



Compendium IT transtec

Publication
Andrea Schneider / Dieter Weisshaar



Auteur :

Björn Gruner

en collaboration avec :

Andreas Ackermann, Stefan Barth, Wolfgang Bauer,
Corinne Brucker, Dieter Bodemer, Franz Bochtler, Milka Kriegelstein,
Senol Meral, Marco Poggioli, Winfried Reiser, Marco Sanna,
Benjamin Schnauffer, Ute Textor, Guido de Vries

Réalisation :

Björn Gruner

Mise en page et composition :

Grufi Design, Stuttgart

Impression et reliure :

Imperimerie universitaire Heinrich Stuert, Wuerzburg



THE EUROPEAN IT FACTORY

© transtec AG, Tuebingen

Waldhoernlestrasse 18
72072 Tuebingen, Allemagne
www.transtec.de
transtec@transtec.de
Tel.: 0049 (0) 7071/703-0

1ère Edition 2003

L'ouvrage et ses annexes sont protégés par les droits d'auteur. Toute utilisation, autre que celles autorisées par la législation, est soumise à l'approbation préalable et écrite de transtec AG. Tous droits réservés, en particulier pour la traduction, la reproduction, la présentation, la copie de textes, graphiques et tableaux, l'émission par radio ou autre moyen de communication de données, la copie par microfilm ou la reproduction par tout autre moyen et la sauvegarde sur des supports informatiques, même pour une mise en valeur partielle d'extraits.

Tous les noms de produits, marques publicitaires, noms commerciaux, appellations etc. sont utilisés sans garantie de libre emploi et peuvent être des marques déposées.

Les informations contenues dans cette publication ont été réunies avec le plus grand soin. Ni transtec AG, ni les éditeurs, auteurs ou autre collaborateurs mentionnés, ni la rédaction n'assument la responsabilité juridique ou une quelconque responsabilité en cas de données erronées, et leurs conséquences.

ISBN 3-00-011427-0

Edition anglaise :

ISBN 3-00-011425-4

Edition française :

ISBN 3-00-011426-2



Nous sommes désormais continuellement confrontés aux technologies de l'information. Que ce soit à l'occasion d'une formation, dans la vie professionnelle, en voyage ou même chez-soi, les technologies de l'information nous épaulent dans presque tous les domaines de la vie quotidienne. Mais, lorsque nous sommes face à une terminologie compliquée, nous atteignons rapidement nos limites de compréhension. Il s'ensuit que certaines choses nous échappent, voir même que nous ne soyons plus en mesure de comprendre des processus entiers. Une utilisation objective se voit ainsi limitée par notre manque de connaissance. Les experts informatiques, de par leur jargon spécialisé, sont en partie responsables de cette confusion. Confusion que nous souhaitons aussi pouvoir éclaircir.

Il existe dès lors un énorme déficit en informations remaniées et structurées de manière compréhensible. Le compendium IT, actualisé et présenté sous forme de livre, a pour but de combler ce déficit et de contribuer à une meilleure compréhension des technologies de l'information. Dans ce contexte, l'expérience accumulée au cours des dernières décennies par les employés qualifiés de transtec AG a contribué à la rédaction de cet ouvrage de référence. Des termes et des procédés complexes vous sont présentés de manière plus intelligible.

La société transtec AG est un acteur majeur sur le marché informatique européen et da été classé par IDC en 9^{ème} positiondes fabricants de serveurs, et même en 6^{ème} position en Allemagne.

Dieter Weisshaar, Chairman of the Management Board of transtec AG



L'idée de rédiger un livre reprenant les termes spécialisés usuels dans le domaine IT ainsi que les produits correspondants détaillés donnait raison à transtec AG. Il s'agit en fait du développement constant de la Partie Conseil, les fameuse pages jaune, du catalogue semestriel de produits, qui constitue depuis des années un élément très apprécié en matière de communication. Cette source d'informations s'avère précieuse aussi bien pour un président de comité de direction que pour un ingénieur de développement, un administrateur de réseau, un acheteur IT, voire un rédacteur en chef d'un magazine informatique.

Ce sont des gens qui se voient quotidiennement confrontés aux technologies de l'information et qui font face à des questions toujours nouvelles. Qu'est ce qu'un lecteur AIT? De quoi se compose une transmission sans fil ? Quelles sont les architectures d'ordinateurs existantes ?

Le compendium IT répond à ces questions et à bien d'autres encore, de manière concise, simple, intelligible et complète. Il s'adresse aux responsables IT dans le domaine public et industriel, aux étudiants, aux écoliers et bien entendu à tous ceux qui s'intéressent aux technologies de l'information.

Ce nouvel ouvrage de référence deviendra pour vous un outil indispensable pour toutes les questions relevant du domaine complexe des technologies de l'information. Il est tout simplement complet et cohérent.

Andrea Schneider, Director of Marketing of transtec AG

Tuebingen, Mai 2003

	page
1. Architectures d'ordinateurs	10
1.1 Systèmes basés sur Intel	10
1.2 Systèmes RISC de Sun et transtec	16
2. Systèmes d'exploitation	18
2.1 Windows	18
2.2 Systèmes d'exploitation Unix	27
2.3 Virus informatiques	31
3. Cluster	32
4. Bus de mémoire	36
4.1 Guide	36
4.2 Interface SCSI	36
4.3 Fibre Channel	42
4.4 SSA	50
4.5 Interface ATA (IDE)	51
4.6 Interface USB	52
4.7 FireWire 1394	52
5. Hard Disks and RAID	54
5.1 Guide	54
5.2 Disques durs	54
5.3 Disques virtuels (mémoire RAM)	59
5.4 Lecteurs de disquettes	60
5.5 Lecteurs de disques amovibles	60
5.6 RAID	61
6. Réseaux de stockage	70
6.1 Guide : Centralisation de stockage	70
6.2 Storage Area Network (SAN)	71
6.3 iSCSI	73
6.4 Network Attached Storage (NAS, archivage lié au réseau)	73
7. Enregistreurs de bandes magnétiques	75
7.1 Processus d'enregistrement de bandes linéaires	75
7.2 Processus d'enregistrement de piste diagonale	78
7.3 Autres processus d'enregistrement	82
7.4 Logiciel pour enregistreur de bandes magnétiques	83

8. Mémoires optiques	84
8.1 Lecteurs CD-ROM	84
8.2 Lecteurs CD-R et CD-RW	85
8.3 Lecteurs DVD	86
8.4 Lecteurs magnéto-optiques	87
8.5 Perspectives futures	88
9. Mémoires vives	89
9.1 Technologies des mémoires	89
9.2 Modules de mémoire	93
9.3 Termes relatifs à la mémoire	95
10. Communication	97
10.1 Définition	97
10.2 Conditions préalables à une communication réussie	97
10.3 Types de communication	97
11. Standards et normes	99
11.1 Définition Norme	99
11.2 Types de normes	99
11.3 Organismes importants de normalisation en IT	99
12. Le modèle de référence OSI	101
12.1 Introduction	101
12.2 Structure	101
12.3 Couches	102
13. Procédés et techniques de transmission	104
13.1 Introduction	104
13.2 Signal	104
13.3 Fonctionnement parallèle	103
13.4 Transmission de signes	105
13.5 Fonctionnement	105
14. Personal Area Networks - PANs	106
14.1 Définition	106
14.2 Méthode de transmission	106

15. Réseaux locaux LAN (Local Area Network)	110
15.1 Définition	110
15.2 Procédés d'accès	110
15.3 Ethernet et 802.3 LAN	111
15.4 Adresses MAC	112
15.5 Standards Ethernet	113
15.6 Topologies en anneau	116
15.7 Protocoles/standards	118
15.8 Matériel - composants actifs	121
15.9 Matériel - composants passifs	126
15.10 Gestion	129
16. Metropolitan Area Networks - MANs	130
16.1 Définition	130
16.2 Technologies de transmission pour la création d'un MAN	130
17. Wide Area Networks - WANs	132
17.1 Définition	132
17.2 L'adressage sur le WAN	132
17.3 Les protocoles sur le WAN	133
17.4 La diffusion de données sur le WAN	137
17.5 Les modes de transmission sur le WAN	138
17.6 Technologies du WAN	139
17.7 La transmission de données sur le WAN	140
17.8 Sécurité sur les WAN	154
17.9 Matériel informatique pour le WAN	167
18. LAN Core Solutions	174
18.1 Introduction	174
18.2 Nouvelles stratégies pour réseaux	175
18.3 Solutions actuelles	176
18.4 Réseaux avec noyau distribué	177
18.5 Création d'une Distributed Fabric dans un réseau	179
18.6 Une nouvelle orientation pour les réseaux d'entreprise	182
18.7 Résumé	182

19. Périphériques de saisie	183
19.1 Claviers	183
19.2 Souris et trackballs	183
19.3 Scanners	184
19.4 Lecteurs de codes-barres	186
20. Communication des données	188
20.1 Commutation CVS (Clavier, Vidéo, souris)	188
21. Terminaux	189
21.1 Les terminaux alpha	189
21.2 Les terminaux X-Window	189
21.3 PC et stations de travail	191
21.4 Windows Based Terminals (WBT)	191
21.5 Network Computer (NC)	192
21.6 Network PC	194
22. Périphériques de sortie	195
22.1 Ecrans	195
22.2 Projecteurs LCD	201
22.3 mprimantes	202
23. Multimédia	207
23.1 Appareils photos numériques	207
23.2 Applications linguistiques	207
23.3 Traitement des signaux vidéo	208
23.4 Systèmes de conférence vidéo	211
24. Onduleurs	212
24.1 Problèmes, causes et effets	212
24.2 Technologies	213
24.3 Dimensionnement des onduleurs	217
24.4 Alarme, interfaces, communication sur le réseau	218
24.5 Déconnexion	219

1. Architectures d'ordinateurs

Les chapitres suivants donnent un bref aperçu des systèmes basés sur Intel ainsi que des plus courantes stations de travail RISC proposées actuellement sur le marché et fabriquées par Sun et transtec.

L'élément principal pour les systèmes, et aussi l'élément souvent le plus onéreux, est l'unité centrale (CPU).

Le sujet d'actualité dans le domaine des processeurs est certainement le passage des architectures 32 bits à 64 bits. La plupart des architectures RISC, telle SPARC par exemple, ont déjà franchi le pas. Pour l'architecture Intel IA64, Itanium en est le premier processeur. Il a été produit au cours de l'été 2001. L'Itanium 2, son successeur, est disponible depuis fin 2002. AMD livrera l'Athlon 64 (version Desktop) et l'Opteron (version serveur) à partir du deuxième trimestre 2003. Ce qui importe dans le sujet, ce n'est pas seulement la disponibilité du hardware, mais surtout les systèmes d'exploitation adaptés. Microsoft Server 2003, le successeur de Windows 2000 supportera la technologie 64 bits. Pour les premiers systèmes, Microsoft a mis au point une version Windows 2000 spécialement équipée de la fonctionnalité 64 bits. Linux, quant à lui, propose déjà un noyau supportant 64 bits. Pour l'utilisateur, les avantages au niveau de la performance dans une architecture 64 bits ne se feront réellement sentir que lorsque les applications, elles aussi, seront disponibles en 64 bits.

1.1 Systèmes basés sur Intel

1.1.1 Processeurs

Les PC sont essentiellement équipés processeurs Intel. Cependant les produits du concurrent AMD sont en nette progression et Intel doit, de plus en plus souvent, céder ses records de vitesse à AMD.

A l'époque des processeurs Pentium et Pentium Pro, le choix de la carte mère était encore assez simple. Aujourd'hui, les différents modèles de processeurs et la multiplicité des chipsets rendent la tâche de plus en plus difficile. Rien que pour les emplacements de processeurs, les possibilités sont nombreuses et en plus, la technologie ne survit pas très longtemps. Pour cette seule raison, il est quasi impossible d'équiper des systèmes de plus d'un an avec les tous nouveaux processeurs. Lors de la planification de vos investissements, n'oubliez donc pas que seuls la mémoire principale et les disques durs peuvent subir ultérieurement et sans difficulté une extension.

1.1.2 Bus de données

Le choix relatif au système de bus est relativement simple, puisque pour l'instant, seuls deux types déterminants de bus pour PC sont disponibles : le bus PCI et le bus AGP. D'autres bus tels les bus ISA, EISA ou Microchannel ne jouent plus aucun rôle. Pratiquement chaque système actuel comprend des emplacements PCI et un emplacement AGP. Le bus AGP ne supporte cependant

que des cartes graphiques.

Ci-dessous, un aperçu de tous les systèmes bus, utilisés actuellement dans les PC et les serveurs

Bus PCI

Dans sa première version, le bus PCI fonctionne déjà avec 32 bits et 33 MHz. Un bus PCI peut atteindre un taux de transfert maximum de 133 Mo/s. Dans la version 64 bits, ce taux maximum est de l'ordre de 267 Mo/s. Le net avantage du bus PCI est son indépendance par rapport au type de processeur. PCI peut ainsi être mis en oeuvre avec d'autres processeurs que ceux d'Intel et notamment avec des processeurs SPARC, par exemple. Le bus PCI est parrainé par Special Interest Group. Cette association compte dans ses rangs presque tous les grands constructeurs de processeurs, de cartes meres, de disques durs, de contrôleurs et de cartes graphiques.

PCI-X

En raison des exigences toujours croissantes en matière de performance des serveurs, la capacité des bus PCI sera insuffisante à très court terme. C'est pourquoi, le comité PCI Steering s'est attelé à la rédaction de la spécification PCI-X. Cette spécification fut développée à l'origine par IBM, Compaq et Hewlett Packard. PCI-X autorise l'utilisation d'un emplacement avec 133 MHz et des autres emplacements avec 66 ou 100 MHz, pour pouvoir atteindre un débit de 1 Go/s, ce qui correspond au double de PCI. Un aspect essentiel de PCI-X est la compatibilité en amont, ce qui signifie que les cartes PCI-X fonctionnent dans les systèmes PCI et vice versa. PCI-X-2.0 est prévu pour procéder à une nouvelle augmentation du débit de données. Double Data Rate et Quad Data Rate devraient permettre d'augmenter les taux de transfert au maximum à 2,1 voire 4,2 Go/s. Vous trouverez plus d'informations sur la page d'accueil de PCI-SIG : www.pcisig.com

PCI Express

Dans l'avenir, PCI-X devrait être remplacé par PCI Express (créé sous le nom de 3GIO (3rd Generation I/O)). PCI Express est un "bus série sur voies", modulable jusqu'à 32 voies simultanées pouvant circuler dans les deux sens. Chaque voie peut transmettre jusqu'à 250 Mo/s dans les deux sens avec la fréquence prévue de 2,5 GHz, autrement dit au maximum 2 x 8 Go/s. PCI Express devrait être disponible dès 2004.

InfiniBand

InfiniBand est une autre proposition d'interface hautement performante pour serveurs, conçue par InfiniBand Trade Association. InfiniBand découle de la fusion des groupes Future et NGIO. Contrairement à PCI-X, InfiniBand n'offre pas de compatibilité en amont, mais a par contre l'avantage de pouvoir offrir des fonctions tout à fait nouvelles. InfiniBand rejoint de très près les concepts fondamentaux de Fibre Channel : les systèmes sont connectés à une "usine" E/S au moyen d'un ou plusieurs adaptateurs Channel (Host Channel Adapter-HCA). Des contrôleurs de stockage ou de réseau sont de nouveau connectés à cette usine par des adaptateurs Target Channel (Target Channel Adapter - TCA). Dans InfiniBand, l'adressage s'effectue par des adresses Ipv6, de

telle sorte que le nombre d'appareils pouvant fonctionner simultanément est pratiquement illimité. La largeur de bande est extensible jusqu'à 6 Go/s. La longueur du câblage peut atteindre 17 m avec un câble en cuivre, et jusqu'à 100 m avec la fibre de verre. La construction de systèmes plus petits est tout à fait possible avec InfiniBand, car dans le serveur, les systèmes bus sont complètement inutiles. Vous trouverez plus d'informations sur la page d'accueil de InfiniBand TA : www.infinibandta.org

AGP

Accelerated **G**raphics **P**ort est un emplacement, conçue par Intel pour une carte graphique. Avec les cartes graphiques classiques, une partie de la mémoire graphique disponible est utilisée pour les textures. Afin de pouvoir représenter des détails toujours plus fins et des résolutions toujours plus élevées, la mémoire intégrée sur les cartes a été gonflée. Pour les applications standards, cette mémoire est toutefois inutilisée. Le concept d'AGP définit que la carte graphique accède directement aux données stockées dans la mémoire principale. L'application graphique choisit les données textures selon la taille, la couleur et la résolution optimale et les met à disposition de la carte AGP. Le processeur et l'interface AGP échangent les données avec 66 MHz et 32 bits, ce qui correspond à un taux de transfert de 266 Mo/s. De plus, la carte AGP peut utiliser le mode 2x ou le mode 4x. Par le mode 2x, les données sont transmises par les deux flancs du signal de synchronisation et le taux de transfert atteint ainsi 533 Mo/s, c'est-à-dire 4 fois les vitesses atteintes avec un bus PCI. Le mode 4x permet encore plus. Aux AGP 4x s'ajoutent encore les signaux complémentaires d'impulsion AD_STB0# et AD_STB1#, qui forment avec les impulsions standard des couples différentiels de transmission. Ces quatre impulsions travaillent effectivement avec 133,34 MHz. La transmission dans les AGP 4x s'effectue également par les flancs ascendants et descendants des impulsions AD. Grâce aux 133,34 MHz des signaux d'impulsion, on atteint quatre cycles par séquence AGP, ce qui correspond concrètement à 266,67 MHz et à une bande passante théorique de 1.017 Mo/s.

AGP est compatible en aval avec PCI : les PCI-Busmaster et les cartes graphiques Framegrabber, par exemple, permettent d'écrire des données sur la carte graphique AGP via la bus PCI. La bande passante élevée dont dispose la carte graphique AGP pour accéder à la mémoire principale a entraîné la migration vers la technologie SDRAM avec 133 MHz ou les modules Rambus comme technologie de mémoire principale.

I2O

I2O (Intelligent I/O) est aussi un développement Intel. I2O est basé sur le processeur d'E/S Intel i960 RP, lequel représente un sous-système complet sur un chip. Grâce au pont « On-Chip PCI-to-PCI » le processeur d'E/S i960 RP peut être directement connecté au bus PCI. Le processeur i960 RP libère le CPU du traitement des interruptions d'entrée/sortie (E/S) et augmente la performance globale du système. Cependant, ce processeur nécessite l'utilisation de logiciels spécialement écrits pour lui. Malgré tous ces avantages, le standard d'interface I2O n'a jamais pu vraiment s'imposer et est aujourd'hui pratiquement abandonné.

Interface "carte PC"

Le terme interface "carte PC" décrit un standard de carte enfichable de la taille d'une carte de crédit, défini par la **P**ersonal **C**omputer **M**emory **C**ard **I**nterface **A**ssociation (**PCMCIA**) en septembre 1990. Les premiers produits à répondre à ce standard furent les simples cartes mémoire. Ce standard s'est élargi peu à peu, de telle sorte que d'autres matériels furent développés et mis en oeuvre : Par exemple, les cartes, modem et adaptateurs LAN.

Les cartes PC ont toutes les mêmes dimensions (85,6 x 54 mm) et disposent d'une prise de 68 connexions réparties sur deux rangs. Selon leur type, elles ont différentes épaisseurs : Type I (3,3 mm) pour la plupart des cartes mémoire, type II (5 mm) pour les cartes et type III (10,5 mm) pour les disques durs. Une carte de type III prend généralement la place de deux emplacements de type II superposés. Le nouveau développement du standard de carte PC s'appelle CardBus et contient des extensions pour permettre une consommation d'énergie réduite, une compatibilité améliorée et des performances plus élevées. La spécification du CardBus décrit un bus 32 bits semblable à un bus PCI, cadencé à 33 MHz et doté d'un taux de transfert de données maximum de 132 Mo/s. Cela permet au CardBus de reporter les caractéristiques du bus PCI sur un équipement de la taille d'une carte de crédit et permet ainsi au PC de disposer de matériel traitant des flux de données E/S élevés (par ex. Fast Ethernet). Le standard de la carte PC est compatible en aval avec le standard PCMCIA. Cela signifie que les anciennes cartes PCMCIA fonctionnent dans le nouvel emplacement Cardbus. En revanche, les nouvelles cartes d'interface PC ne peuvent pas être utilisées dans les anciens emplacements PCMCIA.

Les domaines d'application pour la carte d'interface PC se situent au niveau des ordinateurs portables. Ces systèmes disposent d'un nombre limité d'interfaces externes et n'ont pas d'emplacements internes pour une carte d'extension. Les emplacements pour les carte PC offrent une possibilité d'extension idéale.

1.1.3 Disques durs

Avant de se décider pour l'achat d'un modèle de disque dur précis, il faut au préalable avoir répondu à la question suivante : doit-il s'agir d'une solution IDE ou bien SCSI ?

La taille des disques durs s'aligne sur l'application et sur le système d'exploitation utilisé. Le standard des disques durs de PC se situe désormais aux alentours de 80 Go, ce qui s'explique aisément par la chute vertigineuse qu'a connu le prix du Mo de mémoire de masse ces dernières années.

1.1.4 Ecrans et cartes graphiques

Le choix d'une carte graphique doit impérativement prendre en compte l'existence ou non d'un pilote de carte graphique approprié au niveau du système d'exploitation qui sera mis en œuvre (comme par ex. pour Windows XP). Seule l'existence du pilote approprié au niveau du système d'exploitation permet de bénéficier de la résolution maximale de la carte graphique et de la fréquence de rafraîchissement maximale de l'écran. La qualité d'une carte graphique dépend

essentiellement du processeur graphique et de la mémoire vidéo qu'elle exploite. Le choix de l'écran n'est pas non plus sans importance. Il doit répondre à tous les critères définissant un poste de travail ergonomique (haute résolution, faible niveau de rayonnement, excellente fidélité des couleurs, etc.) et correspondre à la puissance demandée par la carte graphique. Une carte graphique émettant un signal vidéo, dont la fréquence est supérieure à celle que peut traiter l'écran, est susceptible d'endommager celui-ci. Etant donné que, d'une manière générale, un écran doit satisfaire les exigences imposées par l'évolution des applications plus longtemps que les autres composants d'une installation informatique, il serait judicieux de ne pas se laisser intimider par le prix plus élevé d'un écran de bonne qualité.

1.1.5 Systèmes d'exploitation

Nous nous abstenons ici de recommander un système d'exploitation précis. Celui-ci dépend avant tout des applications à mettre en oeuvre. Ce choix relève entièrement de l'appréciation de l'utilisateur.

Signalons que la taille de la mémoire vive nécessaire pour travailler raisonnablement est un point décisif dans le choix du système d'exploitation. Il se peut que la capacité mémoire effectivement nécessaire dépasse largement les recommandations du fabricant.

Pour certains systèmes d'exploitation, l'extension mémoire minimale recommandée atteint 16 Mo. Pour les applications actuelles, cela ne suffit plus. Dès que l'on désire installer Windows 98 ou Windows ME, le système doit au moins comprendre 32 Mo et, par exemple pour un pack comme Microsoft Office, au moins 64 Mo. Sinon, le microprocesseur perdra trop de temps à déplacer les données de la mémoire vive vers le disque dur et vice-versa. Sous Windows NT ou Windows 2000, l'obtention d'une vitesse de travail acceptable exige 128 Mo. Pour Windows XP, il s'agit même de 256 Mo. Dans le monde Unix, les exigences en matière de mémoire vive dépendent de la version utilisée. En présence d'une interface utilisateur graphique, il faut cependant disposer d'au moins 64 Mo.

1.1.6 Applications standard

Les applications standard sont : traitement de texte, banques de données, tableaux et représentations graphiques. Un lecteur-enregistreur de bandes magnétiques ou de disques MO (magnéto-optique) se révèle souvent être une option très utile, dès lors que l'on travaille avec des programmes de gestion de banques de données ou des logiciels de présentation graphique. Les volumes de données générés par ce type d'application ne peuvent généralement plus être maîtrisés par un simple lecteur de disquettes. Rappelons que les lecteurs DVD-ROM conviennent pour les applications graphiques, et les cartes son pour les applications multimedia. L'utilisateur désireux d'exécuter des présentations à partir de son PC (exposés, séminaires de formation, etc.) sera sans doute bien avisé d'acquérir un projecteur LCD.

1.1.7 Applications spécifiques

Les “applications spécifiques” telles que : programmes multimédia, programmes de conception assistée par ordinateur (CAO), logiciels de retouches graphiques ou de Desktop Publishing (DTP) soumettent l'ordinateur à des exigences supérieures à celles des applications standard. L'équipement du système doit être de meilleure qualité, surtout en matière de processeurs et de mémoire principale. Les lecteurs DVD sont aussi entre temps devenus un équipement standard. L'acquisition d'un système de sauvegarde approprié apparaît là encore comme une sage précaution.

1.1.8 Applications réseau

Lorsque l'on travaille sur un serveur de réseau, le périphérique graphique joue généralement un rôle non négligeable. Pour ce type d'application, un simple écran VGA suffit. Lors de la conception d'un système, la fréquence du processeur, le bus de données et le contrôleur de disque dur doivent pouvoir travailler de manière optimale avec le support mémoire. La carte réseau mise en oeuvre devrait également disposer des meilleures performances. Certains serveurs permettent un fonctionnement serveur non dédié. En d'autres termes, le serveur peut aussi être utilisé comme station de travail. Nous déconseillons cependant ce procédé, car il entrave fortement la performance des fonctions du serveur.

Même si certaines cartes mères dotées de la fonctionnalité Power-Management peuvent être utilisées sur un serveur, cette fonction est tout de même à déconseiller. En effet, après un stand-by (le mode de fonctionnement économique, encore appelé “veille”), les temps de réponse des stations raccordées peuvent durer quelques secondes.

Un système de sauvegarde approprié constitue en revanche une extension réellement utile d'un serveur de réseau. Il sera installé soit dans le serveur soit sur une station de travail. Un tel système de sauvegarde ne suffit pas à lui seul pour garantir que le serveur ne perdra jamais de données. La solution optimale dans ce contexte consiste à faire appel à un système RAID. Et dans tous les cas, un onduleur est vivement recommandé.

Avec l'accroissement constant du nombre de stations raccordées, même le serveur de réseau le plus performant atteindra tôt ou tard ses limites.

Sur les réseaux très sollicités, il convient de vérifier si une réorganisation du réseau initial en plusieurs sous-réseaux, reliés entre eux par des ponts ou des routeurs, ne réduirait pas la charge du réseau.

La configuration d'une station de travail dépend toujours des applications que l'on souhaite utiliser. Une station de travail ne nécessite pas obligatoirement un disque dur. En effet, un « boot-ROM » monté sur la carte réseau permet de redémarrer directement à partir du disque dur du serveur.

1.2 Systèmes RISC de Sun et transtec

1.2.1 Processeurs

Sun Microsystems présente la troisième génération de la famille des microprocesseurs UltraSPARC. Le processeur UltraSPARC III a été développé pour pouvoir faire face à la croissance fulgurante d'Internet et au traitement de quantités énormes de données qui y est lié. Il établit de nouvelles références en matière de flexibilité, puissance et taux de transfert de données. Sun Microsystems offre actuellement trois types de processeurs : **Ultra IIe, UltraSPARC III** et le nouveau **UltraSPARC IIIi**. Ces processeurs existent avec différentes fréquences.

Les processeurs UltraSPARC de Sun sont cadencés à 360, 400, 450 et 480 MHz et disposent d'une mémoire cache L2 pouvant atteindre 8 Mo. Ces processeurs sont mis en oeuvre dans toutes les stations de travail UltraSPARC. Un serveur d'entreprise (Enterprise Serveur) peut quant à lui recevoir jusqu'à 106 CPU (Sun Fire 15K). Les modèles Ultra IIe ne sont disponibles qu'en version monoprocesseur avec 500 MHz. Le nouveau UltraSPARC III est actuellement cadencé à 600, 750, 900 et 1050 MHz. SUN propose des cadences atteignant 2,1 GHz. transtec offre dans beaucoup de domaines des solutions de remplacement au modèle original Sun, ne représentant aucune différence ou seulement à quelques détails près.

1.2.2 Bus de données

Deux bus système différents sont disponibles pour la connexion de cartes d'extension sur les machines Sun :

Le **SBus** existe en deux versions. La version 32 bits avec un taux de transfert de 40 Mo/s et 64 bits avec un taux de transfert de 100 Mo/s. Le système reconnaît automatiquement le type de carte installée et adapte la vitesse en fonction. Le second bus système présent dans tous les modèles actuels (Ultra60 et Ultra450, mais aussi dans les tous nouveaux systèmes Ultra III « Blade 1000 » et « SunFire 280R » par exemple) est le **bus PCI**. Les modèles PCI supportent les spécifications du bus PCI dans une configuration 64 bits, 66 MHz et atteignent un débit théorique de 528 Mo/s. L'offre en cartes supplémentaires reste encore fortement limitée. La plupart des fabricants de cartes ne fournissent que des pilotes destinés aux systèmes d'exploitation Windows. Solaris, quant à lui, nécessite des pilotes dédiés. Cependant, le bus PCI a complètement remplacé le SBus dans tous les systèmes.

Le bus UPA, mis en oeuvre dans tous les systèmes UltraSPARC, sert de bus processeur. En fonction du modèle, la machine dispose jusqu'à 64 emplacements UPA.

L'architecture Ultra Port (UPA) fait appel à un Cross Bar Switch interne qui relie et coordonne la CPU, la mémoire et les composants entrée/sortie (E/S) du système. UPA réalise une excellente performance avec un taux de transfert de 2,4 Go par seconde. La technologie UPA utilise de manière efficace la performance du processeur UltraSPARC 64 bits avec un processing de 64 bits intégré.

1.2.3 Bus de périphériques

Les nouveaux ordinateurs de Sun intègrent une interface FireWire (IEEE 1394) et un bus USB. L'Universal Serial Bus sert principalement à connecter le clavier et la souris. Un Fibre Channel Arbitrated Loop sera destiné à l'avenir aussi bien aux disques durs internes qu'aux systèmes de stockage externe RAID. Une interface UltraSCSI est également prévue pour les périphériques externes. Le réseau est connecté via une interface 100 Base-T. Le CREATOR "Frame Buffer" est enfiché sur un emplacement UPA et garantit une performance élevée pour toutes les applications graphiques haut de gamme. La carte CREATOR associe la mémoire linéaire d'un "Frame buffer" et la connexion directe de l'architecture UPA 128 bits au "Visual Instruction Set" (jeu d'instructions graphiques) du processeur UltraSPARC.

1.2.4 Systèmes d'exploitation

Solaris est le système d'exploitation le plus répandu sur les systèmes SPARC. Il a déjà fait ses preuves et il est reconnu pour sa stabilité. La version courante, Solaris 8 est une version qui maîtrise complètement les 64 bits et dont les performances et la fiabilité sont remarquables, en particulier en matières d'applications Java. Vous trouverez de plus amples informations relatives au Solaris 8 dans le chapitre Systèmes d'exploitation.

Le système d'exploitation Linux est également disponible mais n'est pas encore très répandu.

2. Systèmes d'exploitation

Les chapitres suivant proposent un bref aperçu des systèmes d'exploitation courant Microsoft et Unix.

2.1 Windows

2.1.1 Windows 2000

Microsoft Windows 2000, connu aussi auparavant sous la dénomination Windows NT 5.0, a été doté d'une multitude de caractéristiques et de fonctions nouvelles par rapport à Windows NT. Citons l'administration, les possibilités de modularité et d'extension de la gestion des volumes de stockage et des composants matériels. Microsoft offre Windows 2000 en quatre versions :

Windows 2000 Professional correspond à la station de travail Windows NT et gère une mémoire pouvant atteindre 4 Go maximum, ainsi que deux processeurs.

Windows 2000 Server est le successeur du serveur Windows NT et offre le support matériel pour une mémoire principale de 4 Go max. et quatre processeurs. Cette version Server contient déjà les services terminaux Windows et remplace Windows NT4.0 Terminal Server Edition.

L'édition Windows NT Enterprise est remplacée par **Windows 2000 Advanced Server**. Elle supporte une mémoire vive de 8 Go et 8 processeurs. En plus des fonctions de Windows 2000 Server, le IP-Loadbalancing (avec max. 32 serveurs) et Failover-Clustering pour deux serveurs sont également supportés.

Le **Windows 2000 Datacenter Server** représente le nec plus ultra. Il supporte jusqu'à 32 processeurs et une mémoire vive de 64 Go. Il offre les fonctions supplémentaires suivantes : Failover-Clustering pour quatre serveurs et le contrôle de processus pour la gestion de charge. Une caractéristique également très importante réside dans la possibilité de supporter des serveurs virtuels. Plusieurs instances du système d'exploitation peuvent fonctionner sur des serveurs à processeurs multiples, par ex. : deux serveurs virtuels dotés chacun de 4 processeurs peuvent être installés sur un serveur à huit processeurs.

Installation de Windows 2000 : L'installation de Windows 2000 sur un ordinateur sans système d'exploitation s'effectue par un CD de démarrage. La gestion matérielle « Plug-and-Play » fait désormais aussi son entrée avec Microsoft Windows 2000. Un autre avantage par rapport à Windows NT est qu'un rechargement est rarement nécessaire. Le support USB est également implémenté dans Windows 2000. Contrairement au serveur Windows NT, il n'est pas nécessaire de déterminer dès l'installation, si le serveur Windows 2000 doit être utilisé en tant que contrôleur de domaines. Grâce à l'assistant de configuration, le service destiné au répertoire actif (service répertoire particulière pour la gestion utilisateur) peut également être installé ultérieurement.

Mécanismes de réparation : Windows 2000 est équipé d'un mode de chargement amélioré et protégé. Un mécanisme de réparation amélioré supplémentaire est implémenté dans la ligne

de commande.

Administration : Microsoft Windows 2000 implémente "Active Directory" en tant que plate-forme centrale. Elle simplifie la gestion et l'accès au réseau et aux ressources du système. Les utilisateurs de Windows NT, peuvent être créés et gérés dans le répertoire actif suivant une hiérarchie divisée. La structure de la gestion utilisateurs n'est pas la seule caractéristique de Windows 2000, il a réellement dépassé aussi la barre des 20-40.000 utilisateurs par domaine qu'assurait NT. Un système de configuration centrale ainsi que la console Microsoft Management Console (MMC) configurable sont des caractéristiques nouvelles.

La technologie IntelliMirror permet de configurer de manière centralisée des postes de travail Windows 2000. Un répertoire actif permet de créer de manière centrale la configuration de référence, accessible alors à l'utilisateur ou à des groupes. L'utilisateur retrouve toujours sur tous les postes de travail Windows 2000 la même configuration et les logiciels nécessaires à l'utilisateur sont installés automatiquement sur chaque poste de travail. Il peut également être établi que la configuration ne puisse pas être modifiée par l'utilisateur.

Souplesse et extension : Windows 2000 supporte 64 Go de mémoire physique. Deux ou plusieurs serveurs peuvent travailler avec le serveur Cluster de Microsoft. Les serveurs se surveillent mutuellement, et l'autre prendre en cas de panne d'un des serveurs l'autre prendre le relais sans occasionner d'interruption. Lors d'une utilisation normale, les serveurs peuvent se répartir le travail entre eux afin d'atteindre une puissance de calcul plus élevée.

Gestion de stockage : NTFS implémente un système de quotas permettant à l'administrateur de définir la capacité de disque allouée à chaque utilisateur. L'extension EFS (Encryption File System) permet l'encryptage de données sensibles au niveau du fichier ou du répertoire.

Grâce au système de fichiers partagés DFS, les structures de répertoires et de fichiers partagés sur les serveurs Windows 2000 NT, Netware et Unix sont rassemblées de manière logique pour obtenir une meilleure vue d'ensemble. De cette manière, les utilisateurs trouvent très facilement les fichiers dans le réseau.

Gestion matériel : La fonctionnalité Plug-and-Play permet d'utiliser sans problème des cartes PC dans les machines. De plus l'extension du Windows Driver (WDM) devrait permettre l'utilisation des mêmes drivers pour Windows 98 et Windows 2000.

Fonctions de sécurité : Pour augmenter la sécurité d'exploitation, Windows 2000 empêche d'effacer les fichiers importants pour le système d'exploitation. Il n'autorise en outre que l'installation de pilotes certifiés par Microsoft.

Sécurité du réseau : L'interface de sécurité "Security Service Provider Interface" (SSPI) dans Microsoft Windows NT 4.0 est déjà implémentée, par exemple dans le Manager LAN NT, ainsi que le Secure Sockets Layer (SSL). Dans Windows 2000, SSL sera étendu et l'authentification Kerberos selon Kerberos5 sera également introduite. De plus, le support de Cartes Smart est intégré dans Windows 2000, pour augmenter la sécurité lors du login d'utilisateurs ou lors de la signature numérique de e-mails.

2.1.2 Windows XP

Windows XP se démarque immédiatement par sa conception claire qui permet une utilisation intuitive, même par des utilisateurs relativement inexpérimentés. Outre le nouveau design, une grande quantité de fonctions ont été rajoutées.

Le **menu de démarrage remanié** groupe les applications utilisées le plus fréquemment afin de pouvoir y accéder facilement. Les cinq programmes d'usage le plus courant sont affichés en premier, le programme d'e-mail ainsi que le navigateur Web standard sont toujours disponibles. De plus, il est possible d'ordonner la barre des tâches avec le **nouveau groupage de celles-ci**. Les fichiers ouverts sont maintenant affichés et groupés selon l'application.

Outre le design, Windows XP contient une série de nouveautés qui **renforcent le confort d'utilisation**. Windows sort bien plus vite de sa fonction de repos : toutes les applications sont immédiatement prêtes à l'emploi. Plusieurs personnes peuvent aussi exploiter un PC, ensemble ou en parallèle. Chaque utilisateur dispose d'un compte propre. Le changement d'utilisateur se fait facilement et rapidement. Les applications ouvertes avant le changement continuent toutefois de tourner. Ainsi, il n'est par exemple pas nécessaire d'interrompre le téléchargement d'un fichier depuis Internet lors d'un changement d'utilisateur car toutes les applications ouvertes suivent leur cours en arrière plan.

Le **support matériel** a lui aussi été grandement amélioré. Les périphériques comme les caméras numériques, les scanners ou les caméras vidéo DV sont reconnues automatiquement et toutes les fonctions d'enregistrement, de traitement et de sortie offertes par Windows XP peuvent être utilisées à tout moment.

Les performances aussi ont progressé sensiblement. Le premier effet de cette progression est visible dès la mise en route de l'ordinateur. Après plusieurs mises en route avec le même matériel et les mêmes logiciels, Windows XP charge les fichiers de démarrage sur le disque dur pour un accès plus rapide. Cette fonction dénommée **"Prefetching"** associée à un Login réseau optimisé permet à Windows de démarrer 34% plus rapidement qu'avec les versions Windows antérieures. La même fonction a aussi pour effet d'assurer un démarrage plus rapide des programmes.

Les **capacités multitâches accrues** sont assistées entre autres par l'utilisation des périodes d'arrêt pour des activités système, l'adaptation de l'interface utilisateur aux possibilités de l'ordinateur et une gestion efficace de la mémoire vive.

Les portables exploitent **les modes attente et repos**. En mode attente, le système arrête l'écran, les disques durs et autres périphériques mais continue d'alimenter la mémoire vive contenant les documents et les programmes ouverts. Après la remise en route, le travail peut être repris là où il a été arrêté, et ce en moins de 2 secondes avec les portables les plus récents. Si l'on met le portable en mode repos, les données contenues dans la mémoire vive sont inscrites sous forme comprimée sur le disque dur et l'ordinateur est complètement arrêté. La remise en route depuis ce mode dure un peu plus longtemps, la fenêtre de bureau se présente cependant de la même manière

qu'avant la mise en repos. Les fonctions de Power-Management introduites par Windows 2000 ont été encore améliorées. Le repos et l'attente fonctionnent bien plus rapidement et de manière bien plus fiable, ce qui protège les batteries d'ordinateurs portables et augmente la durée de mobilité. Windows XP permet, avec le **bureau à distance** d'avoir accès depuis n'importe quel endroit à l'ordinateur Desktop de la société avec toutes les applications, documents et liaisons réseau qu'il contient. Il est possible via une connexion Internet ou téléphonique de joindre le PC de société et d'y ouvrir une session virtuelle avec laquelle le bureau Windows habituel apparaît sur l'ordinateur distant. Comme tous les programmes du PC de société tournent en local et que seules les entrées de la souris et du clavier, et les sorties image, doivent être transmises, le bureau à distance est parfaitement approprié pour les liaisons modem ou RNIS.

Les réseaux hertziens (WLAN 802.11b) sont supportés par Windows XP Professional en série. Windows XP Professional reconnaît et configure tout automatiquement, dès qu'une liaison LAN existe ou qu'un roaming de cellule hertzienne a lieu. Des certificats répartis ou enregistrés sur Smart-Cards ainsi que le processus d'authentification 802.1X assurent une sécurité maximale contre l'écoute lors des transmissions (aussi bien au niveau des réseaux Ethernet câblés que des réseaux hertziens).

Windows XP Professional reconnaît les réseaux et leurs réglages TCP/IP de telle sorte que la **connectivité réseau** des PC existe automatiquement et soit préservée y compris lors du roaming. Si le réseau n'impose pas de configuration automatique, Windows XP propose de travailler avec des réglages TCP/IP alternatifs. De cette manière, l'utilisateur de Notebook peut obtenir sa configuration TCP/IP depuis un serveur DHCP dans le réseau de l'entreprise et travailler chez lui avec des adresses TCP/IP fixes.

