutting down interface eth0:      [ OK ]
Shutting down loopback interface:  [ OK ]
Setting network parameters:        [ OK ]
Bringing up loopback interface:    [ OK ]
Bringing up interface eth0:        [ OK ]
```

Danser la samba

Jusqu'à présent, vous pensiez sans doute que la samba était une danse brésilienne faite de rythmes joyeux et de pas complexes. Dans l'univers Linux, *Samba* est un programme de partage de fichiers et d'imprimantes qui permet à Linux d'imiter un serveur de fichiers et d'impression afin que des ordinateurs sous Windows puissent avoir accès à des répertoires Linux et des imprimantes. Pour utiliser Linux en tant que serveur de fichiers ou d'impression sur un réseau Windows, vous devrez apprendre à danser la samba.

Comprendre Samba

Les systèmes de fichiers de Linux et de Windows étant très différents, il n'est pas possible de créer un serveur de fichiers Linux en vous contentant d'accorder aux utilisateurs sous Windows un accès aux répertoires Linux. Les ordinateurs clients Windows ne parviendraient pas à accéder aux fichiers des répertoires Linux car les différences entre les deux systèmes sont trop importantes. En voici quelques-unes :

- ✓ Les fichiers de Linux différencient la casse mais pas ceux de Windows. Par exemple, sous Windows, *Fichier1.txt* et *fichier1.txt*, c'est pareil. Sous Linux, ce sont deux fichiers différents.
- ✓ Sous Linux, les noms de fichiers peuvent contenir un point. Sous Windows, un seul point est autorisé (pour séparer le nom de son extension).
- ✓ Windows propose des attributs comme *Lecture seule* ou *Archive*. Ils n'existent pas sous Linux.

Plus fondamentalement, la mise en réseau sous Windows est fondée sur un protocole *SMB* (*Server Message Block*, bloc de message de serveur) qui gère les échanges des données de fichiers entre les serveurs de fichiers et les clients. Linux n'est pas doté d'un support SMB. C'est pourquoi Samba est requis.

Samba est un programme qui simule le comportement d'un serveur basé sur Windows en implémentant le protocole SMB. Par conséquent, lorsque vous faites tourner Samba sur un serveur Linux, les ordinateurs sous Windows, au sein du réseau, considèrent le serveur Linux comme un serveur Windows.

À l'instar d'un serveur Windows, Samba crée et désigne des répertoires en tant que partages. Un *partage* est simplement un répertoire rendu accessible aux autres utilisateurs via le réseau. Chaque partage présente les éléments suivants :

- ✓ **Un nom de partage.** C'est le nom sous lequel le partage est connu sur le réseau. Il doit, autant que possible, ne pas dépasser huit caractères.
- ✓ **Un chemin.** C'est le chemin vers le répertoire qui est partagé sur l'ordinateur Linux. Exemple : `\Users\Doug`.
- ✓ **Une description.** C'est un texte bref qui décrit le partage.
- ✓ **Un accès.** C'est une liste d'utilisateurs ou de groupes auxquels un accès au partage a été accordé.



Samba propose aussi un programme client qui permet aux ordinateurs sous Linux d'accéder à des serveurs de fichiers Windows.

Pourquoi les concepteurs de *Samba* ont-ils choisi ce nom pour leur programme ? Simplement parce que le protocole de communication des serveurs de fichiers et d'impression sous Windows s'appelle *SMB* (*Server Message Block*). Il suffit d'ajouter deux voyelles à SMB pour obtenir Samba.

Installer Samba

Si vous n'avez pas installé Samba lors de l'installation de Linux, vous devrez le faire maintenant. La manière la plus simple consiste à utiliser l'outil de gestion livré avec GNOME : insérez le CD-ROM de la distribution Fedora puis cliquez sur Oui pour donner votre accord pour démarrer le programme autorun. Dans la fenêtre Gestionnaire de paquets qui apparaît, sélectionnez le groupe Serveur de fichiers Windows, ce qui entraîne l'installation de Samba.



Samba sera *inutilisable* si vous activez les paramètres par défaut du pare-feu de Linux sur l'ordinateur qui exécute Samba. Le pare-feu Linux a été conçu pour empêcher les utilisateurs d'accéder à des services de réseau comme Samba. Il est prévu pour s'interposer entre Internet et votre réseau local et non entre Samba et le réseau local. Bien qu'il soit possible de configurer le pare-feu pour n'autoriser l'accès à Samba qu'au réseau interne, il est recommandé d'utiliser le pare-feu sur un ordinateur séparé. En procédant ainsi, l'ordinateur équipé du pare-feu peut se concentrer sur sa tâche de filtrage, le serveur de fichiers se concentrant sur ses tâches de serveur.

Démarrer et arrêter Samba

Avant de pouvoir utiliser Samba, vous devez démarrer ses deux « daemon » (un *daemon* est un processus qui s'exécute en arrière-plan) : `smbd` et `nmbd`. Tous deux peuvent être activés simultanément en démarrant le service `smb`. Utilisez cette commande dans l'interpréteur :

```
service smb start
```

Dès que vous modifiez la configuration (ajout d'un nouveau partage, création d'un nouvel utilisateur Samba...), vous devez arrêter et redémarrer le service avec cette commande :

```
service smb restart
```

Si vous préférez, vous pouvez arrêter et démarrer le service avec deux commandes distinctes :

```
service smb stop
service smb start
```

Si vous n'êtes pas certain que Samba est en cours d'exécution, entrez cette commande :

```
service smb status
```

Un message vous indiquera si les *daemon* `smbd` et `nmbd` sont en cours d'exécution.

Pour que Samba soit activé automatiquement au démarrage de Linux, utilisez cette commande :

```
chkconfig -level 35 smb on
```

Pour vous assurer que la commande `chkconfig` a bien fonctionné, entrez cette commande :

```
chkconfig -list smb
```

Vous devriez obtenir une sortie semblable à celle-ci :

```
Smb          0:off  1:off  2:off  3:on   4:off  5:on   6:off
```



Les services peuvent être configurés séparément pour démarrer automatiquement à chacun des six *niveaux de démarrage* de Linux. Le *niveau de démarrage 3* est l'opération classique sans un serveur X, le *niveau 5* est l'opération normale avec un serveur X. Ainsi, configurer `smb` pour démarrer aux niveaux 3 et 5 rend `smb` disponible, que vous utilisiez ou non une interface graphique.

Il est aussi possible de démarrer et d'arrêter Samba en utilisant l'outil Configuration du service, illustré dans la Figure 25.7. Faites défiler la liste des services jusqu'à ce que vous trouviez le service `smb`. Dans la barre d'outils, trois boutons servent à démarrer, arrêter ou redémarrer un service.

Utiliser l'outil de configuration du serveur Samba sous Fedora

La distribution Fedora est dotée d'un outil très pratique, basé sur GNOME, qui simplifie la configuration de Samba. Pour le démarrer, exécutez la commande `Système/Administration/Samba`. La boîte de dialogue Configuration du serveur Samba apparaît, comme le montre la Figure 25.8. Cet utilitaire permet de configurer les paramètres de base du serveur et de gérer les partages.

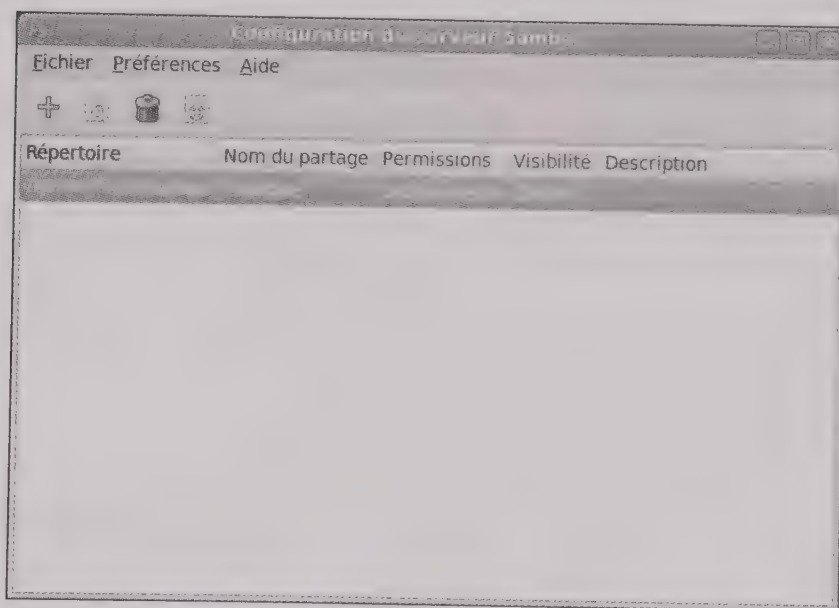


Figure 25.8 : Utilisation de l'outil de configuration du serveur Samba.

Pour rendre le serveur Samba visible sur le réseau, choisissez `Préférences/Paramètres du serveur`. Vous accédez à une boîte de dialogue permettant de définir le nom du groupe de travail (qui doit correspondre à celui du groupe de travail ou du domaine auquel le serveur Samba doit appartenir) et d'entrer une description du serveur. Vous pouvez aussi spécifier quelques paramètres de sécurité de base qui contrôlent la manière dont les utilisateurs accèdent au serveur Samba.

Quatre types d'authentification peuvent être définis pour le serveur Samba :

- ✓ **Domaine.** Ce mode configure le serveur Samba pour qu'il puisse utiliser un contrôleur de domaine Windows pour vérifier l'identité de l'utilisateur. Si vous spécifiez cette option, vous devez :



- Fournir le nom du contrôleur de domaine dans le champ Serveur d'authentification.

- Spécifier Oui pour le champ Crypter les mots de passe.

✓ **Serveur.** Ce mode configure Samba pour utiliser un autre serveur Samba pour authentifier les utilisateurs.

Si vous gérez plusieurs serveurs Samba, cette fonction permet de définir des comptes utilisateurs sur un seul d'entre eux. Ensuite, indiquez dans le champ Serveur d'authentification le nom du serveur Samba chargé des authentifications.

✓ **Partage.** Ce mode accorde des autorisations distinctes aux utilisateurs, pour chaque partage auquel ils tentent d'accéder.

✓ **Utilisateur.** Il exige des utilisateurs qu'ils fournissent un nom d'utilisateur valide ainsi que leur mot de passe lorsqu'ils se connectent pour la première fois à un serveur Samba. Cette authentification leur accorde l'accès à tous les partages du serveur, sous réserve des restrictions qui peuvent avoir été appliquées à un compte.

Le mode Utilisateur est le mode par défaut.