Windows XP correspond à la génération suivante de la technologie Windows 2000 éprouvée et est ainsi encore plus stable que son prédécesseur. Le nouveau moteur Windows se fonde sur l'architecture 32 bits fiable de Windows 2000, qui se distingue par un modèle de sauvegarde totalement protégé. Le programme d'installation du système d'exploitation peut déjà prendre en compte via Internet les mises à jour de sécurité et de compatibilité si on le souhaite, même si celles-ci ne sont arrivées sur le marché qu'après l'apparition du CD-ROM de Windows XP.

Windows Update (les mises à jour de Windows) maintiennent le système à la jour. Les packs service, la résolution de problèmes et les pilotes pour les nouveaux matériels peuvent être téléchargés, automatiquement si on le désire, par Microsoft depuis Internet.

Un grand nombre de programmes qui ne tournaient pas sous Windows 2000 fonctionnent sous Windows XP. Si un programme ne pouvait être exécuté que sous Windows 95 ou 98, il y a de grandes chances qu'il puisse tourner sous le nouveau système d'exploitation. Si malgré tout une application plus ancienne n'est pas supportée par Windows XP, il est possible de l'exécuter dans un **mode de compatibilité** spécial qui reprend les caractéristiques de versions Windows antérieures.

Windows XP accorde à la **qualité des pilotes de périphériques** la plus haute priorité car

ils concourent de manière importante à la stabilité du système. Dès l'installation d'un nouveau composant, il est affiché si le pilote a été testé et certifié par Microsoft. Si un pilote non certifié et ne fonctionnant pas correctement est installé, il est possible de revenir au pilote précédent qui fonctionnait en l'espace de quelques secondes. Avec le concept "Side-by-Side DLLs", plusieurs versions d'un driver peuvent être utilisées en parallèle de telle sorte que chaque application tourne avec la version qui lui est la plus appropriée. Si, en dépit du traitement sensiblement amélioré des pilotes, un problème devait tout de même survenir, la fonction de **restauration du système** permet de rappeler une configuration antérieure du système, et d'annuler ainsi les changements de configuration intermédiaires, même plusieurs semaines après.

La sécurité est un leitmotiv de Windows XP. Les fichiers stratégiques peuvent être enregistrés avec un codage et il est possible de protéger certaines zones contre un accès indésirable avec mot de passe et nom d'utilisateur. Le **système de codage (Encrypting File System) EFS** permet d'enregistrer les fichiers contenant des informations particulièrement confidentielles sur le disque dur ou sur les serveurs du réseau. Ainsi, les données, y compris les ordres en ligne, sont protégées de manière fiable contre les accès indésirables. Le nouveau support multi-utilisateur d'EFS permet à plusieurs utilisateurs légitimes de coder et de voir en commun des fichiers confidentiels.

Le **Firewall Internet (Internet Connection Firewall, ICF)** intégré à Microsoft XP protège automatiquement les données contre les accès non autorisés depuis Internet. La fonction doit simplement être activée pour la liaison connexion à distance ou LAN désirée. Pour toutes ses opérations de codage, Windows XP Professional fait appel à une clé 128 bits. Windows XP comporte de nombreuses autres caractéristiques de sécurité comme par exemple le protocole d'authentification Kerberos V5, Internet Protocol Security (IPSec), les directives de sécurité à définition centralisée et bien d'autres.

Un ensemble de caractéristiques de Windows XP facilite l'installation et l'administration du système d'exploitation, permettant ainsi de diminuer les coûts pour ces postes dans les entreprises. Nous présentons ici uniquement une sélection de ces caractéristiques :

Pour les sociétés qui souhaitent installer Windows XP Professional sur plusieurs PC, Microsoft a prévu des mécanismes éprouvés pour **l'installation automatique**. Cela permet de préconfigurer des installations sans surveillance de Windows XP de telle manière que le processus d'installation puisse avoir lieu de manière fiable sans interaction de la part de l'utilisateur. Les images de systèmes d'exploitation, y compris pour les PC ayant un équipement matériel disparate, peuvent être créées facilement et installées automatiquement via le réseau avec les services d'installation à distance (RIS) compatibles avec Windows 2000.

Intéressant pour les multinationales et les institutions pédagogiques : Windows XP Professional supporte l'**"Interface Utilisateurs Plurilingues" (MUI)** : Cet outil permet d'équiper un PC avec plusieurs interfaces utilisateurs en même temps (anglais, allemand, espagnol etc.). Ainsi, chaque utilisateur obtient le bureau Windows dans la langue qu'il préfère.

Afin d'éviter l'exécution d'applications indésirables sur Windows XP Professional, les administrateurs peuvent faire appel aux **directives de limitations logicielles**. Cela permet de limiter les postes de

travail aux programmes importants pour l'entreprise.

Windows XP dispose de nombreuses nouvelles directives en complément à celles de groupe déjà présentes sous Windows 2000 afin d'obtenir une administration encore plus complète basée sur les directives via le répertoire actif. Avec le nouveau **"Resultant Set of Policy" (RSOP)** de Windows XP Professional, les administrateurs disposent d'un outil performant pour planifier et contrôler l'effet des diverses directives de groupe utilisées sur des utilisateurs et ordinateurs précis. Pour les utilisateurs souvent en route avec leur ordinateur portable, les directives de groupe, sur base du lieu, s'avèrent extrêmement utiles. Si l'utilisateur est au bureau, les directives de groupe de l'entreprise prévalent. En déplacement ou à la maison, l'utilisateur peut exploiter les fonctionnalités de Windows XP Professional pour PC indépendants ou petits LAN sans avoir pour cela à effectuer une nouvelle configuration.

L'outil **USMT (User State Migration Tool)** permet une reprise facile de toutes les données et réglages personnels d'un utilisateur depuis le système original dans Windows XP. Les réglages préférés de bureau, les options de répertoire de Windows Explorer, la configuration Internet et les favoris, l'accès e-mail, les messages et le répertoire d'adresses, lecteurs et imprimantes réseau, répertoires précis etc. peuvent être transmis sans difficulté.

Windows XP offre un **support** complet et intégration End-to-End **pour tous les supports numériques**. Impression et enregistrement, affichage et lecture, archivage et envoi... Windows XP vous accompagne pas à pas en prenant le contexte en compte et propose automatiquement toutes les tâches exécutables. Windows XP met en valeur audio, photo et vidéo comme jamais auparavant. Le lecteur Media Player peut créer des fichiers MP3 et lire des DVD vidéo sur le PC à l'aide d'éléments enfichables séparés. Si une caméra numérique ou un scanner sont connectés au PC, Windows XP les reconnaît automatiquement.

Windows XP reconnaît les fichiers se trouvant dans tel ou tel répertoire et n'affiche pas seulement une vue miniature mais propose les actions les plus probables pour chaque type de support dans la nouvelle barre des tâches : les données audio, dans le répertoire "ma musique", sont immédiatement jouées par simple clic de la souris.

Avec le centre d'aide et de support **Assistance à Distance** intégré à Windows XP, on peut à tout moment appeler à l'aide des collègues ou un centre de support interne à la société. Au lieu d'avoir à décrire le problème à un spécialiste par téléphone, l'expert peut afficher la solution à distance clairement directement sur son propre écran. Si l'expert appelé est invité par les contacts en ligne de Windows Messenger ou par e-mail, il obtient l'autorisation d'afficher sur son propre écran le contenu de l'écran du PC faisant problème, pour fournir une aide lors de la résolution ou pour résoudre lui-même le problème. L'utilisateur peut suivre pas à pas et conserve dans tous les cas le contrôle. A la fin de la session de support à distance, l'autorisation de l'expert d'accéder au PC de l'utilisateur est supprimée automatiquement. En entreprise, cet outil centralisé et complet de Windows XP permet de réduire le nombre de demandes d'aide au centre de support interne, réduisant du même coup les dépenses liées aux problèmes de matériel et de logiciel.

2.1.3 Windows Server 2003

Le nouveau Microsoft Windows Server 2003 sera disponible à compter d'avril 2003. De nombreuses fonctions ou caractéristiques ont été étendues ou ajoutées par rapport à Windows 2000 Server. Windows Server 2003 sera disponible dans les versions suivantes :

Windows Server 2003, Standard Edition

Traitement multiprocesseur symétrique double (Symmetric Multiprocessing, SMP)
2 Go de mémoire vive

Windows Server 2003, Enterprise Edition

Traitement multiprocesseur symétrique octuple (Symmetric Multiprocessing, SMP)
Cluster comprenant jusqu'à huit noeuds
RAM 32 Go en version 32 bits et RAM 64 Go en version 64 bits
Hot Add Memory
Accès mémoire non uniforme (NUMA)

Windows Server 2003, Datacenter Edition

Traitement multiprocesseur symétrique 32 fois (Symmetric Multiprocessing, SMP)
64 Go de mémoire vive en version 32 bits et 128 Go en version 64 bits
Windows Sockets : Accès direct pour SAN
Cette version sera uniquement disponible via le Windows Datacenter-Programm offrant un pack composé de matériel, logiciel et services.

Windows Server 2003, Web Edition

Traitement multiprocesseur symétrique (Symmetric Multiprocessing, SMP)
Deux Go de mémoire vive
Windows Server 2003, Web Edition est dédié à l'utilisation en tant que serveur Web. Les serveurs équipés de ce système d'exploitation peuvent être membres d'un domaine de répertoire actif mais ne peuvent offrir eux-mêmes ce type de service. Cette version ne sera disponible que chez certains partenaires.

Vue d'ensemble des caractéristiques principales de Windows Server 2003 :

Services Web XML : Les services Web XML contiennent des composants, réutilisables et fondés sur les standards industriels, qui font appel à des fonctions d'autres applications indépendamment du processus selon lequel les applications ont été conçues, ainsi que du système d'exploitation, de la plate-forme ou des appareils avec lesquels il y est accédé. Les réglages de sécurité IIS 6.0 sont bloqués lors de l'installation afin de pouvoir n'exécuter que les services nécessaires. L'administrateur peut, comme il l'entend, activer ou désactiver la fonctionnalité de serveur, à l'aide de l'assistant Lockdown pour la sécurité IIS.

Service de répertoire : Les réglages de sécurité du répertoire actif pour les ressources réseau et utilisateurs concernent le réseau complet et contribuent à un réseau sûr "End-to-End". Grâce à une synchronisation, à une réplication efficace ainsi qu'à la sauvegarde d'informations de login

dans des contrôleurs de domaines annexes, le répertoire actif reste rapide et stable y compris avec des liaisons WAN peu fiables.

Administration des mises à jour : L'actualisation automatique permet de télécharger systématiquement les mises à jour importantes du système d'exploitation, comme par exemple les mises à jour de sécurité et les patches. Les administrateurs peuvent décider quand doivent être exécutées ces importantes mises à jours du système d'exploitation.

Firewall Internet : Le Firewall Internet du serveur rend la liaison vers Internet plus sûre.

Support de matériel serveur : Des outils spéciaux testent les nouveaux pilotes afin d'assurer un fonctionnement correct du serveur.

Contrôle des applications : Les applications exécutées sous Windows Server 2003 peuvent d'abord être testées, par exemple pour contrôler un éventuel endommagement de la mémoire de l'application (Heap) ou au niveau de la compatibilité.

Suivi d'événement serveur : Le nouveau protocole permet aux administrateurs de consigner la durée de fonctionnement précise. Il note les événements Windows dans un fichier de protocole lors de l'arrêt du serveur.

Assistant de configuration de serveur : L'assistant de configuration de serveur guide les administrateurs pas à pas à travers l'installation de divers types de serveurs comme par exemple les serveurs de fichiers, les serveurs d'impression ou les serveurs d'accès à distance. Les composants respectifs sont donc installés et configurés correctement dès le début.

Assistant d'administration de serveur : L'assistant d'administration de serveur constitue une interface pour l'administration en continu du serveur et facilite les tâches générales comme l'ajout de participants au réseau et de nouvelles autorisations.

Administration de serveur à distance : Avec "le Desktop à distance pour l'administration" (auparavant connu comme service de terminal en mode d'administration à distance), les administrateurs peuvent administrer un ordinateur depuis pratiquement n'importe quel autre ordinateur dans le réseau.

Copie de sécurité : Cette fonction permet une autorisation au réseau en fonction des horaires. Les administrateurs peuvent alors sauvegarder le contenu de répertoires du réseau et s'informer plus tard de leur état à ce moment précis. Les utilisateurs de Desktop peuvent restaurer des fichiers ou des répertoires supprimés avec les autorisations du réseau sans que l'administrateur n'ait à intervenir.

Serveur de terminaux : Avec le serveur de terminaux, un utilisateur peut accéder à des programmes exécutés sur le serveur. L'utilisateur peut par exemple accéder à un Desktop Windows XP Professionnel virtuel et à des applications Windows sur base x86 même si son matériel ne lui permet pas d'exécuter ces programmes en local. Le serveur de terminaux offre cette possibilité pour tous les appareils Client, sur base Windows ou non.

Les fonctions supplémentaires de l'Enterprise Edition comprennent :

Service Cluster : Le service Cluster de Windows Server 2003, Enterprise Edition et Datacenter Edition supporte le Clustering comprenant au maximum huit nœuds. Cela augmente la flexibilité pour l'ajout ou la suppression de matériel dans un environnement Cluster réparti dans des locaux séparés. L'administration de Cluster est complétée par des options de modularité améliorées.

Diverses configurations de Cluster sont possibles :

- Configuration d'un Cluster avec mémoire attribuée
- Configurations à plusieurs Clusters dans un réseau d'archivage (Storage Area Network, SAN)
- Clusters répartis sur plusieurs sites.

Services métarépertoires : Les entreprises peuvent intégrer avec l'aide de Microsoft Metadirectory Services (MMS) des données personnelles de plusieurs répertoires, banques de données et fichiers.

MMS permet d'afficher les données personnelles dans un masque unique, d'intégrer les processus de travail et de synchroniser les données personnelles à niveau supérieur à l'organisation.

Hot Add Memory : Cette caractéristique permet d'étendre la mémoire vive de l'ordinateur pour les applications et le système d'exploitation en cours de fonctionnement. Il n'est pas nécessaire de rebouter le serveur, ce qui évite tout arrêt. Hot Add Memory n'est actuellement possible que sur les serveurs car ceux-ci disposent du support matériel indispensable.

Accès mémoire non uniformisé (NUMA) : Le progiciel du système peut créer un tableau dénommé "Static Resource Affinity Table" qui décrit la topologie NUMA du système. A l'aide de ce tableau, Windows Server 2003, Enterprise Edition peut utiliser NUMA sur des processus d'application ainsi que sur des réglages d'affinité standard, la planification Thread et les fonctions de gestion de la mémoire. De plus, les applications d'informations de topologie utilisant les API NUMA deviennent disponibles.

Répertoire de session pour les services de terminal : Cette fonction de compensation de la charge permet aux utilisateurs de reprendre la session après une interruption de la liaison du terminal. Cette caractéristique est compatible avec la compensation de charges de Windows Server 2003 et est supportée par les produits tiers correspondants.

Les fonctions supplémentaires de la version Datacenter comprennent :

Mémoire physique étendue : Elle augmente la capacité de la mémoire vive à 64 Go. Sur les

plate-formes Intel dotées d'une architecture 64 bits, le support maximum atteint 16 To.

Windows Sockets : Accès direct pour les SAN : Ces performances octroient aux applications Windows Sockets sur base des protocoles TCP/IP les avantages de réseaux d'archivage (Système Area Network, SAN) sans modification particulière. La partie importante de cette technologie est un service Windows Socket à plusieurs couches qui émule le TCP/IP par des services SAN internes au système.

2.2 Systèmes d'exploitation Unix

Les systèmes d'exploitation Unix sont encore largement majoritaires dans le monde des postes de travail. Pour être exact, il convient ici de parler d'une véritable famille de systèmes d'exploitation car chacun des constructeurs fournit ses produits avec sa propre version Unix, qui diffère des autres au moins sur le plan de l'interface utilisateur. Cependant, cette diversification semble se ralentir depuis que certains constructeurs s'efforcent de porter leurs systèmes respectifs vers d'autres architectures.

Les implémentations Unix peuvent être regroupées en deux standards distincts : celui de Berkeley Unix (BSD) et celui de AT&T's System V Release 4 (SVR4). Ce dernier est en passe de prendre le dessus (les nouvelles versions Unix suivent ses spécifications). En règle générale, on peut affirmer que lorsqu'un programme a été écrit pour l'un de ces deux standards, il peut être porté sans trop de difficulté vers un autre système de ce même standard.

Il existe également différents standards en matière d'interface utilisateur (GUI - Graphical User Interface). Mais les dernières en date suivent toutes la norme X11. Depuis quelques années vient largement en avant le standard MOTIF, qui repose également sur les définitions X11. De plus en plus d'implémentations Unix utilisent cette interface utilisateur tandis que la concurrence (OPENLOOK, par exemple) perd du terrain.

2.2.1 Linux

Linux est un système d'exploitation multi-tâches et multi-utilisateurs librement accessible. Linux est un développement initial de Linus Torvalds. Le reste du développement a ensuite été pris en charge par une multitude de concepteurs informatiques de par le monde. Dès ses débuts, Linux a été proposé en GPL (General Public Licence). Cela signifie que ce système d'exploitation peut être distribué, exploité et complété librement et sans frais. Les développeurs informatiques ont accès à l'ensemble du code. Ils peuvent très facilement ajouter des nouvelles fonctions, trouver et, le cas échéant, éliminer des erreurs de programmation. Avec ce système, les pilotes de nouveaux adaptateurs (contrôleurs SCSI, cartes graphiques, etc.) peuvent ainsi être intégrés en un temps record.

Linux est aujourd'hui utilisé avec succès par des millions d'utilisateurs à travers le monde. Les groupes d'utilisateurs sont très variés : des utilisateurs individuels aux instituts de formation, des universités aux centres de recherches, des utilisateurs commerciaux aux entreprises. Chacun a estimé que Linux était une alternative intéressante par rapport aux autres systèmes d'exploitation.

Le vaste support réseau de Linux, comportant différents serveurs comme Appletalk, Netware ou Lan Manager ainsi qu'une multitude de protocoles réseau, font de Linux un système serveur réseau fiable et stable.

Une des solutions de se prouver Linux est de le télécharger gratuitement, à partir d'un site Internet. En agissant ainsi, on obtient un système d'exploitation personnel pour le prix de la communication téléphonique, c'est-à-dire pour quasiment rien. Il est en fait plus simple de faire appel à ce que l'on appelle une distribution, offerte par différentes sociétés et qui comprend outre, un grand nombre d'applications, un programme qui simplifie grandement l'installation de Linux.

Les distributions se différencient essentiellement dans les composants, comme les environnements de programmation, les logiciels réseau et les interfaces graphiques. Nous recommandons les distributions de SuSE ou de Red Hat. En effet, celles-ci ont fait leurs preuves et contiennent une large documentation ainsi qu'une installation guidée. Les systèmes Linux de transtec sont en principe certifiés et proposés avec les nouvelles versions de SuSE et Red Hat.

Outre leurs distributions pour PC et stations de travail, aussi bien SuSE que Red Hat proposent des packs spéciaux pour les serveurs. Chez SuSE il s'agit de SuSE Linux Enterprise Server. Ce pack, outre sa composition spéciale pour l'exploitation des serveurs, se distingue aussi par les points suivants : tout d'abord SuSE réalise des tests complets pour garantir la compatibilité des packs les uns avec les autres ainsi qu'avec les applications business importantes. SuSE garantit aussi le support pour le pack y compris après la disparition de la version concernée et ce pendant deux ans. Autre point important dans le domaine Business : la disponibilité de patches et de mises à niveau. SuSE propose en outre des packs spéciaux pour des utilisations particulières comme par ex. serveur Email ou Firewall.

Le développement de ces packs reflète la tendance générale : Linux est de plus en plus mis en oeuvre dans des systèmes commerciaux et offre pour de nombreuses utilisations une base fiable et économique.

2.2.2 SunOS/Solaris

Solaris 8

La version Solaris 8 constitue la deuxième génération en technologie 64 bits. Grâce au support de la version 6 de IP, Solaris 8 met fin aux limitations de Windows et des autres environnements.

De nombreuses adresses Internet (plus qu'un 1 suivi de 38 zéros), une mémoire principale de 18 exa-octets et jusqu'à un million de traitements simultanés sont supportés. Le système d'exploitation

Solaris 8 supporte également les technologies les plus récentes allant du Desktop (bureau) à Internet. Sont compris également Java 2SE, très important dans les entreprises pour le développement d'applications centrées sur le Web, le Java Media Framework pour le Media-Streaming, les extensions vidéo de serveur X, la synchronisation de PDA (par ex. Palm Pilot) et le traitement sur réseau en temps réel. Solaris 8 offre des capacités supplémentaires typiques du Mainframe : jobs, projets et aptitude de comptabilité pour le calcul de l'utilisation de l'ordinateur (idéal pour un Service-Provider), reconfiguration dynamique automatique pour l'amélioration du temps de fonctionnement, et enfin le hot patching pour modifier de manière dynamique le système d'exploitation, sans devoir éteindre l'ordinateur. Un outil d'installation Web rend l'installation du logiciel très simple. Les applications Solaris déjà existantes sont compatibles avec Solaris 8. Solaris 8 est incontournable pour tous les systèmes dotés d'un processeur Ultra III ou Ultra IIe.

Solaris 9

Grâce à un grand nombre de composants logiciels intégrés, l'environnement du système d'exploitation Solaris 9 se transforme en plate-forme de services étendue. Un serveur d'applications sur base J2EE (plate-forme Java2, Enterprise Edition) et un serveur de répertoires LDAP (Lightweight Directory Access Protocol) comme base de l'administration des identités font tout autant partie de la fourniture que Solaris Volume Manager, Solaris 9 Resource Manager et un grand nombre d'autres produits.

Par un investissement fortement réduit pour les applications clés de l'infrastructure, l'environnement du système d'exploitation Solaris 9 contribue à une diminution des coûts d'exploitation totaux. L'intégration avec l'**environnement Sun Open Net (Sun ONE)** ouvre de nouvelles perspectives pour l'augmentation de l'efficacité ainsi que de nouveaux terrains d'application pour les systèmes d'ordinateurs. Comme les services sont mis à disposition par la plate-forme Sun ONE, les serveurs Web, les serveurs d'application et les serveurs de répertoires se laissent tout aussi bien intégrer que les systèmes de données, la gestion des volumes et la planification de capacité et de sécurité.

Avec le **serveur de répertoires Sun ONE Directory Server** totalement intégré et le **serveur d'applications Sun ONE Application Server** inclus dans la fourniture, Solaris 9 simplifie la mise à disposition sur demande de services fiables et modulaires sans coûts supplémentaires. Dans les mises à jours à venir, le serveur d'applications Sun ONE Application Server sera totalement intégré. Il en résultera que Solaris 9 sera le seul système d'exploitation à disposer d'un serveur d'application J2EE et d'un serveur de répertoires LDAP complètement intégrés dans le système d'exploitation de base.

L'environnement de système d'exploitation Solaris 9 contribue aussi à la diminution des coûts grâce à de nouvelles caractéristiques comme **la planification de la capacité** et la gestion des modifications. Les extensions de systèmes sont installées rapidement et sans problème et des processus pour lesquels il fallait jusqu'à présent sacrifier quatre heures et plus ne durent plus que vingt minutes grâce aux caractéristiques comme **Solaris Flash Software**. Une commande de configuration précise et complète permet aux administrations d'économiser un temps précieux lors de travaux de routine et la gestion du système est dans l'ensemble plus efficace. **Solaris 9**

Resource Manager crée au moyen d'une administration intégrée des ressources, les conditions préalables à une consolidation du serveur avec les outils du système d'exploitation, si bien qu'il n'est plus nécessaire d'acquérir des produits supplémentaires. **Solaris Volume Manager** assure une haute disponibilité des données et une fiabilité maximale lors du travail avec l'environnement de système d'exploitation Solaris 9.

Avec des solutions de sécurité livrées en standard et des **services de sécurité totalement intégrés**, l'environnement du système d'exploitation Solaris 9 garantit le haut niveau de sécurité indispensable pour la mise au point de services en réseau. Le système d'exploitation Solaris dans sa nouvelle version fournit un plus décisif de sécurité grâce à toute une série de caractéristiques-clés.

SunScreen 3.2 constitue un Firewall qui supporte sans complexe la comparaison avec des produits disponibles séparément. **Solaris Secure Shell** offre des fonctions intégrées pour l'accès à distance codé et sécurisé. Solaris 9 comporte encore Secure LDAP, la version 5 de Kerberos Server ainsi que l'accès sécurisé via Sun ONE Portal Server. Toutes ces fonctionnalités de sécurité font partie intégrante du système d'exploitation de base, si bien qu'une sécurité étendue de toutes les applications est incluse sans coûts additionnels.

Les exigences dans le domaine des entreprises et du High Performance Computing (HPC) rendent incontournables les environnements 64 bits modulaires à haut degré de fiabilité. Avec Solaris 9 et les processeurs UltraSPARC III à technologie cuivre, les applications tournent plus rapidement sans nouvelle compilation, sans avoir à intervenir dans le code source et sans modification de l'architecture.

La **commande de mémoire intégrée au processeur** UltraSPARC III permet une localisation des codes et des données de telle sorte que les performances du système avec une optimisation correspondante des serveurs peuvent augmenter de 5 à 40 %.

Le processeur UltraSPARC III dispose d'un **Dual Translation Lookaside Buffer (DTLB)** supportant les grandes pages de mémoire, ce qui triple presque la puissance HPC (mesures effectuées selon le Benchmark SWIM).

Un algorithme d'un nouveau genre pour le Page Coloring augmente les performances du système pour les charges typiques de serveur jusqu'à 10 %.

Le nouveau Solaris se distingue par de nombreuses caractéristiques contribuant à accroître la disponibilité et à réduire les coûts d'exploitation. Cela comprend entre autres l'intégration du logiciel **Sun Cluster 3.0** et des fonctions pour l'administration de la configuration. Les profils Sun RAS de par leur technologie, constituent une solution idéale pour l'optimisation des plate-formes de clients. Une fréquence réduite de défauts, une élimination facilitée des défauts, des périodes d'arrêt non prévues plus rares et une productivité plus élevée engendrent au total une réduction des coûts et une efficacité améliorée.

2.3 Virus informatiques

Les nombreux virus informatiques qui circulent désormais sur presque toutes les plates-formes et les systèmes d'exploitation constituent un sujet préoccupant. Actuellement, ils se propagent très souvent par le courrier électronique ou via Internet.

Les différents types de virus

Un virus informatique est constitué d'une séquence d'instructions dont l'exécution modifie une zone mémoire en y enregistrant une copie de son propre code. La zone mémoire considérée peut être indifféremment un fichier exécutable, un programme sur disquette, un disque dur, ou une zone de la RAM.

Les virus fichiers

Les virus fichiers se greffent dans certains programmes spécifiques et adoptent ensuite plusieurs stratégies. La propagation du virus a lieu à chaque fois que le programme déjà contaminé est appelé. **Les virus résidants** sont encore plus sophistiqués. Leur propagation a ainsi lieu à chaque fois que le programme est exécuté. Ce type de virus est plus difficile à éliminer et résiste parfois même à un redémarrage à chaud de l'ordinateur. Aujourd'hui, la majorité des virus peut être rangée dans cette catégorie. Les **virus de type surnois (stealth)** sont conçus pour échapper à la vigilance des programmes antivirus, des programmes de contrôle de parité et, en principe, de tous les programmes de surveillance disponibles. Ils disposent d'un mécanisme de camouflage, qui leur permet de dissimuler leur existence aux systèmes sur lesquels ils s'implantent. **Les virus polymorphes** constituent aujourd'hui la famille de virus la plus moderne et la plus dangereuse. On range dans cette catégorie les virus qui changent de forme à chaque nouvelle infection. Habituellement, ils adoptent un nouveau code informatique utilisant une clé différente à chaque contamination.

Les virus système, pour se propager, s'attaquent pour leur part à certains éléments spécifiques d'un système d'exploitation (masterbootrecord, partitionbootrecord, diskbootsector, FAT, root, etc.). Ces zones système sont associées au support informatique concerné. Une propagation ne peut donc avoir lieu que si le support informatique contaminé est utilisé.

Les virus du type Bootsector ils ne s'attaquent qu'aux secteurs de démarrage d'une disquette ou d'un disque dur. La propagation de ce type de virus est assez lente puisque l'infection n'a lieu qu'à chaque redémarrage à partir du support.

transtec recommande de contrôler les systèmes en permanence avec des logiciels anti-virus adaptés. Cela permet d'anticiper des problèmes massifs.

3. Cluster

Cluster Haute Disponibilité

Un cluster **Haute Disponibilité** est la réunion de plusieurs systèmes en un groupe géré et dirigé via un logiciel cluster. Sur le plan matériel, un cluster est un groupe de minimum deux serveurs indépendants pouvant accéder aux mêmes données, et qui servent le même groupe de clients. Dans le contexte technique actuel, cela signifie le plus souvent que ces serveurs sont reliés par des bus E/S courants et à un réseau normal pour l'accès client. Sur le plan logique, un cluster représente une unité de gestion au sein de laquelle n'importe quel serveur peut proposer un service disponible à tout client autorisé. Les serveurs doivent avoir accès aux mêmes données et posséder un système de sécurité commun. Au stade actuel de la technique cela sous-entend aussi que les serveurs dans un cluster ont en général la même architecture et qu'ils tournent sous la même version de système d'exploitation.

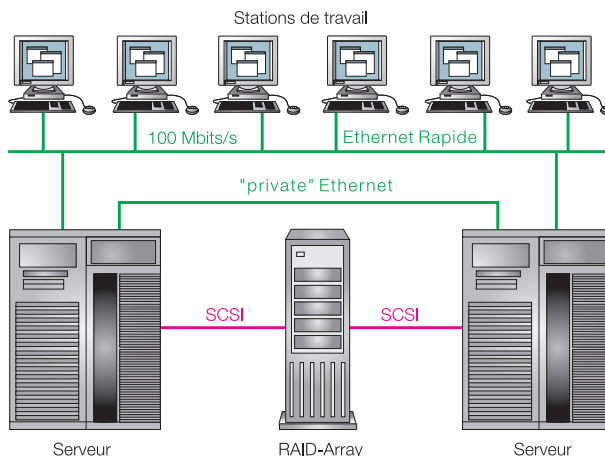
Bien qu'il existe diverses possibilités concernant la manière dont les clusters peuvent être composés, tous offrent les trois avantages suivants :

- Haute disponibilité avec tolérance des erreurs au niveau des données et des applications
- Modularité des ressources matérielles
- Gestion simple des systèmes étendus ou à forte croissance.

Plus grande disponibilité

Dans les départements stratégiques d'une entreprise, la disponibilité sans faille de certains services (par ex. serveur Web, banque de données ou système de fichiers réseau) est une condition sine qua non du succès de l'entreprise. Les causes les plus courantes des problèmes de disponibilité de ces services sont différentes formes de pannes de système. La panne peut être causée par le matériel, le logiciel, l'application ou le fonctionnement. Il est possible de se prémunir contre de telles pannes si l'on emploie un cluster comme serveur d'applications ou serveur de données. Les clusters offrent également, outre leur capacité de calcul redondante et leurs composants I/O et de mémoire, la possibilité de passer d'un serveur défaillant à un autre serveur pouvant le remplacer sans causer d'interruption. C'est ainsi que les clusters assurent une grande disponibilité des services serveurs, même en cas de panne.

Le croquis montre un cluster simple, composé de deux serveurs connectés et d'un système RAID servant à l'enregistrement des données.



- En cas de panne de logiciel ou de matériel dans un serveur, ou si le serveur lui-même tombe en panne, l'autre serveur reprend la relève
- Si une interface de réseau d'un serveur est défaillante, entraînant une rupture de liaison avec les clients, ceux-ci peuvent toujours recourir au deuxième serveur
- Si un bus E/S ou un adaptateur E/S tombe en panne, il est toujours possible de retourner les données du système RAID via un autre chemin
- Si un disque tombe en panne, les données restent disponibles grâce au système RAID.

Dans tous les cas, les serveurs et les clients doivent reconnaître la panne et l'éliminer. Il y a certes arrêt des applications serveurs, mais seulement pendant quelques secondes grâce à l'usage d'un cluster, au lieu de plusieurs minutes voir de plusieurs heures avec les méthodes de restauration habituelles.

Extensibilité

L'extensibilité est un avantage supplémentaire de l'architecture en cluster qui permet un élargissement des applications au-delà de la capacité d'un serveur. Beaucoup d'applications comportent des threads (tâches) pour des activités relativement différenciées qui n'interagissent qu'occasionnellement. Des applications à plusieurs threads peuvent tourner en tant que processus pseudo-parallèles sur un serveur avec un processeur ou en tant que processus réellement parallèles dans des systèmes multiprocesseurs symétriques (SMP).

Dans un cluster des groupes de threads d'applications peuvent tourner sur différents serveurs puisque les serveurs ont accès aux mêmes données. Quand une application devient trop grande pour un serveur, un deuxième serveur peut être installé afin d'obtenir un cluster et d'augmenter ainsi la capacité d'utilisation.

Pour que les serveurs puissent avoir accès aux mêmes données, il faut qu'il y ait coordination. Elle peut se faire au moyen d'une application, d'un gestionnaire de données ou d'un système de fichiers répartis. Quand cette coordination manque dans un cluster, plusieurs serveurs ne peuvent avoir en même temps directement accès à n'importe quel fichier. Il est cependant possible, même avec cet accès restreint, d'implémenter quelques applications. Les applications peuvent être réparties de telle façon que les divers programmes utilisent des données différentes.

Gestion plus simple

Le troisième avantage des clusters est une gestion plus simple. Les cluster simplifient la gestion de système en augmentant l'étendue des applications, des données et des domaines d'utilisateurs, gérés par un seul système. La gestion de système englobe entre autres les domaines suivants :

- Le système d'exploitation
- Le middleware
- La mise à jour des applications
- La gestion des comptes utilisateur
- La gestion de configuration
- La sauvegarde des données.

La complexité et les coûts de cette gestion dépendent de la taille et, en particulier, du nombre des systèmes à gérer. Par exemple, la sauvegarde quotidienne est nécessaire pour tous les serveurs qui enregistrent des données importantes, indépendamment de la quantité des données à sauvegarder. Les changements de comptes utilisateur doivent être aussi actualisés sur tous les serveurs auxquels l'utilisateur a accès.

Les clusters permettent de diminuer le nombre de systèmes individuels, et par conséquent, les coûts pour la gestion en rassemblant un grand nombre d'applications, de données et d'utilisateurs sur un seul système informatique. L'avantage est qu'un système cluster ne comporte à la fois qu'un seul principe de comptes utilisateur, d'autorisation d'accès aux données, de règles de sauvegarde des données, de gestion de banques de données etc. Bien que chacun des systèmes résultant de différentes architectures cluster puisse varier, il est normalement plus économique de gérer un seul cluster au lieu d'un nombre correspondant de systèmes serveurs non connectés.

La répartition de la charge entre chacun des serveurs cluster se produit automatiquement. Les clusters Unix comme les clusters open VMS offrent la répartition de la charge automatique et la possibilité d'extension. Actuellement, Windows 2000 Cluster offre simplement une meilleure disponibilité. Avec le serveur cluster de Windows 2000 Advanced Servers, deux serveurs peuvent être reliés à un cluster. Windows 2000 Data Center Server offre quant à lui la possibilité de relier

quatre serveurs. La fonction de répartition de charge IP automatique, indépendante du serveur cluster permet la répartition d'applications Web sur maximum 32 systèmes.

High Performance Computing (HPCC) / Beowulf Cluster

L'architecture cluster Beowulf se compose en principe d'un certain nombre de nœuds et d'un ou plusieurs ordinateurs d'accès. Les ordinateurs d'accès sont désignés comme Front End ou comme Server Node. Un utilisateur se connecte, le plus souvent à distance, uniquement sur ce Server Node. De là, il peut réserver et utiliser un nombre indéfini de nœuds de calcul pour son travail (sa tâche de calcul). Conformément à cela, les périphériques d'entrée ou de sortie, tels que clavier, souris ou écran sont dès lors inutiles pour les nœuds de calcul. Tout comme les ordinateurs d'accès, ils ne requièrent aucun matériel spécifique, mais utilisent en règle générale les systèmes processeurs standard x86 ou Alpha. La connexion des systèmes s'effectue via n'importe quelle infrastructure réseau. Le système d'exploitation utilisé est toujours libre (Linux, FreeBSD, etc.)

Un cluster Beowulf représente une solution économique pour les tâches requérant une performance de calcul importante. L'installation d'un tel cluster n'est cependant pas simple, car il n'existe aucun progiciel prêt à l'emploi. Le cluster doit, pour respecter les exigences, se composer de plusieurs éléments logiciels et l'application doit ensuite être programmée en parallèle. Il est toutefois aussi possible d'utiliser un ordinateur avec des tâches non parallèles comme ferme de calcul.

Cluster haute disponibilité avec le logiciel Linux Failsafe

Le logiciel cluster Linux Failsafe est un système haute disponibilité universel, librement configurable et tolérant aux erreurs, permettant d'installer certains services en redondance. En cas de panne, un service peut être transféré par le logiciel automatiquement ou manuellement sur un autre nœud. Une panne ne trouve pas toujours son origine dans le matériel : elle peut également provenir d'une erreur d'application, de procédures inefficaces ou d'un état critique du système. Il faut donc l'identifier et la traiter en conséquence. Les différents nœuds du cluster doivent dans la majorité des cas pouvoir accéder à des zones communes de données, pour reprendre l'état des données en cas de panne. Dans ce cas, il peut être fait appel à une architecture RAID SCSI ou SAN, qui permet aux serveurs de reprendre les zones de données en cas de panne. Si cette opération est menée à bien, le serveur cluster actif redémarre les services et les met à disposition sous la même adresse IP. Le temps mort d'un service est ainsi calculable et contrôlable dans une certaine mesure, puisque vous pouvez configurer différents critères pour régler le transfert du service. Des systèmes serveurs redondants adéquats atteignent un pourcentage de disponibilité de 99,99 %.

4. Bus de mémoire

4.1 Guide

Les bus périphériques permettant l'intégration de disques durs, de lecteurs de bandes et de sauvegardes optiques au système de bus (PCI, SBus et équivalents) sont sous entendus par le terme "bus de mémoire". Alors qu'il y avait initialement un grand nombre de bus propriétaires, qui ne jouent de nos jours qu'un rôle secondaire ou inexistant, (par ex. : IPI, DSSI en environnement numérique, SSA principalement d'IBM), trois standards se sont imposés : ATA (IDE) comme solution économique pour les systèmes de mémoire internes, le bus SCSI en particulier dans le domaine des stations de travail et la Fibre Channel, qui utilise aussi le protocole SCSI, pour les hautes performances. Les stations de travail et les ordinateurs portables font aussi appel aux bus périphériques généraux FireWire et USB (Universal Serial Bus) pour l'intégration de produits de stockage avec l'aide d'adaptateurs ATA.

4.1.1 Bus parallèles par rapport aux bus série

Les bus parallèles semblaient à l'origine pouvoir fournir un fort potentiel en largeur de bande supplémentaire : en comparaison aux liaisons série, le débit est multiplié par 8, 16 voire 32. Ainsi, le bus SCSI a été défini à l'origine avec 8 bits puis avec 16 bits. Il y avait aussi des projets de bus avec 32 bits mais ces derniers n'aboutirent pas. L'IDE a été exploité dès le début avec une largeur de bus de 8 bits.

De nouveaux standards avec des performances plus élevées ont été obtenus, grâce à des protocoles plus intelligents et à une sécurité de transmission accrue ; mais aussi grâce à une augmentation de la fréquence. Cette augmentation de la vitesse de transmission atteint maintenant ses limites : la synchronisation des signaux de données parallèles est de plus en plus difficile. On arrive ainsi dans une impasse au niveau du développement des bus parallèles avec pour conséquence que les bus série actuels sont parfois plus rapides que les bus parallèles. Les bus de stockage à venir seront de ce fait tous série : ATA et SCSI deviendront respectivement ATA série (S-ATA) et SCSI série. La Fibre Channel était conçue comme bus série dès l'origine.

4.2 Interface SCSI

La SCSI (Small Computer Systems Interface) est à l'origine un bus de disques durs, de sauvegarde de masse, parallèle à 8 bits, ultérieurement défini comme bus entrée/sortie série, qui s'est très largement répandu pour la connexion à différents systèmes d'ordinateurs et de disques durs de tout type mais également de scanners et d'autres périphériques.

Les avantages de SCSI résident au niveau de son taux de transfert de données maximal relativement élevé, de sa souplesse et de sa facilité de configuration.

Avec SCSI, une certaine intelligence est déjà présente dans le lecteur, car SCSI n'est pas une interface classique, mais un bus périphérique via lequel les lecteurs et l'adaptateur CPU peuvent communiquer. La première norme SCSI a été définie comme standard par ANSI en 1986. En fait, un système à trois niveaux se cache derrière ce concept : instruction, protocole et interface. Le noyau de SCSI est constitué par les instructions primaires SCSI (SPC - primary commands). Elles doivent pouvoir être adressées à tous les périphériques. Sur cette base, des instructions spécialisées sont définies pour des groupes de périphériques spécifiques, Controller Commands (SCC) pour adaptateurs, Block Commands (SBC) pour disques durs, Stream Commands (SSC) pour lecteurs de bandes, Multimedia Commands : sur ces commandes repose donc le niveau "instruction". Sous ce niveau, on trouve le niveau protocole, lequel concerne les protocoles des différents types d'interfaces. Ces protocoles logiques déterminent la façon suivant laquelle une instruction SCSI sera appliquée sur chaque interface. Ils règlent également l'intercommunication des périphériques. L'interface SCSI classique (8 bits et 16 bits SCSI) fait appel au protocole "interlocked" (IPC). Les interfaces récentes utilisent plutôt leurs propres protocoles : Serial Storage Protocol (SSP) pour SSA et le Generic Packetized Protocol (GPP), qui permettent aux fabricants de types d'interface différents d'accéder plus facilement à SCSI.