Pour chaque utilisateur du réseau qui doit accéder au serveur Samba, vous devez :

1. Créer un compte utilisateur Linux.

2. Créer un compte utilisateur Samba spécifique.



Le compte utilisateur Samba est associé au compte utilisateur Linux existant. Aussi le compte Linux doit-il être créé en premier.

Pour créer un compte utilisateur Samba, exécutez la commande Préférence/Utilisateurs Samba dans la fenêtre de configuration du serveur Samba. La boîte de dialogue Utilisateurs Samba apparaît, comme le montre la Figure 25.9. C'est là que vous pouvez créer, modifier ou supprimer des utilisateurs.

Pour être utile, un serveur de fichiers doit proposer plusieurs *ressources* partagées, configurées pour être accessibles via le réseau. Là encore, vous utiliserez le programme Configuration du serveur Samba pour gérer les

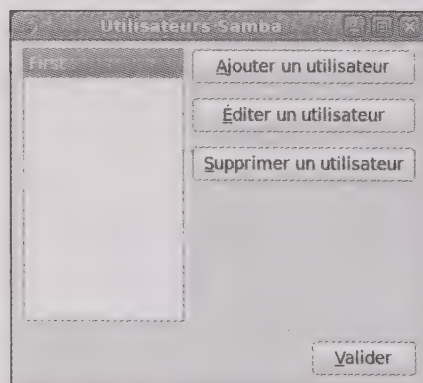


Figure 25.9 : La boîte de dialogue Utilisateurs Samba présente une liste des utilisateurs Samba.

partages. Pour ajouter un partage, cliquez sur le bouton Ajouter un nouveau partage Samba. La boîte de dialogue Créer un partage Samba s'ouvre (Figure 25.10). Vous pouvez :

- ✓ Entrer le chemin du répertoire à partager.
- ✓ Saisir une description du partage.
- ✓ Choisir l'accès en lecture seule ou en lecture-écriture.
- ✓ Ouvrir l'onglet Accès si vous souhaitez imposer des restrictions, par exemple, à des utilisateurs spécifiques.

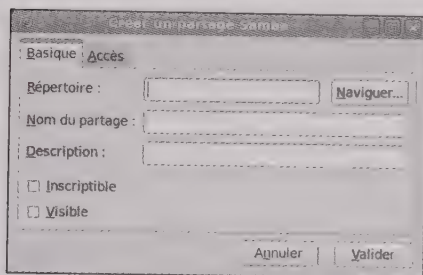


Figure 25.10 : Boîte de dialogue Créer un partage Samba.



Quand vous créez un nouveau partage avec le programme Configuration du serveur Samba, le partage doit être immédiatement visible par les autres utilisateurs du réseau. Si ce n'est pas le cas, essayez de redémarrer le serveur Samba, comme je l'ai décrit dans la section « Démarrer et arrêter Samba », précédemment dans ce chapitre.

Chapitre 26

Créer un réseau Macintosh

Dans ce chapitre :

- ▶ Mettre en place un réseau Macintosh.
 - ▶ Utiliser un réseau Macintosh.
 - ▶ Mélanger des PC et des Mac.
-

Jusqu'à présent, ce livre n'a traité que de la mise en réseau de PC, comme si Microsoft était le seul concepteur de systèmes d'exploitation. Pour être politiquement correct, il fallait au moins parler de l'existence d'une espèce d'ordinateurs totalement différente : le Macintosh d'Apple.

Ce chapitre vous montre comment créer un réseau Macintosh et mélanger des Mac et des PC sur un même réseau. Il ne s'agit pas d'une étude approfondie sur le sujet mais cela constitue une bonne base pour démarrer.

Tout ce qu'il faut savoir pour monter un réseau Macintosh

Les sections suivantes présentent les notions importantes sur la mise en réseau d'ordinateurs Macintosh, que vous devez connaître avant d'effectuer votre câblage.

Protocoles réseau Mac

Tout Macintosh, depuis le premier construit en 1984, dispose d'une fonctionnalité réseau. Bien entendu, les nouveaux Mac proposent des fonctionnalités réseau intégrées bien meilleures que celles des anciens modèles. Les

derniers-nés d'Apple possèdent des cartes Ethernet gigabits intégrées et des fonctions réseau évoluées qui font partie du système d'exploitation réseau et sont semblables à celles de Windows. Ce qu'il y a de formidable avec les réseaux Macintosh, c'est que les cartes réseau sont intégrées : pas besoin de s'embêter à installer et configurer le réseau.

Au départ, les ordinateurs Macintosh utilisaient des protocoles réseau appelés *Apple Talk*. Au milieu des années 1990, Apple Talk a été remplacé par un schéma réseau nommé *Open Transport*.

La génération actuelle de Mac utilise les protocoles normalisés TCP/IP. Le seul protocole ayant subsisté de l'époque d'Apple Talk et qui est toujours utilisé aujourd'hui est AFP, qui permet le partage de fichiers. Pour vous initier à ce protocole, lisez l'encadré « Quoi de neuf du côté de l'AFP ? »

Mac OS X Server

Apple commercialise également un système d'exploitation réseau dédié, Mac OS X Server (X se prononce *dix* et non *x*), conçu pour les ordinateurs PowerMac G3 et les versions ultérieures. Mac OS X Server repose sur Mach, un noyau du système d'exploitation UNIX. Ainsi, Mac OS X Server peut effectuer de nombreuses tâches de serveur avec une efficacité comparable à celle de n'importe quel système d'exploitation réseau, y compris Windows 2000, NetWare et UNIX.

Mac OS X Server est la version serveur du système d'exploitation Mac OS X, couramment utilisée sur les ordinateurs clients Macintosh.

Mac OS X Server intègre les applications et les fonctionnalités suivantes :

- ✓ Le **serveur Web Apache**, identique à celui qui tourne sur les systèmes Windows et Linux.
- ✓ **NetBoot**, une fonctionnalité qui simplifie l'administration des ordinateurs clients.
- ✓ Des **services de fichiers via AFP**.
- ✓ **WebObjects**, un outil haut de gamme de création de pages Web.
- ✓ **QuickTime Streaming Server** qui permet au serveur de diffuser des programmes multimédias sur le réseau.

Tout ce qu'il faut savoir pour utiliser un réseau Macintosh

Voici quelques-unes des questions qui se posent le plus souvent une fois le câblage du réseau installé. À noter que les sections suivantes partent du principe que vous vous servez d'AppleTalk et de Mac OS X. Les procédures peuvent quelque peu varier si vous travaillez dans un environnement Open Transport ou avec une version antérieure de Mac OS.

Quoi de neuf du côté de l'AFP ?

Dans l'univers Apple, AFP ne désigne pas la célèbre agence de presse mais AppleTalk Filing Protocol. C'est la partie d'Apple Talk qui gère le stockage et l'accès des fichiers sur le réseau. AFP permet le partage de fichiers avec des ordinateurs non Macintosh. En effet, vous pouvez intégrer des Mac dans tout système d'exploitation réseau qui reconnaît AFP. NetWare et toutes les versions de Windows depuis Windows 95 utilisent AFP pour prendre en charge les Mac dans leurs réseaux.

Au cas où vous seriez intéressé (vous devriez l'être), AFP est un protocole de la couche de présentation. Reportez-vous au Chapitre 30 si vous n'avez pas la moindre idée de ce que c'est.

Configurer un Mac pour travailler en réseau

Avant d'accéder au réseau, vous devrez configurer votre Mac en activant AppleTalk et en lui attribuant un nom et un mot de passe.

Activer AppleTalk

Une fois tous les câbles en place, vous devez activer AppleTalk. Voici comment procéder :

1. Choisissez **Sélecteur** dans le menu **Apple** (la pomme).
2. Cochez la case **Activé**.
3. Fermez le **Sélecteur**.

Spécifier un nom et un mot de passe

Vous devez ensuite spécifier un nom d'utilisateur, un mot de passe et donner un nom à votre ordinateur. Ce processus permet aux autres utilisateurs du réseau d'accéder à votre Mac. Voici comment faire :

1. Ouvrez le tableau de bord **Partage de fichiers** depuis le menu **Apple** (**Apple/Tableaux de bord/Partage de fichiers**).
2. Saisissez votre nom dans le champ **Possesseur**.
3. Saisissez un mot de passe dans le champ **Mot de passe**.

N'oubliez pas de le mémoriser.

4. Pour identifier votre ordinateur, tapez un nom parlant dans le champ **Nom de l'ordinateur**.

D'autres utilisateurs du réseau pourront identifier votre ordinateur grâce à ce nom.

5. Cliquez sur le bouton **Fermer**.

Accéder à une imprimante réseau

Accéder à une imprimante réseau avec AppleTalk revient à accéder à une imprimante locale. Si le réseau comprend plusieurs imprimantes, ouvrez le **Sélecteur** pour sélectionner l'imprimante que vous souhaitez utiliser. Le **Sélecteur** affiche toutes les imprimantes disponibles sur le réseau ; choisissez-en une. Et gardez ceci à l'esprit :

- ✓ **N'oubliez pas d'activer l'impression en tâche de fond pour l'imprimante réseau.** Si vous ne le faites pas, le Mac sera bloqué jusqu'à ce que l'imprimante ait terminé de traiter votre travail d'impression, ce qui peut prendre longtemps si quelqu'un d'autre a décidé d'imprimer, juste avant vous, un rapport de 500 pages. Quand vous activez l'option **Impression en tâche de fond**, votre travail est redirigé vers un fichier puis envoyé à l'imprimante pendant que vous passez à une autre tâche.

Pour activer l'impression en tâche de fond :

1. Choisissez **Apple/Sélecteur**.
2. Dans le **Sélecteur**, sélectionnez une imprimante.
3. Cochez la case **Impression en tâche de fond**.

- ✓ **N'activez pas l'impression en tâche de fond si un serveur d'impression dédié a été installé.** Dans ce cas, les données à imprimer sont automatiquement rassemblées sur le disque du serveur d'impression, si bien que votre Mac n'a même pas à attendre que l'imprimante soit libre.

Partager des fichiers avec les autres utilisateurs

Pour partager les fichiers de votre Mac avec les autres utilisateurs, vous devez les configurer en tant que ressources partagées. Vous pouvez partager un disque entier ou des dossiers. Si vous le voulez, vous pouvez aussi limiter l'accès à quelques utilisateurs.

Avant de pouvoir partager des fichiers avec les autres utilisateurs, vous devez activer la fonctionnalité de partage de fichiers d'AppleTalk. Voici comment vous y prendre :

1. **Choisissez le tableau de bord Partage de fichiers dans le menu Apple.**
2. **Cliquez sur le bouton Activer dans la section Partage de fichiers du tableau de bord.**
3. **Cliquez sur le bouton Fermer.**

Pour partager un fichier ou un dossier, cliquez une fois sur le fichier ou le dossier. Ouvrez ensuite le menu Fichier, cliquez sur Lire les informations puis choisissez Partage dans le sous-menu qui apparaît. Vous pouvez aussi utiliser la section Partage de la fenêtre Infos pour restreindre l'accès au fichier ou au dossier.