Le niveau le plus bas est finalement celui de l'interface, où les divers supports de transmission physiques sont définis.

L'avantage de ce modèle modulaire s'est avéré lors de l'introduction de nouvelles technologies série : Fibre Channel et SSA peuvent sans problème être intégrés dans ce standard répandu qu'est SCSI. Il en résulte des frais moindres et l'introduction de nouvelles interfaces sur le marché se fait plus rapidement.

L'expansion de l'interface SCSI, uniquement parallèle à l'origine (1 et 2), vers une interface série est dénommée SCSI-3. Cette dernière est compatible en aval aux versions parallèles. L'utilisation d'interfaces série (Fibre Channel, SSA) permet d'obtenir des taux de transfert de données bien plus élevés et de faire disparaître la répartition donnée par les SCSI parallèles dans une phase plus rapide de données (20 Mo/s pour une Ultra SCSI) et dans une phase plus lente de commande (5 Mo/s). Les divers protocoles et interfaces seront décrits plus précisément par la suite.

Interfaces parallèles SCSI

SCSI parallèle

- SCSI-1
- SCSI-2
- Ultra SCSI
- Ultra2 SCSI
- Ultra160 SCSI
- Ultra 320 SCSI

SCSI Série

- SSA
- Fibre Channel
- Fibre-Channel-Arbitrated-Loop (FC-AL)

Interface SCSI	Bits de données	Taux de transfert Mo/s	Nbr. de Lecteurs	Longeur maxi. Bus SCSI (m)
Single-Ended	8	5	7	6
Single-Ended-Fast	8	10	7	3
Single-Ended-Ultra	8	20	7	1.5*
Single-Ended-Wide	16	20	15	3
Single-Ended-Wide-Ultra	16	40	15	1.5*
Differential	8	5	7	25
Differential-Fast	8	10	7	25
Differential-Ultra	8	20	7	12.5
Differential-Wide	16	20	15	25
Differential-Wide-Ultra	16	40	15	12.5
Ultra2 LVD	16	80	15	12
Ultra160	16	160	15	6
Ultra320	16	320	15	6

* 3 m avec 4 lecteurs

Interfaces parallèles SCSI

4.2.1 SCSI parallèle

SCSI-1

La première norme SCSI fut la norme SCSI-1. Elle ne supportait au départ que les disques durs et les lecteurs de bande. Même quant à sa performance exceptionnelle, SCSI-1 n'est plus très concurrentielle. Le « overhead » lors du transfert de données (à savoir la proportion de données induites par l'opération de transmission elle-même par rapport aux données que l'on veut transmettre) atteint parfois les 90 %. Le taux de transfert en mode asynchrone atteignait maximum 1Mo/s et en mode synchrone 5 Mo/s. La SCSI-1 a été abandonnée depuis 1990.

SCSI-2

La norme SCSI-2 a été développée en 1986 et présente des améliorations fondamentales. Le jeu d'instructions de la norme SCSI-2 contient une série de commandes supplémentaires permettant un meilleur support des disques durs, des lecteurs de bandes et de disques magnéto-optique, des CD-ROM, des scanners ou encore des jukebox. Outre le nouveau jeu standardisé d'instructions (Common Command Set), la norme SCSI-2 intègre également un taux de transfert maximal plus élevé de 10 Mo/s (Fast-SCSI, avec la largeur de bus habituelle de 8 bits) et permet d'augmenter la largeur du chemin de données à 16 bits (Wide-SCSI). Une combinaison de Fast et Wide SCSI permet d'atteindre des taux de transfert de près de 20 Mo/s. L'indication de la compatibilité SCSI-2 d'un périphérique ne garantit pas nécessairement toutes les performances de SCSI-2 (Fast et Wide SCSI compris). En règle générale cependant, les lecteurs actuels sont dotés de Fast SCSI. De manière un

peu maladroite, les versions Wide SCSI (bus de données 16 bits) de SCSI-2 sont souvent désignées sous l'appellation norme SCSI-3, de même la version non-Fast-SCSI-2 est désignée comme étant la norme SCSI-1.

Ultra SCSI

La cadence de transfert a, une fois encore, été doublée avec Ultra SCSI, qui est une extension absolument compatible de SCSI-2 avec les versions antérieures. Un doublement de la cadence sur le bus permet de faire progresser le taux de transfert dans les mêmes proportions et d'atteindre 20 Mo/s (8 bits) et 40 Mo/s (16 bits). Cela ne concerne cependant que le taux de transfert de données. La transmission d'instructions s'effectue toujours à un taux de 5 Mo/s. Les câbles et les connexions ont également été conservés pour des raisons de compatibilité. L'augmentation de la performance a son prix : la longueur de câble autorisée passe à 1,5 m pour les périphériques Single Ended et à 12,5 m pour les périphériques différentiels. Une terminaison active est absolument requise afin de garantir une transmission parfaite.

Afin de faciliter la configuration des bus SCSI pour les utilisateurs, la spécification Ultra SCSI possède la caractéristique SCAM (SCSI Configuration Auto Matically) qui permet à un périphérique raccordé de se configurer lui-même. L'implémentation de SCAM sur les périphériques dépend cependant du "bon-vouloir" des fabricants.

Ultra2 SCSI (LVD - Low Voltage Differential)

Les produits faisant appel à Ultra2 SCSI sont présents sur le marché depuis 1998. Là aussi, le taux de transfert de données a été doublé et est passé à 80 Mo/s avec 16 bits. La version 8 bits disparaîtrait peu à peu. Comme la longueur du câble en "Single-Ended" encore une fois divisée par 2, rendrait le bus pratiquement inutilisable, ce standard n'a été défini que comme LVD (Low Voltage Differential), un câblage différentiel travaillant uniquement avec un tiers de la tension du signal. La longueur maximum du câble est de 12 m.

Pour garantir la compatibilité de ce standard, les lecteurs Ultra2 sont dotés d'une interface à auto-détection, permettant une utilisation sur les contrôleurs usuels Single-Ended (pas sur les différentiels) mais seulement à la vitesse Ultra SCSI. Il est nécessaire cependant d'utiliser un terminateur même à l'intérieur de l'ordinateur.

Ultra160 SCSI

Ultra160 nécessite le même câblage que pour Ultra2 LVD SCSI. Un taux de transfert deux fois plus important a été atteint grâce à la transmission de données sur les flancs ascendant et descendant du signal.

Ultra320 SCSI

Les premiers produits disposant de l'Ultra 320 sont disponibles depuis l'été 2002. Il n'est pas encore certain que la largeur de bande double une fois encore, car les standards série comme Fibre Channel et ATA série, plus tard aussi SCSI série vont remplacer petit à petit le SCSI parallèle.

L'Ultra 320 présente déjà de grosses difficultés techniques lors de la réalisation de solutions de stockage externes.

SCSI-3

SCSI-3 reprend aussi bien les normes de SCSI parallèle que celles de l'interface série, laquelle sera décrite plus loin.

Standards de transmission SCSI

Les interfaces SCSI parallèles existent en différentes versions qui se différencient selon le mode de transmission. Les signaux SCSI peuvent être transmis sur des bus SCSI 8 bits ("narrow") ou 16 bits ("wide SCSI"). Un bus 8 bits peut accueillir jusqu'à 7 lecteurs, tandis qu'un bus de 16 bits peut lui recevoir 15 lecteurs. Ces deux largeurs de bus disposent d'un câblage de type Single-ended (SE) ou différentiel (D) ou Low Voltage Differential (LVD). Avec le câblage SE-SCSI, chaque signal n'est transmis que sur une ligne, avec le D-SCSI par contre, sur deux lignes torsadées. Celles-ci sont protégées ainsi contre les influences électriques. Les avantages de D-SCSI sont : une meilleure résistance contre les perturbations et donc une longueur de câble plus importante. Le seul désavantage, comparé à SE-SCSI, est le coût élevé des lecteurs, de l'adaptateur et du terminateur.

Lors de l'acquisition d'un sous-système, il est important de vérifier que l'interface SCSI de l'adaptateur correspond à celle du lecteur. En règle générale, les périphériques 8 bits peuvent être connectés sur un bus 16 bits, mais il est important de respecter un certain nombre de règles de configuration.

Les versions SCSI Single-ended, différentielles ou LVD ne peuvent pas être branchées simultanément sur un même bus. Cela pourrait provoquer des dégradations au niveau du lecteur et sur le contrôleur. Seuls les lecteurs LVD sont autonomes sur Single-ended.

Transfert de données synchrone et asynchrone

Sur le SCSI parallèle, il existe les modes de transfert de données asynchrone et synchrone (plus rapide). En mode asynchrone, chaque octet est envoyé et confirmé séparément. En mode synchrone, plusieurs octets peuvent être envoyés en une fois. Grâce à la réduction significative de données, ce dernier procédé garantit un taux de transfert plus élevé. Tous les périphériques peuvent travailler en mode asynchrone. Les lecteurs ou contrôleurs synchrones vérifient lors de l'établissement de la liaison handshaking que l'interlocuteur à l'autre bout de la ligne supporte le mode synchrone. Le mode de transfert est alors choisi automatiquement. Les lecteurs SCSI et autres adaptateurs actuels supportent en général le mode synchrone.

Câbles pour SCSI parallèle

Afin de garantir un transfert de données sans perturbation ni erreur, il faudra vérifier si les câbles correspondent aux critères de sélection présentés ci-dessous :
un câble SCSI doit répondre aux normes UL (Underwriter Laboratories) et CSA (Canadian Standard

Association). Les fils doivent être en cuivre et torsadés (si possible cuivre étamé). Ils doivent être torsadés par deux. Le faisceau de câbles doit, en plus, être torsadé sur une longueur de 1 m. L'ensemble du câble nécessite de plus un double antiparasitage. Il peut être réalisé avec une feuille d'argent et une gaine de fils électriques tressés qui recouvrent l'âme du câble. Les câbles destinés à la connexion de plusieurs périphériques au bus doivent être courts et si possible avoir tous la même longueur. Cette précaution permet de réduire considérablement les perturbations sur le bus. En Wide-SCSI, comme la transmission de données SCSI s'effectue avec 16 bits au lieu de 8, les câbles SCSI 50 pôles ne suffisent pas. Wide-SCSI utilise dès lors des câbles 68 pôles. Comme il n'y a pas de différence entre les câbles SCSI Single-ended et différentiels, ils peuvent être utilisés pour les deux types d'interface.

Terminaison du système

L'augmentation du taux de transfert de données s'accompagne d'exigences plus élevées vis à vis des câbles de données et des terminaisons bus SCSI. SCSI différentiel et les terminaisons actives gagnent en importance.

Les bouchons actifs, contrairement aux bouchons passifs, travaillent avec un régulateur de tension intégré. L'alimentation de la terminaison est maintenue constamment à 2,85 V. Les terminaisons passives utilisent un pont diviseur de tension, qui maintient la tension autour de 3 V. La tension veut donc varier selon le type et la longueur de câble.

Le Forced Perfect Terminator (FPT) est une autre variante de terminaison de bus active surtout utilisée dans le monde IBM (RS/6000). Il adapte l'impédance du bus SCSI de façon dynamique. Lors de l'utilisation de terminaisons FPT, il faut veiller à en utiliser sur les deux côtés du bus, donc également sur le côté de l'adaptateur SCSI.

L'utilisation de terminaisons actives est vivement recommandée car, contrairement aux terminaisons passives, elles protègent beaucoup mieux le bus SCSI contre les perturbations électromagnétiques.

Connexion de sous-systèmes

Les possibilités suivantes s'offrent pour le raccordement de sous-systèmes SCSI externes :

1. Si aucun système externe n'est jusqu'ici connecté au port SCSI, un câble SCSI pour la plate-forme en question est requis. Par ailleurs une terminaison est nécessaire. La longueur maximale de câble doit toujours être prise en considération, y compris les câbles utilisés pour les boîtiers (ordinateur, disques, etc...)
2. Si des sous-systèmes externes munis de connecteurs HD68 existent, le câble inclus dans la livraison permet de connecter ou d'interposer le nouvel ensemble au sein des ensembles existants.
3. Si des sous-systèmes externes existants ne sont pas munis de connecteurs HD68, deux possibilités se présentent
 - Le nouveau sous-système est connecté au dernier boîtier. Il faut cependant veiller à échanger le câble standard contre un câble doté du connecteur correspondant. Un bouchon correspondant muni d'un connecteur HD68 est requis.

- Le nouveau sous-système est connecté en premier directement à l'ordinateur. Dans ce cas, il faut remplacer le câble standard contre un câble adapté à l'ordinateur. En outre, un câble supplémentaire est requis pour la connexion du nouvel ensemble aux ensembles déjà existants. Les câbles adéquats figurent dans le chapitre Câbles et bouchons SCSI.

4.2.2 SCSI série

Comme l'Ultra320 est apparemment le dernier standard SCSI parallèle réalisable, l'accent est actuellement porté sur les standards SCSI série. Ils sont supposés être plus économiques que la Fibre Channel décrite ci-dessous et permettre la création de bus SCSI avec des taux de transmission plus élevés. Les premiers produits ne sont pas attendus avant 2004 ou 2005.

4.3 Fibre Channel

Le nom Fibre Channel peut induire en erreur, dans la mesure où ce nouveau bus n'est pas exclusivement défini pour la fibre optique mais s'applique aussi aux câbles cuivre. Sur les deux supports de transmission sont prévus des taux de transfert atteignant de 12,5 Mo/s à 400 Mo/s. Le taux de transfert physique est encore plus élevé (de 132 Mbit/s à 2 Gbits/s). Le taux de données brutes en résultant est utilisé pour constituer un code de 8 à 10 bits, lequel permet un contrôle d'erreur simple. Différents types de câbles peuvent être combinés au sein d'un système Fibre Channel. La variante la plus simple est un câble paire torsadé protégé. Selon les distances ou les taux de transfert, on utilisera des câbles fibre optique ou cuivre. Une seule et unique interface permet ainsi d'installer des systèmes d'entrée de gamme économiques et de haut de gamme. Les connexions en fibre optique verre seront raccordées à l'aide d'un connecteur Duplex-SC ou LC, les connexions en cuivre par un connecteur Dsub à 9 pôles ou à l'aide d'un connecteur à 9 pôles (HSSDC - High Speed Serial DC).

Fibre Channel est la désignation générale d'une série de normes, qui a été développée par ANSI (American National Standards Institute), et qui doit encore être approfondie pour créer de nouveaux protocoles servant à une transmission d'informations flexible. Ce projet a commencé en 1988 sous la forme d'une extension de la norme Intelligent Peripheral Interface (IPI) Enhanced Physical et a pris plusieurs directions.

Les objectifs principaux de ce projet sont :

- Supporter différents types d'interfaces physiques
- Proposer un moyen de mettre en réseau ces différents types d'interfaces
- Permettre une transmission à haute vitesse de grandes quantités de données
- Le protocole logique est transporté par l'interface physique, ce qui permet le transport de différents protocoles via une interface physique commune (éventuellement simultanément)
- Diminuer la charge des interfaces physiques, sans cesse plus nombreuses qui n'ont qu'une largeur limitée.

On peut trouver Fibre Channel dans des systèmes de taille très différente, mais il est actuellement avant tout utilisé dans les gros systèmes informatiques.

Actuellement, on peut trouver des interfaces systèmes à fibre optique dans certains systèmes Desktop et dans certaines stations de travail. L'utilisation d'interfaces Fibre Channel très rapides va se développer dès que leur vitesse et leurs fonctions seront connues des utilisateurs. A cela s'ajoutent les petits groupes de travail qui doivent être reliés au moyen d'échanges de données par liaisons à haut débit.

Il faut évoquer ici deux protocoles fondamentaux pour la communication entre périphériques : les canaux et les réseaux. Le terme de « canal » se rapporte normalement à une interface E/S périphérique (à un ordinateur hôte) transportant de grandes quantités de données entre l'hôte et le périphérique. La sollicitation du système est maintenue aussi réduite que possible grâce à une transmission des données dans le matériel au moyen d'une participation faible, voire néante de logiciels dès qu'une opération E/S débute. En revanche, le terme de « réseau » se rapporte à une interface E/S impliquant généralement de nombreuses petites transmissions avec une forte sollicitation du système, généralement due à la sollicitation d'un logiciel au niveau du flux d'informations. Les réseaux soutiennent en règle générale une communication host-to-host.

Canaux

Les canaux sont généralement présents dans un environnement fermé, structuré et prévisible au sein duquel tous les périphériques pouvant communiquer avec un hôte sont connus par avance et où chaque changement nécessite également des modifications du logiciel hôte. Ces niveaux de connaissance plus complexes sont maîtrisés par la plupart des canaux.

Le système hôte contient toutes les données des canaux connectés à cet hôte. On emploie parfois l'image d'un environnement maître-esclave dans ce contexte. Des périphériques comme des lecteurs de disques ou de bandes magnétiques ou bien des imprimantes sont connectés directement au système hôte. L'hôte joue alors le rôle de maître, et les périphériques sont les esclaves.

Les canaux sont utilisés pour la transmission de données. Par données, on entend des fichiers contenant des informations qui peuvent représenter plusieurs milliers d'octets. Une exigence importante concernant la transmission des données est le transfert parfait, le retard de transmission venant ensuite.

Réseaux

A l'opposé, les réseaux sont généralement présents dans un environnement ouvert, non structuré et donc imprévisible. Chaque hôte ou chaque périphérique peut communiquer à chaque instant avec n'importe quel autre périphérique. Cette situation implique un support logiciel plus intensif pour le contrôle de l'autorisation d'accès, pour l'installation de séances de transmission et pour des transactions routing adaptées au bon service logiciel.

Cet environnement non structuré pour lequel tous les périphériques connectés sont égaux en droits est appelé environnement Peer-to-Peer. Plusieurs stations de travail serveurs peuvent être connectés. Chaque système y est indépendant par rapport à l'autre, et à l'occasion ils échangent des informations à l'aide de protocoles réseau. Par rapport à des systèmes de même type, une station de travail et un serveurs sont égaux en droits. Dans cette mesure, cet environnement est comparable avec le réseau téléphonique au sein duquel chaque appareil téléphonique dispose des mêmes prérogatives. C'est la raison pour laquelle on le compare souvent à un réseau téléphonique.

Les réseaux ne sont pas seulement utilisés pour la transmission de données sans erreur, mais aussi pour la transmission vocale et vidéo, pour lesquelles une restitution dans les temps est primordiale et la transmission sans erreur secondaire. Si par exemple la transmission via vidéo se produit avec du retard, les données seront inutiles ; par contre, si un ou deux pixels manquent, on ne remarquera rien, aussi longtemps que l'image n'est pas brouillée.

Protocoles supportés

Fibre Channel tente de combiner les points positifs de ces deux procédés de communication opposés au sein d'une nouvelle interface E/S, satisfaisant à la fois les besoins des utilisateurs de canaux et ceux des utilisateurs de réseaux.

Fibre Channel supporte le transfert de ATM (Asynchronous Transfer Mode), IEEE 802 et de toute autre opération réseau. Toute personne familiarisée avec Internet Protocol (IP), E-Mail, File Transfer, les communications à longue distance et les autres services Internet constateront que, dans Fibre Channel, ces protocoles sont supportés avec de nouveaux débits.

La contribution importante de Fibre Channel est que ces deux types d'interfaces, canaux et réseaux, peuvent partager désormais le même support physique. Ces dernières années, les canaux E/S ont été conçus dans ce sens, afin d'intégrer les applications réseau (à l'aide par exemple de SCSI, pour la connexion de deux stations de travail). De la même manière, les réseaux, au moyen de protocoles de transfert de données réseau déplacent des données entre les systèmes et les serveurs de fichier (par exemple Network File System (NFS)).

Avec Fibre Channel, il est désormais possible d'utiliser le même support physique et le même protocole de transport physique à travers un port matériel commun, afin de gérer les activités de canal ou de réseau. On peut envoyer des informations à un réseau, qui est connecté par Fibre Channel à la paroi arrière d'une station de travail, tout en utilisant Fibre Channel afin de communiquer en mode interne avec les périphériques (par exemple les disques durs et les lecteurs de bandes magnétiques).

Les caractéristiques du protocole de Fibre Channel : Fibre Channel ne contient pas d'instructions de commande comme par exemple SCSI et IPI, mais met à disposition un mécanisme permettant

d'engager d'autres protocoles sur Fibre Channel. Fibre Channel sert de support pour ces instructions de commande, de telle sorte que le destinataire peut distinguer entre les deux. Cela implique que différentes instructions de commande d'anciennes interfaces E/S, pour lesquelles des investissements logiciel étaient jusqu'à présent nécessaires, sont utilisées directement sur Fibre Channel.

La séparation entre les opérations E/S et les interfaces E/S physiques est une caractéristique importante de Fibre Channel et permet l'emploi simultané de différentes instructions de commande. Les différentes instructions de commande, comme par exemple SCSI, IPI-3, IP sont utilisées habituellement sur leurs propres interfaces, tandis que Fibre Channel définit un mécanisme de transfert physique unique et commun pour ces instructions de commande.

Fibre Channel

- Ne connaît pas le contenu ou la signification des informations transmises
- Augmente la connectivité d'une douzaine à une centaine, voir même à un millier de périphériques
- Augmente la distance maximale entre les périphériques
- Multiplie le taux de transmission par quatre ou par cinq, par rapport aux canaux les plus répandus, et par cent par rapport aux réseaux les plus courants.

Dans les lignes qui suivent, nous allons décrire comment Fibre Channel permet l'assemblage d'un réseau.

Topologie de réseau

Les appareils Fibre Channel sont aussi appelés « nœuds » (nodes en anglais), l'un d'eux ayant au minimum un port afin de permettre un accès à l'extérieur (c'est-à-dire à d'autres ports). L'ensemble des composants qui relient deux ou plusieurs ports entre eux est appelé topologie. Tous les systèmes Fibre Channel possèdent ces deux éléments : nœuds avec ports et topologies.

Chaque port Fibre Channel utilise un couple de conducteurs - un conducteur pour transmettre les informations allant au port, et un autre pour transmettre les informations venant du port. Fibre Channel emploie des conducteurs électriques ou bien des conducteurs à fibre optique. Ce couple de fibres est appelé « lien » (Link en anglais) et fait partie de chaque topologie.

Les données sont toujours transmises en unités (nommées "frames" ou trames) à travers ces liaisons. La norme Fibre Channel définit trois topologies, mais l'accent est surtout mis sur une topologie, appelée également "système Fabric", qui sera détaillée ci-après.

Topologie Fabric

Un système Fabric permet des couplages dynamiques entre des nœuds à travers des ports connectés à ce système. A noter que, dans cette application, l'expression Fabric peut valoir comme synonyme pour des expressions comme switch ou routeur. Chaque port dans un nœud, nommé N_port ou

NL_port, est connecté au système Fabric à travers une liaison. Chaque port dans un système Fabric est nommé F_port. Chaque nœud peut communiquer avec n'importe quel autre port connecté à d'autres F_ports du même système Fabric, à l'aide des services du système Fabric. Dans cette sorte de topologie, toutes les opérations de parcours pour les trames sont réalisées par le système Fabric à la place des ports.

Ce service "point à point" ou "Peer-to-peer" est un élément essentiel de la conception de Fibre Channel. Un système conçu pour des services « Peer-to-Peer » peut être utilisé de telle sorte que le procédé de communication « maître-esclave » de type hôte soit émulé. De cette manière, Fibre Channel peut supporter simultanément les protocoles canal et réseau.

Comparable à un système téléphonique

La fonction du système Fabric est comparable à un système téléphonique. On compose un numéro, le système téléphonique trouve le chemin pour accéder à l'appareil souhaité, le téléphone sonne et la personne appelée répond. Lorsqu'un poste de transmission ou une liaison tombe en panne, l'entreprise de télécommunications conduit l'appel par d'autres voies. La personne qui appelle ne s'en aperçoit que rarement. La plupart d'entre nous ignorent les liaisons intermédiaires que l'entreprise de télécommunication réalise pour que notre appel puisse avoir lieu.

Nous donnons pourtant quelques informations à l'entreprise de télécommunication concernant notre appel. Le numéro de téléphone commence par exemple (aux USA) par le chiffre 1 - suivi de dix chiffres sous la forme d'un indicatif local (3), d'un numéro de poste de transmission (3), ainsi que d'un numéro d'abonné (4). Si le numéro de téléphone ne commence pas par le chiffre 1, l'appel est considéré comme local et seuls sept chiffres sont alors utilisés. Ces informations permettent à la société de télécommunications de créer la liaison. Le numéro d'appel correspond à l'adresse ID Fibre-Channel. Une partie de l'adresse ID est employée afin de déterminer le domaine concerné du système Fabric, et le reste sert à rechercher le port spécial.

Il faut signaler que le système téléphonique n'est pas impliqué dans le contenu de la conversation entre les deux personnes participant à la communication téléphonique. Il assure simplement la liaison. De la même façon, Fibre Channel se charge de la liaison, et les protocoles établis (par exemple SCSI ou IPI) sont chargés des instructions. Ces protocoles jouent un rôle semblable aux langages dans les systèmes téléphoniques. Fibre Channel et les autres protocoles doivent être considérés comme un élément à part entière de l'échange d'informations.

Le système Fabric peut être composé d'un ou plusieurs éléments Fabric. Comme dans le système téléphonique, nous ne sommes pas au courant (ou du moins c'est le moindre de nos soucis) du nombre de commutateurs (postes de transmission) par lesquels nous devons passer, tant que nous sommes connectés avec le bon destinataire.

Un système Fabric est aussi appelé topologie intermédiaire ou encore topologie intermédiaire - point de couplage. Le routage se produit à travers différents commutateurs, les éléments Fabric interprétant l'adresse ID recherchée dès que celle-ci arrive dans chaque élément Fabric.

Le système Fabric peut être implémenté physiquement comme élément Fabric individuel avec plusieurs F_ports ou bien il peut être implémenté en série de plusieurs éléments Fabric semblables et reliés entre eux. Le routage, ou bien la transmission de toutes les connexions est transparente pour les deux N_ports, qui sont connectés à la bordure extérieure de Fabric.

Quand la topologie est séparée des nœuds, comme c'est le cas dans le système téléphonique et Fibre Channel, de nouvelles technologies peuvent être introduites pour les conducteurs. De nouveaux débits et de nouvelles fonctions peuvent être implémentés dans le système Fabric, sans que les investissements précédents soient perdus dans les nœuds existants. Fibre Channel permet une combinaison de périphériques supplémentaires à débits ou caractéristiques différents.

Autres topologies

En plus de la topologie système Fabric, la norme Fibre Channel définit deux topologies supplémentaires. L'une porte le nom de topologie point-to-point » avec seulement deux ports connectés. Dans ce cas il n'y a pas de routage. La troisième topologie s'appelle Arbitrated Loop". Il s'agit alors d'une topologie simple et économique pour la connexion de plusieurs douzaines de NL_ports à un loop. Les ports dans une topologie Arbitrated Loop (qui s'appellent NL_ports et FL_ports) se distinguent à peine des N_ports et des F_ports. Ils contiennent toutes les fonctions des N_ports et des F_ports et peuvent tout à fait travailler dans un système Fabric. Le FL_port est un port dans un système Fabric qui traite le protocole Arbitrated Loop.

Dans Arbitrated Loop, chaque port voit toutes les communications (comme dans le protocole Token Ring) et ignore les communications qui ne possèdent pas de protocole Token Acquisition.

Afin de permettre une meilleure compréhension de la topologie du système Fabric, poursuivons la comparaison avec le système téléphonique : vous composez le numéro de téléphone d'un ami. Vous n'avez pas besoin de connaître le cheminement exact réalisé par le système téléphonique jusqu'à chez votre ami. La régulation de l'acheminement est effectué par le système téléphonique. Le système Fabric de Fibre Channel a la même fonction : on donne une adresse de destination, et le système Fabric transfère les données jusqu'à la destination N_port.

Si vous composez un mauvais numéro de téléphone, l'entreprise de télécommunication vous informe que le numéro demandé n'existe pas. Le système Fabric rejette des trames pour des destinations non valables d'une manière comparable.

De la même manière que les entreprises de télécommunications peuvent configurer de nombreux parcours entre des points différents afin de proposer un service fiable, un système Fabric peut disposer de nombreuses voies entre des éléments Fabric, afin de générer la circulation. Cela permet la mise à disposition de voies de réserve au cas où un élément ou une liaison tomberaient en panne.

Les topologies système Fabric et Arbitrated Loop de Fibre Channel peuvent être combinées dans un système, afin de doter les nœuds d'une diversité de niveaux de service et de capacité. De plus, le système Fabric peut utiliser d'autres réseaux comme par exemple SONET ou ATM via SONET entre les éléments Fabric, et ce afin de surmonter les distances trop importantes entre les nœuds, distances qui ne pourraient être surmontées par une liaison entre N_ports. Ces liaisons spéciales peuvent exister entre des éléments Fabric répartis sur un grand espace géographique et qui ne sont pas connectés directement à des nœuds.

L'ajout d'autres types de liaisons entre des éléments Fabric, appelés ports d'extension ou E_ports, accroît la valeur de chaque lecteur connecté au système Fabric. Certaines fonctionnalités de Fibre Channel permettent à des ports avec débits et types de médias différents de communiquer entre eux. Ceci est aussi bien réalisable sur de longues que de courtes distances à condition qu'un système Fabric soit présent.

Il est possible de procéder à des améliorations technologiques dans le système Fabric lui-même sans que les N_Ports n'aient à être modifiés de quelque manière que ce soit. L'utilité principale de la nouvelle technologie est communiquée indirectement aux intermédiaires en raison du plus grand débit. Le débit, la fiabilité et la distance de communication étant augmentés à l'intérieur du système Fabric.

Combien de N_ports peuvent être implémentés ? Le système Fabric n'est limité que par le nombre de N_ports affiché dans l'entête de la fenêtre décrivant l'adresse de destination. Cette limitation est d'à peu près de 16 millions de ports, qui peuvent être inscrits en même temps dans un système Fabric avec une adresse ID 24 bits. Cette limitation est largement suffisante pour les systèmes individuels intégrés.

Dans la topologie de système Fabric, l'adresse ID est subdivisée en trois parties : domaine (8 bits), secteur (8 bits) et port (8 bits), ce qui représente un total de 24 bits. Ces éléments sont comparables avec ceux d'un numéro de téléphone, avec son indicatif, ses numéros de postes de transmission et son numéro d'abonné.

Cinq couches sont définies dans cette norme, caractérisées chacune par FC-x.

FC-0

Définit les parties Fibre Channel physiques, de même que le type de supports, les connexions ainsi que les caractéristiques de performance optiques et électriques nécessaires pour les connexions de port. Cette couche est décrite dans la norme FC-PH.

FC-1

Définit le protocole de transmission, de même que le code 8 bits /10 bits, la suite de la transmission verbale et de l'enregistrement des erreurs. Cette couche est décrite dans la norme FC-PH.

FC-2

Définit le protocole de signalisation et le protocole Framing, de même que la structure de la fenêtre, le contenu de l'entête de la fenêtre et les règles d'application. Il définit en plus certains cadres indépendants du protocole et des protocoles comme par exemple l'inscription de l'utilisateur (login). La norme FC-PH consiste principalement en une description de cette couche.

FC-3

Définit les services utilisés en commun, pouvant être disponibles sur différents ports dans un nœud. Pour cette couche il n'y a pas de norme.

FC-4

Définit le Mapping entre les couches Fibre Channel inférieures et les instructions de commande qui utilisent Fibre Channel. Ici vous trouvez SCSI, IPI-3, HIPPI et SBCS. Chacune de ces instructions de commande contient une norme distincte, des tierces personnes intéressées ne devant pas se charger inutilement d'informations étrangères au système. Si vous travaillez avec SCSI-3, vous n'êtes certainement pas intéressé par IPI-3 ou HIPPI.

Plusieurs N_ports par nœud sont aussi autorisés. Si un nœud possède plus qu'un N_port, les couches FC-0 et FC-2 sont reproduites pour chaque N_port. Les couches FC-3 et FC-4 sont utilisées en commun par différents N_ports. La couche pour les services utilisés en commun n'a pas jusqu'à aujourd'hui de composants définis. De nouvelles fonctions de cette couche seront établies au cours des travaux de développement ultérieurs associés à cette norme.

Dans la couche FC-4, un nœud ne peut pas accueillir toutes les options différentes autorisées par la norme. Chaque nœud peut implémenter un ou plusieurs services. Dans la couche FC-0, on ne peut implémenter qu'une option de type médias ou une option débit dans un N_port. Chaque port dans un nœud peut cependant implémenter une combinaison différente de débit et de média. La couche FC-2 supporte aussi de nombreuses options, parmi lesquelles un fabricant particulier doit être choisi. Quelques groupes industriels travaillent déjà à la définition de profils spécifiant le domaine d'exploitation indispensable pour quelques applications (par exemple SCSI, HIPPI, IPI-3, etc.). Il n'y a pas d'option dans la couche FC-1.

Lors du développement d'un produit ou de plans d'acquisition, si une option d'extension est prévue, un FC-4 pourra entrer en considération, de telle sorte qu'une liste d'exigences de port soit disponible, si l'extension doit être réalisée. Un fabricant de systèmes qui intègre le protocole IPI-3 et planifie l'installation d'Internet Protocol (IP) devrait soigneusement examiner les deux FC-4 avant qu'il se décide pour un design port, les exigences étant différentes.

Fibre-Channel-Arbitrated-Loop (FC-AL)

Fibre Channel AL (Arbitrated Loop) est une version plus compacte de Fibre Channel. Le mot "arbitrated loop" décrit la topologie du type de Fibre Channel conçu pour les périphériques locaux et les disc arrays. Les 127 ports "loop" maximum (NL_Ports) sont organisés en structure annulaire. Seule une connexion point à point est possible. Chaque paquet arrive d'abord au port de lecture du périphérique. Celui-ci vérifie s'il doit traiter l'information. Si cela n'est pas le cas, il émet à nouveau l'information via son port écriture. Pour réaliser cet échange de données, le périphérique doit s'assurer du contrôle du bus. Un échange de données en parallèle de plusieurs appareils (comme dans la définition générale de Fibre Channel) n'est pas possible.

Outre la connexion câble normale, FC-AL supporte aussi l'architecture dite "fond de panier" (backplane) afin de mieux pouvoir maîtriser les "disc arrays". Ici, les disques durs sont connectés au fond de panier par un connecteur SCA à 40 pôles (Single Connector Attachment), qui transporte aussi bien les données que le courant d'alimentation. Si aucun périphérique n'est connecté sur un port, celui-ci sera ignoré par la logique du fond de panier et le cercle restera fermé. Une autre tâche du fond de panier consiste à configurer automatiquement le lecteur et à contrôler la fonction hot plug, à savoir le changement de lecteur à chaud, en cours de fonctionnement. Les Fibre Channel Hubs utilisent le même principe. Dans un Fibre Channel Loop, le cercle est interrompu et le bus est bloqué lorsqu'un appareil tombe en panne ou qu'un câble est défectueux. Le hub franchit chaque port inutilisé ou bloqué par des dérangements. De cette manière, le flux des données vers les autres appareils n'est pas interrompu et le bus continue de travailler normalement. Les produits FC-AL sont proposés depuis l'automne 1996. Bien qu'au début ils se concentraient sur les systèmes RAID haut de gamme, ils sont aujourd'hui de plus en plus appréciés pour répondre aux exigences des serveurs plus petits.

4.4. SSA

SSA (Serial Storage Architecture) est une interface haute performance, qui interconnecte les périphériques entrée/sortie de toutes les plates-formes.

Cette interface série, ressemblant à un bus, a été développée par IBM sur la base de la technologie IBM-9333 et est utilisée essentiellement pour la connexion de disques durs. Il est possible d'interconnecter jusqu'à 128 périphériques.

Si, comme Fibre-Channel, l'interface SSA est une connexion point à point, elle ne dispose en revanche que de 2 canaux d'écriture et de 2 canaux de lecture. Sur chaque canal (écriture/lecture) un taux maximal de transfert de 20 Mo/s est possible, ce qui correspond à un taux de transfert cumulé de 80 Mo. Cette performance n'est cependant obtenue qu'à la condition que le rapport écriture/lecture soit égal à 1:1 et que l'adaptateur accède à des données réparties sur au moins 4 disques.

Un câble paire torsadée normal sera suffisant pour connecter deux stations séparées par une distance de 20 m. Des câbles de fibre optique sont utilisés pour des distances jusqu'à 680 m. Autrement dit : 94 % des données sont des données utiles. Cependant, seuls quelques fabricants (comme IBM, Siemens ou Micropolis) supportent l'interface SSA. La relève est maintenant complètement prise en charge par la technologie Fibre Channel Arbitrated Loop.

4.5 Interface ATA (IDE)

Dans le domaine PC, IDE (Integrated Drive Electronics) est une interface très répandue. IDE a complètement évincé ST506, le standard d'interface précédent. Deux disques durs sont possibles par interface IDE. Dans le cas où deux disques durs doivent être raccordés, le premier doit être configuré comme maître, le second comme esclave. Rappelons que les disques durs IDE sont en standard toujours configurés comme maître et non comme esclave.

Les interfaces IDE (également appelées bus AT ou encore ATA pour AT-attachment) utilisées jusqu'ici, avaient un taux de transfert théorique maximal d'environ 4,3 Mo/s. Dans la pratique, cependant, ce taux plafonne autour de 2 Mo/s. Elle ne peut être utilisée avec d'autres périphériques. Pour faire face aux exigences toujours croissantes, les interfaces IDE ont été perfectionnées :

Fast-ATA et Enhanced IDE

Ces deux produits se distinguent essentiellement au niveau de la stratégie marketing appliquée. Les implémentations et fonctionnalités de ces deux produits sont en revanche très semblables. Fast-ATA et Enhanced IDE restent tous les deux compatibles avec les adaptateurs et disques durs de la génération précédente. Ils utilisent le même câble à 40 pins.

Il existe des extensions sous le nom ATAPI (AT Attachment Packed Interface) pour le Enhanced IDE permettant de raccorder des périphériques comme les CD-ROM, les scanners, les lecteurs de bandes etc. de manière comparable au SCSI.

UltraATA

Pour le UltraATA, comme pour le Ultra SCSI, la fréquence de l'interface Fast-ATA sur le bus est élevée. Ainsi, Ultra ATA atteint un taux de transfert de données de 33 Mo/s sur le bus.

UltraATA/66, UltraATA/100 et UltraATA/133

Après trois adaptations, la cadence atteint maintenant 133 MHz. Les exigences en matière de câblage sont par contre plus strictes depuis ATA100, en raison du taux de fréquence élevé. Un câble particulier à 80 pôles est nécessaire. Cependant, comme le connecteur ne doit pas être changé, il sera possible de brancher des disques et des contrôleurs plus anciens, au prix bien entendu d'une performance inférieure.

S-ATA

Si ces dernières années, les technologies ATA ont marqué le pas face à SCSI, en particulier en raison de leur prix avantageux, le nouveau standard va encore renforcer cette tendance. Ici encore, c'est une technologie série qui s'impose face au parallèle : ATA série (S-ATA) constitue un bus qui, premièrement propose un fort potentiel de croissance pour les taux de transfert et deuxièmement possède toute une série de caractéristiques SCSI, comme par exemple le Command-Queueing. S-ATA est ainsi approprié pour les applications à grandes sollicitations E/S, garantissant les puissances élevées nécessaires aux systèmes RAID.

De fait, les premières grandes applications seront des systèmes RAID. En effet, lors du lancement de S-ATA, il faut compter avec des difficultés : une utilisation simultanée d'ATA série et parallèle n'apportera rien. D'un autre côté, les CD-ROM ATA se feront attendre, car leur coût reste encore élevé.

4.6 Interface USB

USB (Universal Serial Bus) est un standard pour la connexion à un ordinateur d'appareils externes (par ex. : Imprimante, modems, clavier, écran, appareils photos digitaux, etc.). L'avantage de l'interface USB réside dans l'intégration facile de périphériques supplémentaires. Le contrôleur USB reconnaît si des périphériques supplémentaires ont été connectés, installe automatiquement les drivers requis et met en oeuvre le système. Des configurations nouvelles et complexes des systèmes PC font désormais partie du passé. Théoriquement, 127 périphériques externes peuvent être connectés à l'interface USB. Le passage à l'USB Version 2, avec des taux de transmission plus élevés et certaines extensions de protocole, a lieu actuellement.

De plus amples informations sur l'USB sont disponibles sur www.usb.org.

4.7 FireWire 1394

FireWire (IEEE 1394) est un bus de données série grande vitesse pouvant assurer des débits jusqu'à 800 Mbits/s. A l'origine utilisé par Apple, il est surtout employé pour relier des périphériques multimédia tels que les caméscopes et les appareils photo numériques à un ordinateur. Le standard a été défini en 1995. Le bus autorise des bandes passantes élevées, ce qui est important surtout dans le domaine vidéo. Il est possible de relier en série 16 périphériques sur une distance de 72 m (4,5 m par lien). Cependant, il existe aussi des ponts, permettant un nombre plus élevé de

services en cascade (maximum 1023 ponts sont permis).