Accéder aux fichiers partagés

Pour accéder aux fichiers depuis un autre Mac, suivez cette procédure :

1. **Choisissez le Sélecteur dans le menu Apple.**
2. **Cliquez sur l'icône AppleShare dans la fenêtre du Sélecteur.**
3. **Cliquez sur le nom de l'ordinateur auquel vous voulez accéder (si votre réseau comporte des zones, vous devrez tout d'abord cliquer sur la zone concernée).**
4. **Cliquez sur OK.**

Un écran de connexion apparaît.

5. **Si vous êtes un utilisateur enregistré sur l'ordinateur, cliquez sur le bouton Enregistré et saisissez votre nom et votre mot de passe. Autrement, cliquez sur le bouton Invité puis sur OK.**

Une liste des dossiers et des disques partagés apparaît.

6. **Cliquez sur ceux auxquels vous voulez accéder.**

Une case à cocher apparaît à côté de chaque élément de la liste. Si vous cochez cette case, vous vous connecterez automatiquement au fichier ou au disque partagé dès que vous démarrerez votre ordinateur.

7. Cliquez sur OK.



Avec Mac OS 8.5 ou ultérieur, vous pouvez également employer le navigateur réseau, qui figure dans le menu Apple, pour accéder aux disques et dossiers réseau. Dans le menu Apple, ouvrez simplement le navigateur réseau, double-cliquez sur le serveur qui héberge le disque ou le dossier partagé puis double-cliquez sur le disque ou le dossier que vous voulez utiliser.

Tout ce qu'il faut savoir pour mettre en réseau des Mac et des PC

La vie serait bien trop ennuyeuse si les Mac vivaient d'un côté de la rue et les PC de l'autre. Si votre entreprise dispose de Mac et de PC, il y a de fortes chances pour que vous finissiez par les mettre tous en réseau. Heureusement, il existe des solutions :

- ✓ Si votre réseau comporte un serveur OS X Server, vous pouvez utiliser le client Windows livré avec OS X Server pour connecter n'importe quelle version de Windows au serveur. Cela permet aux utilisateurs de Windows d'accéder aux imprimantes et aux fichiers partagés sur le serveur Macintosh.
- ✓ Les versions Windows Server possèdent une fonctionnalité nommée Services pour Macintosh qui permet aux ordinateurs Macintosh d'accéder aux fichiers et aux imprimantes gérés par Windows Server, sans avoir à installer un logiciel client particulier sur les Mac.
- ✓ Avec NetWare, vous devez acheter un logiciel client NetWare pour vos ordinateurs Macintosh. Une fois ce dernier installé, les Mac pourront accéder aux fichiers et aux imprimantes gérés par vos serveurs NetWare.



Le plus gros problème que pose la cohabitation de Mac et de PC sur un réseau est les divergences des règles de nommage des fichiers observées par Mac OS et Windows. Par exemple :

- ✓ Les noms des fichiers Macintosh sont limités à 31 caractères et ceux des fichiers Windows à 255 caractères.

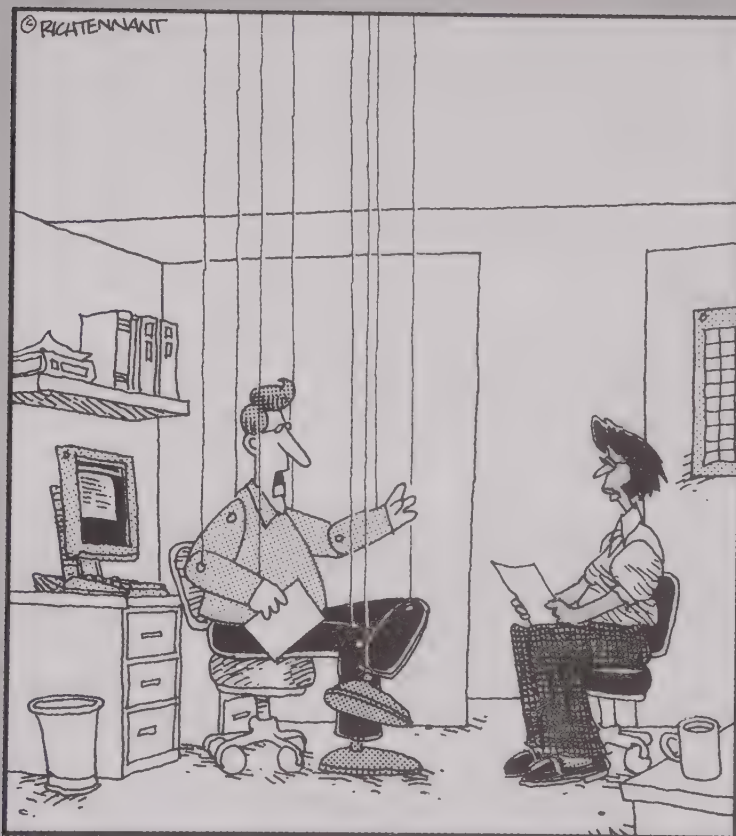
- ✓ Bien qu'un nom de fichier Macintosh puisse comprendre n'importe quel caractère *hormis le double point*, les noms de fichiers Windows ne peuvent pas contenir la barre oblique inversée, les signes inférieur et supérieur et quelques autres caractères excentriques.



Le meilleur moyen de résoudre ce conflit avec les noms de fichiers est d'employer des *noms courts* (moins de 31 caractères) et de choisir les lettres, chiffres et symboles les plus courants comme les traits d'union et les tirets bas. Bien qu'il soit possible de transformer les noms de fichiers en infraction avec les règles utilisées par le système pour les mettre en conformité avec Windows et Macintosh, cela génère parfois des noms ambigus ou incompréhensibles.

Septième partie

Les dix commandements



« Franchement, je vous avoue que l'idée d'un avenir
100 % sans fil m'angoisse terriblement. »

Dans cette partie...

Si vous conservez ce livre dans vos toilettes, les chapitres qui suivent seront ceux que vous lirez le plus souvent. Chacun d'eux présente dix (ou plus ou moins dix) commandements qu'il faut connaître, relatifs à différents aspects du réseau. Je ne vous en dis pas plus, les voilà, en direct !

Chapitre 27

Plus de dix grosses erreurs réseau

Dans ce chapitre :

- ▶ Faire des économies sur les câbles.
- ▶ Éteindre ou redémarrer un serveur alors que des utilisateurs sont connectés.
- ▶ Supprimer des fichiers importants sur le serveur.
- ▶ Copier un fichier du serveur, le modifier et le recopier sur le serveur.
- ▶ Relancer une impression parce que l'imprimante ne réagit pas.
- ▶ Supposer qu'un serveur est correctement sauvegardé.
- ▶ Se connecter à Internet sans vérifier les mesures de sécurité.
- ▶ Installer un WAP sans autorisation.
- ▶ Penser qu'il est impossible de travailler quand le serveur est en panne.
- ▶ Manquer d'espace disque sur un serveur du réseau.
- ▶ Accuser systématiquement le réseau.

À peine aviez-vous enfin appris à ne pas commettre les erreurs les plus énormes en informatique, comme vous servir du tiroir de votre lecteur de disque en guise de porte-gobelet, que le réseau a atterri sur votre bureau. Vous pouvez maintenant faire plein de bêtises qui feront mourir de rire un fondu d'informatique tant elles lui sembleront élémentaires. Bon d'accord, personne n'a eu à lui dire de ne pas rayer les disques, il est né avec un gène supplémentaire qui lui a donné une connaissance instinctive de ces choses-là.

Voici la liste des erreurs les plus fréquemment commises par les novices en matière de réseau. Ne tombez pas dans le panneau et votre geek préféré n'aura pas le plaisir de se moquer de vous.

Économiser sur le câble

Si votre réseau compte de nombreux ordinateurs ou si les machines sont situées dans des pièces différentes, vous feriez bien d'opter pour un câblage de qualité professionnelle, comprenant des prises murales, un panneau de jacks et des commutateurs d'excellente qualité. Il est bien sûr tentant de réduire les coûts en achetant des concentrateurs bon marché et en tirant directement du câble au rabais des concentrateurs vers chaque ordinateur du réseau. Mais, à terme, ce principe s'avérera bien plus coûteux qu'un investissement initial dans un câblage de qualité.

Voici quelques-unes des raisons pour lesquelles il ne faut pas négliger le câblage :

- ✓ Un bon câblage dure bien plus longtemps que tous les ordinateurs qu'il relie, comptez dix ou quinze ans. À cet âge, les ordinateurs de votre réseau seront dans un musée de l'informatique depuis belle lurette.
- ✓ Le câblage est un travail difficile. Personne n'aime vraiment aller dans les greniers, passer la tête dans les faux plafonds, aller à la pêche aux câbles à travers les murs. Si vous vous en chargez vous-même, faites-le dans les règles de l'art, sinon vous devrez recommencer dans quelques années. Bâissez quelque chose de durable.
- ✓ Aujourd'hui, les utilisateurs de votre réseau sont peut-être tout à fait satisfaits du réseau à 100 Mbps mais, dans quelques années, ils vous réclameront un débit atteignant le gigahertz. Si vous faites des économies en utilisant du câble de catégorie 5 à la place du 6 plus onéreux, vous risquez de devoir le remplacer dans quelque temps.
- ✓ Vous pouvez être tenté de tirer les câbles à travers les murs, après avoir simplement percé un trou, directement vers les ordinateurs ou vers un commutateur, au lieu d'opter pour des prises murales modulaires et des cordons de connexion. C'est un mauvais calcul car les fils d'un câble sont pleins et conçus pour durer longtemps, uniquement s'ils ne sont pas trop souvent manipulés. Si vous tirez un câble à fils pleins directement vers un ordinateur, les fils seront soumis à des tensions dès que quelqu'un débranchera le câble. Rien que le fait d'ôter la poussière à l'arrière de la machine peut malmener le câble et, tôt ou tard, l'un des fils du câble cassera. Les cordons de connexion sont constitués de fils torsadés et non pleins et peuvent donc être manipulés sans risque de rupture. Et, en cas de défaillance d'un cordon de connexion, vous pouvez le remplacer vous-même pour quelques euros.

Le Chapitre 5 explique comment câbler comme un professionnel.

Éteindre ou redémarrer un serveur alors que des utilisateurs sont connectés

La manière la plus simple d'envoyer les utilisateurs de votre réseau au diable consiste tout simplement à éteindre le serveur pendant qu'ils sont connectés. Le redémarrer en appuyant sur le bouton de réinitialisation peut avoir des effets désastreux.