En tant que média de connexion, FireWire utilise un câble spécial à 6 pôles se composant de deux fils Paire Torsadée blindés et de deux fils supplémentaires pour l'alimentation.

FireWire ne joue plus un rôle d'importance qu'en environnement Apple.

5. Disques durs et RAID

5.1 Guide

Il s'agit ici de mémoires de données primaires. Sous ce terme, on entend la mémoire de masse qui rend les données disponibles en Random Access (accès direct aux blocs d'information). La mémoire à semi-conducteurs et les lecteurs de disques magnétiques, tels que lecteurs de disques durs et de disquettes, font partie de cette catégorie.

Pour gérer de grandes quantités de données supérieures à la capacité d'un disque dur tout en assurant une sécurité accrue contre les défaillances, les disques durs sont réunis en RAIDs (Redundant Arrays of Independent Disks).

5.2 Disques durs

Les disques durs (également appelés disques "Winchester" ou magnétiques) sont les mémoires de masse habituellement utilisées pour les applications standard. Ils font appel à un mode d'enregistrement magnétique et peuvent être lus et écrits de manière illimitée. Les disques durs sont catégorisés en fonction de la capacité, de l'interface de bus et du facteur de forme. S'y ajoutent des caractéristiques de performances comme la vitesse de rotation et les durées d'accès.

5.2.1 Capacité

La capacité des mémoires de masse s'exprime en giga-octet. On distingue la valeur brute et la valeur nette. La capacité brute correspond à la capacité théorique maximale du lecteur. Cette valeur est obtenue en multipliant la densité maximale en bits avec la longueur des pistes, le nombre de pistes et le nombre de surfaces de disques. La capacité nette indique la capacité réelle utilisable sur un disque.

La capacité nette indiquée par le fabricant se différencie de la véritable capacité nette utilisable. Cela s'explique d'une part, par le fait qu'entre les blocs, 10 à 20% de la capacité brute d'un disque est exclusivement dédiée à des tâches de correction d'erreurs et des tâches d'adressage. Et d'autre part, par le fait que fabricants de disques et fournisseurs de systèmes d'exploitation ne sont pas unanimes quant à la définition d'un méga-octet : les fabricants de disques partent du principe que $1 \text{ Mo} = 1.000 \times 1.000 \text{ octets} (=1.000.000 \text{ octets})$ alors que les fournisseurs de systèmes d'exploitation considèrent que $1 \text{ Mo} = 1.024 \times 1.024 \text{ octets}$, soit 1.048.576 octets ou signes. De plus, le système de gestion de fichiers utilise un espace disque pour stocker les données de gestion (par ex. SunOS prélève en plus environ 10% du système de fichiers en tant que réserve immobile. L'utilisateur ne voit pas cette réserve lorsqu'il entre la commande df). La capacité nette d'un disque dépend finalement de son formatage. L'indication de cette grandeur peut ainsi légèrement varier

en fonction de la définition retenue.

La capacité d'une mémoire de stockage dépend de l'application qu'elle va héberger. En particulier pour les applications audio/vidéo, les programmes graphiques et les applications de PAO, qui sont gourmandes en données. Mais les systèmes d'exploitation et les logiciels d'utilisation sollicitent pour eux-mêmes une telle part du volume de mémoire, qu'un disque dur à capacité impressionnante au préalable s'avère très rapidement saturé avec les logiciels et les données. On prévoit actuellement un doublement annuel de l'espace de stockage nécessaire.

De manière générale, la capacité des disques durs doit être déterminée avec largesse car l'espace nécessaire est souvent supérieur à celui initialement prévu. Il faut également tenir compte du fait que l'exploitation d'un disque, à un niveau trop proche de la saturation, réduit généralement les performances du système de manière sensible. Simultanément, l'achat d'un disque de grande capacité se heurte à la constante chute des prix de ce type de produit. Acheter un lecteur avec des capacités inférieures, puis l'échanger contre un disque plus important, peut s'avérer moins onéreux que l'achat immédiat d'un grand lecteur. Il est donc recommandé d'acheter un disque d'une capacité suffisante pour couvrir les besoins sur une année.

Malheureusement, des disques durs assez grands ne sont pas disponibles pour tous les systèmes d'exploitation. Il faut noter les restrictions suivantes concernant les stations de travail HP9000. Pour les modèles 7xx sous HP-UX 9.01 (avec le patch PHKL_3325) ainsi que HP-UX 9.03 - 9.05, seuls des disques de capacité inférieure à 2,147 Mo peuvent servir de disques de démarrage (plus précisément, seuls les systèmes de fichiers inférieurs à 2³¹ sont reconnus). Comme support de données, les disques ne peuvent dépasser 4,294 Mo (soit inférieur à 2³²). Les modèles HP9000/7xx sous HP-UX 10.xx et supérieur et les modèles HP9000/8xx sous HP-UX 9.xx et supérieur disposent d'un LVM (Logical Volume Manager). Celui-ci autorise des disques de démarrage de 4,294 Mo et des disques de données ayant une capacité illimitée (juste limitée en pratique par le nombre de systèmes fichiers possible pour chaque SCSI-ID). Si un système de fichiers dépasse les 4,294 Mo, le gestionnaire logique de capacité le divise en plusieurs fichiers logiques et permet ainsi de contourner la limitation de 2³² octets.

Pour les modèles HP9000/3xx et 4xx sous HP-UX, les disques de démarrage de même que les disques servant au support des données ne peuvent dépasser 2,147 Mo. La même remarque vaut également pour DOMAIN-OS où de surcroît les disques doivent être adaptés à SCSI-1.

Des limitations de capacité existent également sous DOS, Win3.1, Win3.11 et Windows 95. Une seule partition peut être configurée et active au sein du système. La partition active est en règle générale la partition boot. La taille maximale des partitions est malheureusement toujours de l'ordre de 2 Go, la taille du disque dur est de 8 Go. Il est à noter que la taille des blocs disque est de 32 Ko pour une partition de 2 Go, cela signifie que lorsqu'un fichier de 250 octets est chargé, il occupe quand même un bloc de 32 Ko. La seule façon d'échapper à cette contrainte réside dans la configuration d'un bloc de 8 Ko, ce qui pour une partition de l'ordre de 500 Mo est

automatiquement le cas. La taille maximale pour Windows NT et Windows 2000 est de 16 exaoctets (16 millions téraoctets). La taille maximale du disque dur dépend donc uniquement du contrôleur SCSI. La taille de partition peut facilement atteindre un ordre de grandeur de 20 Go. Il y a des limitations de systèmes de fichiers à 2 Go sous Sun Solaris 1.x (pas sous Solaris 2.x). Puisqu'un maximum de sept partitions peut être installé, les limites du disque dur se portent donc à 14 Go. AIX 3.x de IBM présente également une limitation des systèmes de fichiers de l'ordre de 2 Go. AIX étant doté d'un LVM (Logical Volume Manager), les disques peuvent supporter un nombre quasi illimité de partitions. AIX 4.x supporte des systèmes de fichiers jusqu'à maximum 64 Go. Par conséquent, des disques durs plus importants ou des ensembles RAID peuvent être sollicités en tant que systèmes de fichiers.

Certains systèmes d'exploitation plus anciens (IBM AIX3.5, SGI IRIX5.x, Sun Solaris1.x) mettent un terme au formatage des disques durs de plus de 8 Go. Avant d'acheter un disque dur plus grand, il convient de vérifier si un patch adéquat est existant.

5.2.2 Interfaces de bus de mémoire

La production actuelle se concentre sur les disques durs avec interface ATA, SCSI et Fibre Channel. Alors que ATA ou SCSI (rarement FC) sont principalement utilisés en interne, seules SCSI ou FC sont utilisés en externe.

Vous trouverez de plus amples informations concernant les différences entre les interfaces au chapitre bus de mémoire. Les disques durs ATA sont de plus en plus utilisés y compris dans les systèmes RAID (voir ci-dessous).

5.2.3 Format

Le format désigne le diamètre du support de données, à savoir celui du (des) disque(s) se trouvant dans le boîtier. Outre ces disques, le boîtier contient des têtes de lecture et d'écriture, la mécanique permettant le mouvement de ces têtes (bras d'accès), le moteur et l'électronique.

Le marché propose actuellement des disques au format 2,5, 3,5 et 5,25 pouces. Des disques plus petits de 1,8 ou 1,3 pouces sont également disponibles. Les disques durs existent en hauteur normale (82 mm), demi-hauteur (41 mm) et "low profile" (25,4 mm = 1 pouce) et également en hauteur de 19 et 12,5mm. Les versions 3,5 pouces sont les versions les plus demandées et atteignent des capacités nettes de 300 Go. Les disques plus grands de 5,25 pouces ne sont plus produits.

5.2.4 Performances

Parallèlement à la vitesse du processeur et bien sûr à la taille de la mémoire, les performances du système de stockage principal sont des facteurs déterminants du temps de réponse global d'un ordinateur. Les données devant être transmises à partir du disque dur, doivent correspondre en un bloc dans la mémoire principale, sinon elles doivent aussi être rechargées. Avec la quantité croissante de données transmises par le bus, la mémoire principale devrait être également adaptée. La performance est définie, en premier lieu, par le temps d'accès et, en second lieu, par le taux de transfert de données. Le temps d'accès est calculé à partir du temps requis pour de multiples processus séquentiels.

Lorsqu'un programme veut lire ou écrire des données, le système d'exploitation génère une requête qui sera transmise au contrôleur du disque. Le temps requis par cette procédure s'appelle la consommation CPU du système d'exploitation. Cette requête conduit le lecteur à positionner les têtes de lecture/écriture en un point spécifique de la surface du disque. Le temps nécessaire à cette dernière opération s'appelle le temps de positionnement.

La valeur du temps de positionnement indiquée correspond en fait à un temps de positionnement moyen, à savoir : le temps requis par la tête de lecture pour parcourir un tiers de la distance maximale à travers le disque. Le temps d'immobilisation (settling time) correspond au temps dont la tête de lecture a besoin pour s'immobiliser et s'arrêter complètement après un positionnement. Les lecteurs modernes prennent déjà en compte le temps de positionnement dans le setting time. Une fois la tête de lecture/écriture positionnée sur la bonne piste, il lui faut encore attendre que le bloc d'information souhaité se positionne en dessous.

Cela s'appelle le temps de latence ou encore le temps de rotation. Le temps indiqué par les constructeurs est celui correspondant à la moitié de la rotation du disque. Cette grandeur dépend donc exclusivement de la vitesse de rotation du disque. Une vitesse de rotation de 7.200 r/min conduit par exemple à un temps de latence de 4,17 ms. Les données seront alors transmises et ce, d'abord du disque dur vers le contrôleur de disque dur. A ce stade intervient le taux de transfert (interne) du disque. Il indique la quantité d'octets transférée par seconde. Parfois une fréquence est également indiquée. En divisant cette fréquence par 8, on obtient le taux de transfert en bits. Plus le taux de transfert d'un disque est élevé, plus le temps de transfert requis pour les données est minime. Lorsque les données arrivent au contrôleur du disque, ce dernier les transmettra à l'adaptateur CPU SCSI par l'intermédiaire du bus SCSI. Le taux de transfert du bus SCSI atteint 320 Mo/s. De plus amples informations sur les bus SCSI se trouvent dans le chapitre consacré aux bus de mémoire.

Plus le temps de transfert global est court, plus la performance du système est élevée. Ceci est particulièrement valable pour les systèmes d'exploitation qui ne peuvent traiter d'autres tâches durant cette période (MS-DOS, par exemple). Les tableaux comparatifs de taux de transfert sous-entendent en général des conditions optimales, à savoir que la tête est déjà positionnée, qu'u

cyindre entier est lisible, etc. La taille des blocs (nombre d'octets par secteur) influence elle aussi le taux de transfert. 512 octets/secteur est la valeur la plus répandue. Les disques peuvent également être formatés avec maximum 4.096 octets/secteur, ce qui laisse plus de place au stockage des données, parce que le volume d'informations de formatage est plus réduit. Le taux de transfert net est dès lors encore plus élevé. Cependant, ce formatage n'est pas compatible avec tous les systèmes d'exploitation et ne se justifie pas avec toutes les applications. En résumé : plus la taille des fichiers fréquemment lus ou écrits sur le disque est petite, plus la taille de secteur doit être réduite (ex : bases de données). Plus les fichiers sont grands, plus il sera intéressant de créer de grands secteurs (par ex. pour le traitement d'images).

Pour les lecteurs SCSI, c'est en outre souvent les taux de transfert via bus SCSI qui sont indiqués. Comme une mémoire tampon est montée dans les lecteurs SCSI, les taux de transfert indiqués correspondent seulement au taux de transfert entre la mémoire tampon du disque et celle de l'adaptateur. Le taux de transfert de la surface du disque vers la mémoire tampon de l'adaptateur CPU est sensiblement plus faible.

Comme la plupart des applications ne lisent et n'écrivent que quelques blocs, qui ne génèrent en fait qu'un faible volume de transfert par requête, le taux auquel le disque transfère les données à l'adaptateur n'est que secondaire. En revanche, plus les données sont segmentées sur le disque, plus le nombre d'opérations élémentaires de lecture sera élevé. Il faut veiller à ce que, dans la chaîne de transfert : disque - contrôleur du disque - adaptateur CPU SCSI - mémoire RAM, les vitesses de transfert soient synchronisées.

Pour améliorer les performances, il est également possible de faire appel à des contrôleurs (sur les disques comme sur les contrôleurs CPU) utilisant une mémoire cache.

Un cache multisection est particulièrement avantageux. Le cache fait l'objet d'une gestion dynamique et est divisé en plusieurs zones. Les données sont stockées dans une zone du cache, en fonction du nombre de zones du disque dont elles proviennent. L'accès aux données disponibles dans le cache est entièrement affranchi des délais dépendants des composants mécaniques.

Ces contrôleurs gèrent les requêtes d'écriture de la même manière que les contrôleurs non munis de cache : chaque bloc d'écriture est transféré vers le disque. La différence tient au fait que ce type de contrôleur se souvient de l'adresse du bloc et en conserve le contenu dans sa mémoire interne : le cache. Cette technique permet de réduire le nombre d'accès au disque dur. On utilisera les contrôleurs de disques avec mémoire cache dans les cas de figure suivants : capacité de mémoire RAM insuffisante, disques traitant un grand nombre de requêtes lecture/écriture, faible nombre de blocs par requête. Dans cette catégorie entrent par exemple les systèmes de disques destinés à des bases de données et, de manière plus générale, ceux destinés à des applications recourant fréquemment et en alternance aux opérations de lecture/écriture sur le même fichier. De tels contrôleurs permettent de ramener le temps d'accès moyen à des valeurs inférieures à 1 ms.

Il existe différents types d'antémémoire : Read, Read-ahead et Write-back. Lors d'un accès "lecture" sur un read-cache, la mémoire recherche le bloc adéquat. Dès que le bloc sera trouvé, il sera immédiatement transféré. Dans ce cas, l'accès aux données est complètement affranchi des délais de positionnement et de rotation du disque. Si le bloc n'est pas trouvé dans l'antémémoire, il sera récupéré au niveau du disque.

Avec un cache Read-ahead, les blocs suivant la lecture d'un bloc défini sont lus à l'avance et enregistrés dans la mémoire cache. Avec un cache Write-back, les blocs devant être écrits sont enregistrés dans un premier temps dans la mémoire cache et seulement ensuite écrits sur le disque dur, si aucun autre ordre d'écriture ou de lecture n'intervient. Les accès en écriture sont ainsi plus rapides pour l'utilisateur. Cette technique présente cependant le risque que les données enregistrées dans la mémoire cache soient perdues en cas de panne de courant. Avec le Read-ahead-cache, cela ne représente aucun problème, par contre avec le Write-back-cache, la structure des données peut être détruite.

C'est la raison pour laquelle il convient, lorsque l'on a choisi d'utiliser un cache Write-back, de s'équiper aussi d'un onduleur.

En fonction de la taille de la mémoire cache, de la logique de sa gestion (choix des blocs à écraser lorsque la mémoire cache est saturée) et du type d'application, il est possible de réduire les accès disques de plus de 90% et, en conséquence, d'améliorer considérablement le taux de transfert.

De nombreux systèmes d'exploitation (Windows NT, NetWare, Unix et OS/2 par exemple) réservent automatiquement une partie de leur mémoire de travail à la mémoire cache. Le fait de disposer de plus de mémoire de travail permet une augmentation considérable des performances globales du système.

5.3 Disques virtuels (mémoire RAM)

Si la rapidité d'un disque est insuffisante pour certaines applications, il est possible d'utiliser des disques à semi-conducteurs (disques RAM et disques « solid state »). Les disques RAM ou disques virtuels font appel à un programme spécifique qui transforme une partie de la mémoire de travail en un disque virtuel permettant le stockage des données. La solution « solid state » est plutôt une solution matérielle faisant appel à une interface bus et à des modules de mémoire. Dans les deux cas, l'accès à la mémoire de travail se fait exactement comme sur un disque normal. Il est donc tout à fait possible de créer des fichiers comme sur un disque dur réel puis de les relire.

Avantage : le temps de positionnement et le temps de latence d'accès au disque physique sont court-circuités. Le transfert de données peut être effectué à la vitesse maximale.

Inconvénient : même avec une batterie de sauvegarde, une telle solution de sauvegarde ne peut être adoptée en permanence. Cette solution est aussi nettement plus coûteuse qu'un disque de

même taille. Enfin, il faut impérativement disposer d'un système d'alimentation d'appoint, puisque même de courtes interruptions de l'alimentation en courant peuvent aboutir à la perte de données.

5.4 Lecteurs de disquettes

La technique de disquette est basée sur un petit disque amovible, magnétisable, avec un temps d'accès aux données de 150 à 250 ms. Principal avantage : ce format est largement diffusé et facilite donc l'échange avec d'autres systèmes. Désavantage : une capacité de stockage faible (de 360 Ko à 2,88 Mo). Cette capacité n'est plus suffisante, depuis que des ordinateurs performants ont fait leur réapparition tant dans les entreprises que chez les particuliers.

Les lecteurs ZIP IOMEGA ont permis de pallier à cet inconvénient. Les capacités de sauvegarde atteignant 750 Mo sont suffisantes pour des progiciels de petite et moyenne taille. De plus, le rapport qualité/prix est excellent.

Depuis la mi-1999, Sony a mis sur le marché un lecteur de disquettes HiFD qui, de par sa capacité de mémoire de 200 Mo, a pris le relais sur les lecteurs habituels. Ce lecteur est compatible avec les lecteurs utilisés actuellement et peut lire les disquettes de 1,44 Mo.

Toutefois, cette "hauteur de vol" à laquelle la tête de lecture se déplace au-dessus du disque de sauvegarde pourrait conduire à ce que l'on appelle un "crash de la tête". Un tel contact entraîne normalement la perte des données sauvegardées. Cela peut également concerner les lecteurs de disques amovibles, décrits ci-dessous.

5.5 Lecteurs de disques amovibles

Les disques amovibles permettent de gérer un volume important de données sans pour autant perdre de temps. De plus, ce type de système se prête très bien aux applications critiques, lorsque les données doivent être enfermées dans un coffre, pendant la nuit par exemple.

L'utilisation de disques amovibles est recommandée lorsqu'un utilisateur, un programmeur par exemple, travaille sur plusieurs sites et doit pouvoir accéder en permanence à ses données. Comme ses données sont stockées sur un disque dur, une perte de données est toujours possible. Il est donc prudent d'entreprendre une sauvegarde sur un autre support.

Alors que les systèmes de disques amovibles étaient fabriqués comme un produit indépendant (Iomega, Syquest) les disques durs standard (souvent avec un facteur de forme de 2,5") et leurs tiroirs adaptés sont maintenant plus généralement utilisés, car la sécurité de transport s'est énormément améliorée grâce aux nouvelles technologies, en particulier sous l'influence des ordinateurs portables.

5.6 RAID

Les performances des processeurs et des mémoires de travail doublent en moyenne tous les ans. La capacité des périphériques de stockage double aussi, mais seulement tous les deux ans. Et enfin on peut compter avec un temps moyen de positionnement deux fois moindre, seulement tous les sept ans. Il y a ainsi un décalage de technologie entre les disques durs et les processeurs.

Il est donc nécessaire d'utiliser des techniques qui, malgré le retard de développement des technologies de disques durs, soient compatibles avec les vitesses des processeurs et les quantités de données des systèmes actuels et ce, grâce à une vitesse d'accès et à une capacité élevées.

Le temps MTBF (MTBF = Mean Time Between Failure = le temps moyen entre deux défaillances de disques durs) s'élève aujourd'hui à plus de 500.000 heures. Pour 100 disques durs connectés à un ordinateur, la moyenne est d'une défaillance par semestre. Même si l'on peut compter sur l'amélioration de la fiabilité des disques durs, cette situation n'est, en l'état, pas acceptable. Des systèmes résistants aux défaillances sont donc nécessaires.

Sous le terme RAID se regroupent des technologies, qui rassemblent plusieurs lecteurs en systèmes principaux plus importants et aussi partiellement résistants aux défaillances. Le terme RAID signifie Redundant Array of Independent Disks. Souvent, certains préfèrent lire ou écrire en lieu et place "independent".

Redundant = résistant aux défaillances, sous-entend qu'une panne sur l'un des disques du système ne doit pas altérer le fonctionnement du système complet ni entraîner de perte de données. RAID englobe souvent les technologies utilisées telles que le mirroring (recopie complète d'un ou de plusieurs disques à partir d'un contrôleur), le duplexing (même principe, mais via deux contrôleurs distincts) et le striping (combinaison de plusieurs disques en une seule unité logique et distribution des blocs de données sur ces disques).

Plusieurs niveaux RAID font l'objet de discussions dans la littérature spécialisée. La notion de niveau dans le concept RAID peut prêter à confusion, Le niveau RAID 1, par exemple, ne se base absolument pas sur le niveau RAID 0. Il serait plus approprié de parler ici de types RAID.

Avant d'entrer dans le détail des niveaux de RAID, vous trouverez ci-dessous certaines réflexions concernant l'accès aux disques car l'amélioration des performances en passant des lecteurs indépendants aux RAID dépend pour beaucoup de l'application :

Le panachage entre les accès écriture et lecture ainsi que la longueur moyenne d'un transfert sont des points importants.

Si l'on exclut provisoirement du champ de notre analyse l'utilisation des mémoires cache, le tampon Read-ahead et toutes autres techniques améliorant la performance, un accès lecture sur un disque isolé est aussi rapide qu'un accès écriture. Ce qui n'est pas le cas pour un périphérique RAID qui se comporte différemment selon le niveau. Les performances varient également suivant que les requêtes sont courtes (la plupart du temps un ou peu de blocs) ou longues (la plupart du temps plusieurs centaines de blocs). Le premier type est surtout utilisé pour les applications du type base de données, transactionnelle, ou encore applications commerciales multi-utilisateurs. Le deuxième

type, généralement pour le traitement d'images, l'utilisation d'ordinateurs puissants ou la saisie technique/économique de données. Chaque concept RAID, ci-dessous exposé se caractérise de manière différente suivant que la longueur de la requête est courte ou longue.

Les systèmes RAID ne représentent pas une solution sur mesure à tous les problèmes de flux de données. Une solution RAID n'est pas forcément toujours plus rapide que des lecteurs isolés utilisés de manière conventionnelle. Même lors de l'utilisation de l'un des types RAID décrits ci-après, la répartition des données devrait être optimisée. En partant du principe, qu'une petite quantité de données est souvent sollicitée et que la plupart des données n'est utilisée que rarement, il serait souhaitable de mettre en place un système hiérarchique avec disque virtuel (par ex, en mémoire RAM) pour les données utilisées constamment, une mémoire de masse rapide (éventuellement copiée) pour les données utilisées souvent, une mémoire de grande capacité et d'accès moyennement rapide (RAID par exemple) pour les données moins souvent utilisées. Enfin, il peut être fait appel à un système d'archivage (lecteur de disques optiques avec chargeur automatique) pour les données rarement utilisées.

5.6.1 Niveau RAID

Il existe différentes méthodes pour répartir des données sur plusieurs disques durs afin d'obtenir un débit et une sécurité maximum. Elles sont catégorisées en niveau RAID. Mais le terme est trompeur : un niveau RAID plus élevé ne signifie pas nécessairement une redondance ou une performance plus élevée. Chaque niveau RAID a ses propres avantages et inconvénients et le choix du niveau approprié dépend de l'application. Les critères de sélection sont : la vitesse d'écriture, la vitesse de lecture et le degré de redondance (autrement dit les coûts).

5.6.1.1 RAID niveau 0

Ce type de RAID signifie entrelacement. Cette méthode consiste à assembler plusieurs petites unités de disques pour composer une grande unité logique. Le facteur d'entrelacement indique la taille du fragment stocké sur une unité physique. Plus ce facteur est petit (le plus souvent un octet), plus le débit de transfert moyen s'en trouvera amélioré et ce indépendamment de la longueur des requêtes de lecture ou d'écriture, puisque toutes les unités dans un RAID-0 sont transférées simultanément.

Cette technique présente néanmoins des inconvénients, dans le cas de requêtes d'écriture par petits blocs : si l'on raccourcit la longueur physique des blocs sur le disque (pour des blocs de 512 octets et en utilisant 4 disques durs, par ex. adoption d'une longueur de requête de 128 octets), la capacité totale du disque se trouvera diminuée par les entêtes associées à chaque bloc. En laissant la longueur des blocs physiques à la longueur standard, la capacité du disque n'est pas diminuée mais il faut alors, pour écrire un seul bloc, lire au préalable tous les blocs physiques (répartis sur les différents disques durs) contenant des segments du bloc que l'on se propose d'écrire. Les informations partielles sont alors remplacées. Après quoi, l'écriture des différents blocs peut

effectivement avoir lieu.

Avec un petit facteur d'entrelacement, RAID 0 offre d'excellentes performances à la lecture ou l'écriture de grands blocs, mais laisse apparaître de grosses lacunes pour des transferts de petits blocs.

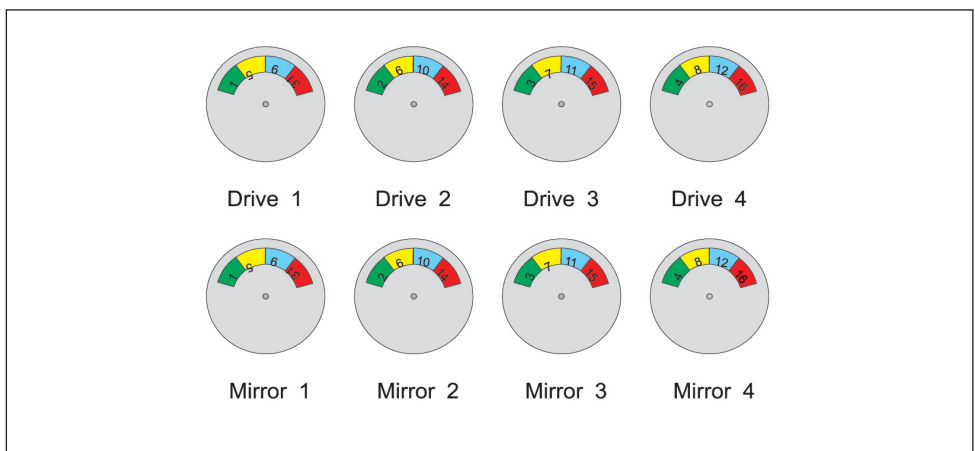
Les inconvénients de RAID 0 apparaissent encore plus clairement lorsque l'on compare un système RAID 0, non pas avec un disque dur traditionnel (de capacité totale comparable) mais avec plusieurs petits disques durs pouvant traiter des petites requêtes simultanément.

Si l'on choisit un facteur d'entrelacement important (plusieurs blocs), la performance aussi bien de lecture que d'écriture pour des transferts courts reste comparable à celle d'un disque dur traditionnel. Il est aussi possible de traiter plusieurs petites requêtes simultanément sur des disques différents.

Un problème majeur subsiste cependant pour les deux versions : dans le cas d'une défaillance d'un seul des disques de l'ensemble, l'accès à la totalité des données est impossible. Pour cette raison, on dit souvent que RAID 0 (striping) n'est pas un véritable système RAID : la sécurité de donnée n'est pas améliorée.

La technique de l'entrelacement gérée par le CPU de l'ordinateur est disponible sous différents systèmes d'exploitation, soit sous forme logicielle, soit directement installée sur le contrôleur de disques. Les disques durs ne communiquant généralement avec le contrôleur que par l'intermédiaire d'un unique canal de transfert de données et les requêtes ne pouvant donc être traitées que de manière séquentielle (et non parallèle), les gains de performances que l'on pourrait attendre d'une solution « contrôleur » se révèlent dans la pratique être assez minces.

5.6.1.2 RAID niveau 1



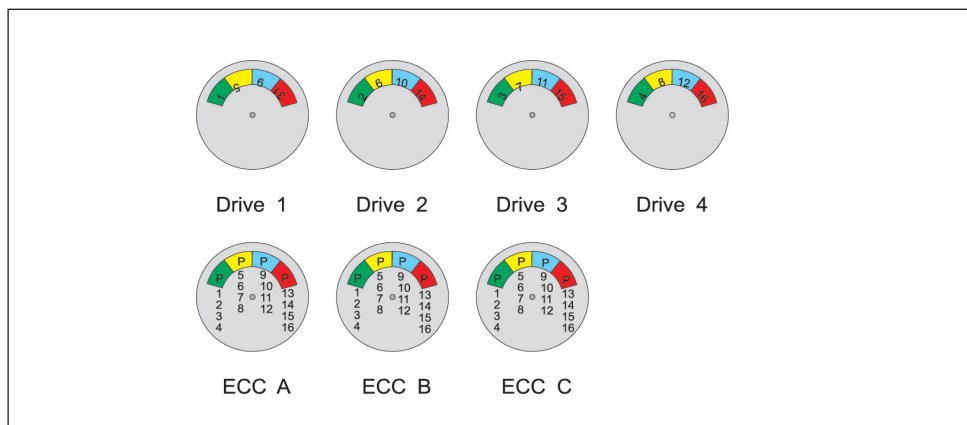
RAID 1 définit la technique du disque miroir (mirroring). Le principe consiste à dupliquer toutes les données d'un disque sur tous les autres disques du set RAID. Avantage : en cas de défaillance d'un disque, les données restent disponibles. Les performances en écriture restent comparables à celles d'un disque classique ou d'un système RAID 0 (pour autant que les disques soient répartis sur les canaux), si l'on part du principe que la charge supplémentaire du système causée par la double écriture n'a pas d'importance.

Dans le meilleur des cas, il est même possible de doubler les vitesses en lecture par la répartition des requêtes de lecture sur deux disques (ou deux sets), qui peuvent lire les données de façon indépendante.

Mais, RAID 1 est une technique onéreuse et seule la capacité d'un disque dur est à la disposition des données originales, le reste est réservé aux données redondantes. RAID 1 est très simple à implémenter.

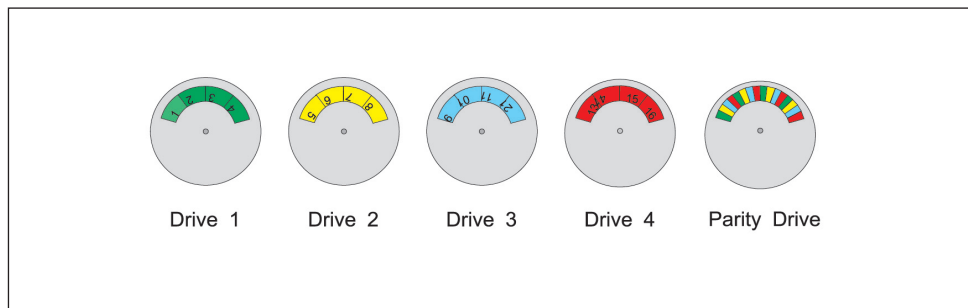
Le mirroring (de disques isolés) est disponible sous forme solution logicielle ou matérielle (contrôleur de disques) pour différents systèmes d'exploitation.

5.6.1.3 RAID niveau 0+1



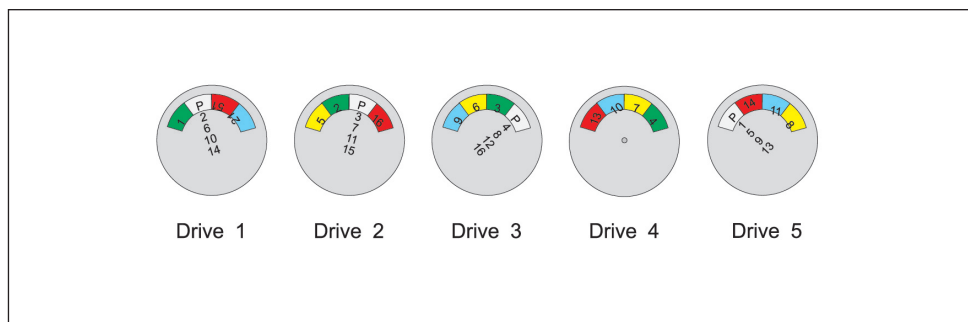
RAID 0+1, parfois aussi appelé RAID 10, associe les techniques du mirroring et du striping. La moitié de la capacité totale est effectivement miroitée. La haute sécurité du système est ici comparable aux performances de RAID 0. Dans la plupart des cas, cette solution RAID est également la plus rapide, mais là encore l'argument utilisé à l'encontre de RAID 1 s'applique : le coût de cette solution est élevé, puisqu'elle exige un doublement du nombre des disques durs.

5.6.1.4 RAID niveau 4



Alors qu'avec RAID 1 et RAID 0+1, la sécurité contre les pannes exige le doublement du nombre des disques durs et qu'avec RAID 0, elle n'est absolument pas assurée, RAID 4 fait appel au concept de parité pour améliorer la sécurité. Pour chaque groupe de x disques durs traités par la technique du striping, on ajoute seulement un disque supplémentaire sur lequel le n -ième bit est en fait le bit de parité formé à partir de chacun des n -ièmes bits de l'ensemble des x autres disques. Lorsqu'un disque dur tombe en panne, son contenu peut être reconstitué, bit pour bit, à partir des $(x-1)$ autres disques et du disque de parité. L'écriture de données implique automatiquement l'actualisation du disque de parité. Cette opération exige la lecture des deux blocs. À partir des données lues et des nouvelles données, la nouvelle valeur du bit de parité pourra être calculée. La rapidité est donc inférieure à RAID 0 ou RAID 1.

5.6.1.5 RAID niveau 5



Avec RAID 4, l'accès au disque de parité est nécessaire pour chaque accès en écriture. Ce disque se révèle rapidement être le goulot d'étranglement du système. Selon RAID 5, les données tout comme les indicateurs de parité, sont répartis par blocs sur l'ensemble des disques physiques. Chaque disque joue en sorte le rôle de disque parité pour une zone de blocs déterminée. Il en résulte

une amélioration des accès en lecture et en écriture, puisque les requêtes et accès physiques sont répartis sur plusieurs unités.

Par contre, pour de petites requêtes et en se basant sur le nombre d'accès par unité de temps et par méga-octet, un ensemble RAID 5 est largement moins performant qu'un disque dur isolé.

5.6.1.6 Autres niveaux RAID

En complément des niveaux RAID exposés ci-dessus (définis par l'Université de Berkeley et considérés comme quasi standard), il existe de nombreuses versions élaborées par les constructeurs de matériels, mais qui ne sont en fait que des modifications de la version exposée ci-dessus.

Dans quels cas faut-il implémenter RAID ? Il existe deux possibilités : l'application de RAID est confiée soit au contrôleur situé entre l'ordinateur et les disques (comme carte dans l'ordinateur ou dans un boîtier séparé), soit implantée au niveau de l'ordinateur même. Avantage de la première solution : l'ordinateur est déchargé de l'administration du RAID. Avantage de la deuxième solution : on évite le passage de toutes les données par le point d'engorgement que constitue le contrôleur RAID, ce qui permet des débits plus importants découlant de l'utilisation simultanée de plusieurs accès de transferts.

Un certain nombre de constructeurs de disques et de contrôleurs proposent des ensembles RAID. Ces systèmes diffèrent les uns des autres au niveau des caractéristiques techniques suivantes :

Une implémentation simple de RAID consiste à rattacher plusieurs disques durs à un bus SCSI et à les gérer par une logique du type RAID ou par un concept similaire. D'autres versions proposent des solutions où chaque disque dispose de son propre contrôleur. Cela a pour effet de sécuriser l'ensemble car même lors d'une défaillance du contrôleur, les données restent accessibles. Les disques durs peuvent être montés de façon fixe. Il est cependant préférable, même si cette solution est plus onéreuse, de monter les disques isolés de telle sorte qu'ils puissent être remplacés, même sous tension afin que l'accès aux données ne soit pas interrompu (hot swap). Les ensembles RAID les plus performants savent reconstruire les données (après un échange de disque) sans interrompre l'exploitation normale de l'ensemble.

La sécurité d'un ensemble RAID dépend aussi d'autres éléments. C'est ainsi que l'alimentation joue un rôle primordial : lorsque tous les disques dépendent d'une alimentation secteur unique, la probabilité de défaillance (mais pas nécessairement la probabilité de perte de données) est plus élevée qu'en présence d'une alimentation séparée pour chaque disque ou d'une alimentation redondante. En extrapolant ce raisonnement, il paraît logique de dupliquer d'autres composants de l'ensemble RAID tels que le câble, le contrôleur et les autres connecteurs.

Une dernière mise en garde : d'après la fréquence et la probabilité des pannes, on part du principe que les pannes de disques durs sont statistiquement indépendantes les unes des autres. En pratique,

force est de constater que les choses se passent différemment : c'est le plus souvent un événement externe (pic de tension, foudre,...) qui est à l'origine d'une augmentation ponctuelle du risque de défaillance sur plusieurs composants. Cela remet en cause la notion même de MTBF pour un système RAID.

Même avec un système RAID, assurant un temps moyen élevé entre deux défaillances, il ne faut jamais négliger la copie de sauvegarde : RAID ne protège pas d'une manipulation intempestive d'effacement ou d'une erreur de logiciel, qui détruit les données. Les virus, le cheval de Troie et les bombes ne seront pas évincés par RAID.

5.6.2 Critères de sélection RAID

Les systèmes RAID améliorent l'accessibilité des données mais pas la performance. Leur vitesse est souvent inférieure à celle des disques durs isolés. La mise en œuvre d'un ensemble RAID des niveaux 0 à 5 se justifie pour le stockage de grandes quantités de données, lorsque le nombre d'accès est assez réduit ou lorsque les données sont soumises à des requêtes de transfert importantes. RAID offre une possibilité avantageuse de configurer des mémoires de masse. Pour des données à accès régulier, il est plus efficace d'utiliser des disques durs isolés et sécurisés par l'emploi de la technique du mirroring. Pour l'accès très fréquent aux données, c'est à un disque virtuel (en mémoire RAM) qu'il convient de faire appel. Afin de décharger l'ordinateur, il est préférable d'effectuer l'opération de miroir au niveau du contrôleur ou de l'adaptateur CPU. Afin d'obtenir d'un taux de transfert élevé pour de longs transferts, le striping devrait autoriser plus de chemins de données vers l'ordinateur et être basé dans le CPU.

Dans tous les cas, le branchement d'un RAID (et d'un ordinateur) à un onduleur est vivement recommandé, afin d'assurer en permanence la disponibilité absolue des données.

5.6.3 Implémentations RAID

Les disques durs peuvent être connectés de trois manières différentes à un RAID : par un logiciel RAID, par un contrôleur RAID dédié monté dans l'ordinateur ou en système RAID externe, considérés par les contrôleurs standard comme disques durs normaux, même s'il sont inhabituellement volumineux.

5.6.3.1 RAID logiciel

Windows, Solaris, Linux et bien d'autres systèmes d'exploitation offrent déjà la possibilité en standard de rassembler plusieurs disques dans un système RAID. Il suffit que les disques durs soient reliés de façon interne ou externe à un adaptateur SCSI. La configuration s'effectue alors via le système d'exploitation, comme Windows NT. Cette solution est peu onéreuse et simple à installer mais présente également des désavantages. Elle influence la performance du système, notamment lorsqu'il s'agit de transmettre de grandes quantités de données ou lorsque les accès au RAID sont

faits simultanément par plusieurs utilisateurs (sur réseau par exemple). La totalité des opérations de calcul (répartition sur les différents disques durs et calcul de la parité) est prise en charge par le processeur de l'ordinateur ce qui pourra éventuellement ralentir le système. Un autre inconvénient est le fait que le système d'exploitation de l'ordinateur est chargé via un disque de démarrage, qui ne peut être redondant, puisque la configuration RAID n'est disponible qu'une fois le système d'exploitation chargé. De plus, toutes les données relatives à la configuration RAID sont stockées sur ce disque de démarrage. Si ce dernier venait à tomber en panne, le système RAID ne serait plus opérationnel. Les solutions matérielles RAID suivantes, munies d'un contrôleur séparé, permettent de contourner cet handicap.

5.6.3.2 Matériel RAID interne avec contrôleur RAID PCI

Dans ce cas le contrôleur RAID se charge de la totalité des opérations de calcul, à l'identique d'un RAID externe. Ainsi les contrôleurs travaillent indépendamment de la charge CPU et de façon constante. Les données relatives à la configuration RAID se trouvent sur tous les disques durs du système RAID et sont ainsi protégées même si l'un des disques ou le contrôleur venait à tomber en panne. Lors de l'échange du contrôleur ou d'un disque les données de configuration RAID sont reconstruites grâce aux informations stockées sur les disques.

Les contrôleurs RAID sont équipés de prises de connexion internes et d'une connexion externe pour les disques durs SCSI. Cela permet de raccorder les disques durs du système RAID directement à l'ordinateur ou en externe.