Si votre réseau comporte un serveur de fichiers dédié, il ne vous prendra probablement pas l'envie de l'éteindre ou de le redémarrer. Mais si votre réseau est configuré en pair-à-pair, où chaque station de travail (dont la vôtre) se double d'un ordinateur serveur, réfrérez ces pulsions qui vous poussent à éteindre ou redémarrer votre ordinateur. Quelqu'un pourrait être en train d'accéder à un fichier ou à une imprimante au même moment.

Avant d'éteindre ou de redémarrer un serveur, vérifiez si quelqu'un est connecté. Si c'est le cas, demandez-lui poliment de se déconnecter.

Rappelez-vous aussi que la plupart des problèmes de serveur n'exigent pas un redémarrage. Il suffit souvent de redémarrer un service défaillant pour tout remettre en ordre.

Supprimer des fichiers importants sur le serveur

Sans réseau, vous pouvez faire tout ce que vous voulez sur votre ordinateur, vous serez la seule personne qui en pâtira. Un peu comme un « crime sans victime ». Mettez votre ordinateur en réseau et vous avez une certaine responsabilité sur les épaules. Vous devez apprendre à agir comme un membre responsable de la communauté réseau.

Cela signifie que vous ne pouvez pas supprimer des fichiers sur le serveur du réseau au gré de vos caprices, simplement parce que vous n'en avez pas besoin. Ils peuvent ne pas vous appartenir. Vous ne voudriez pas que quelqu'un supprime vos fichiers, n'est-ce pas ?

Faites tout particulièrement attention aux fichiers dont le serveur a besoin pour fonctionner. Par exemple, certaines versions de Windows utilisent un dossier nommé `wgpo0000` pour recevoir le courrier électronique. Si vous supprimez ce dossier, votre messagerie disparaît.



La première fois que vous tenterez accidentellement de supprimer un fichier important d'un partage réseau, vous serez surpris de découvrir que la corbeille ne fonctionne pas pour les fichiers du réseau. La corbeille conserve une copie des fichiers que vous supprimez du disque dur de votre ordinateur mais pas des fichiers supprimés des partages réseau. Par conséquent, vous ne pouvez pas récupérer un fichier accidentellement supprimé du réseau.

Copier un fichier du serveur, le modifier et le recopier sur le serveur

Il est parfois plus facile de travailler sur un fichier du réseau si vous le copiez d'abord sur votre disque local. Vous pouvez alors y accéder plus efficacement depuis votre application car vous n'avez pas à avoir recours au réseau. C'est particulièrement vrai pour les grosses bases de données qui doivent être triées ou dont il faut extraire des états.

Vous allez droit dans le mur si vous copiez le fichier sur le disque local de votre PC, le modifiez, puis en recopiez une version mise à jour sur le serveur. Pourquoi ? Parce que quelqu'un d'autre fait peut-être la même chose au même instant. Dans ce cas, les mises à jour de l'un d'entre vous (celui qui recopie en premier le fichier sur le serveur) seront perdues.

Copier un fichier sur un disque local ne pose pas de problème, tant que vous ne projetez pas de le modifier ou de le recopier sur le serveur.

Relancer une impression parce que l'imprimante ne réagit pas

Que faites-vous si vous avez envoyé quelque chose à l'imprimante et que rien ne se passe ?



- ✓ **Bonne réponse :** Je cherche pourquoi rien ne s'est passé et je résous le problème.
- ✓ **Mauvaise réponse :** Je relance l'impression en espérant que ça fonctionne. Certains utilisateurs continuent d'envoyer des données encore et encore, en espérant qu'un de ces jours, elles seront imprimées. Le résultat est plutôt gênant quand quelqu'un résout finalement le problème de bourrage papier et que trente exemplaires de la même lettre sont imprimés sous son nez ou que trente exemplaires de votre document sont imprimés sur une autre imprimante parce que vous avez sélectionné la mauvaise.

Supposer que le contenu du serveur est toujours correctement sauvegardé

Certains utilisateurs partent malheureusement du principe que le réseau est une forme de bureaucratie efficace et organisée, entièrement digne de confiance. En réalité, c'est loin d'être vrai. Ne croyez jamais que les fadas chargés d'effectuer des sauvegardes quotidiennes du réseau accomplissent leur devoir correctement. Gardez un œil sur eux. Effectuez une inspection surprise : déboulez dans la salle des machines en gants blancs et demandez à voir les bandes de sauvegarde. Vérifiez la rotation des bandes pour vous assurer que les sauvegardes de plusieurs jours de travail sont disponibles.

Si les procédures de sauvegarde ne vous semblent pas très fiables, faites en sorte de ne jamais perdre de données. Sauvegardez fréquemment vos fichiers les plus précieux sur des clés USB ou mieux sur un CD-RW.

Se connecter à Internet sans se soucier de la sécurité

Si vous connectez à Internet un ordinateur non relié à un réseau, seule cette machine subira les conséquences d'une infection virale ou d'une intrusion malveillante. En revanche, s'il s'agit d'un ordinateur en réseau, vous exposez l'ensemble du réseau.



Attention : ne connectez jamais une machine à Internet sans prendre des mesures de sécurité.

- ✓ Comment vous protéger et préserver le réseau des virus ?
- ✓ Comment être certain que les documents figurant sur votre serveur de fichiers ne seront pas tout à coup accessibles au monde entier ?
- ✓ Comment éviter que des pirates informatiques pénètrent sur votre réseau pour voler votre fichier clientèle et vendre les numéros des cartes de crédit de vos clients au marché noir ?



Ces questions et le thème de la sécurité Internet sont traités dans le Chapitre 23.

Installer un point d'accès sans fil sans autorisation

Brancher n'importe quel appareil sur le réseau sans demander la permission à l'administrateur réseau, ÇA NE SE FAIT PAS. Mais les points d'accès sans fil (WAP) sont insidieux. Nombreux sont les utilisateurs à se laisser prendre au discours marketing : les réseaux sans fil sont d'une simplicité enfantine, il suffit de brancher un point d'accès pour que votre assistant personnel ou appareil de poche soit immédiatement connecté.

Le problème, c'est que tout le monde peut en faire autant dans un rayon de trois cents mètres autour de votre point d'accès sans fil. Il faut donc mettre en place des mesures de sécurité supplémentaires pour être sûr qu'aucun pirate, équipé d'un ordinateur sans fil et installé sur votre parking ou de l'autre côté de la rue, ne va pénétrer sur votre réseau.

Si vous pensez que c'est très peu probable, réfléchissez-y à deux fois. Il existe plusieurs sites Internet clandestins qui divulguent des cartes répertoariant les réseaux sans fil non sécurisés dans les grandes villes. Pour de plus amples informations sur la sécurité des réseaux sans fil, lisez le Chapitre 9.

Penser qu'il est impossible de travailler quand le réseau ne fonctionne pas

Il y a quelques années, j'ai réalisé que je ne pouvais pas travailler sans électricité. Victime d'une panne de courant, je ne pourrais même pas allumer une bougie et travailler avec un papier et un crayon car le seul taille-crayon que je possède est électrique.

Certains adoptent la même attitude à l'égard des réseaux : ils s'imaginent que si le réseau ne fonctionne pas, ils n'ont plus qu'à rentrer chez eux. Pas toujours ! Ce n'est pas parce que votre ordinateur est connecté à un réseau qu'il ne fonctionne pas si ce dernier plante. Il est vrai que si le réseau essuie une grosse tempête, vous ne pourrez pas accéder à ses périphériques : impossible de récupérer des fichiers stockés sur les disques réseau et d'utiliser les imprimantes réseau. Mais vous pouvez toujours vous servir de votre ordinateur en local donc accéder aux fichiers et aux programmes stockés sur votre disque dur et utiliser votre imprimante locale (si vous avez la chance d'en avoir une).

Manquer d'espace sur un serveur

Le manque d'espace disque sur un serveur du réseau est l'erreur la plus désastreuse qui puisse vous arriver. Lorsque vous achetez un nouveau serveur avec des centaines de gigaoctets d'espace disque, vous pensez que jamais vous ne manquerez de place. Cependant, il est étonnant de constater la vitesse à laquelle les utilisateurs arrivent à remplir des centaines de gigaoctets d'espace disque.

Les problèmes commencent lorsque la capacité disque descend à quelques gigaoctets d'espace libre. Windows a du mal à s'exécuter et les temps de réponse du serveur s'allongent. Des erreurs apparaissent et dès qu'il n'y a plus d'espace libre, les utilisateurs viennent faire le siège de votre bureau et vous imposent de régler le problème immédiatement.

- ✓ La méthode pour éviter cette situation malheureuse est de surveiller quotidiennement l'espace disque libre sur vos serveurs. Vous pouvez aussi suivre l'évolution de l'occupation des disques chaque semaine et prendre en compte les tendances des projets. Par exemple, s'il reste 100 Go sur votre serveur de fichiers et si vos utilisateurs augmentent leur espace disque de 5 Go par semaine, vous savez que vous manquerez très probablement d'espace disque dans 20 semaines. Avec ces renseignements, vous n'aurez aucune difficulté à anticiper.
- ✓ Ajouter des disques supplémentaires à vos serveurs n'est pas toujours la meilleure solution. Avant d'acheter plus de disques, vous devriez :
 - Rechercher les anciens fichiers devenus inutiles et les supprimer du disque après les avoir éventuellement archivés.
 - Appliquer des quotas aux utilisateurs pour leur imposer des limites à la taille disque disponible sur le réseau.

Accuser systématiquement le réseau

Certains utilisateurs prennent toujours le réseau pour l'idiot du village responsable de tous les incidents. Les réseaux posent des problèmes mais ils ne sont pas à l'origine de tous les maux :

- ✓ Si votre moniteur affiche seulement des lettres en capitales, c'est probablement parce que vous avez appuyé sur la touche Verr.Num. N'accusez pas le réseau.
- ✓ Si vous avez renversé du café sur votre clavier, c'est de votre faute. N'accusez pas le réseau.

- ✓ Si votre lecteur de CD est bourré de pâte à modeler, il faut bien que les enfants s'amuse^{nt}.
- N'accusez pas le réseau.

Vous avez saisi ?

Chapitre 28

Les dix commandements du réseau

Dans ce chapitre :

- ▶ Tu sauvegarderas et nettoieras tes disques durs religieusement.
- ▶ Tu préviendras tes utilisateurs avant d'intervenir sur le réseau.
- ▶ Tu conserveras un stock raisonnable de matériel de rechange.
- ▶ Tu formeras tes utilisateurs.
- ▶ Tu documenteras la configuration du réseau.

***B** éni soit l'administrateur réseau qui n'est pas guidé par l'ignorance, ne marche pas dans la voie de l'oubli, ne règne pas sur le royaume des blancs-becs mais encense la divine loi du Réseau, objet de sa méditation permanente. »*

Réseau 1,1

Et vint donc le temps où ces dix commandements du réseau furent transmis de génération en génération pour être inscrits sur le front des experts informatiques et placardés sur leurs portes. Obéissez à ces dix commandements et votre destin, celui de vos enfants et celui des enfants de vos enfants, sera clément.

I. Tu sauvegarderas ton disque dur religieusement

La prière est une bonne chose mais quand il est question de sauvegarder les données de votre réseau, rien ne vaut un bon vieux calendrier de sauvegarde respecté religieusement. Si c'était une véritable Bible réseau, vous trouveriez ici même une note vous invitant à lire les versets du Chapitre 22.

II. Tu protégeras ton réseau contre les infidèles

Vous souvenez-vous du colonel Flagg dans le film *M.A.S.H.*, qui se cachait dans des poubelles à la recherche de Commies ? Vous ne voulez pas devenir comme lui mais, d'un autre côté, vous ne voulez pas non plus ignorer le risque d'être détruit par un virus, ni celui que votre réseau soit envahi par des pirates informatiques. Vérifiez que votre connexion Internet est sécurisée par un pare-feu et interdisez tout accès à Internet qui ne respecterait pas les règles de sécurité.

Pour contrer les menaces virales, installez un programme antivirus sur chaque ordinateur du réseau et expliquez aux utilisateurs comment s'en servir. En outre, faites en sorte que les utilisateurs soient bien conscients du danger de propagation des virus via les pièces jointes de courriers électroniques.

III. Tu préserveras la pureté de ton disque réseau et le débarrasseras des vieux fichiers

N'attendez pas qu'il ne reste plus que 1 Go d'espace libre sur votre disque de 500 Go pour penser à y mettre de l'ordre. Programmez régulièrement des séances de nettoyage : parcourez les fichiers et les répertoires du disque réseau et supprimez tout ce qui n'est plus utilisé.

IV. Tu ne bidouilleras point les fichiers de configuration du réseau, à moins que tu ne saches ce que tu fais

Les réseaux sont fragiles. Une fois le vôtre installé et opérationnel, n'y touchez plus à moins de maîtriser les événements. Faites tout particulièrement attention si vous avez l'impression de savoir ce que vous faites. Ce sont ceux qui pensent savoir ce qu'ils font qui se retrouvent souvent dans la panade !

V. Tu ne convoiteras point le réseau d'autrui

La convoitise est une maladie courante chez les administrateurs réseau. Si votre réseau fonctionne bien avec un débit de 100 Mbps, ne convoitez pas le réseau du voisin qui est à 1 000 Mbps ; à quoi bon l'envier ? Si vos utilisateurs sont heureux avec Windows XP, résistez à l'envie de les faire migrer vers Windows Vista ou Windows 7, à moins que vous n'ayez une très bonne raison. Et si vous disposez de Windows Server 2003, sachez que fantasmer sur Windows Server 2008 est un péché capital.

L'envie vous guette surtout si vous êtes amateur de gadgets. Il y a toujours un meilleur commutateur à acheter ou quelque protocole réseau à convoiter. Ne cédez pas à ces bas instincts !

VI. Tu préviendras tes utilisateurs avant d'intervenir sur le réseau

Par courtoisie, essayez d'avertir plusieurs fois vos utilisateurs avant de couper le réseau pour effectuer des tâches de maintenance. Évidemment, vous ne pouvez pas prévoir les problèmes à l'avance. Mais, si vous envisagez d'ajouter un nouvel ordinateur au réseau le jeudi matin, il est préférable de prévenir tout le monde deux jours avant plutôt que deux minutes avant.

VII. Tu conserveras un stock raisonnable de matériel de rechange

Il n'est pas normal que votre réseau reste inutilisable durant deux jours parce qu'un câble s'est cassé. Vérifiez toujours que vous disposez d'un stock minimal de pièces de rechange pour le réseau. Par chance, le Chapitre 29 donne la liste des dix éléments que vous devez conserver dans votre placard.

VIII. Tu ne voleras point le programme d'autrui sans licence

Que diriez-vous si l'inspecteur Clouseau débarquait dans votre bureau, regardait par-dessus votre épaule pendant que vous exécutez Excel depuis un serveur et vous demandait : « Avez-vous une *cilence* ? »

« Une *cilence* ? » répondriez-vous, intrigué.

« Oui, une *cilence*. La loi du *cilence* vous interdit formellement d'avoir recours à un programme informatique sur le réseau sans *cilence*. »

Vous ne voulez pas enfreindre la loi, n'est-ce pas ? Alors assurez-vous d'avoir les licences appropriées pour les applications que vous exécutez sur votre réseau.

IX. Tu formeras tes utilisateurs sur l'art d'utiliser le réseau

Ne blâmez pas les utilisateurs parce qu'ils ne savent pas comment utiliser le réseau. Ils n'y sont pour rien. Si vous êtes administrateur réseau, votre travail consiste à former les utilisateurs pour qu'ils sachent comment se servir du réseau.

X. Tu graveras la configuration du réseau sur des tables de pierre

Au cas où vous traverseriez le Jourdain, qui d'autre pourrait connaître quelque chose de votre réseau si vous ne laissez aucune trace écrite ? Un morceau de nappe ne fera pas l'affaire. Notez tout dans un carnet officiel, nommé *Bible du réseau*, et protégez-le comme s'il était sacré.

Dans deux mille ans, quand les archéologues exploreront les grottes de votre région, ils trouveront votre documentation réseau cachée dans une jarre et s'émerveilleront de la méticulosité avec laquelle les hommes de notre temps archivaient leur configuration réseau.

Ils en tireront probablement des conclusions ridicules : que nous apportions, par exemple, à une divinité nommée TCP/IP des offrandes sous la forme de paquets de données brûlés, mais c'est d'autant plus drôle.

Chapitre 29

Dix choses à conserver dans son placard

.....

Dans ce chapitre :

- ▶ Ruban adhésif
 - ▶ Outils.
 - ▶ Câbles de rechange.
 - ▶ Connecteurs supplémentaires.
 - ▶ Barres chocolatées.
 - ▶ Carte réseau supplémentaire.
 - ▶ Quelques commutateurs bon marché.
 - ▶ Documentation complète du réseau, gravée sur des tables de pierre.
 - ▶ Manuels et CD du réseau.
 - ▶ Dix exemplaires de ce livre.
-

La première fois que vous mettez en réseau les ordinateurs de votre bureau, vous devez choisir un placard où stocker des trésors pour le réseau. Si vous n'avez pas de placard, contentez-vous d'une étagère, d'un tiroir ou au moins d'une boîte en carton.

Voici la liste de tout ce qu'il faut conserver à portée de main.

Ruban adhésif

Il a permis à l'équipage d'Apollo 13 de revenir sain et sauf de son expédition lunaire mouvementée. Il ne servira pas souvent à la gestion de votre réseau mais cette anecdote est symbolique : lorsque vous vous rendez compte que les choses vous échappent, il est parfois nécessaire d'improviser pour assurer le bon fonctionnement de votre réseau.

Si vous n'aimez pas le ruban adhésif, fil de fer et chewing-gum feront l'affaire.

Outils

Vérifiez que vous disposez d'un minimum d'outillage informatique, comme l'un de ces kits à 15 euros que vous pouvez trouver dans n'importe quel magasin de bricolage. Vous devez aussi disposer de pinces à couper, de pinces à dénuder et de pinces à sertir convenant au type de câble monté sur votre réseau.

Câbles de rechange

Quand vous achetez du câble réseau, ne prenez jamais la longueur exacte dont vous avez besoin. Il est en effet judicieux de doubler la longueur nécessaire car cela vous permet de mettre de côté le surplus en vue d'une utilisation ultérieure. Vous en aurez certainement besoin un jour : un problème de câble se produira ou vous devrez ajouter un ou deux ordinateurs au réseau et donc tirer des câbles.

Si vous montez votre réseau avec du câble de différentes couleurs, essayez de garder sous la main au minimum des segments de dix mètres dans chacune des couleurs.



Je vous conseille d'acheter vos câbles en ligne. Vous bénéficierez de prix très avantageux !

Connecteurs supplémentaires

Ne soyez pas non plus à court de connecteurs. Si vous employez du câble à paires torsadées, vous vous apercevrez que les connecteurs s'usent très vite. Achetez les connecteurs par lots de vingt-cinq, cinquante ou cent pour avoir des réserves.

Barres chocolatées

Emballées dans leur petit emballage individuel, les barres chocolatées se conservent pendant des années. En fait, elles dureront probablement plus longtemps que le réseau lui-même. Vous pourrez ainsi les offrir aux prochains geeks et garantir un support technique réseau aux générations futures.

Cartes réseau supplémentaires

Idéalement, tous vos ordinateurs disposent d'une carte réseau intégrée dans la carte mère. Cependant, il arrive qu'une carte réseau fonctionne mal. Plutôt que de remplacer la carte mère, vous pouvez résoudre le problème en ajoutant une carte réseau peu onéreuse (moins de 20 euros) à utiliser en remplacement de la carte intégrée.

Commutateurs réseau bon marché

Conservez deux ou trois commutateurs réseau bon marché (environ 20 euros) de quatre ou huit ports. Même si vous ne les utilisez pas pour le réseau principal, ils seront utiles lorsque vous ajouterez un ordinateur ou une imprimante dans un bureau et qu'il n'y aura plus de prise disponible. Par exemple, si l'un de vos utilisateurs a besoin très rapidement d'un second ordinateur et qu'il n'y a qu'une prise réseau dans le bureau, plutôt que de tirer un nouveau câble jusqu'au bureau de l'utilisateur, branchez un commutateur sur la prise réseau et connectez les deux ordinateurs au commutateur.

Documentation complète du réseau, gravée sur des tables de pierre

J'ai insisté plusieurs fois dans cet ouvrage sur l'importance de documenter le réseau. Ne passez pas des heures à rédiger la documentation de votre réseau si c'est pour la stocker sous une pile de vieux magazines derrière votre bureau. Mettez le carnet dans le placard avec les autres fournitures réseau pour que tout le monde sache où il se trouve. Et conservez des sauvegardes des fichiers Word, Excel ou autres ayant servi à constituer le carnet dans un coffre ignifugé ou sur un autre site.



Ne vous avisez pas de noter les mots de passe dans le carnet ! Honte à vous, rien que d'y avoir pensé !