5.6.3.3 Matériel RAID externe

Les RAID matériels représentent la solution RAID dite de haut de gamme. Ici, les contrôleurs et les disques durs sont logés dans un boîtier externe autonome par rapport à l'ordinateur. La connexion à l'adaptateur du CPU est assurée par un câble SCSI ou FC.

Le "Backplane", sur lequel le contrôleur et les disques durs sont directement connectés, présente l'avantage de disposer d'un câblage très court et offre ainsi une sécurité de données élevée. L'utilisation d'un contrôleur redondant augmente encore cette sécurité. Dans ce cas, lorsque le contrôleur primaire tombe en panne, l'ensemble RAID commute automatiquement sur le second contrôleur, sans perte de temps et de données. Le contrôleur défectueux peut alors être remplacé en cours de fonctionnement.

Les RAID matériels travaillent, comme le contrôleur RAID PCI, avec une performance constante, indépendamment de la charge CPU. Les données de l'adaptateur SCSI sont directement transmises au contrôleur RAID via le bus SCSI. La totalité des données est alors chargée dans le cache afin de libérer au maximum le bus. Le contrôleur du RAID matériel répartit les données sur les différents

disques et calcule la parité en fonction du niveau RAID choisi. Pendant ce temps, le CPU du système n'est pas encombré par les opérations de l'ordinateur du système RAID. Un cache, de taille suffisamment grande, configuré en tant que cache Write-back, peut contribuer à augmenter considérablement la performance en écriture. La lecture des données se fait de façon identique dans le sens inverse. Comparés aux contrôleurs PCI RAID, les matériels RAID peuvent être installés via la plate-forme.

5.6.4 RAID IDE

Un nombre sans cesse plus élevé de systèmes RAID externes est exploité en interne avec des disques durs IDE (ATA). Ils sont connectés à l'ordinateur via SCSI ou Fibre Channel.

Les RAID IDE répondent à la définition originale de RAID en tant que "Redundant Array of Inexpensive Disks", avec un accent sur "inexpensive" (peu coûteux).

Plus tard, il devint normal de lire "independent disks" (disques isolés) au lieu d'"inexpensive disks", car le concept "peu coûteux" était difficilement compatible aux systèmes RAID très chers à l'origine.

Pourtant le concept se trouvant derrière RAID était : l'utilisation de disques bon marché avec une faible durée de vie est compensée par la redondance du système.

Bien entendu, personne n'utilisera un RAID IDE dans les situations nécessitant des performances élevées. En effet, le débit de données lors de l'écriture ou de la lecture de grands fichiers est entre-temps devenu impressionnant, ce qui n'est pas le cas du débit E/S. Pour les banques de données, les disques IDE sont trop lents. (Cela ne changera pas non plus avec la première génération d'ATA série, mais seulement quand des caractéristiques SCSI comme le Command Queuing seront intégrées dans le standard).

Même dans les réseaux de stockage basés sur Fibre Channel (Storage Area Network), seule une partie de la capacité en données est utilisée pour les banques de données. Il existe aussi une demande en serveurs de fichiers, en serveurs Email, en archives et autres réseaux de stockage. Les coûts peuvent être réduits de manière drastique lorsque plusieurs serveurs se partagent un RAID tel qu'un RAID IDE. Les banques de données et les autres applications intensives en E/S ont alors de la place sur les RAID Fibre Channel bien plus coûteux.

Une autre application idéale pour les RAID IDE avec interface FC est aussi due au prix réduit : la sauvegarde Near-Line devient aussi abordable sur disques durs grâce au faible coût par Go et est bien entendu beaucoup plus rapide que sur cartouche ou librairie (magnético-)optique. Un argument d'importance primordiale là où les fenêtres de sauvegarde sont de plus en plus courtes.

6. Réseaux de stockage

6.1 Guide : Centralisation de stockage

Alors qu'au cours des dernières années de plus en plus de solutions Mainframe ont été remplacées par des serveurs locaux et des stations de travail nous assistons aujourd'hui de nouveau à une centralisation des serveurs et des ressources mémoire qui y sont liées. La raison est l'utilisation de technologies de bus toujours plus rapides mais aussi, et avant tout, la mise en réseau toujours plus élevée des données.

Evidemment, la centralisation de la mémoire impose des exigences élevées au niveau de la disponibilité. Comme une défaillance peut immobiliser toute une entreprise, il est indispensable que chemins de données et même mémoires soient redondants.

La disponibilité d'un système est mesurée en pourcentage. Une disponibilité de 99,9 % signifie une défaillance moyenne annuelle de 8,8 heures et 99,99 % une défaillance moyenne de 53 minutes, et ainsi de suite.

Un avantage prépondérant lors de la création d'un réseau de stockage est la possibilité d'utilisation simultanée d'un système de stockage (par ex. RAID) par plusieurs serveurs. Les serveurs se partagent la capacité de stockage des données et réduisent ainsi aussi bien les coûts d'achat que l'administration. Ce processus est appelé "consolidation matérielle".

La centralisation des solutions de stockage impose la mise en oeuvre de technologies de réseaux adéquates.

Des technologies mettant les données à disposition y compris à de grandes distances remplacent les Direct Attached Storage (DAS), autrement dit la mémoire directement rattachée aux serveurs individuels via SCSI ou Fibre Channel. Cela peut signifier l'utilisation de Network Attached Storage (NAS). Les systèmes de fichiers sont mis à disposition à d'autres serveurs ou aux clients via le réseau.

D'un autre côté, pour des quantités de données plus importantes et pour assurer des performances plus élevées, une autre technologie qui livre les données à l'ordinateur au niveau des blocs, autrement dit comme un disque local, est souvent privilégiée. Cela a lieu dans les réseaux de stockage (SAN) qui utilisent soit la Fibre Channel rapide ou, depuis peu, quand la vitesse n'est pas la priorité absolue, iSCSI. Dans ce cas, les données SCSI sont transportées via Ethernet. Il s'agit généralement d'un Gbit Ethernet. Un pilote installé sur l'ordinateur laisse la carte Ethernet apparaître comme un contrôleur SCSI.

6.2 Storage Area Network (SAN)

Le LAN permet d'accéder à des systèmes locaux, disposant de protocoles de communication tels TCP/IP, NFS, HTTP. Les LAN sont utilisés pour transmettre des données entre les différents systèmes hôtes et permettre l'accès utilisateur à des systèmes, tels que les stations de travail, les terminaux et les autres appareils. Les LAN manipulent le flux d'informations entre les systèmes hôtes et l'utilisateur. Par contre, SAN permet de partager le flux d'informations avec l'ensemble de l'environnement, c'est-à-dire entre l'ordinateur et les unités de mémoire et finalement entre les unités de mémoire elles-mêmes. Tous les ordinateurs connectés au SAN peuvent donc interpellier les unités de mémoire. Tous comme dans les réseaux LAN Ethernet, FDDI, ATM et Token Ring, il existe aussi avec SAN différentes topologies, pour élaborer un tel Storage Area Network.

Storage Area Network sont des réseaux de mémoire spéciaux, qui relient des serveurs et des systèmes de mémoire par des réseaux de larges bandes. Dans ce réseau, un système d'exploitation installé sur un serveur n'a aucune importance. En d'autres termes, plusieurs serveurs différents peuvent accéder à différents systèmes de mémoire dans un seul réseau. En principe, un simple câble ou deux suffisent pour constituer un Storage Area Network. La technologie SCSI est la méthode la plus connue pour constituer un Storage Area Network dans la forme la plus simple. En raison des restrictions importantes, comme le nombre d'appareils, les distances, les terminaisons, etc., la technologie Fibre Channel est actuellement le support de communication normalement employé pour les SAN. En effet, ces caractéristiques en font un excellent support. Les exigences d'un SAN sont une largeur de bande garantie (vitesse du réseau) et un faible taux d'erreur.

La Fibre Channel offre les avantages suivants :

- Débit de données de 400 Mo/s
- Largeur de bande de 2,0625 Gbit
- 16 millions d'appareils peuvent être interpellés
- Connexion série à encodage 8/10 bits
- Protocole de connexion entre les interfaces, basé sur le matériel
- Configuration flexible de câbles, cuivre ou fibre de verre, distance maximale de 10 km.

Actuellement les taux de transfert de données du Fibre Channel sont en cours d'amélioration, de telle sorte qu'à court terme, ces taux passeront à 4 Gbit et 10 Gbit. Vous pouvez lire d'autres informations sur le Fibre Channel au chapitre Fibre Channel.

Le SAN décharge le LAN, car l'ensemble de l'échange des informations se déroule dans ce réseau mémoire. Si on relie également un lecteur de sauvegarde au SAN et non au LAN et en utilisant un logiciel adéquat, le LAN sera encore plus déchargé. Cela simplifie la gestion des systèmes et garantit des taux de transfert de données plus élevés. Storage Area Network offre la possibilité idéale de centraliser l'ensemble des informations.

La manière la moins compliquée de constituer un Storage Area Network est la connexion point par point via le Fibre Channel. On relie ainsi par exemple un système RAID avec un ordinateur. Pour cela, il suffit de disposer d'un adaptateur hôte (HBA), d'un câble et d'un sous-système Fibre Channel (RAID etc.) et d'une prise Loopback comme terminaison afin de refermer la boucle interne. La simple connexion par câble facilite considérablement l'installation par rapport au SCSI.

Un système plus important est instauré en forme d'anneau via des commutateurs. Cette topologie en anneau est appelée FC-AL et relie plusieurs ordinateurs à plusieurs unités de mémoire. Le FC-AL (Fibre Channel Arbitrated Loop) permet de répartir les appareils, les lignes et le temps utilisateur. Fibre Channel ne nécessite pas forcément un conducteur à fibre optique, mais peut également être réalisée avec un simple câble de cuivre. Le seul désavantage du cuivre réside dans la faible distance qu'il peut couvrir (env. 30 m).

Logiciel SAN

Nous n'avons jusqu'à maintenant traité que l'aspect matériel du SAN. Pour pouvoir répartir les données sur des unités de stockage communes, un logiciel SAN spécifique est toutefois nécessaire. Ce logiciel exploite les réseaux mémoire et permet une répartition des fichiers sur les sous-systèmes de mémoire. Chaque système, indépendamment du système d'exploitation utilisé, peut ainsi à tout moment accéder à l'unité de mémoire et appeler les données. C'est pourquoi on parle d'un système d'exploitation SAN, qui ne repose en fait que sur un système d'exploitation "normal". Les sociétés, telles Veritas, Mercury ou SANergy offrent des logiciels SAN, qui créent des écritures miroir dans le réseau mémoire, qui synchronisent et activent l'unité de mémoire miroir en cas de panne, alors que les applications sont en ligne.

Grâce à ce logiciel, vous pouvez modifier le volume des applications, de manière dynamique et sans interruption. Vous pouvez aussi affecter des unités mémoire ou un groupe d'unités mémoire ainsi qu'un serveur. Certaines applications logicielles SAN supportent le clustering, ce qui garantit une meilleure disponibilité des données à l'intérieur du réseau de mémoire. Avec le clustering, les unités de mémoire ne sont pas explicitement affectées à un serveur particulier, sauf si configuré dans les droits, de telle sorte que l'unité de mémoire soit quand même accessible via le chemin de la sauvegarde en cas de panne du serveur, ou s'il est affecté à un autre serveur.

Un logiciel n'est donc pas absolument nécessaire pour constituer un réseau SAN qui fonctionne. Seules les liaisons adéquates entre les ordinateurs et les unités de mémoire doivent en l'occurrence être établies. Les unités de mémoire sont attribuées finalement à l'ordinateur via le système d'exploitation. Pour ce faire, les outils standard intégrés de manière permanente dans le système d'exploitation respectif suffisent largement. Les fonctions plus larges nécessitent un logiciel supplémentaire.

6.3. iSCSI

SCSI Internet, abrégé sous iSCSI, est un standard créé en automne 2002 qui, tout comme Fibre Channel, transmet des données au niveau du bloc et qui laisse apparaître les disques durs et les autres unités d'archivage comme s'il s'agissait d'unités locales. Mais comme Ethernet sera utilisé comme moyen de transport, cela permet d'un côté, d'utiliser le câblage existant, réduisant ainsi les coûts et le travail et d'un autre côté, de parcourir des grandes distances, car il est aussi possible d'avoir recours au Wide Area Network.

Les premiers fabricants tels que Cisco et Adaptec proposent déjà des produits équipés de cette technologie qui pourront, dans les années à venir, remplacer la Fibre Channel dans toutes les solutions où des performances élevées ne constituent pas la priorité absolue.

Au niveau de l'ordinateur, soit iSCSI sera géré par un pilote qui transformera les données SCSI en TCP/IP et les enverra via Ethernet, soit, ce qui est encore mieux, une carte iSCSI dédiée se chargera elle-même de cette tâche en commun avec un TOE (TCP/IP Offload Engine), un accélérateur Ethernet.

Du point de vue de l'archivage, un serveur spécialisé et dédié, dénommé routeur iSCSI, constituera l'interface avec le réseau. A l'avenir, ces serveurs pourront directement être intégrés dans les solutions d'archivage, tout comme les serveurs d'impression le sont dans les imprimantes et les ponts FC dans les librairies.

6.4 Network Attached Storage (NAS, archivage lié au réseau)

Les besoins toujours croissants en mémoire des PC et des réseaux de postes de travail nécessitent de plus en plus la mise en oeuvre de serveurs de fichiers. Auparavant, cela obligeait à l'achat de PC et de postes de travail supplémentaires. Il est aujourd'hui plus simple et meilleur marché de faire appel à des technologies appelées Network Attached Storage. De même qu'un serveur de communication ou d'impression, on utilise un composant réseau spécialement conçu pour une seule tâche : l'accès aux supports de données (disques durs ou CD-ROM).

Les avantages de cette technologie apparaissent immédiatement :

Installation simplifiée : étant donné que Network Storage Server travaille exclusivement comme serveur de fichier, le travail de gestion se limite à attribuer des adresses réseau et à valider l'espace mémoire à disposition des utilisateurs. Cet espace est alors immédiatement accessible à l'ensemble des utilisateurs autorisés du réseau.

Entretien simplifié : comme les serveurs de stockage travaillent avec des protocoles standardisés, aucun travail d'adaptation n'est nécessaire lors du changement de version du système d'exploitation.

Mises à niveau et changement de configuration simples : Grâce à la mise en oeuvre de Network Storage Server supplémentaires, l'espace mémoire peut être étendu ou reconfiguré sans aucune difficulté.

Flexibilité : les serveurs de stockage réseau sont aussi parfaitement adaptés à une mise en oeuvre

en réseaux mixtes du fait de leurs nombreux protocoles issus par exemple d'ordinateurs Windows, Unix et NetWare.

Toutes les données sont disponibles dans chacun des systèmes d'exploitation définis, comme si elles étaient enregistrées sur un serveur du réseau. L'accès aux données s'effectue selon la procédure typique de la plate-forme utilisée. L'utilisateur a l'impression qu'il a accès aux fichiers comme s'ils étaient tous enregistrés sur un serveur de fichiers tournant sous son propre système d'exploitation.

7. Enregistreurs de bandes magnétiques

Les enregistreurs de bandes magnétiques sont de nos jours principalement utilisés pour la sauvegarde de données de serveurs. Les faibles coûts par Go, pour le lecteur et pour les bandes, ainsi que la possibilité de garder les bandes en toute sécurité pendant plusieurs années, sont des éléments déterminants. Alors que les supports optiques, même à l'ère du DVD, sont encore trop chers pour pouvoir être pris en considération comme support de sauvegarde, le stockage de données sur disques Ultra-ATA est plus souvent privilégié grâce à ses coûts de plus en plus faibles.

Les lecteurs de bandes magnétiques enregistrent les données de manière séquentielle au niveau des blocs. De ce fait, leur avantage réside dans l'écriture de gros blocs d'informations dans un courant de données continu. Par contre, les bandes magnétiques ne sont pas un support approprié pour un accès rapide à des fichiers précis ou à des informations enregistrées de manière éparpillée.

C'est la raison pour laquelle la stratégie de sauvegarde est de plus en plus raffinée. Alors que la sauvegarde de données du week end est toujours réalisée sur bandes magnétiques et conservée en sécurité, les enregistrements de données au cours de la semaine sont effectués sur des systèmes RAID IDE. Cela permet la restauration rapide d'un serveur ou d'un fichier au quotidien et garantit en même temps une protection contre les pertes totales grâce aux bandes.

7.1 Processus d'enregistrement de bandes linéaires

7.1.1 Lecteurs LTO

La technologie **LTO** (**L**inear-**T**ape-**O**pen) a été développée conjointement par Seagate, HP et IBM. Ces fabricants ont aussi été les premiers à proposer les lecteurs appropriés. De nombreux autres fabricants ont accordé une licence à cette technologie et proposent également les lecteurs adéquats. Grâce à cette large coopération entre fabricants, la technologie LTO s'est rapidement imposée sur le marché. Le point fort du format d'enregistrement LTO est constitué par plusieurs canaux linéaires, fonctionnant en serpent. Les données sont écrites sur les pistes, qui réclament toute la largeur de la bande.

Deux formats ont été développés : Accelis et Ultrium. Seul le format Ultrium, cependant, a été mis en production. Le format **Accelis** a été défini pour des accès rapides. Le format Accelis utilise deux bobines de bandes et commence l'accès des données au milieu de la bande, pour réduire le temps d'accès au minimum.

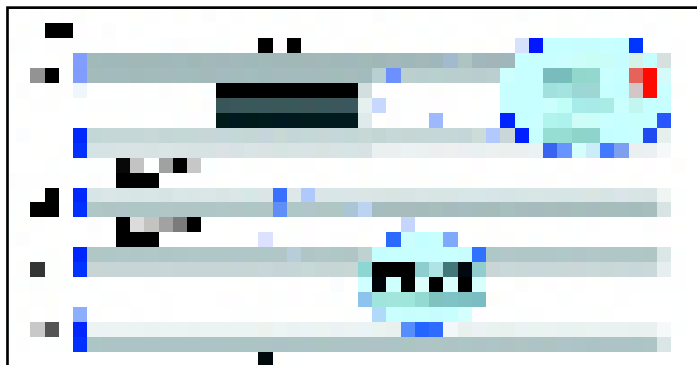
Le trajet jusqu'au début et jusqu'à la fin de la bande est identique. L'avantage de ce principe réside surtout lors de l'écriture ou la lecture de sections de données devant être transmises, il n'a plus aucun effet lorsqu'il s'agit de lire ou d'écrire la bande complète. Une application typique

répondant à ce principe est le HSM (Hierarchical Storage Management), dans laquelle seules quelques données individuelles doivent être lues très souvent. Dans le format Accelis, 256 pistes sont réparties dans deux zones de données. La première génération de ces lecteurs travaillera en compression avec une capacité de 50 Go et un taux de transfert max. de 40 Mo/s.

Le format **Ultrium** est par contre le support optimal pour des grandes capacités et offre une sécurité d'utilisation parfaite dans un environnement automatisé ou standalone. Le support Ultrium ne comporte qu'une bobine de bande et représente une solution idéale pour les programmes de sauvegarde, de récupération et d'archivage.

Le format Ultrium répartit 384 pistes sur quatre zones de données. Entre les zones de données sont constituées des servopistes destinées au positionnement de la tête. Le processus d'écriture sur la bande s'effectue en forme de serpent et sur respectivement huit pistes parallèles. Les données sont écrites à partir de l'intérieur vers l'extérieur, car les zones de données intérieures sont physiquement mieux protégées. La première génération propose une capacité de 200 Go avec compression des données et un taux de transfert maximum de 30 Mo/s. La deuxième génération disponible depuis 2003 offre une capacité et une vitesse deux fois plus importantes.

Ces deux types de cartouches sont équipées d'une mémoire-cartouche sans contact (LTO-CM) de 4 Ko, dans laquelle les informations fabricant et utilisateur sont sauvegardées. La lecture et l'écriture des informations utilisateurs nécessitent le soutien d'un logiciel de sauvegarde.



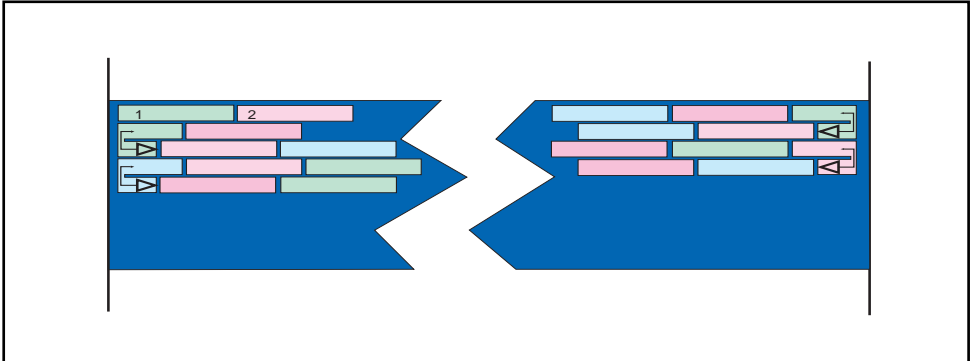
Enregistrement sur piste avec lecteurs LTO

7.1.2 Lecteurs DLT/SDLT

La technologie **DLT (Digital Linear Tape)** fonctionne comme pour la technologie LTO selon le principe de l'enregistrement des données en "linéaire serpenté", de telle sorte que les pistes soient parallèles au bord de la bande. Les bandes magnétiques utilisées sont des bandes 1/2 pouce, logées dans une cartouche compacte. Les trois dernières générations de lecteurs DLT4000, DLT7000 et DLT8000 exploitent le même support DLTtapeIV et atteignent des capacités de sauvegarde

comprimées de 40, 70 et 80 Go.

Jusqu'à présent les données étaient écrites par deux canaux logés au sein des têtes de lecture et d'écriture avec une densité de 62.500 bits/pouce et un taux de transfert de 3 Mo/s. Une unité de donnée se composait de vingt blocs de 4 Ko tous pourvus d'une multitude de procédures prévues pour la reconnaissance d'erreurs (Parity, Cyclic Redundancy Check CRC et Error Detection Check EDC). Les quatre derniers blocs de chaque unité se composent de 4 blocs ECC (ECC error correction check). Avec le nouveau procédé Super DLT, les données sont écrites par quatre canaux logés dans les têtes de lecture et d'écriture, avec une densité de 86.000 bits/pouce. Le taux de transfert s'en trouve nettement élevé et passe à 5 Mo/s. L'unité de données se compose de vingt-quatre blocs de 4 Ko. Ceux-ci sont aussi pourvus de reconnaissance d'erreurs. Les cinq derniers blocs sont des blocs ECC. Une fois l'écriture achevée, le contrôleur DLT fait un test de lecture. Les données écrites sont comparées avec le contenu de la mémoire tampon et corrigées en cas d'erreur. Ces dispositifs de sécurité garantissent une intégrité très élevée au niveau des données.



Enregistrement sur piste avec lecteurs DLT

Un autre avantage de cette technologie réside dans le fait que les bandes et les têtes d'écriture sont moins sollicitées. Ceci, grâce à l'utilisation de têtes magnétiques stationnaires et un entraînement de bande moins complexe. Ainsi les lecteurs DLT permettent de faire passer jusqu'à 500.000 cycles par cartouche. Grâce à la technologie la plus récente, décrite plus haut, les bandes DLTape IV supportent même plus d'un million de cycles.

En 2001, Quantum lança le premier lecteur SuperDLT sur le marché, qui, grâce à la nouvelle technologie, peut d'atteindre une capacité de 220 Go avec un taux de transfert de données de 22 Mo/s (en compression 2:1). Des bandes de meilleur revêtement sont certes nécessaires, mais la taille des cartouches reste la même. Les systèmes sont compatibles en lecture avec DLT8000, DLT7000 et DLT4000, ce qui représente le principal argument de vente de SuperDLT par rapport au LTO. Depuis mi-2002, la deuxième génération de lecteurs SuperDLT, SDLT320, est disponible avec une capacité de 320 Mo et un taux de transfert de 32 Mo/s (en compression 2:1).

Le format DLT VS a été lancé en 2000 pour compléter la gamme de produits DLT vers le bas. La génération VS-160 actuelle peut écrire sur une bande avec une compression de 2:1 jusqu'à 160 Go avec un taux de 16 Mo/s.

7.1.3 Lecteurs ADR

La technologie **ADR** (**A**dvanced **D**igital **R**ecording) a été mise au point par Philips et est utilisée dans les lecteurs OnStream. Les données sont enregistrées sur huit pistes parallèles. Les servo-informations se trouvant entre les pistes de données assurent le positionnement exacte de la tête.

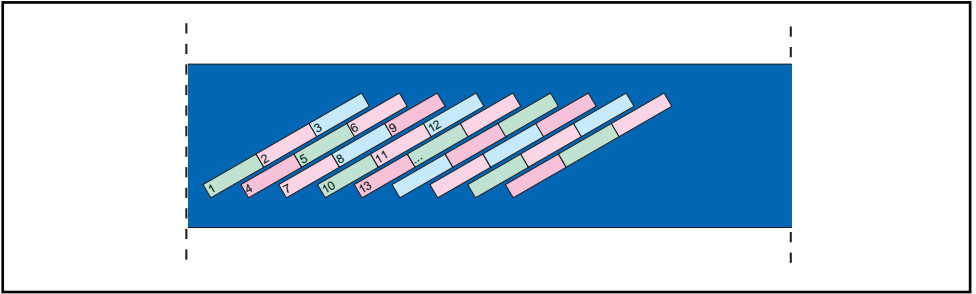
Elles servent également à reconnaître des zones défectueuses de la bande. Les lecteurs ADR offrent un transfert de données variable, de 0,5 à 2 Mo/s, ce qui leur permet de s'aligner sur le taux de données du système et d'éviter largement les longues durées de nouveau positionnement de la bande. Les lecteurs ADR offrent en compression une capacité atteignant 50 Go par cartouche et un taux de transfert max. de 4 Mo/s.

7.2 Processus d'enregistrement de piste diagonale

7.2.1 Lecteurs Exabyte

Grâce à la technique Helical-Scan, les lecteurs de bandes magnétiques des domaines audio et vidéo peuvent atteindre des densités de données impressionnantes. Les têtes de lectures rotatives enregistrent les données sur les pistes disposées en biais par rapport au sens de rotation. Cette disposition originale des pistes permet l'enregistrement des données à une densité très élevée. Les périphériques de sauvegarde, basés sur ce principe et adaptés aux besoins exceptionnels en sauvegarde de données, ont gagné de grandes parts de marché dans le domaine des lecteurs de sauvegarde.

Les lecteurs Exabyte sont issus de la technique vidéo8 et ont été spécialement améliorés pour permettre une utilisation comme périphériques de sauvegarde. Leur technique d'enregistrement a été nettement améliorée. Grâce au volume de données important qu'il est possible de stocker avec un lecteur Exabyte sur une cartouche (max. 40 Go avec cartouche de 170 m avec Exabyte Mammoth), le prix de revient par Go ne cesse de baisser. De par leur faible encombrement, l'envoi postal et le stockage de ces cartouches ne posent aucun problème. De plus, les cartouches les plus récentes autorisent le stockage longue durée. Les fabricants garantissent une durée d'archivage de 10 ans.



Enregistrement sur piste avec lecteurs Helical-scan (DAT, Exabyte, AIT)

7.2.2 Lecteurs DAT

La technologie **DAT (Digital Audio Tape)** est également issue du domaine de l'enregistrement numérique dans le domaine audio et enregistre les données sur bande magnétique selon le procédé Helical-Scan. Un des avantages de la technologie DAT (4 mm) par rapport à Exabyte (8 mm) est l'enroulement moindre de la bande autour de la tête de lecture (90 degrés avec un DAT par rapport à 112 degrés avec un lecteur Exabyte), ce qui permet un allègement de tension de la bande et une mécanique plus simple.

Le format **DDS (Digital Data Storage)** a été mis au point par Sony et HP et s'est imposé comme standard. La concurrence sur ce marché profite largement aux utilisateurs qui voient apparaître sur le marché des techniques de plus en plus performantes. Les lecteurs correspondant au standard DDS-2 ont une capacité de sauvegarde pouvant atteindre 8 Go (120 m Band) avec des taux de transfert jusqu'à 1 Mo/s. La capacité de 8 Go représente une valeur typique avec compression de données de 2:1. En théorie, ces lecteurs peuvent sauvegarder jusqu'à 16Go de données. Ces capacités ne sont cependant pas réalisables dans la pratique.

Les lecteurs, en format DDS-3, peuvent enregistrer jusqu'à 24 Go sur une bande de 125 m avec un taux de transfert de données de 2 Mo/s. Le standard DDS-4 offre en compression, des capacités atteignant 40 Go (bande 150 m) et un taux de transfert max. de 6 Mo/s. Il reste compatible avec DDS-2 et DDS-3. Les lecteurs DDS-3 disposent de caractéristiques spéciales permettant une sauvegarde très fiable.

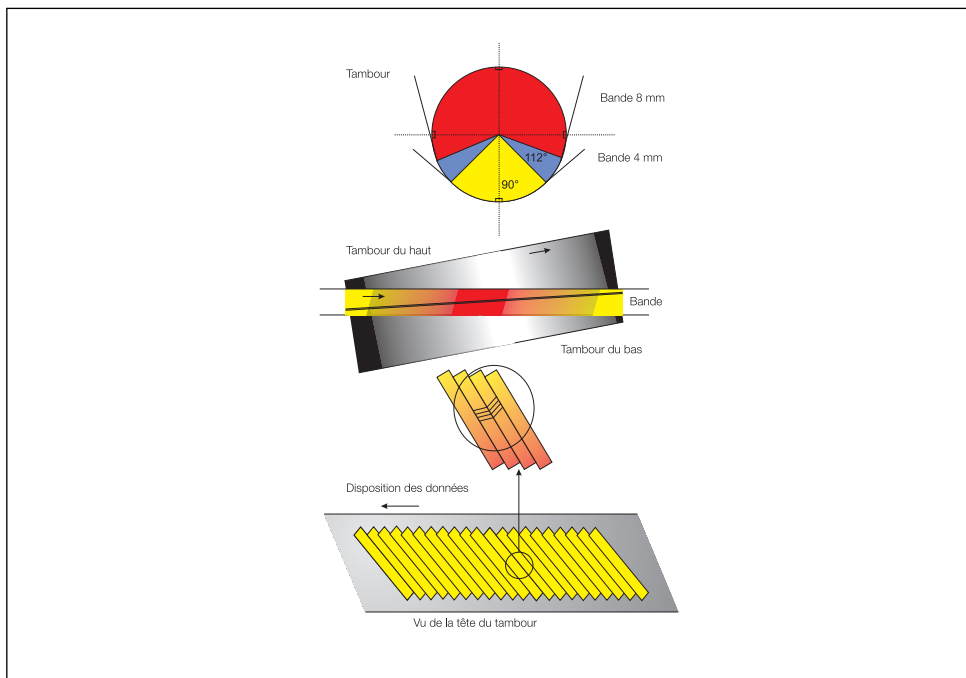
Les premiers modèles de la 5ème génération de lecteurs DDS de Hewlett-Packard et de Seagate sont attendus pour mai 2003. Avec une vitesse pratiquement identique aux DDS-4, ils offrent une capacité native de 36 Go quasiment doublée. Les cartouches correspondantes auront une longueur de 175 mètres. Les lecteurs DAT72 seront toutefois compatibles en lecture et écriture avec les supports DDS-3 et DDS-4.

Une tête de lecture sale ou poussiéreuse est souvent source d'erreur. Le système de nettoyage automatique **Head Cleaner** nettoie automatiquement les têtes toutes les 15 minutes. En combinant

ce système avec une bande de nettoyage, le lecteur fonctionnera correctement pendant de nombreuses années.

Si la bande est endommagée, trop ancienne ou lorsque la bande de nettoyage ne peut plus être utilisée, l'administrateur du réseau reçoit immédiatement une information. Cette caractéristique s'appelle **TapeAlert** et est un nouveau logiciel développé par HP, qui diagnostique les problèmes sur les supports de données au niveau du réseau. De plus, TapeAlert surveille en permanence l'état du lecteur et des supports pendant la sauvegarde.

La fonction de "**Time Tracking**" permet de positionner la tête de lecture au milieu de la piste de données. Cela garantit une lecture fiable de bandes écrites même avec des lecteurs DAT provenant d'autres fabricants. Une caractéristique spéciale des lecteurs DAT d'HP est l'**OBDR** (**O**ne **B**utton **D**isaster **R**ecovery). Un logiciel approprié produit des cartouches de démarrage, qui permettent, en cas d'urgence, de rétablir le système sans avoir besoin de disquettes ou de CD-ROM supplémentaires.



Enregistrement de données Helical-Scan

Il existe pour les lecteurs DAT, comme pour tous les autres lecteurs de bandes, des changeurs de cartouches automatiques. Les modèles les plus simples procèdent au changement séquentiel des cartouches. Les modèles plus chers (« Random-Access ») nécessitent normalement un logiciel adéquat afin de pouvoir utiliser les bibliothèques de bandes (Libraries en anglais). Les bibliothèques de bandes ainsi que les changeurs de cartouches les plus petits sont prévus pour six cartouches et les modèles plus grands sont en mesure d'accueillir plus de 100 cartouches. Ces Jukebox permettent de stocker des données sans l'intervention d'un opérateur.

Il est conseillé d'utiliser uniquement les cartouches DAT conçues spécialement à des fins de sauvegarde. Ces cartouches portent le label DDS pour les lecteurs DAT, et le label D-Eight pour les lecteurs Exabyte. Comme pour tous les lecteurs de bandes magnétiques, il est recommandé de nettoyer régulièrement les têtes d'écriture et de lecture. Il est également conseillé d'utiliser les kits de nettoyage recommandés par le fabricant. Des bandes de nettoyage inadéquates peuvent entraîner des dommages au niveau du mécanisme. En général, il est recommandé de faire un nettoyage après 30 Go ou au moins une fois par mois.

7.2.3 Lecteurs AIT

Les lecteurs **AIT** (**A**dvanced **I**ntelligent **T**ape) ont été lancés sur le marché en 1997 par Sony. Comme Exabyte, basée sur la technologie Heli-Scan, cette technologie est incompatible avec les formats de lecteurs 8 mm précédents, ne serait-ce qu'à cause du format de cartouche différent. La capacité maximum de ces lecteurs est actuellement de l'ordre de 260 Go (100 Go sans compression). Un nouvel algorithme (ALDC-Advances Lossless Ddate Compression) permet d'obtenir des améliorations au niveau du format de compression (env. 2,6). Tout comme un lecteur DAT, ce type de lecteur peut être logé dans un emplacement 3,5". Un nouveau processus d'autonettoyage a été mis au point, réduisant sensiblement la fréquence d'utilisation des cassettes de nettoyage en environnements bureautiques normaux et augmentant la durée de vie des cartouches et des lecteurs.

Lors d'erreurs importantes, le nettoyeur intégré dans la tête est activé automatiquement, et les médias AME contribuent aussi fortement à la réduction des intervalles de nettoyage. L'utilisation de puces de mémoire MIC (Memory in Cassette) dans les cartouches constitue une nouveauté intéressante. Leur taille est de 16 kbits avec des supports de 25/65 Go et de 64 kbits avec tous les autres. Ce processeur permet de sauvegarder des informations sur le contenu de la cartouche, alors que dans les autres technologies, cette sauvegarde n'était possible qu'au début de la bande. Le temps d'accès est de l'ordre de 27 secondes lorsque l'on utilise un processeur MIC. Entre temps, tous les fabricants courants de logiciels de sauvegarde supportent les lecteurs AIT.

Avec les lecteurs AIT-3 disponibles depuis l'été 2001, Sony a pénétré la catégorie de performances des lecteurs LTO et SDLT. Le lecteur atteint en compression avec des bandes de 230 m des taux de transfert de 31 Mo/s avec une capacité maximale de 260 Go. Sony poursuivra le développement du format AIT au moins jusqu'en 2005 avec trois nouvelles générations, atteignant le téraoctet.

Une particularité notable est que ces lecteurs sont compatibles en lecture et en écriture avec tous les modèles précédents.

7.3 Autres processus d'enregistrement

7.3.1 Lecteurs QIC

Les cartouches 1/4" sont enregistrées selon une technique en **linéaire serpenté** à haute vitesse et en plusieurs cycles d'une piste, parallèle en partant du bord de la bande magnétique. Ce serpent in doit aussi passer inoccupé lors de la lecture des données.

Les lecteurs de bandes magnétiques 1/4" fonctionnent avec un format **QIC (Quarter Inch Cartridge)** standardisé et enregistrent en mode streaming (sans interruption). Si la vitesse de transmission d'un système est supérieure à la vitesse d'enregistrement du streamer, les données sont stockées sans interruption (streaming) sur la bande. Si le tampon du streamer est vide, il réclame au système d'autres données.

Pour éviter de créer des sauvegardes avec des interruptions dans le cas d'un ordinateur disposant d'une faible vitesse de transfert, la bande est ralentie et est replacée sur la fin de l'enregistrement en cas d'absence temporaire de données à sauvegarder. Le bloc de données suivant peut ainsi être enregistré sans interruption L'un des

avantages de la technologie QIC par rapport à la procédure d'enregistrement hélicoïdal tient dans le fait que la bande reste en permanence dans sa cartouche, ce qui lui garantit une durée de vie bien plus élevée.

7.3.2 Lecteurs Mainframe

Malgré sa technologie "grisonnante", le lecteur de bandes 1/2", reste un support très utilisé, en particulier pour l'échange de données entre gros ordinateurs ("mainframes"). Il est certain qu'à l'avenir ces lecteurs seront graduellement remplacés par de nouveaux périphériques de sauvegarde moins encombrants et surtout moins onéreux. Une bande magnétique 1/2" dispose en règle générale de 9 pistes d'écriture.

Une grande bande magnétique (730 m) permet d'enregistrer 23 Mo pour une densité de 800 bpi (bytes per inch), 46 Mo pour 1600 bpi, 92 Mo pour 3200 bpi et 180 Mo pour 6250 bpi. Comparé aux autres systèmes de bandes magnétiques, disposant d'une capacité de stockage de 10 Go, les performances d'un lecteur 1/2 pouce sont relativement modestes. D'autres inconvénients existent : les temps de sauvegarde et de restauration ainsi que l'encombrement relativement important du lecteur et des cartouches.

7.4 Logiciel pour enregistreur de bandes magnétiques

7.4.1 Logiciel de sauvegarde

Une sauvegarde est indispensable en raison de l'éventuelle perte de données (erreur humaine, défaillance technique, sabotage ou virus). Il est possible de réaliser une sauvegarde sans le support d'un logiciel, cependant pour de grands volumes de données et de l'utilisation de bibliothèques, une sauvegarde n'est presque plus faisable sans logiciel adéquat. Des logiciels facilitent la sauvegarde quotidienne et proposent de nombreux utilitaires permettant la gestion des données à sauvegarder et déjà sauvegardées (archivage et HSM). Les développements exigés des sauvegardes de données engendrent une révision et une amélioration constantes des logiciels existants.

Les besoins en matière de capacités croissent plus rapidement que la capacité des médias. L'acquisition de disques durs en nombre toujours plus élevés occasionne des coûts plus élevés et incite à la mise en œuvre de procédés d'archivage utilisant des médias peu onéreux mais plus lents. Cela entraîne d'un autre côté un travail d'administration important.

7.4.2 Logiciel HSM

Le logiciel **HSM** (**H**ierarchical **S**torage **M**anagement) est en mesure de prendre en charge cette tâche d'administration de façon autonome. En fonction des paramètres fixés, tels que fréquence d'accès, taille et âge des fichiers, les données sont évaluées et, selon les besoins, sauvegardées sur des supports de plus en plus économiques/lents, comme par exemple du disque dur vers une cartouche amovible, puis vers des bandes bibliothèques et enfin vers des bandes externes. Dans le dernier cas, l'administrateur sera averti qu'il doit introduire la bande adéquate.

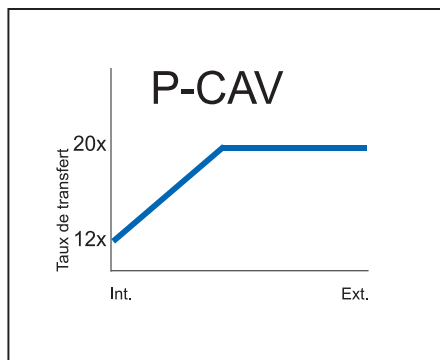
Un système de fichier virtuel montre à l'utilisateur toutes les données, qu'elles soient réellement présentes sur le disque dur ou qu'elles aient été transposées. Lorsque l'on ouvre un fichier, celui-ci est tout d'abord retransféré sur le disque dur. L'utilisateur ne remarque que le ralentissement du temps d'accès. Le temps d'accès requis pourra sembler trop long à certains utilisateurs. Dans le pire des cas, lors d'une transposition sur supports externes, le temps d'attente peut atteindre 30 minutes ou plus. Mais il faut garder à l'esprit que les accès à ces données (80% des données) sont très rares (moins d'un fois par mois). Pas plus de 5% des données sont consultées plus d'une fois par semaine.

8. Mémoires optiques

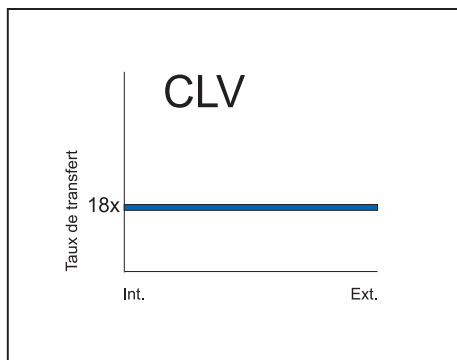
Tout comme les CD-ROM, les disques optiques se sont imposés. Grâce aux nouvelles technologies comme CD-R et CD-RW et à l'augmentation des capacités due au développement de la technologie DVD, ce secteur connaît un véritable essor. Les technologies magnéto-optiques font également partie de ce domaine.