Si vous décidez de graver la documentation du réseau sur des tables de pierre, pensez au grès. C'est joli, ça ne coûte pas cher et c'est très facile à mettre à jour (il suffit de frotter l'ancienne information puis de graver la nouvelle à la place). Gardez cependant à l'esprit que le Coca Light attaque le grès, n'en renversez pas dessus. Surtout, n'oubliez pas de stocker les tables sur une étagère renforcée.

Manuels et CD du réseau

Les manuels ne méritent sans doute pas le prix Goncourt mais ce n'est pas une raison pour les jeter. Mettez-les dans le placard, avec tous les outils et objets liés au réseau.



Conservez les manuels et les CD de tous les logiciels et applications installés sur le serveur avec tout ce qui concerne le réseau.

Dix exemplaires de ce livre

Évidemment, vous tiendrez à conserver sous la main assez d'exemplaires de ce livre pour en donner à chacun de vos utilisateurs. Plus ils en sauront, moins ils viendront vous importuner.

Hum... dix exemplaires ne suffiront pas ! Vingt devraient faire l'affaire.

Chapitre 30

Dix couches du modèle OSI

Dans ce chapitre :

- ▶ Couche physique.
- ▶ Couche de liaison des données.
- ▶ Couche réseau.
- ▶ Couche de transport.
- ▶ Couche de session.
- ▶ Couche de présentation.
- ▶ Couche des applications.

Le terme OSI a des airs de nom de services secrets. En fait, dans le cadre de cet ouvrage du moins, les initiales sont celles d'*Open Systems Interconnection*, interconnexion de systèmes ouverts. Plus exactement, on parle de « modèle de référence OSI », ou plus simplement de « modèle OSI ».

Le modèle OSI divise les divers aspects d'un réseau informatique en sept couches distinctes. Elles se superposent comme des pelures d'oignon : chacune englobe celle qui se trouve dessous et masque ses détails.

Le modèle OSI n'est pas un standard de réseau comme le sont l'Ethernet ou le protocole TCP/IP. C'est plutôt un cadre de travail à l'intérieur duquel les divers standards trouvent leur place. Le modèle OSI spécifie quels aspects des opérations de réseau sont pris en charge par les différents standards de réseau. Dans un certain sens, le modèle OSI est une sorte de standard des standards.

Les trois premières couches sont appelées *couches inférieures*. Elles concernent le matériel, c'est-à-dire la façon dont les informations sont envoyées d'un ordinateur à un autre sur le réseau. Les couches 4 à 7, appelées *couches supérieures*, concernent les applications, notamment la relation avec le réseau au travers d'interfaces logicielles.



Oui, je sais, le modèle OSI a *sept* couches et non dix. La partie « Les dix commandements » regroupe plusieurs chapitres qui présentent *environ* dix éléments. Dans ce cas, il y en a sept, donc presque dix !

Couche 1 : Physique

La toute première couche du modèle OSI est la *couche Physique*. Elle concerne les caractéristiques physiques du réseau, comme le type de câble qui relie le matériel, le type de connecteur utilisé, la longueur maximale des câbles, etc. Par exemple, le standard Ethernet du câble 100BaseT spécifie les caractéristiques électriques du câble à paires torsadées, la taille et la forme des connecteurs, la longueur maximale des câbles, etc.

La couche Physique spécifie aussi les caractéristiques électriques des signaux utilisés pour transmettre des données sur les câbles, d'un nœud de réseau à un autre. La couche Physique ne définit aucune signification particulière à ces signaux autre que les valeurs binaires élémentaires 0 et 1. Les niveaux plus élevés du modèle OSI doivent affecter une signification aux bits transmis par la couche Physique.

Le *répéteur* est l'un des types de périphériques les plus communément utilisés sur un réseau. Il sert à régénérer les signaux lorsque la transmission doit s'effectuer sur une longueur de câble plus élevée que celle autorisée par la couche Physique ou s'il faut répartir un signal entre plusieurs câbles.

L'ancien concentrateur 10BaseT est aussi un périphérique de couche Physique. Techniquement, un concentrateur est un *répéteur multiport* car il est censé régénérer chaque signal reçu avant son acheminement vers les autres ports. Les répéteurs et les concentrateurs n'examinent pas les signaux qu'ils régénèrent. S'ils le faisaient, ils travailleraient au niveau de la couche Liaison des données et non de la couche Physique. Ce qui nous amène à la...

Couche 2 : Liaison des données

La *couche Liaison des données* est la basse des couches auxquelles une signification est affectée aux bits transmis sur le réseau. Les protocoles de liaison de données portent sur des éléments comme la taille de chaque paquet de données à envoyer, la technique utilisée pour que chacun soit délivré à son destinataire ou le moyen utilisé pour s'assurer que des nœuds ne transmettent pas de données sur le réseau en même temps.

La couche Liaison des données fournit aussi des outils de base pour la détection et la correction des erreurs, afin de garantir que les données reçues sont

identiques à celles envoyées. Si une erreur irrécupérable se produit, le standard de liaison des données doit spécifier comment le nœud sera informé de l'erreur afin qu'il puisse retransmettre les données.

Au niveau de la couche Liaison des données, chaque périphérique du réseau possède une adresse appelée *adresse MAC* (*Media Access Control*, contrôle d'accès au support). C'est en fait la véritable adresse du matériel, qui lui est attribuée lors de sa fabrication.

L'adresse MAC de la carte réseau d'un ordinateur peut être affichée en ouvrant une fenêtre d'invite de commande et en tapant la commande `ipconfig /all`, comme le montre la Figure 30.1. Dans cet exemple, l'adresse MAC (appelée *adresse physique* dans la sortie) de la carte réseau est 00-21-5D-BF-54-42.

```

C:\Users\B...>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : E4300
Suffixe DNS principal . . . . . : 
Type de nœud . . . . . : Hybride
Soutage IP activé . . . . . : Non
Proxy WMC activé . . . . . : Non

Connexion réseau sans fil Connexion réseau sans fil :
Description . . . . . : Liaison WiFi Intel(R) 5100 AGN
Adresse physique . . . . . : 00-21-5D-BF-54-42
DHCP activé . . . . . : Non
Configuration automatique activée . . . . . : Oui
Adresse IPv6 de liaison locale . . . . . : fe80::daa:81aa:5dfa:89fb%19(préférée)
Adresse IPv4 . . . . . : 192.168.1.20(préférée)
Masque de sous-réseau . . . . . : 255.255.255.0
Passerelle par défaut . . . . . : 192.168.1.1
IDV4 DHCPv6 . . . . . : 162330877
GUID de liaison DHCPv6 . . . . . : 00-21-5D-BF-54-42-00-21-5D-BF-54-42-FC
Services DNS . . . . . : 192.168.1.1
NetBIOS sur IPv4 . . . . . : Activé
  
```

Figure 30.1 : Affichage de l'adresse MAC d'une carte réseau.



L'une des fonctions les plus importantes de la couche Liaison des données est de permettre aux paquets d'être envoyés en toute sécurité sur un support physique, sans subir les interférences produites par d'autres nœuds qui tenteraient d'envoyer des paquets en même temps. Pour cela, Ethernet a recours à une technique appelée CSMA/CD.

Sur la plupart des réseaux, les commutateurs sont les périphériques de couche Liaison des données les plus couramment utilisés. Un commutateur est semblable à un concentrateur, sauf qu'au lieu de se limiter à régénérer les signaux entrants avant de les envoyer vers les différents ports, il examine l'adresse MAC de tout paquet entrant afin de déterminer vers quel port il doit l'envoyer.

Couche 3 : Réseau

La *couche Réseau* gère les tâches de routage des messages du réseau d'un ordinateur à un autre. Les deux protocoles de couche 3 les plus connus sont IP (usuellement apparié à TCP) et IPX (normalement apparié à SPX afin d'être utilisé sur des réseaux Novell et Windows).

L'une des fonctions importantes de la couche Réseau est l'*adressage logique*. Comme vous le savez, chaque périphérique de réseau possède une adresse physique appelée « adresse MAC », qui lui est attribuée en usine. Quand vous achetez une carte réseau, son adresse MAC est fixe et ne peut être modifiée. Comment ferez-vous alors si vous désirez utiliser une autre convention d'adressage pour faire référence aux ordinateurs et autres périphériques du réseau ? C'est là qu'intervient la notion d'*adressage logique*, qui permet d'octroyer à un périphérique du réseau un emplacement auquel il est accessible grâce à une adresse que vous lui affectez.

Les adresses logiques sont créées et utilisées par des protocoles de couche Réseau comme IP ou IPX. Le protocole de couche Réseau traduit les adresses logiques en adresses MAC. Par exemple, si vous utilisez IP comme protocole de couche Réseau, les périphériques du réseau reçoivent des adresses IP comme 207.120.67.30. Le protocole IP devant recourir au protocole de couche Liaison des données pour envoyer réellement des paquets à un périphérique, il doit savoir comment traduire l'adresse IP d'un périphérique en adresse MAC correcte. Vous pouvez demander à la commande `ipconfig` d'afficher l'adresse IP de votre ordinateur. Celle visible dans la Figure 30.1 est 192.168.1.100.

Une autre fonction importante de la couche Réseau est le *routage*, c'est-à-dire la détermination du chemin à suivre dans le réseau. Le routage entre en jeu dès qu'un ordinateur d'un réseau doit envoyer un paquet vers un ordinateur d'un autre réseau. Dans ce cas, un périphérique de couche Réseau appelé *routeur* envoie le paquet vers le réseau de destination. Une autre caractéristique importante des routeurs est la possibilité de les utiliser pour relier des réseaux utilisant deux protocoles de couche 2 différents. Par exemple, un routeur peut être utilisé pour connecter un réseau local Ethernet à un réseau étendu fonctionnant avec d'autres protocoles de bas niveau, comme le T1.

Couche 4 : Transport La *couche Transport* est la couche de base à partir de laquelle un ordinateur du réseau communique avec un autre ordinateur du réseau. C'est dans cette couche que vous trouverez l'un des protocoles les plus connus : TCP. La principale fonction de la couche Transport est d'assurer la fiabilité et l'absence d'erreur des paquets qui cheminent sur le réseau. Pour cela, la couche Transport établit des connexions entre les périphériques du réseau, accuse la réception des paquets, signale les paquets qui n'ont pas été reçus et renvoie ceux qui, à l'arrivée, sont corrompus.

Dans bien des cas, le protocole de la couche Transport scinde les messages de grande taille en paquets plus petits qui peuvent être envoyés efficacement sur le réseau. Le protocole de la couche Transport rassemble les messages à réception, s'assurant que la totalité des paquets d'une transmission a été reçue sans perte de données.

Couche 5 : Session

Comme son nom l'indique, la *couche Session* établit des *sessions* (instances de communication et d'échange de données) entre les nœuds du réseau. Une session doit avoir été établie avant que des données puissent être transmises sur le réseau. La couche Session s'assure que les sessions sont correctement établies et maintenues.

Couche 6 : Présentation

La *couche Présentation* est responsable de la conversion des données envoyées sur le réseau d'un type de représentation en un autre. Par exemple, la couche Présentation peut appliquer des techniques de compression sophistiquées afin qu'un nombre plus réduit de données, en termes d'octets, représente l'information envoyée sur le réseau. À l'autre extrémité de la transmission, les données sont décompressées par la couche Transport.

La couche Présentation peut aussi crypter les données avant leur transmission et les décrypter à l'autre extrémité, grâce à des techniques que même Champollion ne saurait percer.

Couche 7 : Application

Couche la plus élevée du modèle OSI, la *couche Application* concerne les techniques utilisées par les programmes d'application pour communiquer avec le réseau. Le nom de cette couche prête quelque peu à confusion car des programmes d'application comme Word ou Excel ne font en réalité pas partie de la couche. En fait, la couche Application représente le niveau auquel les programmes d'application interagissent avec le réseau, au travers d'interfaces de programmation, pour recourir aux services du réseau. L'un des protocoles de couche Application les plus connus est HTTP (*HyperText Transfer Protocol*, protocole de transfert hypertexte), qui est l'un des piliers du World Wide Web.

Index



Symboles

/, 384
\\ 384
10Base2 107
10Base5 107
10BaseT 107
100BaseT 107

A

Accéder aux dossiers partagés 254
Access 64
 accès par réseau 65
ACL 287
Adaptateur USB sans fil 191
Ad-hoc 194
 mode (réseaux sans fil) 184
Administrateur réseau 19, 258, 260
Adressage logique 434
Adresse(s)
 de classe A 122
 de classe B 123
 de classe C 124
 de messagerie 213
 de transfert 213
DNS 173
IP 117, 120, 172, 369
 statique 131
 privée 128
 publique 128
MAC 120
ADSL 204
Alias 212

Alimentation secourue 159
Analyseur de protocole 265
Antenne 185
Antivirus 375
Apache 225, 228
Apple 403
AppleTalk (Macintosh) 405
Applications
 de publication 224
 de transaction 225
ARCnet 91
arp 264
Arrêt de Windows, boîte de dialogue 323
ART 187
ATA 241
ATL (Acronyme de Trois Lettres) 11
Attributs personnalisés 215
Audio-conférences 241
Autorisation(s) 287, 300
 spéciales 288
Autre boîte aux lettres 218

B

Bail 134
Bande passante 93
Bandes
 fiabilité 347
Barres
 chocolatées 429
 obliques 384
 obliques inversées 384

- Base de données Access 64
 - accès par réseau 65
 - de répertoire 148
- Baseline Security Analyser 265
- Bibliothèque(s) 330
 - de bandes 339
 - utilisateurs 331
- Binaire 117
- Bit 118
 - d'archive 340
- BlackBerry 243, 245, 248
- Blindé 94
- BNC 111
- Boîte
 - à outils 97
 - aux lettres fonctionnelle 219
 - de réception 252
- Brochage 98
- BSS 193
- Bus, topologie 90

C

- C\$ 290
- Câblage 17
 - à paire torsadée 17, 318
 - coaxial 92
 - connexions, dépannage 319
 - économies 415
 - installation 101
 - paire torsadée 92
 - répéteurs 110
 - supplémentaire 428
- Câble 92, 204, 318, 414
 - brochage 98
 - catégories 93
 - croisé 101
 - plenum 95
 - PVC 95
 - réseau 17
 - STP 95
 - UTP 92, 94
 - téléphoniques 17

- Calendrier 252
- Canal sécurisé 254
- Carnet du réseau 262, 425, 429
- Carte
 - PCI sans fil 191
 - réseau 16, 75, 307
- Certification 267
- Chemin 397
 - UNC 39
- Cheval de Troie, virus 374
- Circuit-level gateway 372
- Client
 - DHCP 138, 325
 - DNS 143, 325
 - Outlook 216
 - serveurs et 45
- Coaxial 92
- Collision 105
 - CSMA/CD 188
- Commandes TCP/IP intégrées 264
- Communications
 - locales 241
 - longue distance 241
- Commutateur 17, 103, 433
 - empilable 107
 - réseau 429
- Composants internes 318
- Compte
 - administrateur 361
 - de domaine 270
 - de groupe 363
 - de service 361
 - d'utilisateur 355, 360
 - intégré 360
 - invité 361
 - local 270
- Concentrateur 103, 432
- Conception d'un réseau 72
 - systèmes d'exploitation des serveurs 79
- Configuration 423
 - documentation 425
 - Macintosh pour réseau 405

- Connecter des disques réseau 254
 - connecter (se)
 - automatiquement 28
 - mots de passe 26
 - Connecteurs 100
 - câble UTP 101
 - cartes réseau 108
 - supplémentaires 428
 - Connexion
 - au réseau 181, 168
 - de lecteur 37
 - en guirlande 105
 - Internet 157
 - réseau 318
 - Console(s)
 - de gestion DHCP 136
 - virtuelles 382
 - Contacts 252
 - Copie de sauvegarde 342
 - Correctifs 376
 - Couche
 - application 435
 - liaison des données 432
 - OSI 431
 - physique 432
 - présentation 435
 - réseau 434
 - session 435
 - transport 434
 - Courrier électronique
 - virus 374
 - CSMA/CD 188
 - Ctrl+Alt+Suppr (redémarrer) 323
- D**
- DAT 338
 - Date d'expiration, mots de passe 357
 - Déconnecter (se) 43
 - Dépannage 318
 - connexions de câbles 319
 - messages d'erreur 319
 - DFS 296
 - DHCP 130, 172
 - bail 134
 - exclusion 133
 - réserveation 133
 - serveur 131
 - disque(s)
 - boîte de dialogue Propriétés 74
 - durs 53, 74
 - dur local 31
 - locaux 29
 - point de montage, Linux 384
 - Distributed File System 296
 - Distribution Linux 383
 - DLT 338
 - DNS 143, 173
 - Documentation 425
 - technique 266
 - Documents, partagés 18
 - Domaine 139, 399
 - de diffusion 125
 - Dorsale 309
 - Dossiers 53
 - partagés 29
 - publics 55, 252
 - Dreamweaver 225
 - Droits
 - d'administrateur 359
 - de boîte aux lettres 215
 - droits utilisateur 363
 - DSL 82
 - dynamique 228
- E**
- en ligne, définition 11
 - Epais 107
 - Espace de stockage 19
 - ESS 194
 - État de l'art 331
 - Éteindre le serveur 415
 - Étendue 132
 - Ethernet 90
 - Fast Ethernet 92
 - Gigabit Ethernet 92

Exchange
 général 212
 paramètres avancés 215
 Exclusion 133
 Excuses 333

F

FAI 203
 Fast Ethernet 92
 FAT 363
 FAT32 363
 Fichiers
 hors connexion 65
 HTML 228
 modifier 416
 partager 12
 partagés 407
 réseau 61
 supprimer 18
 supprimer sur le serveur 415
 File d'attente 41
 des impressions 42
 Filtrage de paquets 369
 Fin 107
 Fonctionnalités Exchange 214
 Formation des utilisateurs 329
 Former les utilisateurs 424
 Fournisseur
 d'accès à Internet 203
 de VoIP populaires 242
 Fournitures 430
 FQDN 141
 Free 242
 Fréquence 185
 Frontpage 225

G

Générateur de mots de passe 358
 Gestionnaire
 BlackBerry 248
 d'absence du bureau 252
 de fenêtres, Linux 382

 d'utilisateurs 392
 Gigabit Ethernet 92
 GNOME 385, 389
 Goulet d'étranglement 305
 Groupe 270, 280, 363
 créer 281
 membre 282
 de travail 64
 Guide 98
 GUI, Linux 382
 Guirlande 105

H

Hackers 377
 Hertz 185
 Hors ligne, définition 11
 Hostname 264
 Hôte 120
 Hotfix Checker 265
 HTML 225, 228
 HTTP 435
 Hub 17
 Hypertexte 435
 HyperText Transfer Protocol 435

I

IBSS 194
 ID 387
 Identification 26
 Identité 176
 ID utilisateur 391
 IEEE 91
 IIS 225, 226, 228
 IMAP4 215
 Impression 416
 en tâche de fond 406
 Imprimante 37
 ajouter 38
 en réseau 37
 serveur 78
 Informations
 système 261

- système Microsoft 76
- Infrastructure 80, 192, 308
 - mode (réseaux sans fil) 184
- Innovations 332
- Inspection dynamique des paquets 371
- Installation
 - applications, sur le réseau 13
 - boîte à outils 97
 - câblage 101
 - d'administration 60
 - Linux 386
 - Office 61
- Interface utilisateur graphique (GUI),
 - Linux 382
- Internet 12
 - lignes T1 et T3 205
 - Locator Service 215
 - Protocol 120
- Interrupteur 317
 - de commandes 395
- Intranet 223
 - rudimentaire 228
 - sans serveur Web 228
- Inventaire 73
- IP 172
- ipconfig 264
- iPhone 245
- IPng 124
- IP spoofing 371
- IPv6 120, 124
- IPX/SPX 171
- Itinérance 193

J

- Journal d'événements 327

K

- KDE 385
- Kit de ressources
 - Microsoft Office 60
 - Windows 331

L

- LAN (réseau local) 11
- Largeur de bande 187
- Lecteur
 - de bandes 338
 - réseau mappé 36, 67
 - ressources partagées 12
- LED 105
- Lettres de lecteur
 - connecter 35
- Licence réseau 14
- Lignes
 - privées 205
 - T1 et T3, accès Internet 205
- Limites de stockage 213
- Linus Torvalds 381
- Linux 80, 151
 - comparaison avec Windows 384
 - GNOME 389
 - installation 386
 - interpréteur de commande 390
 - Mandriva 384
 - ouvrir une session 387
 - partitions 384, 385
 - Red Hat 383
 - Samba 396
 - Shell 391
 - Slackware 384
 - SuSE 384
 - TCP/IP 393
 - vue d'ensemble 381
 - X server 387
- Liste de contrôle d'accès 287
- Logiciel
 - de VoIP 240
 - réseau 17
- Login 388
- Logique 119
- Longueur d'onde 185
- LWAN 184

M

MAC 120, 433
 Mac et PC 408
 Macintosh 152, 403
 AppleTalk 405
 configuration 405
 partage de fichiers 408
 partage d'imprimantes 406
 réseau avec PC 409
 Mac OS X Server 152, 404
 NetBoot 404
 QuickTime Streaming Server 404
 WebObjects 404
 Mainframe 18