8.1 Lecteurs CD-ROM

Les CD-ROM sont des disques optiques amovibles ne pouvant être écrits qu'une seule fois. Ce média, disposant de 650 Mo, se prête de façon idéale à la distribution massive de données, comme par exemple la distribution de logiciels, car les coûts de reproduction sont réduits. Les inconvénients des CD-ROM, le fait qu'ils ne soient pas réinscriptibles et la lenteur relative de l'accès aux données (actuellement comprise entre 85-120 ms, suivant le lecteur) ne jouent qu'un rôle secondaire. Ce support de données est extrêmement bon marché et la production en masse est rentable à partir de lots de 100. Les données sont gravées, tout comme pour la fabrication d'un disque, dans le matériel de support.



CAV-Technologie



CLV-Technologie

La vitesse de lecture des lecteurs CD-ROM est comparable au taux de transfert d'un lecteur audio, qui est de l'ordre de 150 Ko/s. La vitesse de lecture d'un lecteur 14x est de l'ordre de 2,05 Mo/s. Les lecteurs CD-ROM actuels travaillent avec une vitesse de 52x et un taux de transfert de données de 7,8 Mo/s. Les lecteurs ayant une vitesse de lecture supérieure à 14x sont basés sur la technologie Partial- **CAV** (Constant **A**ngular **V**elocity). Cette technologie se distingue par un taux de transfert variable à vitesse de rotation égale au sein du CD. Lors de la lecture des pistes extérieures d'un CD, le lecteur passe au procédé habituel **CLV** (Constant **L**inear **V**elocity) qui consiste à adapter la vitesse de rotation avant la lecture. Cela permet d'assurer un taux de transfert de données constant. Les lecteurs de CD-ROM actuels disposent, outre l'augmentation de vitesse obligatoire, d'une

nouvelle caractéristique : **Multiread**. Cela signifie que les lecteurs de CD-ROM peuvent lire les CD-RW réinscriptibles.

On trouve maintenant, outre les lecteurs isolés normaux, des chargeurs de CD-ROM. Le temps moyen requis pour un changement de CD est de l'ordre de 7 à 10 secondes. Les changeurs CD-ROM se prêtent surtout aux applications sur CD-ROM, où l'accès au volume important de données est occasionnel, avec accès direct de l'ordinateur (par ex. applications desktop publishing et multimedia). Les changeurs actuellement disponibles sur le marché permettent la gestion, dans une seule unité périphérique, de volume de données atteignant le téraoctet.

8.2 Lecteurs CD-R et CD-RW

Les enregistreurs CD (CD-R) peuvent, sans grand frais, écrire des CD bruts (Write-once CD). Les données sont écrites sur le CD à l'aide d'un faisceau laser. Par ces enregistreurs, la création d'un seul CD est encore économique. C'est ainsi que des CD-ROM contenant des quantités limitées de données, tels que des catalogues de produits, des produits logiciels ou des ensembles de graphiques sont facilement réalisables. Ces CD sont aussi parfaitement adaptés au stockage longue durée. Ce support de données est très sûr, mais une modification ultérieure des données n'est plus possible.

Tout comme les CD gravés en grande quantité, les CD écrits par un enregistreur CD sont lisibles par tout lecteur CD-ROM classique. Les changeurs intégrant un enregistreur CD permettent de réaliser un archivage peu onéreux et de procéder à des sauvegardes dans des réseaux de petite et moyenne taille. Si la production et la copie de CD deviennent une priorité, il existe sur le marché des nouveaux systèmes de duplication de CD, fonctionnant comme des appareils autonomes.

CD-Rewritable (CD-RW) est une nouvelle technologie permettant de réécrire un média jusqu'à 3.000 fois. Les lecteurs peuvent aussi écrire une seule fois sur les médias CD-R. Les CD-RW peuvent être lus par les lecteurs de CD-ROM dotés de la capacité plurilecture que l'on trouve actuellement dans le commerce (voir le tableau des compatibilités).

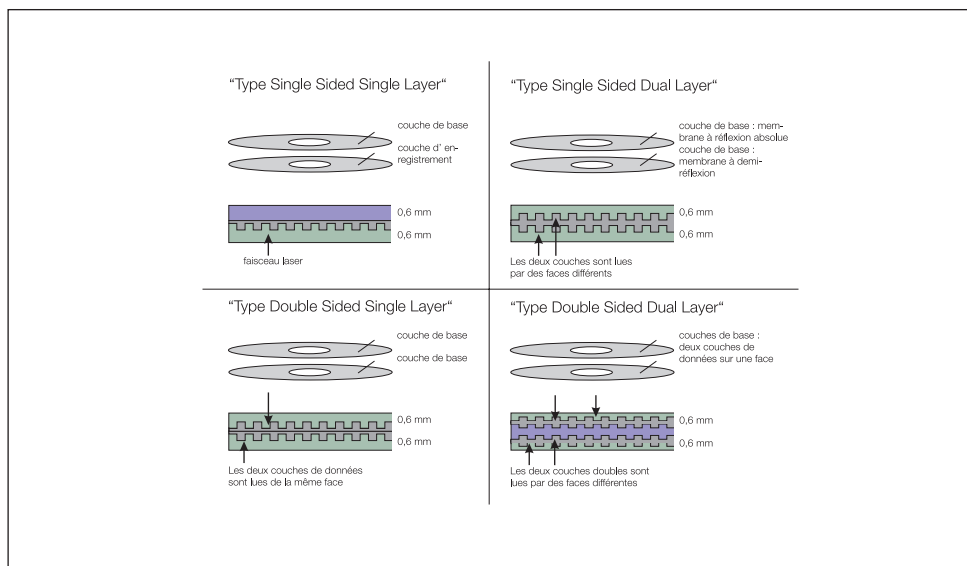
Support	CD-ROM	CD-R	CDRW	DVD-ROM	DVD-R	DVD-RAM	DVD-RW
CD-ROM	R	R	R	R	R	R	R
CD-ROM	R	W/R	W/R	R		R	R
CD-RW	R	W/R	R	R		R	R
DVD-ROM				R	R	R	R
DVD-R				R	W/R	R	R
DVD-RAM						W/R	
DVD-RW							W/R

R = lecture W = écriture

8.3 Lecteurs DVD

Après une longue période où la capacité du CD-ROM était considérée comme suffisante, une nouvelle technologie optique augmentant la capacité des supports à 5,2 Go s'est ensuite développée, sous la pression de l'industrie vidéo avec le **DVD** (**D**igital **V**ersatile **D**isc, auparavant appelé Digital Video Disc). L'utilisation du verso et d'une seconde couche de données devraient bientôt permettre de multiplier par quatre leurs capacités. Cette amélioration de capacité a été réalisée par une diminution de la longueur minimale des pits et une diminution de la distance des spirales du track. Les lecteurs DVD peuvent de plus lire tous les formats CD courants. Les lecteurs-enregistreurs DVD-R sont disponibles sur le marché depuis un certain temps. Mais, leur capacité n'est encore que de l'ordre de 2,6 Go/face.

Le développement du marché des DVD a cependant été freiné par l'absence d'un standard commun à tous les constructeurs. Toshiba, Hitachi et Panasonic ont développé le disque DVD-RAM, caractérisé par une capacité de 2,6 Go par face. Ce système fonctionne avec un caddy. Dans le même temps, Philips, Sony et HP ont concentré leurs efforts sur le disque DVD-RW, un produit offrant une capacité de 3 Go, qui se passe de caddy et pouvant être lu dans les lecteurs DVD à venir. Les lecteurs de DVD-RW sont en plus en mesure de lire le contenu des disques DVD-RW contrairement aux lecteurs DVD-RAM.



Structure d'un support DVD

8.4 Lecteurs magnéto-optiques

La sauvegarde sur disque magnéto-optique, en tant que numéro un de la technique optique, présente certains avantages par rapport aux technologies concurrentes. Les lecteurs de disques magnéto-optiques tracent des données via un laser libre de contact direct et résistant à l'usure, en chauffant et en établissant un champ magnétique sur la surface du disque MO.

Les supports de données peuvent être écrits en **double face** et la lecture des données s'effectue par un rayon laser réfléchi. Les changements de polarité induits à la surface constituent l'information et peuvent être décodés par un laser. L'inscription de MO se déroulait jusqu'ici très lentement. Cela s'explique par le fait, que lors d'une opération d'écriture, le même bloc était traité trois fois : la première fois, le bloc était effacé, à la rotation suivante, le bloc était écrit, et ensuite seulement à la troisième rotation, il était vérifié. Par rapport à une opération de lecture, une opération d'écriture nécessitait deux rotations de plus.

Entre temps, tous les lecteurs magnéto-optiques disponibles sur le marché supportent le mode LIMDOW (Laser Intensity Modulation Direct Overwrite) et peuvent commuter en ce mode. LIMDOW signifie qu'il est possible de remplacer en une seule fois (et non en plusieurs fois comme c'était le cas jusqu'à présent) les anciennes données par les données plus récentes, à savoir écraser une ancienne information par une nouvelle. L'inconvénient d'une moindre performance par rapport aux chargeurs conventionnels, qui ont un peu terni l'image des lecteurs magnéto-optiques, n'a plus raison d'être.

En résumé, les avantages de cette technologie sont les suivants : les supports de données sont de taille réduite, légers et économiques. Les lecteurs peuvent être utilisés par l'ordinateur comme des lecteurs de disques normaux et l'utilisation d'un logiciel de système de fichiers n'est pas nécessaire.

L'utilisation de disques MO s'avère judicieuse lorsque le support de données doit être extrait de l'ordinateur (pour les applications dont la sécurité est critique par exemple) mais où la performance élevée des disques durs Winchester n'est pas requise ou tout simplement trop onéreuse. En outre, les disques MO peuvent être utilisés dans des domaines où l'on désire accéder rapidement et facilement à des sauvegardes sans pour autant devoir copier ou changer préalablement de support de donnée. Les changeurs MO permettent d'archiver un volume de données important. Cependant, CD-RW et les changeurs CD-R sont appelés à remplacer les changeurs MO.

Les disques **WORM** (**Write Once Read Multiple**) sont des disques optiques qui ne peuvent être gravés qu'une seule fois mais peuvent être lus aussi souvent qu'on le souhaite. Depuis l'introduction du CD-R cette technologie ne joue plus un rôle prépondérant.

8.5 Perspectives futures

Les CD-ROM se sont imposés dans le domaine audio et informatique. Les CD-R (inscription unique) et les CD-RW (inscription multiple) vont sans aucun doute, chacun s'appropriant une part non négligable du marché. La situation est un peu différente pour les disques DVD (Digital Versatile Disk). Cette technologie évincera peut-être les CD-ROM dans certains secteurs car la capacité des DVD est bien plus élevée.

Parallèlement aux développements effectués dans le domaine des DVD, les disques vidéo MO font aussi l'objet d'améliorations. Le disque MO-7 (ASMO) est supposé disposer d'une capacité de 6,1 Go. Certains fabricants de lecteurs comme Maxoptix ont également mis sur le marché des produits atteignant une capacité de 5,2 Go, ce qui représente un doublement des capacités actuelles.

Le développement avance actuellement à grand pas dans le domaine des systèmes de mémoire optique. L'association **OSTA** (**O**ptical **S**torage **T**echnology **A**ssociation) est d'une aide précieuse pour obtenir une vue d'ensemble des technologies actuelles et futures. www.osta.org

9. Mémoires vives

Les performances globales d'un ordinateur ne dépendent pas uniquement de la puissance de son microprocesseur, la mémoire vive joue également un rôle central. De nouvelles technologies, des circuits intégrés de plus en plus rapides et des architectures différentes compliquent le choix du module mémoire, convenant le mieux à un ordinateur. Ce chapitre présente quelques termes qu'il est bon de connaître.

9.1 Technologies des mémoires

On distingue aujourd'hui mémoires non volatiles, statiques et dynamiques.

9.1.1 Mémoires non volatiles

Les mémoires non volatiles ont en commun qu'elles conservent leur contenu, c'est-à-dire les données qui y sont enregistrées, même lorsque la tension d'alimentation à leurs bornes est coupée. Les EEPROMs et autres mémoires flash appartiennent à cette catégorie.

EEPROM, E²PROM : Electrically Erasable Programmable Read-Only Memory

Dans la catégorie des EEPROM, on range toutes les mémoires non volatiles dont le contenu peut être modifié ou effacé par une action électrique (et non par un rayonnement ultra-violet, comme c'était le cas avec son prédécesseur EPROM). Il existe différentes architectures qui se différencient par leurs propriétés électriques. On trouve ainsi des EEPROM sur différents modules mémoire, sur lesquels sont enregistrées, sous forme de code, (par ex.SPD sur SDRAM DIMM) les caractéristiques du module en question (tension de service, temps d'accès, structure du banc de mémoire, correction d'erreur, etc. voire même le nom du constructeur) .

Mémoires flash

Les mémoires flash se caractérisent par le fait que chacun des octets peut être adressé ou lu, mais que les opérations d'écriture ou de suppression ne peuvent avoir lieu que bloc à bloc. Les temps d'accès en lecture de ces mémoires sont approximativement deux fois plus élevés que ceux des mémoires dynamiques. Ils se situent actuellement autour de 100 ns. Les mémoires flash ne supportent qu'un nombre limité de cycles de programmation et d'effacement (autour de 100.000). En règle générale, la conservation des données sur ces mémoires est garantie pendant une période de 10 ans. Les mémoires flash existent notamment sous forme de module SIMM, de cartes PC (PCMCIA), de cartes Compact Flash (CF), de cartes miniatures (Miniature Card, MC), et de cartes disquettes Solid State Floppy Disc Card (SSFDC). Indépendamment de leurs formes extérieures, on peut encore classer les mémoires flash en deux sous-catégories : Linear Flash et ATA Flash. Les mémoires Linear Flash possèdent un espace linéaire d'adresses. N'importe quelle adresse peut être sollicitée directement de l'extérieur. Les cartes mémoires ATA flash, par contre procèdent à un

recalcul interne des adresses. Ce type de mémoire peut donc être sollicité comme un disque dur, ce qui peut éventuellement simplifier la programmation des pilotes (drivers). Les modules de mémoire flash sont utilisés comme mémoire de masse ou mémoire de programmes sur les ordinateurs portables (Notebooks), les routeurs de réseau, les imprimantes, les assistants électroniques et les appareils-photo numériques.

9.1.2 Mémoires dynamiques

DRAM : Dynamic Random Access Memory.

DRAM est une mémoire dynamique à accès libre. Il est donc possible d'accéder directement et à tout moment à n'importe quelle cellule de données. Un cas contraire extrême serait par exemple celui des lecteurs de bande. Ce type de mémoire est en général utilisé comme mémoire principale.

Les mémoires dynamiques se caractérisent par le fait qu'elles enregistrent les informations dans un condensateur qui, comme un accumulateur d'électricité, peut conserver une certaine quantité d'énergie pendant un certain temps. Pour stocker par exemple un "1" logique, le condensateur est chargé et pour stocker un "0" logique, il est déchargé. Les condensateurs sont organisés selon une matrice, en rangs et en colonnes.

Pour maintenir un encombrement le plus faible possible des circuits intégrés, ce qui permet d'économiser des connexions et donc des coûts, la commande électrique de ces éléments se fait en deux étapes : l'adresse d'une date est répartie dans la matrice selon une adresse de rang et une adresse de colonne. Ces adresses sont transmises à la puce l'une après l'autre, par l'intermédiaire des mêmes connexions. L'avantage de cette technologie réside dans le fait qu'elle peut être fabriquée en quantités importantes et ainsi, à faible coût. Son inconvénient majeur est que la production du condensateur n'est pas idéale : en effet, tout comme un accumulateur électrique, le condensateur a tendance à se décharger avec le temps. Pour éviter que les données ne deviennent inutilisables, elles doivent être rafraîchies à intervalles réguliers. (Refresh) Cette architecture de base a donné naissance à plusieurs développements que nous traitons dans les paragraphes suivants :

FPM : Fast Page Mode

Les modules mémoire de type FPM (Fast Page Mode) sont un développement des mémoires DRAM standard (Dynamic Random Access Memory). Grâce à des commandes particulières, l'utilisation de ces modules permet de raccourcir, pour certaines applications, les temps de ralentissement dus à la technique. Dans la plupart des programmes ordinateurs, des données corrélées sont traitées par le processeur. Lors d'un accès à un banc mémoire, il est d'usage de transmettre d'abord le rang puis la colonne d'adresses. Lorsque l'on considère deux adresses successives, seule l'indication de la colonne change puisque les données qui se suivent se situent toutes dans la même rangée (on parle également de "page"). Une nouvelle transmission du rang d'adresse inchangé est donc inutile. La mode Fast Page tire profit de cette situation. Les adresses de rang et de colonne sont transmises uniquement lors du premier accès. Lors des accès suivants, seule l'indication de

l'adresse de colonne suffit. Cela permet de raccourcir le délai (temps de cycle) nécessaire pour que les données correspondantes soient disponibles au niveau des connexions de sortie du banc de mémoire. Ce mode doit bien sûr être supporté par le système et par le circuit intégré mis en oeuvre.

EDO : Extended Data Output

Les modules mémoire de type EDO constituent une évolution par rapport aux modules FPM. Certaines techniques de commande permettent aussi, de raccourcir le temps d'accès à la mémoire. Dans le cas des mémoires FPM, le signal électrique des lignes de données est supprimé (ne pas confondre ce signal avec le contenu de la cellule mémoire, celui-ci reste intacte !), lorsqu'une nouvelle information d'adresse est créée. Etant donné que le traitement des données nécessite un certain temps, on s'aperçoit que la mémoire est « paralysée » pendant un certain laps de temps de manière à ce que les signaux électriques sur les lignes des données soient bien reçus puis traités. Dans le cas des mémoires EDO, ce niveau de sortie est conçu de telle sorte que les informations qui s'y trouvent, s'y maintiennent même si une nouvelle adresse est transmise. Cela permet simultanément de traiter le mot de données et de charger l'adresse suivante dans la mémoire. L'ensemble de la procédure permet finalement de raccourcir le temps de cycle du module mémoire.

BEDO : Burst Extended Data Output

En tant que perfectionnement du module mémoire EDO, le module BEDO est la dernière mémoire DRAM asynchrone. Comme ce module est sorti en même temps que les modules SDRAM, il n'est jamais parvenu à s'imposer sur le marché. Il se caractérise par un mode Burst supplémentaire. Après une transmission d'adresses, le module sort le contenu des cellules tout comme dans une mémoire EDO-RAM, mais joint également le contenu des trois cellules suivantes selon un cycle égal à une période par valeur.

SDRAM : Synchronous Dynamic Random Access Memory

Tout comme les technologies FPM et EDO, la technologie SDRAM n'est qu'un nouveau développement des architectures de mémoires existantes ou de leurs modes d'accès. Contrairement à FPM ou EDO, la technologie SDRAM est cependant incompatible avec les technologies précédentes. Cela signifie que les modules SDRAM ne peuvent être montés que dans des systèmes informatiques explicitement compatibles avec cette technologie. Le perfectionnement de la technologie SDRAM n'est rien d'autre que la délocalisation d'une partie du contrôleur de la mémoire vers la puce mémoire. Cette évolution est à comparer avec l'introduction des disques durs IDE (les disques durs SCSI sont peut-être un meilleur exemple dans ce contexte), où le contrôleur a lui aussi été développé en fonction des besoins spécifiques de ces disques puis intégré dans le boîtier du disque. Tout comme les types d'accès des modules FPM et EDO, la technologie SDRAM est très forte lorsqu'il s'agit d'exploiter des données qui se suivent dans un espace d'adresse. L'accès typique à un module SDRAM s'effectue moyennant l'indication du rang et de la colonne d'adresse, comme pour tous les types de module DRAM. Ce qui est différent par rapport aux autres technologies

jusqu'à présent connues, c'est la transmission d'une commande au module SDRAM en parallèle à l'adressage. En fonction de la commande reçue, la puce mémoire réagit par des opérations prédéterminées. Une commande typique pourrait par exemple être : lire l'adresse X ainsi que les trois adresses suivantes. Dans ce cas, la transmission de la commande précise déjà la valeur de l'adresse de départ X. Sans autre intervention, le module mémoire va aussi transmettre les contenus des quatre différentes adresses. Comme le moment, où les données exigées sont effectivement disponibles en sortie du module, doit être parfaitement défini, les SDRAM sont alimentés par un signal horloge qui permet de synchroniser toutes les opérations. L'utilisation de mémoires SDRAM apporte un avantage de rapidité, pour transmettre de grandes quantités de données bloc à bloc. C'est le cas par exemple lors du traitement de graphiques volumineux.

DDR SDRAM : Double Data Rate SDRAM

La technologie DDR SDRAM, souvent appelée aussi SDRAM II, est une version plus rapide de SDRAM. Elle a été conçue pour pouvoir lire des données sur le flanc ascendant et le flanc descendant du système horloge et donc doubler le taux de transfert de la mémoire. Le taux maximal de transfert de cette technologie atteint 1 Go/s.

RDRAM : Rambus DRAM

La mémoire Rambus DRAM repose sur une technologie entièrement nouvelle développée par la société Rambus Inc. La structure interne de la mémoire, dont notamment les longueurs des lignes, les capacités des broches et les variations de tension, a été complètement remaniée et redéfinie. Cette nouvelle structure répond aux exigences sévères en matière de capacité. La mémoire fonctionne sur le flanc ascendant et sur le flanc descendant du système horloge. Une mémoire Rambus à un canal qui grâce à une vitesse de 1,6 Go/s fournit, une capacité trois fois plus importante que celle d'un module SDRAM 64 bits et 100 MHz. Le principal avantage de la technologie Rambus est de pouvoir utiliser en parallèle deux ou quatre canaux Rambus. Deux canaux permettent d'obtenir une largeur de bande de 3,2 Go/s et, avec quatre canaux, une largeur de bande de 6,4 Go/s.

9.1.3 Mémoires statiques

De par leur rapidité, les mémoires statiques sont mises en oeuvre en tant que mémoire cache. Contrairement aux mémoires dynamiques, elles ne nécessitent aucune mise à jour de leurs contenus. Une mémoire statique travaille avec un circuit constitué de plusieurs éléments par cellule. Ce circuit, provenant de la donnée à mémoriser, adopte un certain état de fonctionnement et se verrouille de lui-même, de telle sorte qu'un changement d'état de fonctionnement n'est possible qu'à partir de l'extérieur. Une mémoire statique ne perd son contenu d'informations que lorsque la tension d'alimentation à ses bornes est coupée. En raison de la structure complexe de leurs cellules mémoire, les mémoires statiques ne peuvent être construites qu'avec des densités assez faibles (comparées à celles des mémoires dynamiques). A capacité équivalente, elles sont également

beaucoup plus chères que les mémoires dynamiques.

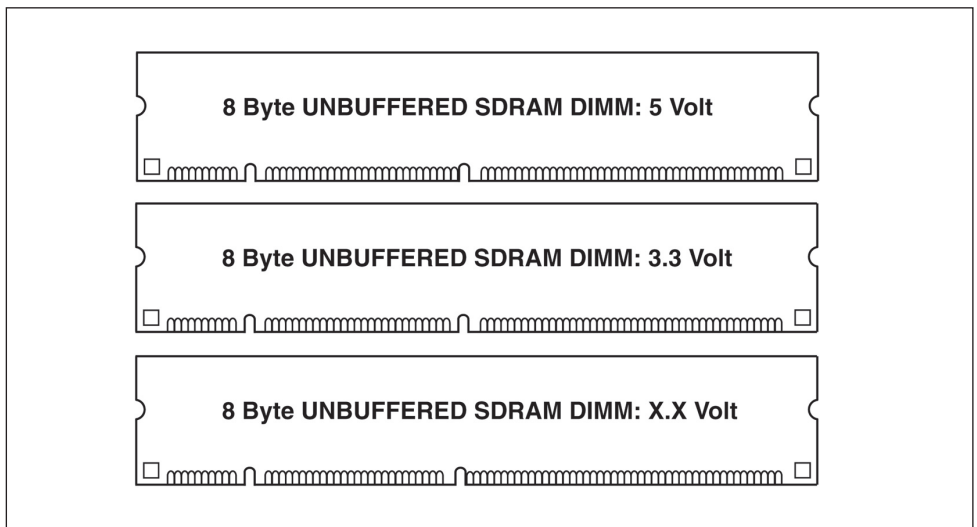
9.2 Modules de mémoire

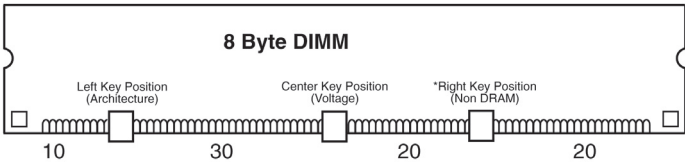
Pourquoi faire appel à des modules ? Les systèmes informatiques modernes exigent des volumes mémoire, en largeur de données (à savoir : le nombre de bits utilisés) tout comme en profondeur d'adresse (à savoir : le nombre de mots de données pouvant être logés dans la mémoire) qu'une seule et unique puce mémoire ne peut contenir. On se résoud donc à construire des modules à partir de puces mémoires individuelles. Ces modules peuvent à leur tour être commandés comme une grosse puce unique. On distingue les différentes formes courantes de modules suivantes :

SIMM : Single Inline Memory Module

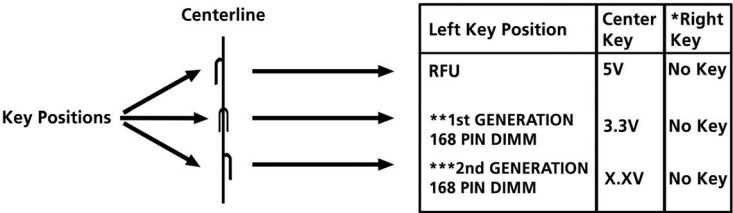
Les contacts électriques des SIMM sont disposés sur chacune des deux faces de la carte-mère mais sont toutefois connectés entre eux. Un module SIMM de 72 broches dispose ainsi de 144 surfaces de contact dont seulement 72, sont pertinentes.

DIMM : Dual Inline Memory Module





Un module DIMM dispose de contacts électriques sur chacune des deux faces de la carte mère, mais dans ce cas, les contacts électriques en vis-à-vis sont électriquement isolés. A taille égale, on dispose ainsi d'un plus grand nombre de contacts électriques (deux fois plus qu'avec un module SIMM comparable). Cela permet de disposer soit d'un plus grand nombre de bits de données, soit d'un plus grand espace d'adresse. Par ailleurs le nombre de connexions destinées aux tensions de service et aux signaux de commande est lui aussi plus important. Cela se traduit par des avantages au niveau du design de la platine et donc des propriétés électriques du module. Les modules DIMM sont aujourd'hui des modules standard dans le domaine des PC, des serveurs et des stations de travail.



9.3 Termes relatifs à la mémoire

Cache

Une mémoire cache est une mémoire relativement petite mais très rapide (généralement en technologie SRAM) qui permet d'entreposer les données fréquemment utilisées entre le processeur et la mémoire vive. Le processeur peut accéder aux données enregistrées dans la mémoire cache beaucoup plus rapidement qu'à celles qui sont stockées dans la mémoire vive. Pour un coût modique, la mise en place d'une petite mémoire-cache peut améliorer la performance d'un ordinateur de manière considérable.

En matière de mémoire cache, on distingue différents niveaux en fonction de la position de la mémoire dans le flux de données.

Cache niveau 0 :

Il découple le flux de données des différentes unités à l'intérieur du processeur. Sa taille est de l'ordre de 1 à 128 octets.

Cache niveau 1 :

Il découple le flux de données internes au processeur de celles de l'extérieur. Taille : de quelques octets (128) à quelques kilo-octets.

Cache niveau 2 :

Il découple le flux de données entre le processeur et le bus mémoire, auquel la mémoire vive est raccordée. Taille : de 256 kilo-octets à plusieurs Mo (méga-octets).

Cache niveau 3 :

Dans le cas des architectures multiprocesseurs, il découple le système de bus séparé du bus mémoire.

Parity/Non Parity :

Des influences extérieures (champs électro-magnétiques, variations de tension, radioactivité, radioactivité naturelle, etc.) peuvent altérer quelques bits de données. Un "1" logique peut être transformé en "0" et inversement. De ce fait, les données enregistrées sont modifiées. Les modules mémoire "Non-Parity" ne stockent que des données et ne permettent pas de détection d'erreur. Les modules du type « Parity », en revanche, permettent de stocker des données ainsi que des informations de contrôle (le bit de parité associé à ces données). Cela fonctionne de la manière suivante : pour un nombre pair de bits de données, le bit de parité est activé ; pour un nombre impair de bits de données, le bit de parité est désactivé. Le contrôle de la parité des données permet d'identifier une erreur à un bit près. Comme la correction d'erreur n'a pas lieu, la plupart des systèmes se contentent seulement de s'arrêter et d'afficher un message d'erreur. En règle générale, on intercale 1 bit de parité par octet (8 bits) de données.

Attention : si à cause d'influences extérieures, le contenu de deux bits dans un mot de données a été modifié, le contrôle de la somme reste identique et l'erreur passe inaperçue. La probabilité pour que cette éventualité se produise est cependant extrêmement faible.

ECC : Error Checking and Correcting

Le procédé ECC permet de reconnaître des erreurs de un et deux bits. Les erreurs d'un bit peuvent même être corrigées. Ce procédé est parfois aussi désigné sous le nom de EDC, Error Detection and Correction. A l'aide d'algorithmes appropriés, l'ordinateur procède par bloc au calcul des sommes de contrôle (d'une manière similaire à CRC). Ces sommes sont enregistrées dans des zones mémoires spécifiques. Ces sommes de contrôle permettent de détecter et de corriger les bits erronés. De même que dans la technologie des CD audio, l'utilisateur du logiciel ne remarque pas ces opérations.

Memorybus

Le memorybus est le système bus, situé entre les E/S et la CPU, qui pilote la mémoire principale à l'aide des circuits intégrés. Il est constitué du bus d'adresse et du bus de données.

Small Outline J-Lead (chip)

Thin Small Outline Package (chip)

Quel type de mémoire convient pour quel ordinateur ?

Les spécifications relatives aux types de mémoire à utiliser sont, dans la pratique, imposées par le constructeur du matériel, qui a défini la mémoire en parallèle aux spécifications du système. Dans la mesure du possible, les serveurs ne devraient être équipés que de modules ECC.

A l'intérieur d'un banc de mémoire, tous les modules doivent être identiques. Les différents bancs en revanche peuvent être parfois panachés (cf. les spécifications du fabricant et du système). En cas de doute, il convient de consulter la notice d'utilisation fournie avec le système.

10. Communication

10.1 Définition

Une communication a lieu entre un émetteur et un récepteur. La communication peut être à simple ou à double sens et a pour but l'échange d'information. Si cette information revêt la forme de données, de texte, d'images ou de paroles, on parle alors de télécommunication.

10.2 Conditions préalables à une communication réussie

Pour une communication réussie, trois conditions préalables prépondérantes doivent être remplies :

- Il y a au moins un émetteur et un récepteur
- Emetteur et récepteur utilise un standard commun
- Emetteur et récepteur parlent la même langue.

10.3 Types de communication

10.3.1 Communication à sens unique

Dans la communication à sens unique, l'échange d'information ne se fait que dans une seule direction. L'émetteur transmet son information au récepteur via le standard commun. Si à la suite de la réception de l'information le récepteur envoie une réponse à l'émetteur, celle-ci est alors à son tour considérée comme une communication à sens unique. Le récepteur devient émetteur et vice-versa.

10.3.2 Communication à double sens

Par opposition à la communication à sens unique, un échange d'information simultané a lieu dans la communication à double sens. Les participants à la communication sont en même temps émetteur et récepteur.

10.3.3 Communication interactive

La communication interactive est un développement de la communication à double sens. L'échange d'information simultané est effectué sur la base du dernier échange d'information. Un dialogue est créé entre les participants à la communication.

10.3.4 Communication ouverte

On parle de communication ouverte (Open System Interconnection - interconnexion à système ouvert) quand les participants à la communication se plient à des règles standardisées de communication. Grâce à la standardisation des règles de communication, tous les participants potentiels à la communication peuvent s'assurer qu'ils peuvent

communiquer avec autant d'autres participants que possible. La possibilité de communication est donc ouverte à tous les participants potentiels à la communication.

11. Standards et normes

11.1 Définition Norme

Par norme on entend une définition universellement reconnue permettant de répondre à un ensemble de données. Avant d'être adoptée une norme passe toujours par un processus de normalisation comprenant plusieurs instances et étapes, processus qui est reconnu et à la fin juridiquement validé. Les principaux critères d'une norme reposent sur sa maturité technique et l'avantage pour l'utilisateur.

11.2 Types de normes

Quand il est question de normes, il faut toujours faire la différence entre **normes, standards industriels, standards propres au fabricant** et **recommandations**.

Les normes ont suivi le processus défini de normalisation (voir définition Norme).

Un standard industriel est un process ou un procédé non normalisé, indépendant du fabricant, répondant à un état de fait et qui en règle générale a fait ses preuves dans la pratique depuis des années.

Au contraire, la norme propre du fabricant repose, elle, sur des process ou procédés spécifiques au fabricant, dont l'application de plusieurs années s'est révélée positive dans la pratique.

La recommandation est la forme de normalisation la moins contraignante. Ni le fabricant ni l'utilisateur ne sont obligés de s'y conformer.

11.3 Organismes importants de normalisation en IT

11.3.1 International Standardization Organization, ISO (Organisation Internationale de Normalisation)

Les instituts nationaux de normalisation de 118 pays collaborent au sein de l'Organisation Internationale de Normalisation (International Standardisation Organisation, **ISO**) dont le siège est à Genève. L'ISO a pour but, grâce à des normes uniformes dans le monde entier, de faciliter sur le plan international l'échange de marchandises et de services et de renforcer les frontières de la collaboration dans le domaine scientifique, technique et économique. En ce qui concerne la communication de données, la norme qui est vraisemblablement la plus connue a été et est développée par l'ISO : **Le modèle de référence OSI**.

11.3.2 Commission Electrotechnique Internationale (CEI)

La **Commission Electrotechnique Internationale (CEI)** a été créée dès 1906 et rattachée ensuite à l'ISO. Elle comprend plus de 600 groupes de travail traitant de normalisation. Les normes élaborées par la CEI sont valables dans le monde entier. La CEI a son siège à Genève, les instituts nationaux de normalisation œuvrent dans plus de cent pays. La CEI est dans le domaine de l'électrotechnique et de l'électronique un organisme de normalisation reconnu. La sécurité électrique, la résistance à la tension et l'isolation, le domaine des éléments des composants électriques, les installations de production, de transport et de distribution de l'énergie électrique, la technique domestique de même que la technique de la télécommunication, de la radio et de l'information font partie des domaines qui sont du ressort de la CEI.

11.3.3 Union Internationale des Télécommunications (UIT)

L'**Union Internationale des Télécommunications (UIT)** a été fondée à Paris le 17 mai 1865 par 20 états et elle est depuis le 15 octobre 1947 une sous-organisation des Nations Unies (ONU) son siège est à Genève. L'UIT est un organisme actif dans le monde entier au sein duquel les gouvernements et le secteur privé de la télécommunication coordonnent la mise en place et l'exploitation de réseaux et de services de télécommunication.

11.3.4 Institut Européen des Normes de Télécommunications (ETSI)

Les normes de télécommunication valables pour l'Europe proviennent de l'**Institut Européen des Normes de Télécommunication (ETSI)** fondé en 1988. Le siège de l'institut se trouve à Sophia Antipolis, un centre de recherche dans le sud de la France. L'ETSI compte 800 membres provenant de plus de 50 pays différents. Les normes européennes de télécommunication émises par l'ETSI reposent le plus souvent sur les recommandations internationales correspondantes (par ex. de l'UIT). L'ETSI modifie ces normes en fonction des besoins européens.

11.3.5 Institute of Electrical and Electrical Engineers (IEEE)

L'**Institut des Ingénieurs en Electricité et en Electronique (IEEE)** dont le siège se trouve dans l'Etat du New Jersey, USA, se consacre entre autres à des tâches de normalisation et regroupe en tant qu'association essentiellement des ingénieurs américains. L'IEEE est divisé en différents groupes de travail ad hoc qui se forment pour le temps que dure l'élaboration de la recommandation d'une norme. Le groupe de travail 802 s'occupe par exemple de la normalisation de réseaux locaux et a largement contribué à la définition de procédures d'accès et de protocoles de sécurité.

12. Le modèle de référence OSI

12.1 Introduction

Le modèle OSI sert de modèle de référence pour tous les systèmes ouverts et normalisés. **OSI** signifie **O**pen **S**ystem **I**nterconnection et fournit un modèle abstrait servant de base pour l'interprétation de systèmes déjà existants ainsi que de référence pour la définition de nouveaux protocoles. Pour comprendre l'évolution du modèle OSI il faut se représenter la structure du monde informatique avant 1980. A cette époque le monde informatique présentait une structure disparate composée de standards spécifiques aux fabricants et qui n'étaient pas compatibles entre eux. Toute adaptation dans le but d'une compatibilité était compliquée et coûteuse. La solution vint avec le modèle de référence OSI qui est basé sur une norme ISO et qui a été adopté en 1984 par l'UIT. Le modèle de référence OSI a pour objectif d'uniformiser des normes afin de permettre la communication entre des systèmes ouverts et normalisés. Le modèle de référence OSI est constamment actualisé en toute flexibilité, c'est-à-dire que les anciens éléments en sont retirés et que de nouveaux y sont ajoutés pour éviter que le modèle de référence ne vieillisse.

12.2 Structure

Le modèle de référence OSI est un modèle en couches, c'est-à-dire que tout le système est divisé en sous-systèmes, en couches (angl. Layer). Les couches présentent chacune une structure spécifique, les sous-systèmes appartenant à la même hiérarchie forment une couche, les couches sont superposées, la couche inférieure servant à la fonction de communication de la couche supérieure. De plus, chaque couche tient à disposition certains services, aussi bien à l'intérieur de la couche elle-même que pour des couches inférieures.

Le modèle de référence OSI présente sept couches au total, que l'on peut répartir en deux catégories. D'une part, les couches de 1 à 4, axées sur le transport et chargées de la transmission des bits proprement dite, et d'autre part, les couches 5 à 7, axées sur les applications et chargées de la commande du fonctionnement et de la présentation de l'information.

Les couches communiquent entre elles selon des règles précises, à savoir les protocoles ; quant aux fonctions de communication élémentaire, elles sont appelées services ou opérations primitives. Il existe quatre classes d'opérations primitives par couche, la demande (Request), l'affichage (Indication), la réponse (Response) et la confirmation (Indication). Dans une communication entre l'instance A (utilisateur du service) et l'instance B (fournisseur du service), reliées par une couche N servant de mise à disposition d'une prestation de service, le Request formule la demande de service de l'instance A à l'instance B qui est informée de cet événement par l'Indication. Vient alors la Response de l'instance B, ce que représente l'accusé de réception de l'affichage précédent. Cette réponse est aussi enfin la confirmation de la demande par le fournisseur.

12.3 Couches

Couche 1, couche de transmission des bits/Layer 1, Physical Layer

La couche de transmission des bits définit les propriétés mécaniques, électriques, fonctionnelles et procédurales des liaisons physiques entre les dispositifs de données (DTE [Data Terminal Equipment]) et les dispositifs de transmission de données (DCE [Data Communication Equipment]). La transmission des bits reçus se fait par une ligne de communication. Des exemples de propriétés sont indiqués ci-après. Du point de vue mécanique il peut s'agir de la dimension des connecteurs ou de l'agencement des broches. Du point de vue électrique, du niveau de tension sur les lignes, par ex. selon les recommandations X et V de l'UIT. Du point de vue fonctionnel, de l'attribution des broches. Du point de vue procédural, des règles générales d'utilisation des lignes d'interfaces.

Couche 2, Couche de liaison des données /Layer 2, Data Link Layer

La couche de liaison des données doit assurer un échange transparent de données. Les flux de bits sont regroupés en blocs de données appelés trames et transférés à la couche de transmission. Ce faisant, les flux de bits traversent des opérations de détection et de correction d'erreurs.

Couche 3, Couche de transmission /Layer 3, Network Layer

La couche de transmission réalise le transport de données entre les systèmes terminaux en passant éventuellement par des nœuds intermédiaires au moyen d'un guidage et d'un acheminement des paquets, c'est-à-dire le routage. Les blocs de données sont des paquets pour les transmissions avec connexions et des datagrammes dans les transmissions sans connexion. Des réseaux entiers peuvent ainsi être reliés entre eux, à condition cependant qu'il y ait une adresse précise. X.25, Frame Relay et IP sont des protocoles typiques de la couche de transmission.

Couche 4, Couche de transport / Layer 4, Transport Layer

La couche de transport procède au transport des données indépendamment du réseau et assure ainsi un échange fiable de données. Les fonctions typiques de cette couche sont le mapping des adresses, la régulation du flux entre les hôtes présentant des vitesses différentes et le multiplexage de liaisons de transport. Les protocoles les plus connus de cette couche sont **UDP** (User Datagramm Protocol) et **TCP** (Transmission Control Protocol). Dans le même temps la couche 4 constitue la transition vers les couches chargées des applications.