 Maintenance 423
 Manuels 430
 Mapping 34
 Masque de sous-réseau 126
 Masquer dans la liste 215
 Matériel de rechange 424
 Matrix 9
 Mémoire 75, 306
 (RAM) 75
 virtuelle 307
 Mes Documents 31
 Messagerie 211
 Messages d'erreur, dépannage 319
 Microsoft Backup 339
 Microsoft Office sur un réseau 59
 Miroir 147
 Mise en attente 241
 Modèles 64
 de document 62
 groupe de travail 62
 utilisateur 62
 Modes (réseaux sans fil)
 ad hoc 184
 infrastructure 184
 Moniteur 318
 Monobrin 95
 Mono-utilisateur 382
 Mot de passe 270
 configuration Macintosh 406

réinitialiser 278
 réutiliser 357

Multibrin 95
 Multitâche 147

N

NAS 286
 NAT 129
 nbstat 264
 NetBIOS 176
 NetBoot 404
 NetMeeting 215
 Netstat 264
 Nettoyage 422
 Network Monitor 265
 NetworkView 262
 nmbd 397
 Nom
 affiché simple 215
 complet 391
 de domaine 139
 de l'ordinateur 176
 de partage 51, 289, 397
 d'étendue 132
 d'utilisateur 27, 270, 390
 ID utilisateur 25
 ordinateurs 25
 ressources réseau 26

NOS 16
 Notation décimale pointée 121
 Noyau 383
 nslookup 264
 NTFS 363
 Noeuds 11
 Numéros de ports 369

O

Octet 121
 Office 59
 en réseau 60

- installation sur réseau 61
 - modèles 64
 - Onde 185
 - Opérations logiques 119
 - Options de remise 213
 - Orange 242
 - Ordinateur
 - familial 251
 - ID utilisateur 26
 - personnel (PC) 18
 - OSI 431
 - Outils 428
 - Outlook 216
 - Mobile Access 214
 - Web Access 214, 252
 - OWA 252
- p**
- Page simple d'intranet 230
 - Paire(s) 94
 - torsadée 17, 92, 318
 - Pandits 224
 - Panneaux de raccordement 102
 - Paquets 91
 - Paramètres du réseau 320
 - Paramètres ILs 215
 - Pare-feu 206, 368
 - Windows 208
 - Partage 289, 400
 - activer 47
 - associer à une lettre de lecteur 37
 - de dossiers 29, 50
 - nom de partage 51
 - partage de fichiers 53, 146, 407
 - partage d'imprimantes 58
 - propriétés 51
 - Samba 401
 - SMB 296
 - PartitionMagic 386
 - Partitions
 - d'amorçage, Linux 385
 - de swap, Linux 386
 - Linux 384, 385
 - racine, Linux 384
 - Passerelle
 - applicative 372
 - Passerelle
 - de niveau circuit 372
 - résidentielle 193
 - Patch 376
 - PC
 - carte sans fil 191
 - réseau avec Macintosh 409
 - PCI, carte sans fil 191
 - PDA 244
 - Peer-to-peer 77
 - Performances 303
 - du réseau 310
 - Périmètre 207, 368
 - Périphérique de stockage 286
 - Personal Digital Assistants 244
 - Phase de conception 72
 - Pilote 39
 - Pince
 - à dénuder 98
 - à sertir 98
 - coupante 98
 - Ping 265
 - Plan du réseau 81
 - Plans 82
 - Plenum 95
 - Plug-and-play 383
 - PocketPC 244
 - Point
 - d'accès sans fil 194, 418
 - de montage, Linux 384
 - Pont 113
 - sans fil 194
 - POP3 215
 - Port 369
 - Portée
 - réseau sans fil 190
 - Porte
 - fermée 353
 - ouverte 353

Principes
réseau sans fil 189

Prise
électrique 317
murale 102
sans électricité 318

Processeurs 74, 306
types 74

Profil
utilisateur 277, 364

Programme
antivirus 375
de création de pages Web 225

Protection électrique 317
Proxy 372

Q

QuickTime Streaming Server 404

R

RAID 286
RAM (mémoire) 75
Rappels 252
Redémarrer
réseau 325
serveur 325
Red Hat Linux 383
Remote Installation Services 155
Répertoire 29
home 391
Répéteur 110, 432
Réseau 120, 225
boîte de dialogue 168
de domaine 26
définition 10
de groupe de travail 26
en étoile 90
hétérogène 146
informatiques 9, 239
interne d'entreprise 224
itinérant 10
local (LAN) 11

Macintosh 403
pair-à-pair 15
privé virtuel 254
redémarrer 325
sans fil 183
sans fil, domestiques 10
serveurs dédiés 77
téléphoniques 239
téléphonique public commuté 240

Réservation 133

Ressources 12
locales 24
réseau 24

Restrictions de remise 212

RIS 155

RJ-45 100

Roaming 193

Rôles du serveur 163

Root 385

Rotation des bandes, sauvegardes 346

Routage 434

Route 265

Routeur 113, 193, 206
pare-feu 254

Ruban adhésif armé 428

S

Samba 396

Sans fil, réseau
portée 190
principes 189

Sauvegarde(s) 337, 338, 417, 422
bibliothèque de bandes 339
complète 341
copie 342
création 346
DAT 338
différentielles 344
DLT 338
Fiabilité des bandes 347
incrémentielles 343
jeux à conserver 347
journalière 342

- locales 345
- logiciels 339
- normales 341
- réseau 345
- rotation des bandes 346
- sécurité 349
- Travan 338
- types 340
- virus 376
- Schéma du réseau 81
- Script d'ouverture de session 283, 365
- Sécurité 148, 351
 - comptes utilisateurs 355
 - droits utilisateur 363
 - mots de passe 357
 - nécessité 352
 - physique 354
 - profils d'utilisateurs 364
- Segments
 - répéteurs 110
- Server Message Block 396
- Serveur 14, 45, 400
 - base de données 79
 - dédié 225
 - de fichiers 78, 285, 290
 - de messagerie 211
 - DHCP 131
 - DNS 143
 - d'impression 78
 - d'imprimante 78
 - ILS 215
 - mandataire 372
 - messagerie 79
 - redémarrer 325
 - Samba 396
 - système d'exploitation 150
 - types 78
 - Web 79
 - Web IIS 226
 - X, Linux 382
- Service
 - d'annuaire 148
 - de sécurité 148
 - DHCP 130
 - DNS 139
 - pack 162
 - VoIP 241
- Session 162, 387
- SFR 242
- Shell, Linux 391
- Sites Internet
 - Windows Update 377
- Skype 240
- SkypeOut 240
- Slackware, Linux 384
- Smartphone 244
- SMB 396
- Smbd 397
- Sous-réseau 125
 - masque 126
- Spectre 187
- SPI, 371
- Spooling 38, 306
- SQL 11
 - Server 79
- SSID 184
- StarOffice 382
- statiques 228
- STL (Sigle de Trois Lettres) 11
- STLE (Sigle de Trois Lettres Etendu) 11
- Stockage réseau 285
- STP 95
- Support de VPN intégré 254
- suppression
 - fichiers 18
- Supprimer un travail d'impression 43
- SuSE Linux 384
- Switch 10, 103
- Synchronisation 214
- Système
 - binaire 117
 - de fichiers 146
 - de fichiers Linux 383
 - d'exploitation
 - d'exploitation multiutilisateur 382
 - d'exploitation réseau 79

T

- T1 205
- T1 et T3, accès Internet 205
- T3 205
- Tableau de bord 390
- Tâches 252
- Taille
 - de la boîte aux lettres 213
 - des segments 308
- TCP/IP 117, 171, 172
- Téléphone portable 244
- Terminer sa session 43
- Tester une connexion réseau 319
- Tête de lecture 348
- Token Ring 91
- Topologies 90
- tracert 265
- Transfert d'appel 241
- Travaux d'impression
 - arrêter 43
 - ordre de la file d'attente 43
- Tunnel crypté 254
- Types de serveurs 78

U

- Ubuntu 383
- UNC 39
- Universal Naming Convention 39
- UNIX 381
- USB, adaptateur sans fil 191
- Usurpation d'adresse IP 371
- Utilisateur 329, 400
 - et ordinateurs Active Directory 211
 - supprimer 280
- Utiliser les imprimantes réseau 254
- UTP 80, 92, 94

V

- Ventilateur 317
- Ver 374
- Version sécurisée du protocole Web
 - HTTP 252

- Virtual Private Networks 254
- Virus 373, 374
 - cheval de Troie 374
 - sauvegardes 376
- Visio 81
- Vitesse du réseau 309
- Voie d'évolution 258
- VoIP 239
- Voisinage réseau 33
- Voix 239
 - sur réseau IP 240
- VPN 149, 254

W

- WAP 191
- Web
 - Serveur 79
- Webcams 14
- WebObjects 404
- Windows
 - comparaison avec Linux 384
 - Mobile 245
 - Server 2008 135
 - Update 377
- Wine 383
- WLAN 184
- World Wide Web 223, 435

X

- X400 215
- X Server 387
- X Window 382
- X Window System 382

Y

- Yosemite 340

Z

- Zone réseau 30

Pour comprendre enfin quelque chose aux réseaux informatiques !

Aujourd'hui, que ce soit en entreprise ou dans le monde de l'Internet, la communication passe par les réseaux informatiques. Du réseau personnel, que l'on installe chez soit en connectant 2 ou 3 ordinateurs, au réseau d'entreprise avec connexion serveur, ce livre vous donne toutes les informations pour choisir le réseau qu'il vous faut, puis pour l'administrer.

Ce livre compte 30 chapitres et chacun d'eux traite d'un aspect différent du réseau, comme l'impression sur le réseau, la connexion des câbles du réseau ou la configuration de la sécurité. Il regorge d'informations et vous pouvez donc aller directement vers le sujet qui vous préoccupe. Si vous voulez avoir une vue générale de la sécurité, lisez tout le chapitre qui traite de la sécurité. Si vous voulez simplement savoir comment générer un mot de passe correct, ne lisez que la section qui traite des mots de passe.

L'ESPRIT DES NULS

- ✓ Le savoir et le savoir-faire des meilleurs spécialistes
- ✓ Une approche sans complexe des sujets traités
- ✓ Tout et seulement tout ce qui vous intéresse
- ✓ Un accès rapide à l'information grâce à un système d'icônes
- ✓ Une bonne dose d'humour



Découvrir comme

- La vie en réseau
- Partager fichiers et imprimantes
- Concevoir et déployer le réseau
- Le protocole TCP/IP
- Installer un serveur
- Configurer les postes clients (Windows XP, Vista ou Windows 7)
- Se connecter à Internet

Renaissance
Medias
Livres Durs



Retrouvez les Nuls
sur www.pourlesnuls.fr

FIRST
Editions