Couche 5, Couche de session / Layer 5, Session Layer

La couche de session réalise la session c'est-à-dire la communication entre les processus. De plus elle organise l'échange de données élargi de processus supplémentaires tels que la commande de dialogue et de communication et la synchronisation en cas de panne du système.

Couche 6, Couche de présentation / Layer 6, Presentation Layer

La couche de présentation établit la communication avec les processus d'application de systèmes d'ordinateurs hétérogènes. Elle s'occupe uniquement de la syntaxe, du traitement et de la présentation uniformes des données. Cela signifie par ex. la transformation de formats de données différents en une forme normalisée, appelée conversion code.

Couche 7, Couche d'application / Layer 7, Application Layer

La couche d'application met à disposition des services pour l'utilisation externe de réseaux d'ordinateurs et constitue ainsi la couche la plus étendue. L'identification de partenaires de communication, la garantie de droits d'accès et la garantie de certaines qualités de service comptent parmi les fonctions possibles.

13. Procédés et techniques de transmission

13.1 Introduction

On peut distinguer plusieurs formes de transmission de données dans les réseaux : Le **signal**, c'est-à-dire la transmission analogique ou numérique, le **fonctionnement parallèle**, c'est-à-dire la transmission asynchrone/asymétrique ou synchrone/symétrique, la **transmission de signes**, c'est-à-dire de bits en parallèle ou en série et le **fonctionnement** sur les modes simplex, half-duplex et duplex ou full-duplex. Les différentes formes de transmission de données sont expliquées ci-dessous. Important : dans un réseau ces formes ne peuvent être considérées séparément; elles se complètent et décrivent ainsi la communication de données dans sa totalité.

13.2 Signal

Fondamentalement les signaux tributaires du temps se divisent en différentes classes. Si une valeur du signal est présente à tout instant on parle de **signal continu**, s'il n'y a pas à tout instant une valeur du signal, on parle de **signal discret**. Si toutes les valeurs du signal sont dans les limites admissibles, on parle de **valeurs continues**, si seules certaines valeurs du signal sont dans les limites admissibles, on parle de **valeurs discrètes**.

Un **signal analogue** peut avoir n'importe quelle valeur entre les maximas négatifs et positifs, c'est-à-dire qu'il s'agit d'un signal continu, à valeur continue. Dans la transmission analogique de données les informations se traduisent par des changements constants de la tension électrique. Ici interviennent les procédés de modulation : modulation de fréquence, d'amplitude et de phase.

Un **signal numérique** ne peut avoir que certaines valeurs, c'est-à-dire qu'il s'agit d'un signal discret à valeur discrète. La représentation d'informations numériques n'utilise que deux signes. Ce procédé est également appelé système binaire. Dans ce contexte le terme binaire signifie qu'un seul des deux états n'est accepté.

13.3 Fonctionnement parallèle

Le fonctionnement parallèle repose sur la couche de sécurité et est utilisé pour la transmission synchrone et asynchrone de données. Il constitue une méthode de réglage temporel des dispositifs d'envoi et de réception.

Dans la **transmission synchrone de données** on distingue la transmission axée sur les bits et la transmission axée sur les signes, des intervalles exacts de temps étant respectés entre l'émetteur et le récepteur; la synchronisation de l'horloge s'effectue par le flanc des données. Un nombre variable de bits de données est regroupé dans un cadre. Le marquage du début du cadre se fait par une en-tête spéciale qui le précède.

La **transmission asynchrone de données** procède selon le principe du démarrage et de l'arrêt.

Cela signifie que le cadre est délimité par un bit de démarrage et un bit d'arrêt, une plage de temps fixe se situant entre les deux. Après le bit d'arrêt il y a retour à la position arrêt en préparation de la prochaine transmission.

13.4 Transmission de signes

Dans la transmission de signes on distingue les **bits en série** et les **bits en parallèle**. Dans la transmission de bits en série, les bits de signes sont transmis les uns après les autres. Au contraire, dans la transmission de bits en parallèle les bits de signes sont transmis en même temps en parallèle.

13.5 Fonctionnement

Dans la communication entre émetteurs et récepteurs dans les systèmes informatiques en réseaux on distingue trois différents modes de fonctionnement, qui sont le **simplex**, le half-duplex et le duplex ou full-duplex. En mode simplex, deux instances sont reliées par une ligne de communication commune. Mais dans ce cas chaque instance ne peut être qu'émettrice ou réceptrice, si bien que la communication ne peut se faire que dans un sens. En mode **half-duplex**, deux instances sont également reliées par une ligne de communication commune. Ici cependant, chaque instance peut être émettrice ou réceptrice, mais une instance ne peut à un moment donné exercer qu'un seul de ces deux rôles. Cela signifie qu'avant de communiquer, les instances doivent se mettre d'accord pour savoir qui sera émetteur et qui sera récepteur, afin que la communication puisse avoir lieu dans les deux sens tout en n'étant possible que dans un sens à un moment donné. En mode **duplex** ou encore full-duplex, deux instances sont reliées par deux lignes de communication communes. Dans ce cas chaque instance peut être en même temps émettrice et/ou réceptrice si bien que la communication peut se faire en même temps dans les deux directions.

14. Personal Area Networks - PANs

14.1 Définition

Le terme de **Personal Area Network** s'applique à la communication d'appareils d'un ou de quelques d'utilisateurs dans un rayon de 10 m. En général on peut distinguer trois domaines. La connexion de périphériques, la connexion d'appareils externes et la connexion de plusieurs systèmes d'ordinateurs pour le transfert de données. Le dernier domaine est cependant plutôt à négliger parce qu'il constitue un cas limite du LAN classique. Etant donné que la plupart des PAN sont installés sans fil, en général on parle également de **Wireless Personal Area Network** (WPAN) ; ce sont finalement deux synonymes qui désignent le même principe. Les deux technologies le plus souvent utilisées sont IrDA et Bluetooth ; nous y reviendrons plus loin en détail.

Le sigle **Personal Area Network** est également utilisé en rapport avec les recherches effectuées par le M.I.T (Massachusetts Institute of Technology). Ces recherches concernent la transmission d'informations numériques à partir de la faculté du corps humain de conduire le courant électrique.

14.2 Méthode de transmission

14.2.1 IrDA (Infrared Data Association)

IrDA (Infrared Data Association) désigne une conception de réseau de transfert de données sans fil. Ses caractéristiques sont une portée courte, un contact visuel et une liaison point à point ; ce concept de réseau est également appelé IrDA Data. Par contre IrDA Control offre la possibilité de connecter plusieurs périphériques pour un transfert de données sans fil, sans contact visuel par l'intermédiaire d'une liaison point à point ou point à multipoint. Il faut cependant considérer que les vitesses d'IrDA Control sont inférieures à celles d'IrDA Data.

14.2.1.1 IrDA Data

IrDA Data a été adopté en tant que norme en 1994. Depuis, plus de 300 millions d'appareils électroniques équipés de ces interfaces sont en service, leur nombre étant en augmentation. Ceci résulte tout simplement du fait que la demande concernant la communication entre les appareils électroniques va croissant. Ceci vaut aussi bien pour des appareils traditionnels de la vie quotidienne que pour des appareils nouveaux provenant du développement de l'électronique.

Protocoles

Font partie des protocoles nécessaires à l'implémentation d'une IrDA Data : PHY (Physical Signaling Layer), IrLAP (Link Access Protocol) et IrLMP (Link Management Protocol).

Physical Signaling Layer (PHY)

En fonctionnement continu la portée est de 1 à 2 m. Pour une version low power la portée atteint de 20 cm à 30 cm au maximum en cas de communication entre des versions low power et standard power. La communication bi-directionnelle est standard pour toutes les spécifications, les volumes de données pouvant atteindre 9600 B/s Infrared (IR), 115 Ko/s Serial Infrared (SIR), 4 Mo/s Fast Infrared (FIR) et de 16 Mo/s Very Fast Infrared (VFIR). Les paquets de données sont contrôlés selon la méthode CRC (Cyclic Redundancy Check) (CRC-16 et CRC-32).

Link Access Protocol (IrLAP)

Le Link Access Protocol fournit une liaison d'appareil à appareil garantissant un échange de données fiable et correct. Il met à disposition des fonctions pour établir et supprimer des liaisons et pour contrôler les erreurs et le flux.

Link Management Protocol (IrLMP)

Le Link Management Protocol offre plusieurs canaux sur une liaison IrLAP. Il contient en plus des fonctions de multiplexage de liaisons IrLAP. En outre l'Information Access Service (IAS) permet de trouver les protocoles et services de différents interlocuteurs sur un réseau IrDA qui constitue la base de communication entre les composants IrDA.

Protocoles optionnels

D'autres protocoles optionnels se trouvent sur les couches 4 et 5 du IrDA Data Protocol Stack. Il s'agit par ex. de **Tiny TP** qui offre un contrôle de flux pour les liaisons IrLMP avec un service optionnel de segmentation. **IrCOMM** représente une émulation de port COM série ou parallèle pour les anciennes applications COM. Il existe en outre **OBEX**, qui offre des services de transfert d'objets analogues à ceux du protocole de transfert hyper-texte du WWW et **IrDA Lite**, qui fournit des méthodes permettant de réduire les dimensions du code de l'IrDA. Enfin, vient le **IrTran-P**, qui offre un service de transfert d'images tel qu'il est utilisé dans les appareils de photo numériques et autres appareils d'enregistrement. Le protocole **IrMC** joue un rôle important dans la communication mobile ; il fournit les spécifications de principes pour l'échange de données entre ces terminaux. Et finalement le protocole **IrLAN** qui décrit l'interface entre des réseaux IR et un LAN (Local Area Network).

14.2.1.2 IrDA Control

IrDA Control est un standard de communication qui permet à des périphériques sans fil de communiquer avec un grand nombre de différents hôtes intelligents.

Protocoles

Les protocoles nécessaires à l'implémentation d'un IrDA Control sont les suivants : PHY (Physical Signaling Layer), MAC (Media Access Control) et LLC (Logical Link Control)

Physical Signaling Layer (PHY)

La portée de IrDA Control est comparable à celle de systèmes infrarouges unidirectionnels. Elle est de 5 m au minimum. Comme pour IrDA Data la communication bidirectionnelle constitue la base de tous les standards, le débit de données atteignant au maximum 75 Ko/s. Les paquets de données sont contrôlés par un procédé CRC (Cyclic Redundancy Check), CRC-8 et CRC-16.

Media Access Control (MAC)

Le Media Access Control permet à un hôte de communiquer avec plusieurs périphériques, mais avec au maximum huit appareils en même temps. Le temps de réaction est court et la latence faible.

Logical Link Control (LLC)

Le Logical Link Control présente les caractéristiques fiables que garantissent le séquençement et un deuxième transfert des données en cas de détection d'erreurs.

14.2.2 Bluetooth

Bluetooth permet de connecter simplement des périphériques par l'intermédiaire d'une interface sans fil. La norme a été introduite par la firme Ericsson qui a donné son nom à Bluetooth. Bluetooth (Dent Bleue) était le surnom du roi Harald II, régnant sur le Danemark voici 1.000 ans et qui continue d'y jouir d'une grande popularité. La norme est promue par le BSIG (Bluetooth Special Interest Group) et a été présentée pour la première fois en 1998. Neuf entreprises forment avec Ericsson le groupe de promoteur, mais entre temps le nombre d'entreprises, membres du groupe d'intérêt, est beaucoup plus élevé.

14.2.2.1 Bluetooth - principes

Bluetooth utilise la bande ISM à 2,4 GHz qui est libre de licence. C'est la bande de fréquence qu'utilisent également les standards IEEE802. 11b et IEEE802. 11g des réseaux WLAN. Il faut considérer trois classes d'émission différentes. La classe d'émission 3 avec une sensibilité de 70 dBm, une puissance de 1 mW, une portée théorique de 10 m et une grandeur de réseau de l'ordre du Piconet. C'est la classe selon laquelle fonctionnent la plupart des appareils Bluetooth actuels. Même si, d'après la définition, ceci est le domaine d'un PAN, le Bluetooth ne se limite pas à cette performance. Des amplificateurs de puissance peuvent augmenter considérablement la puissance de sortie. La classe de signal 2 avec une sensibilité de 4 dBm, une puissance de 2,5 mW, une portée théorique de 30 m et une grandeur de réseau de l'ordre du Nanonet. La puissance maximale est cependant atteinte par la classe de signal 1 avec une sensibilité de 20 dBm, une puissance de 100 mW, une portée théorique de 100 m et une grandeur de réseau de l'ordre du Micronet. Les réseaux des classes d'émission 3 et 2 sont à ranger dans la catégorie PAN, les réseaux de la classe d'émission 1 représentant un cas limite proche du LAN. Il ne faut cependant pas perdre de vue que dans les solutions actuelles de Bluetooth le taux de transfert des données atteint au maximum

1 Mo/s. Des extensions sont toutefois en cours de réalisation ; le taux de transfert de données souhaité est de 2 Mo/s.

Comme indiqué plus haut, Bluetooth utilise la bande ISM à 2,4 GHz, la plage exacte de fréquence de travail se situant entre 2,402 GHz et 2,480 GHz. La méthode d'accès est un procédé rapide de saut de fréquence, le **F**requency **H**opping **S**pread **S**pectrum (FHSS). On assiste à 1.600 sauts de fréquence par seconde sur 79 pas de 1 MHz. Bluetooth offre une ligne à large bande pour la transmission de la parole et de données et il est possible d'utiliser jusqu'à 3 canaux de parole de 64 Ko/s chacun. Il est en principe possible de choisir entre une transmission synchrone et une transmission asynchrone. La transmission synchrone offre un taux de transfert des données de 433,9 Ko/s. Dans la transmission asynchrone il est possible d'atteindre un taux de transfert de données de 723,2 Ko/s dans le sens descendant et 57,6 Ko/s dans le sens ascendant.

Bluetooth présente trois degrés de sécurité ; seul le dernier degré emploie différentes méthodes de cryptage. Ainsi, lors de l'établissement de la liaison, l'authentification peut s'effectuer selon 128 bits et lors de la transmission des données le cryptage peut atteindre de 8 à 128 bits.

14.2.2.2 Bluetooth - réseau

Dans la classe d'émission 3, le Piconet désigne la grandeur du réseau. Dans un Piconet le nombre d'appareils Bluetooth qui peuvent communiquer entre eux est limité à huit. Les appareils Bluetooth s'identifient au moyen d'un numéro d'identification long de 48 bits ; le premier appareil actif dans le réseau fait fonction de maître et est chargé de la commande des sauts de fréquence. Cela signifie qu'au maximum un maître et sept esclaves peuvent travailler dans un Piconet. Par contre 255 autres appareils Bluetooth peuvent être installés en tant qu'esclaves passifs. Pour autant que cela soit nécessaire, ces appareils peuvent être activés par l'intermédiaire du maître. En outre, il est possible de relier plusieurs piconets pour former ce qu'on appelle un Scatternet. Dans ce cas un esclave commun exerce la fonction d'intermédiaire entre deux Piconets.

14.2.2.3 Bluetooth - avantages et inconvénients

La technologie Bluetooth est un enrichissement dans le segment PAN et permet de connecter simplement des périphériques. L'avantage d'une telle norme ouverte est le succès rapide sur le marché. Ceci doit cependant être nuancé car l'acceptation est très inégale selon les secteurs. Tant que les objectifs de développer des composants Bluetooth très bon marché à 1 chip seront respectés, rien n'enrayera l'utilisation à grande échelle. De plus la marque Bluetooth garantit l'interopérabilité des appareils Bluetooth provenant de différents fabricants. Cependant l'utilisation de la bande de fréquence de 2,4 GHz peut entraîner des perturbations avec des composants WLAN qui travaillent également sur la bande ISM conformément aux normes IEEE802. 11b ou IEEE802. 11g. Il faut également être prudent quant à l'utilisation de Bluetooth pour la transmission de données en réseaux parce que cela constitue un cas limite entre WPAN et WLAN. Dans ce domaine les normes selon IEEE802. 11 ont une position beaucoup plus forte sur le marché et font preuve d'une technologie plus mûre.

15. Réseaux locaux LAN (Local Area Network)

15.1 Définition

Depuis le début de l'ère des technologies de l'information, il existe des réseaux présent sur l'ensemble du globe. Le réseau le plus connu est Internet, qui gagne de plus en plus en popularité. L'important est que tous les avantages d'un réseau puissent profiter aux applications tournant tant dans les petits que les gros réseaux. Les réseaux, qui de par leur étendue, se limitent à un site de société ou à un seul bâtiment, sont désignés par le terme **LAN (Local Area Network)**. Un réseau LAN est constitué au minimum de deux PC et peut être étendu à une multitude de PC et de serveurs. Les objectifs d'une telle interconnexion se distinguent en quatre points importants. D'une part le "réseau de données", facilitant l'accès à des données éloignées, et d'autre part le "réseau de fonctions", permettant l'accès à des ordinateurs proposant des services spéciaux, tels que les serveurs par exemple. Mais aussi "réseau de charge", permettant la répartition de charge entre plusieurs ordinateurs, ainsi que "réseau de disponibilité", c'est-à-dire la garantie déployée par des ordinateurs redondants face à la panne. Dans un réseau LAN, il convient encore de faire la distinction entre les structures reliées par câble et celles dites sans fil. Pour une structure sans fil, on emploie également le terme WLAN (Wireless Local Area Network). Dans les paragraphes qui suivent, il sera tout d'abord question du réseau LAN classique.

15.2 Procédés d'accès

Plusieurs ordinateurs ayant accès à un seul et même moyen de transmission, il convient de régler l'accès simultané et réciproque. La classification des systèmes informatiques mis en réseau repose sur les différents procédés d'accès. Deux procédés d'accès principaux sont à distinguer, d'une part le procédé non déterministe et aléatoire, et d'autre part le procédé déterministe et déterminé. L'exemple le plus connu de procédé non déterministe est le CSMA/CD (Carrier Sense Multiple Access/Collision Detection), qui correspond au procédé d'accès dans Ethernet et 802.3 LAN. Les procédés déterministes fonctionnent le plus souvent selon le principe du "Token", comme par exemple les structures de Token Passing (Token Ring I), Early Token (Token Ring II), Time Token (FDDI) et Polling (VG Any LAN). Ci-après, nous abordons plus en détails les procédés CSMA/CD et Token Passing.

15.2.1 CSMA/CD

CSMA/CD est l'abréviation de Carrier Sense Multiple Access/Collision Detection. Carrier Sense (CS) signifie que l'écoute du moyen de transmission s'effectue selon la communication en cours. Par exemple, si une station désire émettre, elle attend jusqu'à ce que le transmetteur soit libre pour commencer elle-même la transmission, après avoir respecté encore un certain délai d'attente. La notion de Multiple Access (MA), quant à elle, correspond à un accès de même droit et concurrent

sur un moyen commun de transmission. Enfin, le terme Collision Detection (CD) exprime la reconnaissance de collisions par l'écoute du moyen de transmission. Lorsqu'une station a détecté une collision avec d'autres paquets lors de sa transmission, elle émet ce qu'on appelle un signal de détresse et toutes les opérations d'émission sont alors interrompues. Après écoulement d'un délai déterminé, la station tente un nouvel essai de transmission. En raison de cette thématique, on désigne également l'Ethernet comme réseau se basant sur la collision, puisqu'il s'y passe en effet une collision suivant son degré de construction et de charge. Il est important de savoir que le CSMA/CD ne peut fonctionner, que si le double de la durée maximale de signal (RTD, Round Trip Delay) entre les deux stations les plus éloignées est plus courte que la durée de transmission du plus petit paquet admissible dans Ethernet, soit 512 bits. A partir de ce principe est née la règle de répéteur 5-4-3, qui est encore en vigueur aujourd'hui. Cette règle stipule que, dans une structure Ethernet, cinq segments maximum peuvent être couplés à quatre répéteurs et trois Inter-Repeater-Links (IRL, liens inter-répéteur).

15.2.2 Token Passing

Contrairement à CSMA/CD, le Token Passing est un procédé déterminé, où il ne se produit aucune collision. Chaque station ne peut émettre, que si elle possède un modèle déterminé de bit, c'est-à-dire le "Token". Ce "Token" donne droit à l'émission et est transmis de station en station à un successeur physique ou logique. Il s'ensuit une limitation du temps maximal d'émission, bien qu'il soit possible de calculer des temps de réaction dans ces réseaux. Après avoir transmis le Token, la station vérifie si le celui-ci a bien été réceptionné par la station suivante. Si la station suivante réceptionne le Token sans indication de la part de son successeur, elle retiendra d'émettre le Token. Si le deuxième essai échoue également, la station est alors considérée comme défectueuse ou non active. Si un alignement de la station suivante s'effectue correctement au moyen du Token, la station précédente défectueuse ou inactive est sautée et ignorée. Les réseaux fonctionnant selon le principe du Token se révèlent être très intéressants pour les applications qui dépendent de temps garantis de réaction.

15.3 Ethernet et 802.3 LAN

Il est important de démarquer les synonymes Ethernet et 802.3 LAN. Initialement, Ethernet a été développé par DEC-Intel-Xerox avec les procédés d'accès CSMA/CD 1980. Ce standard a cependant été récupéré par l'IEEE (Institute of Electrical and Electronics Engineers) et publié comme standard ISO 802.3 LAN 1990. Les standards se distinguent principalement par les différents formats de cadres, bien qu'ils peuvent coexister dans un même réseau. Les composants réseau actuels ne sont plus fabriqués en principe que selon le standard 802.3. Le jargon professionnel continue cependant de parler d'Ethernet. La topologie logique d'un Ethernet repose sur un système bus. La topologie physique, elle, dépend de différents standards de réseau, mais aussi du fait qu'elle puisse accueillir d'autres formes, telles les structures en étoile.

Modèle en couches

Dans le cas d'un LAN 802.3, la couche 2, couche de sécurité/couche 2, couche lien de données, est encore subdivisée en une sous-couche MAC et une sous-couche LLC. La sous-couche MAC (Medium Access Control) régleme l'accès au moyen de transmission ainsi que la répartition de la capacité de transmission, tandis que la sous-couche LLC (Logical Link Control) établit la liaison avec des protocoles de couches OSI supérieures. Il existe trois types de sous-couches LLC. Le type 1 propose une transmission sans liaison, le type 2 une transmission basée sur une liaison et le type 3 une transmission mixte avec ou sans liaison.

Format de paquets

En présence d'Ethernet, il s'agit d'un réseau communiquant des paquets. Autrement dit, les données à transmettre sont réparties en petites unités, c'est-à-dire en paquets, aussi appelés cadres ou frames. Chaque paquet cherche son propre chemin à travers le réseau et en fin de course seulement, est réuni aux autres. La longueur cadre maximale du cadre d'un paquet de type 802.3 LAN équivaut à 1.518 octets, tandis que la longueur minimale est égale à 64 octets. Cependant, les réseaux actuels nécessitent généralement des paquets plus volumineux. Ceux-ci sont désignés par le terme Jumbo Frames, qui contiennent des paquets supérieurs à 1.500 octets. Pour des raisons de compatibilité en amont, les standards Ethernet actuels ont renoncé à une augmentation de la taille des paquets, ce qui entraîne une perte de performance dans les réseaux à grande vitesse. Les cadres Jumbo peuvent comporter jusqu'à 9.000 octets. Au-delà de cette limite, on est confronté à des restrictions en raison du procédé CRC 32 bits utilisé dans le cadre Ethernet. CRC est l'abréviation de **C**yclic **R**edundancy **C**heck, une vérification effectuée au moyen de polynômes de générateur, dont le résultat est obtenu dans le champ du FCS (Frame Check Sequence). Une augmentation supplémentaire serait certes la bienvenue, mais ne sera cependant pas réalisée dans un avenir proche. Les composants supportant les cadres Jumbo sont généralement spécialement identifiés comme tels. De nombreux composants cependant les supportent tacitement jusqu'à un certain point.

15.4 Adresses MAC

Les adresses MAC ou LAN sont les adresses élémentaires permettant d'identifier clairement les composants d'un réseau local. En principe, il existe deux versions différentes de ces adresses, la variante 16 bits et la variante 48 bits. Dans la version à 16 bits, le premier bit indique s'il s'agit d'une adresse individuelle ou d'une adresse de groupe, tandis que les 15 bits restants servent à l'identification du composant. L'adresse de groupe peut être une adresse de groupe multicast ou une adresse broadcast. Actuellement, on fait presque exclusivement appel aux adresses 48 bits. Pour ces adresses, le premier bit sert également à indiquer s'il s'agit d'une adresse individuelle ou d'une adresse de groupe. En outre, le deuxième bit indique s'il s'agit d'une adresse globale ou d'une adresse locale et les 46 bits restants identifient le composant. Pour les adresses globales, les fabricants de puces contrôleurs doivent acheter les 3 premiers bits de l'adresse MAC auprès de

l'IEEE. Cependant, les fabricants disposent généralement d'un éventail d'adresses, qu'ils peuvent utiliser pour leurs puces contrôleurs. Les 3 autres bits de l'adresse MAC sont attribués par le fabricant lui-même. Ceci garantit que les adresses sont uniques dans le monde entier et qu'il n'en existe aucun duplicat, ce qui pourrait engendrer des complications au sein d'un même réseau. Cependant, comme personne n'est contraint à acheter les adresses de l'IEEE, les adresses peuvent également être allouée de manière locale.

15.5 Standards Ethernet

Il existe de nombreuses réalisations possibles de l'Ethernet. Celles-ci se distinguent par leur vitesse, leur procédé de transmission, leur longueur maximale de segment ainsi que leur type de connecteur. Il existe par exemple la nomenclature du standard 10 BASE-5 selon IEEE802.3. Elle indique qu'il s'agit d'un Ethernet avec transmission de base de 10 Mbit/s, dont la longueur maximale de segment est de 500 m. Ci-après seront abordés les standards les plus importants, qui ont trouvé et trouveront toujours leur application dans la pratique.

15.5.1 10 BASE-5

Le standard 10 BASE-5 selon IEEE802.3 indique qu'il s'agit d'un Ethernet avec transmission de base de 10 Mbit/s et une longueur de transmission maximale de 500 m. Le standard 10 BASE-5 est également connu sous le synonyme de Thick-Net, du fait qu'un câble coaxial, RG8, de 50 Ohm est utilisé comme moyen de transmission. Physiquement, le Thick-Net repose sur la topologie de bus, tout en respectant la règle de répéteur 5-4-3. Cela signifie, que dans un Thick-Net, 5 segments maximum, d'une longueur de 500 m maximum, peuvent être reliés entre eux via 4 répéteurs. Il en résulte un maximum de 3 liens IRL (Inter-Repeater-Link). Un maximum de 100 stations peuvent être connectées par segment, en utilisant le type de connecteur AUI (Attachment Unit Interface); la longueur maximale du câble AUI est de 50 m. Le standard 10 BASE-5 était largement adopté dans le passé, mais n'est plus utilisé dans les nouvelles installations.

15.5.2 10 BASE-2

Le standard 10 BASE-2 selon IEEE802.3a indique qu'il s'agit d'un Ethernet avec transmission de base de 10 Mbit/s et une longueur de transmission maximale de 185 m. Le standard 10 BASE-2 est également connu sous le synonyme de Thin-Net ou Cheaper-Net, du fait qu'un fin câble coaxial, RG58, de 50 Ohm est utilisé comme moyen de transmission. Physiquement, le Thin-Net repose sur une topologie de bus, tout en ayant une longueur minimale de segment de 0,5 m entre deux stations et un nombre limité à 4 répéteurs pouvant être commutés entre deux stations. Un maximum de 30 stations peuvent être connectées par segment, en utilisant le type de connecteur BNC T Adapter. Le standard 10 BASE-2 était largement adopté dans le passé, mais n'est plus utilisé dans les nouvelles installations.

15.5.3 10 BASE-T

Le standard 10 BASE-T selon IEEE802.3i indique qu'il s'agit d'un Ethernet avec transmission de base de 10 Mbit/s et une longueur de segment maximale de 100 m avec câblage en cuivre. Un câble paire torsadée répondant à divers standards est utilisé comme moyen de transmission, avec des types de connecteurs RJ-45. Nous aborderons encore en détails les différents standards régissant le câblage dans un chapitre ultérieur. Le standard 10 BASE-T repose physiquement sur une topologie en étoile, dans laquelle un composant actif qui concentre les stations en forme d'étoile entre en action; ce concentrateur sert simultanément d'amplificateur. Le standard 10 BASE-T était largement adopté dans le passé mais, lui non plus, n'est plus utilisé dans les nouvelles installations.

15.5.4 10 BASE-FL

Le standard 10 BASE-FL selon IEEE802.23j indique qu'il s'agit d'un Ethernet avec transmission de base de 10 Mbit/s et une longueur de segment maximale de 2.000 m avec câblage à fibre optique. Le moyen de transmission utilisé ici est un câble duplex à fibre optique, muni très souvent de connecteurs ST. Les différents standards régissant le câblage seront abordés en détail dans un chapitre ultérieur (15.9). Ce standard est une extension de FOIRL (Fiber Optic Inter Repeater Link) et définit la liaison entre les concentrateurs de même qu'entre les stations et les concentrateurs. Le standard 10 BASE-FL était largement adopté dans le passé mais n'est cependant plus utilisé dans les nouvelles installations.

15.5.5 100 BASE-TX

Le standard 100 BASE-TX selon IEEE802.3u indique qu'il s'agit d'un Fast Ethernet avec transmission de base de 100 Mbit/s et une longueur de segment maximale de 100 m avec câblage en cuivre. Un câble paire torsadée en cuivre répondant à divers standards est utilisé comme moyen de transmission, avec des types de connecteurs RJ-45. Les différents standards régissant le câblage seront abordés en détail dans un chapitre ultérieur (15.9). Le standard 100 BASE-TX repose physiquement sur une topologie en étoile, dans laquelle un composant actif qui concentre les stations en forme d'étoile entre en fonction ; ce concentrateur sert simultanément d'amplificateur. Le standard 100 BASE-TX a déjà été adopté dans beaucoup d'installations et est très souvent utilisé dans les nouvelles installations.

15.5.6 100 BASE-FX

Le standard 100 BASE-FX selon IEEE802.3u indique qu'il s'agit d'un Fast Ethernet avec transmission de base de 100 Mbit/s et une longueur de segment maximale de 400 m entre stations et concentrateurs et de 2.000 m entre concentrateurs. Le moyen de transmission ici utilisé est un câble duplex à fibre optique, muni très souvent de connecteurs ST, SC, MT-RJ ou VF-45. Les différents

standards régissant le câblage seront abordés en détail dans un chapitre ultérieur. Le standard 100 BASE-FX repose sur le FDDI (Fiber Distributed Data Interface), qui fonctionne toutefois selon le procédé de Time Token. Ce standard s'est largement imposé et est, lui aussi, utilisé pour des nouvelles installations dans un environnement à fibre optique.

15.5.7 1000 BASE-T

Le standard 1000 BASE-T selon IEEE802.3ab indique qu'il s'agit d'un Gigabit Ethernet avec transmission de base de 1.000 Mbit/s et une longueur de segment maximale de 100 m dans la zone de connexion. Un câble paire torsadée en cuivre répondant à divers standards est utilisé comme moyen de transmission, avec des types de connecteurs RJ-45. Les différents standards régissant le câblage seront abordés en détail dans un chapitre ultérieur (15.9). Le standard 1000 BASE-TX repose physiquement sur une topologie en étoile, dans laquelle un composant actif qui concentre les stations en forme d'étoile entre en fonction; ce concentrateur sert simultanément d'amplificateur. Le standard 1000 BASE-T repose sur les standards 100 BASE-T2 et 100 BASE-T4, qui définissent les propriétés de la transmission via un câble en cuivre de catégorie 3, utilisant plus de deux paires de fils. Pour atteindre une vitesse de 1.000 Mbit/s, chaque paire de fils transmet 250 Mbit/s. Ce standard jouit d'un engouement toujours plus large et est utilisé dans les nouvelles installations.

15.5.8 1000 BASE-SX

Le standard 1000 BASE-SX selon IEEE802.z indique qu'il s'agit d'un Gigabit Ethernet avec transmission de base de 1.000 Mbit/s sur une courte longueur d'onde. En d'autres termes, une longueur d'onde de 850 nm est utilisée afin de ponter un éloignement, selon le type de câble à fibre optique, d'une longueur maximale de 275 m pour des fibres multimode de 62,5/125 microns et de max. 550 m pour des fibres multimode de 50/125 microns. Ce standard utilise une liaison point à point, c'est à dire qu'il utilise le procédé CSMA/CD. En général, les connecteurs utilisés sont de type SC, mais les autres types MT-RJ ou VF-45 sont aussi adoptés. Par rapport à l'alternative en cuivre, ce standard est aussi largement répandu et est également utilisé dans les nouvelles installations à fibre optique.

15.5.9 1000 BASE-LX

Le standard 1000 BASE-LX selon IEEE802.3z indique qu'il s'agit d'un Gigabit Ethernet avec transmission de base de 1.000 Mbit/s sur une longue longueur d'onde. En d'autres termes, une longueur d'onde de 1.300 nm est utilisée afin de ponter un éloignement, selon le type de câble à fibre optique, de max. 550 m pour des fibres multimode de 62,5/125 ou 50/125 microns et de max. 5.000 m pour des fibres singlemode de 9/125 microns. Des distances plus importantes peuvent également être raccordées, mais il s'agit en général de systèmes spécifiques au fabricant, qui ne sont compatibles qu'entre eux. Ce standard utilise une liaison point à point, sans utiliser le procédé

CSMA/CD. Le type de connecteur utilisé est généralement le type SC. Outre le standard 1000 BASE-SX, le standard 1000 BASE-LX est un système appartenant au domaine primaire de fibre optique du câblage structuré et est largement utilisé dans ces environnements.

15.5.10 Auto-négociation

Le protocole **Auto-Negotiation Protocol (ANP)** a été établi dans le cadre du standard Fast Ethernet. Il entre en action lorsque les appareils veulent communiquer au choix entre 10 Mbit/s ou 100 Mbit/s. Le protocole ANP se base sur le protocole Nway de National Semiconductor, dont il est souvent fait mention. Le protocole définit automatiquement la vitesse la plus élevée que les partenaires de communication connectés peuvent atteindre. En outre, le mode de fonctionnement est sélectionné, soit half duplex ou full duplex, comme décrit dans le chapitre sur le procédé de transmission. Le protocole ANP est idéal pour les composants fonctionnant sous 10 BASE-T et 100 BASE-T. Il ne peut cependant pas être utilisé avec le standard 100 BASE-FX, car les différentes longueurs d'onde en transmission optique ne peuvent garantir une interopérabilité. Le protocole ANP est recommandé pour le standard 1000 BASE-T. Le protocole ANP peut engendrer des difficultés, lorsque des stations ne répondent pas aux paquets de contrôle émis, ce qui déclenche automatiquement le mode half duplex. Et si le partenaire de communication a été manuellement activé sur full duplex, la liaison ne peut pas être établie.

15.6 Topologies en anneau

Dans les topologies dites à anneau, les données sont transmises en série dans une direction et généralement transférées de station en station de manière séquentielle. Généralement, une station prend la responsabilité de commande dans l'anneau. De par la structure, la panne d'une station entraîne automatiquement la panne de tout le réseau. En pratique cependant, l'intervention de concentrateurs ou de structures à anneau double permet d'éviter ce cas de figure. Dans les topologies à anneau, la durée de transmission augmente proportionnellement avec l'ajout d'autres stations. Il en résulte d'une part des temps de réaction calculables, mais d'autre part également une diminution de la vitesse de transmission.

15.6.1 Token Ring

Dans un réseau LAN Token Ring selon IEEE802.5, une topologie logique à anneau repose sur une topologie physique en étoile. Dans cette structure, la panne d'une seule station n'entraîne plus la panne de tout le réseau. Le concentrateur utilisé dans cette structure est appelé MAU (Multistation Access Unit). La première configuration de Token Ring permet d'atteindre des taux de transmission de 4 Mbit/s, tandis que la deuxième réalise, elle, des taux de transmission de 16 Mbit/s. La configuration I de Token Ring fonctionne selon le procédé du Token Passing et la configuration II selon le procédé Early Token.

Token Ring a été baptisé selon un modèle de bit déterminé, le fameux Token, qui tourne suivant le parcours d'un anneau. Seule la station disposant du Token libre est capable d'émettre. Après avoir réceptionné l'anneau libre, la station désireuse d'émettre bascule du mode attente en mode émission. Les données à transmettre sont attachées au Token libre, qui est donc occupé par ces données. Cela signifie, qu'aucune des autres stations ne peut modifier son statut lorsque le Token est occupé; elles restent alors en mode d'attente. La station en mode d'émission transmet jusqu'au moment où la transmission est terminée ou encore jusqu'à ce qu'un intervalle de temps précis soit écoulé.

Cette deuxième possibilité permet de respecter des temps de réaction prédéfinis. Lorsque la transmission est terminée, la station émettrice retourne en mode d'attente et libère ainsi le Token dans l'anneau afin de permettre aux autres stations d'émettre à leur tour. Dans la configuration I de Token Ring, la longueur maximale de cadre est de 4.500 octets, le nombre maximum de stations par segment de 260 et l'extension maximale par segment de 150 m pour un câblage UTP et de 250 m pour un câblage STP. Par contre, dans la configuration II de Token Ring, la longueur maximale de cadre est de 16.000 octets, le nombre maximum de stations par segment de 188 et l'extension maximale par segment de 100 m pour un câblage UTP et de 150 m pour un câblage STP.

Il existe cependant ce qu'on appelle des standards propriétaires spécifiques aux fabricants, qu'il faut prendre en considération. Les différents types de câble ont également de l'importance. Une erreur typique commise dans un réseau LAN Token Ring, est le fait d'ajouter des stations fonctionnant à des vitesses différentes. Dans ce cas de figure, la station réceptionne un Token qui n'est pas valable et émet un Beacon (balise), qui paralyse le réseau. On parle dès lors de Beaconsing (balisage). En parallèle au Token Ring existe aussi le standard Token Bus selon IEEE802.4, suivant lequel une topologie logique en anneau repose sur une topologie physique de bus. Le système de Token Bus est cependant peu répandu.

15.6.2 FDDI

FDDI est l'abréviation de **F**iber **D**istributed **D**ata **I**nterface et est une norme ISO créée par ANSI X3T9.5. FDDI est un standard pour les réseaux LAN et MAN, construits sur une structure fibre optique à double anneau et réalisant des taux de transfert de données atteignant 100 Mbit/s. Deux types de stations pouvant y être connectées sont à distinguer : les stations de classe A d'une part et de classe B d'autre part, aussi appelées station DAS (Dual Attached Station) et SAS (Single Attached Station). Les stations de la classe A disposent de deux interfaces et peuvent être connectées de manière redondante à un anneau double fibre optique, tandis que les stations de la classe B ne disposent que d'une seule interface. Dans la configuration standard, on retrouve un anneau primaire et un anneau secondaire. La présence de ces deux anneaux garantit, qu'en cas de panne d'une ligne ou d'une station, la transmission de données puisse se poursuivre. En effet, l'anneau secondaire est activé et forme, ensemble avec l'anneau primaire, un nouvel anneau complet. Ce système ne fonctionne que si les stations concernées directement connectées à l'anneau sont de classe A. La structure en anneau double et la reconfiguration en cas d'interruption garantissent donc une

sécurité face aux pannes. FDDI convient particulièrement aux réseau MAN, car l'éloignement maximal entre deux stations FDDI est de 2 km en présence de fibres multimode et de 10 km en présence de fibres monomode. La plus grande distance que l'on peut ponter est de 100 km. Bien qu'initialement l'interface FDDI ait été conçue pour la fibre optique, il existe entre temps une variante basée sur le cuivre, appelée CDDI (Copper Distributed Data Interface). Avec l'interface CDDI, il n'est plus nécessaire que de ponter la distance de 100 m entre les différentes stations, distance typique au cuivre.

15.7 Protocoles/standards

Chaque station connectée à un réseau nécessite aussi bien un pilote réseau adéquat qu'un pilote de protocole, qui établit les liaisons vers les couches de protocole supérieures. En matière de protocoles LAN, intervient une grande variété de protocoles et non pas un seul. Un protocole est nécessaire pour réaliser la communication entre deux instances. Il représente en fait le langage commun des deux instances. Ci-après sont présentés quelques protocoles LAN importants.

15.7.1 Protocoles

15.7.1.1 NetBIOS

NetBIOS est l'abréviation de **N**etwork **B**asic **I**nput **O**utput **S**ystem. Ce protocole a été conçu par IBM en 1984, il est indépendant du matériel et peut donc être mis en oeuvre dans des réseaux Ethernet et Token Ring. Il réalise une partie de la couche 2 et met à disposition les fonctions des couches 2 et 5. La couche 3 n'est implémentée qu'en tant que couche nulle, où ce protocole n'a pas de fonction de routage. Le routage n'était, à cette époque, pas encore un sujet aussi significatif qu'aujourd'hui. Le NetBIOS permet la communication via des noms symboliques au lieu de réseaux, mais leur nombre en est cependant limité.

15.7.1.2 NetBEUI

NetBEUI est l'abréviation de **N**etwork **B**ios **E**xtended **U**ser **I**nterface, qui est une interface créée par IBM en 1985. Il s'agit d'une interface utilisateur développée reposant sur NetBIOS. Le protocole n'y a pas de fonction de routage non plus, car tout comme le prédécesseur, la couche 3 n'y est implémentée qu'en couche nulle. NetBEUI fournit une performance élevée dans les réseaux locaux comprenant un nombre maximum de 200 stations et est configuré comme protocole standard dans de nombreux systèmes d'exploitation. Si une communication est nécessaire au-delà de la couche 2, d'autres protocoles entrent en jeu, tel le TCP/IP, qui sera abordé plus en détail dans le chapitre WAN.

15.7.1.3 NDIS

NDIS ou **N**etwork **D**river **I**nterface **S**pecification **S**upport est une interface de programmation entre la couche 2 et les protocoles que celle-ci utilise. NDIS fonctionne comme interface indépendante du protocole et sert d'intermédiaire entre le pilote réseau et les protocoles des autres couches.

15.7.1.4 ODI

ODI ou **O**pen **D**ata **L**ink **I**nterface a été développé par Novell et convient pour les piles de protocoles NetWare. ODI travaille sur la couche 2 et simule une carte réseau virtuelle, permettant d'envoyer divers formats de paquets. ODI est indépendant du matériel utilisé et forme l'interface entre les protocoles des couches supérieures.

15.7.2 Standards

Sous le mot standard, on désigne des définitions généralement reconnues comme solution à un état de faits. Le standard parcourt, au sein d'un organe de normalisation, différentes étapes d'évolution, pour représenter en fin de parcours une solution technique mûre. Ci-après, nous abordons les standards LAN de l'IEEE (**I**nstitute of **E**lectrical and **E**lectrical **E**ngineers), un organe américain de normalisation composé d'ingénieurs, qui établissent des normes au niveau international. Le groupe de travail 802 fait progresser les standards relatifs aux réseaux locaux, qui ont fourni une contribution précieuse dans l'industrie IT. Les standards selon IEEE802.1 sont particulièrement intéressants. Ce sont des standards d'un niveau supérieur pour les domaines de LAN/MAN Bridging et de Management.

15.7.2.1 VLAN selon IEEE802.1q

VLAN est l'abréviation de Virtual LAN (LAN virtuel) et permet, au sein d'un réseau Ethernet, d'établir isolément des domaines d'émission séparés l'un de l'autre. Les stations connectées dans un VLAN ne peuvent communiquer qu'avec leurs partenaires de communication à l'intérieur de leur propre VLAN. Si la communication est requise au-delà du VLAN, il faut recourir à des composants actifs, qui travaillent sur la couche 3. Ces composants peuvent être aussi bien des routeurs que des commutateurs à plusieurs couches. Le VLAN donne la possibilité de limiter le trafic de données au sein d'un Ethernet, afin d'augmenter la performance de tout le réseau. Les réseaux VLAN servent en général à réunir différentes unités d'organisation, comme par exemple des départements, au sein d'une société. Les réseaux VLAN selon IEEE802.1q ou VLAN tagging, fonctionnent sur la couche 2 et marquent au moyen de repères spéciaux les cadres Ethernet émis par les stations individuelles, pour les affecter à des VLAN différents. Il s'agit donc ici de VLAN logique et non pas physique, comme c'est le cas par exemple d'un VLAN fonctionnant sur un port. L'administrateur gagne ainsi une flexibilité considérable, dès que les composants actifs supportant la fonction de VLAN

tagging entrent en action. En effet, chaque station d'un appareil peut être affectée à un VLAN déterminé. Et si par exemple, les structures du réseau devaient être modifiées, l'appareil n'en serait nullement perturbé.

15.7.2.2 CoS selon IEEE802.1p

CoS est l'abréviation de **Class of Service**. C'est un moyen de classifier le trafic de données au sein d'un LAN selon différentes applications, par exemple : e-mail, transfert de fichiers, voix, vidéo, etc... Chaque classe est attribuée d'une priorité propre, qui est respectée et traitée de manière correspondante dans la file d'attente. Il est important cependant de ne pas confondre CoS avec QoS (Quality of Service). CoS ne peut attribuer aucune largeur de bande, comme c'est le cas dans QoS, mais assigne une priorité de paquets, qui sont transmis cependant selon le principe du Best-Effort. CoS fonctionne sur la couche 2 et offre tout simplement la possibilité de mieux utiliser les ressources. CoS marque les cadres Ethernet à l'aide de repères spéciaux, qui sont affectés à la classe de chaque groupe. Outre la fonction de CoS, cette technique a aussi recours à la fonction ToS (Type of Service), qui offre une autre possibilité de classe de service, en plus du DiffServ (Differentiated Services). DiffServ fonctionne autrement et analyse le PHB (Port Hop Behaviour), afin d'optimiser l'utilisation de la largeur de bande disponible.

15.7.2.3 Spanning Tree selon 802.1d

Lorsque plus de deux ponts sont mis en oeuvre dans un réseau local, le protocole STP (Spanning Tree Protocol) fait en sorte que la communication n'ait lieu que par un seul pont et qu'aucun Bridge Loops (boucle de ponts) ne se forme. Les ponts séparent les domaines de collision les uns des autres, en analysant le trafic de données et désignant la branche du réseau sur laquelle l'adresse de destination du destinataire doit se trouver. Le trafic de données n'est donc plus réparti sur l'ensemble du réseau, mais limité à quelques branches. Du fait que les ponts analysent le réseau de manière autodidacte, ils sont également appelés ponts transparents. Nous reviendrons sur les différents composants matériels des réseaux locaux dans le chapitre Matériel. Dans un réseau, la coexistence de plusieurs ponts et la liaison de segments sur différentes voies peuvent provoquer ce qu'on appelle des boucles de pont, ce qui peut porter un préjudice durable au trafic de données. Le protocole STP commande le fait que les ponts communiquent entre eux au moyen de BPDU (Bridge Protocol Data Units) et que seuls les trajets les plus efficaces entre deux stations soient utilisés, tout en négligeant tous les autres trajets. En cas de panne d'un trajet, le réseau sera reconfiguré à l'aide d'un algorithme STP afin de trouver le meilleur trajet restant. L'inconvénient du protocole STP est son temps de reconfiguration assez long, de 30 à 60 secondes. L'IEEE a résolu ce problème au moyen du protocole RSTP (Rapid Spanning Tree Protocol) selon IEEE802.1w, dont les temps de reconfiguration sont nettement plus courts par rapport au STP. Ce protocole ne fonctionne cependant pas dans les réseaux Token Ring.

15.7.2.4 Agrégation de liens selon IEEE802.3ad

L'agrégation de liens est un moyen de rassembler plusieurs liens physiques en un seul lien logique, pour augmenter la largeur de bande et garantir la tolérance à la panne. Il s'ensuit que la panne d'un lien entre deux partenaires de communication n'entraîne plus l'interruption de la liaison. La liaison peut être maintenue, en diminuant uniquement la largeur de bande. L'agrégation de liens pour atteindre des largeurs de bande plus élevées est une méthode simple d'utiliser les technologies existantes pour obtenir des taux plus élevés de transfert de données. Elle présente l'avantage de ne pas devoir modifier complètement la technologie réseau existante. L'agrégation de liens est mise en oeuvre dans les réseaux Ethernet cuivre et fibre optique de 100 Mbit/s et 1.000 Mbit/s. L'agrégation de liens Gigabit Ethernet représente cependant un intérêt particulier, car elle permet de combler la lacune tant que la solution économique de 10 réseaux Gigabit Ethernet n'est pas réalisable. Auparavant, on recourait souvent au terme de Trunking ou de Port Trunking, qui est cependant déjà employé dans un autre contexte et qui, en anglais, désigne des réseaux hertziens régionaux. C'est pourquoi le groupe de travail IEEE a choisi le nom de Link Aggregation.

15.8 Matériel - composants actifs

15.8.1 Répéteurs

Un répéteur est un composant actif, qui fonctionne sur la couche 1 d'un réseau LAN Ethernet et qui est responsable des fonctions de régénération. Un répéteur entre en action, lorsque l'extension physique maximale d'un segment est atteinte et qu'elle nécessite alors une augmentation supplémentaire. Le répéteur est responsable des fonctions de régénération, c'est-à-dire qu'il régénère le niveau et la cadence en cours du signal. En outre, le répéteur dispose d'une certaine capacité de reconnaissance d'erreur. Il peut limiter des signaux défectueux ou des collisions à un segment déterminé, ce qui permet d'augmenter la performance. Du fait qu'un répéteur travaille sur la couche 1, il est entièrement transparent au protocole et sert uniquement à étendre le segment au-delà des limites physiques d'une topologie.

15.8.2 Concentrateurs

Un hub ou concentrateur est en principe un répéteur à plusieurs ports et donc un composant actif, qui fonctionne sur la couche 1 d'un réseau LAN Ethernet. Le hub sert de concentrateur dans une topologie en étoile et peut relier plusieurs stations et segments à l'aide de divers connecteurs et moyens de transmission. On distingue différents concentrateurs suivant l'emplacement où ils interviennent, par exemple, concentrateur pour groupe de travail, pour département ou pour entreprise. Selon leur lieu d'intervention, ils se distinguent encore par leur taille et leur extensibilité. La puissance d'un concentrateur est principalement déterminée par ses bus internes, qui forment un fond de panier.

15.8.3 Ponts

Un pont est un composant actif, fonctionnant sur la couche 2 d'un réseau LAN Ethernet. La plupart des ponts mis en oeuvre dans des réseaux LAN Ethernet fonctionnent particulièrement sur la sous-couche MAC et rarement sur la sous-couche LLC. Par contre, dans les autres topologies, telle que le Token Ring par exemple, qui exigent un peu plus d'intelligence, les appareils fonctionnent très souvent sur la sous-couche LLC. Un pont entre en action, d'une part lorsque l'extension physique maximale d'un segment est atteinte et d'autre part, lorsqu'elle nécessite une extension supplémentaire. Le pont est responsable des fonctions de régénération et dispose d'une capacité de reconnaissance d'erreur. Une autre fonction du pont est de séparer les domaines de collision les uns des autres, en analysant les paquets de données en fonction de leur adresse MAC.

Un pont mémorise avec le temps, quelles stations se trouvent sur quels segments et peut dès lors décider, s'il est nécessaire de diffuser le trafic de données sur l'ensemble du réseau. Si transmetteur et récepteur devaient se trouver sur le même segment, la communication est alors limitée à ce segment. On parle dans ce cas de "Learning Bridges", car ces ponts connaissent les adresses du réseau local. Dès qu'un Learning Bridge fait appel au protocole STP (Spanning Tree Protocol), on parle aussi de pont transparent. Les ponts transparents utilisent le protocole STP pour trouver un chemin de communication sans lacet dans le réseau.

Des lacets sont susceptibles d'apparaître, lorsque plusieurs ponts entrent en action et qu'il existe plusieurs voies pour la transmission de données. Les ponts transparents jouent un rôle prépondérant, car ces lacets peuvent paralyser la communication de données. Derrière le terme de pont transparent se cache aussi la propriété de transparence vis-à-vis des stations connectées dans le réseau. Cette propriété repose sur le fait que les ponts ne modifient pas les paquets et qu'ils travaillent uniquement sur la couche 2 d'un réseau LAN. Il existe encore d'autres types de ponts, citons notamment les ponts Encapsulation, Translation ou Source Routing Bridges.

Un pont Encapsulation, comme son nom l'indique, encapsule le cadre d'un protocole dans la zone de données d'un autre protocole, pour pouvoir aussi transmettre des données via des trajets, qui ne sont pas supportés par son propre protocole. Ce type de pont permet par exemple de transmettre des cadres Ethernet via un réseau FDDI. Ce procédé est également souvent appelé Tunneling. L'entête de protocole qu'initie l'imbrication est l'inconvénient de ce procédé, entraînant un gaspillage de la largeur de bande sur le moyen de transmission.

Dans les ponts Translation, les adresses correspondant au type d'un standard de cadre sont traduites en un type d'un autre standard de cadre. Enfin, pour que la communication puisse avoir lieu, les types de cadre de longueur minimale et longueur maximale doivent être adaptés, pour permettre aux deux standards présents de travailler avec ces cadres. Les ponts Source Routing sont utilisés pour permettre la transmission entre deux réseaux Token Ring différents.

15.8.4 Commutateurs

Un commutateur est en principe un pont à plusieurs ports et donc un composant actif, qui fonctionne sur la couche 2 d'un réseau LAN Ethernet. Dans cette configuration, les commutateurs, comme leur nom l'indique, sont responsables des fonctions de commutation et servent de concentrateur dans les réseaux organisés en étoile. Le noyau d'un commutateur forme ce que l'on appelle la fabrique de commutation, qui détermine la performance. Il est encore à noter que les taux de réacheminement et de filtrage caractérisent la capacité d'un commutateur. Le taux de réacheminement décrit le nombre maximal de paquets de données pouvant être transportés à la seconde, tandis que le taux de filtrage désigne le nombre maximal de paquets de données traités et d'adresses MAC gérables. On fait encore une distinction entre les commutateurs suivant leur procédé de commutation ; ils sont de type Cut-Through, Fragment-Free et Store-and-Forward. Les commutateurs de type Cut-Through font simplement passer les paquets de données, de telle sorte à maintenir le temps de ralentissement le plus court possible.

Une fois l'adresse d'expédition communiquée, le commutateur n'attend pas la fin de la transmission des données, mais fait passer les données directement. Dans ce procédé, mise à part l'adresse d'expédition, les informations contenues dans le paquet n'ont pas d'importance. Ceci permet de réduire considérablement le temps de ralentissement. Dans le type de commutateur Fragment-Free, un certain laps de temps est respecté pour éviter toute collision dans le segment de destination. Le type de commutateur le plus fréquemment employé est cependant celui de Store-and-Forward, qui sauvegarde provisoirement les données dans le commutateur avant de les transférer. L'avantage de ce procédé réside dans le fait que les données sont soumises à une opération de reconnaissance et de correction d'erreur. Mais cet avantage a aussi un inconvénient, à savoir qu'il induit un temps de ralentissement beaucoup plus important.

Commutation de couche 3

Cette technique est de plus en plus mentionnée sous la notion de couche 3 ainsi que sous d'autres synonymes. Dans ce paragraphe, nous apporterons un peu plus de lumière sur cette technique. En effet, comme déjà mentionné ci-dessus, cette technologie est chapeautée par tout un groupe de synonymes, en plus de la notion de commutation de couche 3. Il est parfois fait mention de routeurs de commutation, de commutation de couche 4, voire même de commutation à plusieurs couches. Tous ces termes désignent pourtant la même et unique technologie, que nous définissons dans ce qui suit par le terme de commutation de couche 3.

Il est faux de croire, que seuls la largeur de bande ou la commutation de paquet puissent augmenter la performance d'un réseau. Les avantages d'un commutateur de couche 3 proviennent du fait que les composants décisifs, outre la commutation de paquet, sont le processus de routage et les services de réseau intelligents. Ces trois facteurs forment effectivement le fondement sur lequel est construit un commutateur de couche 3. Un commutateur de couche 3 peut s'interpréter comme routeur hautement performant destiné à des réseaux locaux; comparé à un commutateur classique de couche 2, il fonctionne sur les couches supérieures du modèle de référence OSI.

L'implémentation physique est elle aussi différente de celle des routeurs classiques.

Dans les routeurs classiques, la commutation de paquets repose sur des moteurs à microprocesseurs, tandis que dans les commutateurs de couche 3, cette commutation fonctionne selon des technologies basées sur le matériel, à savoir des circuits ASIC (Application Specific Integrated Circuits). Il en résulte que les routeurs classiques travaillent selon une vitesse exprimée en Kpps, tandis que la vitesse des commutateurs de couche 3 est exprimée en Mpps. À part ces implémentations différentes, les routeurs classiques et les commutateurs de couche 3 ont beaucoup de points communs. Grâce au processus de routage, la commutation de paquets d'un commutateur de couche 3 basée sur du matériel est dirigée dans la bonne direction. Le processus de routage est une implémentation faisant appel à un logiciel mais qu'il convient de considérer comme indépendante de la commutation de paquets. Le processus de routage repose sur des protocoles tels que RIP, RIPv2, OSPF, OSPFv2, qui commandent les paquets et la direction d'acheminement. Ces protocoles génèrent donc des tableaux de routage, qui représentent les structures de réseau en constante modification. Un commutateur de couche 3, non doté des protocoles de routage adéquats, est pour ainsi dire un appareil dépourvu de chauffeur.

Les services réseau intelligents (Intelligent Network Services) constituent un autre avantage du commutateur de couche 3. Il s'agit des fameux value-added Services, tels que la gestion, la sécurité, le protocole IP multicasting et la qualité de service (QoS). Dans ce contexte, la qualité du service est à souligner plus particulièrement. Le terme de QoS désigne tous les procédés pouvant influencer le trafic de données, de telle sorte que le destinataire reçoive le service dans une qualité déterminée. Le rôle toujours plus important que joue le QoS s'explique par le type des données transmises. Auparavant, il s'agissait principalement de transfert de fichiers et de courriers électroniques. Depuis, les applications des domaines de la parole et de la vidéo sont de plus en plus répandues. Ces applications dépendent de la qualité des services en matière de temps de latence, de taux de perte de paquets ainsi que de largeur de bande. Pour obtenir une fonction QoS, l'institut de normalisation IEEE propose un grand nombre de solutions diverses. Actuellement, les modèles QoS émanant des fabricants sont peu homogènes et la préférence va souvent à des solutions propriétaires d'un seul fabricant. Malheureusement, la flexibilité en matière d'équipement de réseau souffre de cet état de fait. D'autres services réseau intelligents permettent aussi d'augmenter la performance générale d'un réseau et ceci sans devoir augmenter les largeurs de bande. Cet avantage ainsi que les autres déjà décrits ci-avant, favoriseront à l'avenir l'utilisation des commutateurs de couche 3.

Cascading/Stacking

Dans le contexte des solutions de commutation s'intercalent aussi les notions de stacking et de cascading (empilement et cascade). Ces deux termes font référence à la possibilité de relier un ou plusieurs commutateurs en une seule unité et ce, de plusieurs manières. La différence essentielle entre le cascading et le stacking est la suivante : dans le cascading, les commutateurs sont reliés entre eux par des ports standard et dans le stacking par des ports d'empilement spéciaux. Dans le cascading, l'interface entre les deux appareils peut devenir un goulot d'étranglement et avoir des effets néfastes sur la performance du réseau. Par contre, dans le stacking, on fait appel,

pour relier plusieurs commutateurs, à des ports spécialement prévus à cet effet. Les deux appareils peuvent dans ce cas être reliés entre eux avec la largeur de bande totale et former une unité. Dans les solutions de stacking, il est possible d'aborder la pile physique de commutateurs comme un commutateur logique via une adresse IP. La maintenance des appareils s'en trouve considérablement simplifiée. Il ne faut cependant pas oublier que les solutions d'empilement peuvent être spécifiques selon le fabricant ou le produit. Il existe une autre solution d'empilement que le système classique, proposée par de nombreux fabricants. Elle permet de gérer de manière centrale, en un seul empilement, des commutateurs répartis sur le réseau, même si ceux-ci ne sont pas reliés physiquement entre eux. Cette solution est cependant l'alternative extrême par rapport à l'empilement classique.

Commutateurs modulaires

Considéré d'un point de vue matériel, on peut faire la distinction entre deux types fondamentaux de commutateurs. Ce sont d'une part les commutateurs à configuration fixe, qui sont déterminés par la structure de leurs ports et qui sont surtout mis en oeuvre dans la zone frontière et d'autre part, les commutateurs modulaires, à configuration flexible de par leur structure de port, surtout mis en oeuvre dans la zone code.

Remarquons toutefois que de nombreux commutateurs utilisés dans la zone frontière des réseaux locaux sont également extensible de manière modulaire. Ces commutateurs disposent d'une configuration de ports fixe dotée d'emplacements supplémentaires extensibles pour accueillir d'autres modules, pouvant être équipés de divers modules d'interface. En présence d'une offre variée de modules différents, une installation peut être effectuée en toute flexibilité à partir de standards Ethernet et des interfaces de supports. Actuellement on distingue deux types de modules. D'une part les modules uplink, convenant généralement uniquement pour un type déterminé d'appareil d'un fabricant bien précis. Cependant, les fabricants de produits réseau ont concentré leurs efforts, pour développer un standard de module homogène. Le résultat de ces efforts est le GBIC, abréviation de **Giga bit Interface Converter**. Les modules GBIC sont des modules Gigabit Ethernet, pouvant se loger en principe dans tous les emplacements de module GBIC. A cause de développements spécifiques aux fabricants divers et malgré un standard de module et un facteur de forme homogène, une interopérabilité générale n'a pas pu être assurée. Les modules GBIC permettent même de relier de manière flexible des commutateurs de zone frontière.

Les commutateurs modulaire que l'on rencontre dans la zone code, peuvent généralement être configurés de façon entièrement modulaire. Un module constitué d'un châssis, de tiroirs pour contrôleurs commutateurs et pour interfaces, permet de réaliser une multitude de configurations de ports. En raison de la fonction centrale de ces commutateurs, les composants existants sont généralement redondants afin d'éviter la panne totale du réseau.

15.9 Matériel - composants passifs

Quand on parle de composants passifs dans la technique réseau, il s'agit du câblage du réseau. La constante modification des technologies réseau soumet le moyen de transmission physique à des exigences toujours différentes. Les critères de sélection d'un câblage sont insensibilité aux parasites, possibilités d'extension et surtout les éloignements à palier, ainsi que les vitesses de transmission et bien sûr le coût du câblage. Le câblage doit présenter une sécurité d'investissement et pouvoir s'utiliser même avec des standards futurs. Le choix des composants passifs doit dès lors répondre aux exigences les plus sévères, car ils sont la base d'un réseau performant.

15.9.1 Câblage structuré

Un modèle de structure pour des méthodes universelles de câblage a été conçu pour la technique de câblage. Dans ce contexte, une structure est synonyme de moyens de transmission aussi similaires que possible pouvant réaliser la transmission du plus grand nombre possible d'applications. La réalisation s'effectue par la formation de différents degrés de hiérarchie. Le **domaine primaire** caractérise un câblage reliant plusieurs bâtiments entre eux, souvent au moyen de routes redondantes de câblage, qui commencent et s'arrêtent à des répartiteurs d'étages. En raison des éloignements à palier, le domaine primaire fait en général appel au câblage à fibre optique. Dans le **domaine secondaire**, les répartiteurs de bâtiments sont reliés aux répartiteurs d'étages, et on parle alors de domaine vertical. Enfin, dans le **domaine tertiaire**, les répartiteurs d'étages sont reliés aux appareils finaux, et on parle alors de domaine horizontal.

15.9.2 Concept de système dorsal

Parallèlement au développement du câblage structuré sont nés deux concepts essentiels de segment fédérateur. Le segment fédérateur forme au sens propre du terme, l'épine dorsale d'un réseau, que toutes les données parcourent vers les stations connectées.

Dans le concept de **Collapsed Backbone**, le segment fédérateur est concentré sur un seul concentrateur puissant et toutes les stations sont reliées directement à ce concentrateur. L'avantage de ce concept repose sur le fait qu'il n'existe aucun autre composant actif qui puisse engendrer des temps de ralentissement, et que chaque station connectée dispose théoriquement de l'entière bande de la largeur de bande du trajet connecté. Cette centralisation permet de réduire les structures fastidieuses de bâtiments avec pièces de répartition et de construire un réseau redondant plus facilement et à moindre coûts d'installation. Il ne faut pas occulter cependant les désavantages de ce concept. Il entraîne un câblage fastidieux, car chaque station doit être connectée de manière individuelle. De plus, le concentrateur central doit disposer d'une forte densité de ports, qui correspond au nombre d'appareils à connecter. Cette structure occasionne également un seul point de panne (single point of failure).

Le concept de **Distributed Backbone** emprunte une autre méthode. Dans ce concept, de nombreux répartiteurs d'étages se réunissent en une horizontale et mènent les étages au répartiteur central de bâtiments. Il s'ensuit une tolérance plus élevée à la panne des composants grâce à cette décentralisation. Le câblage est moins fastidieux et peut être réalisé à l'horizontale avec un câblage cuivre beaucoup plus économique. Le désavantage reste cependant le nombre de composants actifs par lequel il faut passer, ce qui entraîne des temps de ralentissement. La largeur de bande disponible pour les stations finales se réduit proportionnellement aux nombres de stations connectées au répartiteur d'étages. De plus, des modifications structurelles deviennent très compliquées.

15.9.3 Câblage cuivre

Le câblage de cuivre s'est largement imposé et de nombreux standards Ethernet l'ont adopté. Un câblage cuivre a l'avantage d'une installation rapide, flexible et économique. Ses désavantages sont par contre la sensibilité aux influences électromagnétiques et la possibilité de ne palier que des distances très courtes. Le câblage cuivre intervient dès lors le plus souvent dans les domaines tertiaire et secondaire. La pratique a porté son choix sur deux moyens principaux de transmission : le câble coaxial et le câble paire torsadée. Le câblage coaxial intervient dans les standards Ethernet 10 BASE-5 et 10 BASE-2. Le standard 10 BASE-5 fait appel à un câble RG48 épais muni de connecteurs AUI (Attachement Unit Interface), tandis que le standard 10 BASE-2 fait appel au câble RG58 fin avec connecteurs BNC (Bayonet Neil Concelman).

Le câble est construit comme suit : il est constitué d'une ligne noyau, qui est entourée d'une isolation en PVC ou Teflon et d'une ligne cuivre ou aluminium. Celles-ci sont aussi entourées d'un blindage extérieur. Le câble paire torsadée est utilisé depuis le standard 10 BASE-T dans tous les standards Ethernet basés sur le cuivre et est équipé de connecteurs RJ-45. La paire torsadée désigne un câble de cuivre avec une ou plusieurs paires de fils enroulées sur elles-mêmes. Les câbles destinés aux standards Ethernet basés sur le cuivre disposent de quatre paires de fils torsadées, soit au total 8 fils. Tous les services destinés à la transmission nécessitent deux paires de fils. La distinction entre les différents câbles paire torsadée dépend du type de blindage ainsi que des catégories normalisées. Selon le blindage, on distingue les types de câbles suivants :

UTP pour **Unshielded Twisted Pair**, ni les paires de fils entre elles, ni l'ensemble des paires de fils ne sont blindées vers l'extérieur. S/UTP ou **Screened / Unshielded Twisted Pair**, signifie que les paires de fils ne sont pas blindées l'une par rapport à l'autre, mais toutes les paires de fils disposent d'un blindage vers l'extérieur. STP pour **Shielded Twisted Pair**, signifie que les paires de fils sont blindées l'une par rapport à l'autre, mais l'ensemble des paires de fils ne sont pas blindées vers l'extérieur. S/STP ou **Screened / Shielded Twisted Pair**, signifie que les paires de fils sont blindées l'une par rapport à l'autre et que l'ensemble des paires de fils sont blindées vers l'extérieur. Le câble cuivre est encore réparti en plusieurs classes de puissance. Ces classes de puissance définissent les exigences minimales de propriétés électriques d'un trajet de transmission. Les catégories les plus courantes sont la catégorie 3, avec une largeur de bande de 16 MHz selon EN 50173, la catégorie 5, avec une largeur de bande de 100 MHz selon EN 50288-2-1, la catégorie 6, avec une largeur de bande de

250 MHz répondant au standard Draft International de juillet 2002 et enfin la catégorie 7, avec une largeur de bande de 600 MHz selon EN 50288-4-1. Les câbles cuivre de la catégorie 3 conviennent pour le standard Ethernet 10 BASE-T, ceux de la catégorie 5 pour le standard Ethernet 100 BASE-T, ceux de la catégorie 5 renforcée et en particulier ceux de la catégorie 6 et 7 conviennent pour le standard Ethernet 1000 BASE-T.

15.9.4 Câblage fibre optique

Le câblage à fibre optique s'est largement imposé et de nombreux standards Ethernet l'ont adopté. Les arguments en faveur du câblage à fibre optique sont son insensibilité aux influences électromagnétiques, des taux élevés de transmission et des distances couvertes importantes. Dans le registre des désavantages, citons l'installation difficile et la flexibilité limitée, ainsi que les composants optiques actifs et passifs onéreux. C'est pourquoi le câblage cuivre est généralement utilisé dans les domaines secondaire et primaire. Le câble à fibre optique, quant à lui, se compose d'une gaine en matière synthétique, subdivisée en tampon secondaire et primaire, qui protègent la fibre optique. Les signaux lumineux sont transmis dans le noyau, qui à son tour est enveloppé d'une gaine appelée Glass Cladding (gaine). La différence entre le noyau et la gaine de la fibre optique s'exprime par l'index de réfraction. Il existe deux types importants de fibres optiques : les fibres dites multimode et les fibres dites single ou monomode.

En multimode, le faisceau lumineux est transmis en plusieurs modes. Les fibres de la catégorie multimode possèdent un noyau à index de réfraction plus élevé que celui de la gaine, de telle sorte que la lumière est totalement réfléchie à la surface de contact. Le multimode possède en outre un index de réfraction parabolique, partant du centre du noyau vers la surface de contact, ce qui diffuse la lumière sous forme d'ondes. Aujourd'hui, il est fait essentiellement usage des fibres multimode. Les fibres à single mode, comme leur nom l'indique, transmettent la lumière en un seul mode. Au travers du diamètre étroit du noyau d'une fibre single mode, la diffusion de la lumière est presque rectiligne, ce qui entraîne une dispersion moins importante et les distances à couvrir peuvent ainsi être plus grandes. Le critère décisif qui marque la différence entre ces fibres optiques est sans nul doute le diamètre du noyau et de la gaine de la fibre. Dans les fibres multimode, il existe deux diamètres courants de 62,5/125 et 50/125 microns. Par contre, les fibres single mode ne possèdent qu'un seul diamètre de 9/125 microns. En fonction du standard Ethernet observé et du moyen de transmission utilisé, différentes distances peuvent être couvertes. En présence du standard 1000 BASE-SX, un diamètre de 62,5/125 microns peut couvrir de 220 à 275 m et un diamètre de 50/125 microns peut lui couvrir une distance de 500 m à 550 m. Avec le standard 1000 BASE-LX, des fibres de diamètre 62,5/125 et 50/125 microns couvrent des distances de 550 m et, avec un diamètre de 9/125 microns, même des distances atteignant 5.000 m. Indépendamment de la fibre optique, de nombreux connecteurs peuvent être utilisés, par ex. ST, SC, MT-RJ ou VF-45.

15.10 Gestion

Dans des réseaux locaux complexes, la fonction de gestion réseau est un outil dont l'administrateur ne peut se passer, pour pouvoir contrôler son réseau. Dans ce contexte, le protocole SNMP (Simple Network Management Protocol) revêt toute son importance. SNMP a été conçu en 1988 et forme la base de la gestion dans les réseaux TCP/IP. Ce protocole repose sur les couches du modèle de référence OSI, qui se concentrent sur les applications. L'objectif du développement de SNMP visait l'indépendance par rapport au logiciel et au matériel, de même qu'un recours minimal aux ressources du système. Un environnement SNMP se compose d'une station de gestion, dotée d'un logiciel correspondant de gestion SNMP, ainsi que de composants réseau, équipés d'agents SNMP adéquats. Les agents SNMP sont réglementés par le MIB (Management Information Basis), qui détermine les propriétés des composants réseau. Son rôle est de garantir que la station de gestion ne réclame que les données que l'agent est en mesure de livrer. Les tâches essentielles de la gestion consistent en la surveillance, la commande, le diagnostic et l'analyse de problèmes.

Le fonctionnement est simple : la station de travail réclame les données aux agents SNMP, pour les traiter en conséquence et permettre enfin à l'administrateur de les exploiter. Il existe maintenant trois versions de SNMP, qui sont continuellement adaptées aux besoins actuels. Le MIB possède lui aussi une deuxième version, le MIB-II, qui supporte une série de nouveaux protocoles, livrant des informations encore plus détaillées. Grâce à l'identification d'objet, le MIB-II est compatible avec le MIB-I. En ce qui concerne, la gestion, il faut encore citer le RMON, qui est l'abréviation de **Remote Monitoring**. La fonction de RMON est un MIB développé pour permettre une gestion de réseau proactive. Le MIB réclame un appel régulier d'informations, ce qui entraîne une charge supplémentaire pour le réseau. Contrairement au RMON, qui lui, laisse l'appareil lui-même rassembler et sauvegarder les informations. En effet, à l'aide du RMON, l'administrateur peut établir des valeurs seuils, de telle sorte qu'un message ne soit généré que lorsque cette valeur seuil est dépassée. La charge du réseau s'en trouve ainsi considérablement réduite. N'oublions pas cependant, que le RMON doit analyser chaque cadre, ce qui entraîne des temps de ralentissement ayant une influence négative sur la performance du réseau. Le RMON1 travaille sur les couches 1 et 2, tandis que le RMON2 fonctionne sur les couches 3 et 7 du modèle de référence OSI.

Le RMON2 n'a pas remplacé le RMON1, il en représente seulement une extension, pour obtenir la transparence sur des couches de protocoles supérieures. Tous ces composants sont d'une aide précieuse pour l'administrateur dans sa tâche de gestion des réseaux locaux, qui est absolument indispensable dans des structures complexes. Il ne faut cependant pas oublier, que l'utilisation de composants de gestion est susceptible à son tour d'entraîner des temps de ralentissement dans le réseau. Le principe physique selon lequel "chaque analyse modifie l'état actuel du réseau" doit dès lors rester constamment présent à l'esprit.

16. Metropolitan Area Networks-MANs

16.1 Définition

On appelle **Metropolitan Area Networks (MAN)** des réseaux qui du point de vue de leur extension dans l'espace se situent entre les réseaux locaux limités à un endroit (LAN) et les Wide Area Networks (WAN).

De par sa conception un MAN est un réseau reliant les uns aux autres des réseaux séparés, en général des LAN. Grâce à la liaison entre ces LAN à l'intérieur d'un MAN, tous les avantages inhérents aux LAN ouvrent les portes sur un domaine d'utilisation plus large.

Du point de vue spécifique, un MAN est en fait lui-même un réseau séparé, distinct d'autres réseaux, créé par un exploitant et utilisé pour proposer des services.

Du point de vue de son extension dans l'espace, un MAN peut atteindre jusqu'à 150 kilomètres, mais s'étend sur au moins 2 kilomètres. Il est typique de créer des MAN pour les régions à forte concentration urbaine et pour les villes et leurs organismes ou en tant que réseau pour les campus d'universités.

En dehors de l'utilisation classique pour le transfert de données, un MAN a pour fonction de fournir des services à valeur ajoutée tels que téléphonie IP, transmission image et vidéo par IP ou encore un routage avantageux pour tous les utilisateurs connectés. De plus il est également possible de créer dans un MAN des réseaux locaux virtuels indépendamment des sites et des organisations.

Les réseaux des villes sont aujourd'hui basés sur SDH, une technologie de connexion logique des câbles et de connexion logique entre les utilisateurs. Etant donné que SDH est uniquement une technique de mise à disposition de lignes et de connexions logiques et non une technique de transmission, il faut, dans le cas d'une offre de service, utiliser une technique de transmission, telle ATM.

En comparaison avec un WAN, la mise en service dans un MAN est réalisée à un niveau qualitatif très élevé en raison des technologies grande vitesse FDDI, DQDB ou également ATM utilisées, et surtout avec des temps de transmission courts. Une autre technologie commence à pénétrer dans le domaine à grande vitesse des MAN : Ethernet avec sa nouvelle phase d'évolution, Ethernet 10 gigabits.

16.2 Technologies de transmission pour la création d'un MAN

16.2.1 Distributed Queue Dual Bus (DQDB)

DQDB a été défini par le groupe de travail IEEE 802.6 dans le cadre de la normalisation de MAN et peut servir d'ossature pour un MAN sur les distances atteignant 100 kilomètres et plus.

Ce procédé permet aussi bien la transmission asynchrone que la transmission isochrone par exemple

d'un langage codé. De par sa conception DQDB correspond à deux bus sur fibre optique qui fonctionnent de façon unidirectionnelle en sens contraire. Il est possible de réaliser une topologie en étoile ou en anneau. Chaque noeud d'une structure DQDB en anneau est raccordé aux deux bus et communique avec les autres noeuds en lui envoyant des informations par l'un des deux bus. Le choix du bus est fonction de la direction de la communication. Le double bus supporte au niveau inférieur les liaisons full-duplex, étant donné qu'un bus sert respectivement de liaison lecture ou écriture.

L'IEEE propose comme systèmes de transmission normalisés pour DQDB, le G0.703 avec une vitesse de 34 ou 139 Mbit/s, ou SDH avec 155 Mbit/s selon les normes G0.707, G0.708 et G0.709.

Les technologies de transmission FDDI et ATM, de même que la norme G0.703 et SDH avec les normes qui s'y rapportent, sont également utilisées dans les LAN et les WAN et sont de ce fait décrites dans les chapitres correspondants.

17. Wide Area Networks - WANs

17.1 Définition

On appelle **Wide Area Networks** (WAN ou encore réseaux à grande distance) des réseaux généralisés dont les dimensions dépassent les frontières régionales. Les utilisateurs connectés les utilisent aussi bien pour leurs affaires qu'à titre privé. Leur étendue dans l'espace peut atteindre jusqu'à 1.000 et même 10.000 km.

La technologie de transmission utilisée est soit une technologie de transmission par paquets soit une technologie de commutation de ligne. Les WAN sont aussi souvent composés de plusieurs réseaux reliés entre eux par exemple par RNIS, X 25 ou ATM. Sur les WAN, la sécurité de transmission est de nos jours assurée par des Virtual Private Networks (VPN).

Le réseau analogique utilisé pour la téléphonie est un exemple de WAN auquel nous nous sommes habitués depuis des décennies et dont nous ne pourrions plus nous passer. Sur ce réseau le débit des données est de 56 Kbit/s. En raison de la demande accrue en débits plus élevés sur les WAN, suite à l'apparition de nouveaux services, tels que la vidéo et la parole par IP, il est possible d'attendre maintenant sous ATM des débits de 622 Mbit/s. Mais avec le développement d'Ethernet 10 Gigabit nous sommes à la veille de voir une migration vers des débits encore plus importants.

En Europe les WAN sont le plus souvent exploités par des fournisseurs de télécommunications.

17.2 L'adressage sur le WAN

Sur le WAN l'adressage est basé sur les adresses de l'Internet Protocol (IP) qui sont attribuées aux composants actifs de réseau reliés au WAN par l'intermédiaire de **netid** et aux hôtes par l'intermédiaire de **hostid**. Les adresses IP sont uniques et se composent dans la version 4 de 32 bits divisés, pour faciliter les choses, en 4 octets. Deux adresses IP font cependant exception à ce schéma.

L'adresse IP dans laquelle tous les bits de l'ID de l'hôte valent « 0 » et l'adresse dont tous les bits valent « 1 ». La première sert à la description générale d'une adresse réseau, la deuxième est une adresse Broadcast réservée. Le NIC attribue les netids alors que les hostids sont attribués respectivement par les détenteurs des netids.

On distingue trois sortes d'adresses de classes de réseau :

Avec les adresses de classe A, on peut adresser 128 réseaux étant donné que pour eux le premier octet constitue l'adresse du réseau mais que le premier bit dans cet octet est un « 10 ». Les trois octets restants sont destinés à être distribués à des hôtes, ce qui théoriquement permet d'attribuer des adresses distinctes à 16.777.214 hôtes.

Avec les adresses de classe B on peut adresser 16.384 réseaux avec chacun 65.534 hôtes. Dans les réseaux de classe B les deux premiers bits du premier octet de l'adresse IP sont définis par « 10 » et distinguent ainsi les réseaux de classe B en tant que tels. De manière générale, les

deux premiers octets constituent le netid et les deux derniers octets constituent l'hostid.

Les adresses de classe C permettent d'adresser 2.097.152 réseaux différents comprenant chacun jusqu'à 254 hôtes. Dans la classe C les trois premiers bits du premier octet sont identifiables grâce aux valeurs « 110 ». Le quatrième est le seul à être utilisé pour attribuer des adresses IP à des hôtes. Les trois autres octets servent à l'attribution de netids.

Etant donné que suite à la croissance explosive d'Internet les adresses IPv4 disponibles commencent à s'épuiser, on n'attribue pratiquement plus d'adresses IP uniques qu'aux composants actifs de réseau directement connectés sur le WAN. Tous les périphériques connectés derrière l'interface avec le WAN reçoivent des adresses provenant du domaine de gestion privée qui ne sont cependant plus clairement identifiables dans le monde entier. Afin d'éviter des erreurs d'acheminement, les adresses IP sont identifiées à l'interface avec le WAN au moyen de Network Address Translation (NAT) comme appartenant au réseau connecté.

Afin de palier au problème du nombre insuffisant d'adresses IPv4, une nouvelle structure d'adresse a été développée : dans la version 6 de l'Internet Protocol (**IPv6**), qui est compatible avec IPv4.; l'adressage repose sur le système hexadécimal. Une adresse IPv6 est longue de 128 bits et elle est composée d'une série de huit tranches de 16 bits. Cela signifie que IPv6 présente quatre fois plus d'octets que IPv4.

En dehors de la plus grande place disponible pour les adresses et donc de la possibilité d'attribuer à chaque hôte une adresse unique au monde, l'avantage décisif de l'adressage IPv6 par rapport à IPv4 réside dans le fait qu'il permet le Site Multihoming. Grâce au Site Multihoming les hôtes peuvent se voir attribuer plusieurs adresses IPv6, ce qui en pratique leur permet d'utiliser les services de plusieurs fournisseurs d'accès. De plus l'adressage IPv6 présente un format d'en-tête fixe, ce qui augmente nettement l'efficacité du traitement des paquets avec lequel ils sont adressés. De plus IPv6 offre la possibilité d'utiliser des Security Header.

17.3 Les protocoles sur le WAN

Par protocoles WAN on entend les familles de protocoles qui se trouvent sur la couche 3 du modèle de référence ISO/OSI. Les protocoles de couche 3 aujourd'hui les plus répandus, y compris les protocoles de transport et de routage, sont présentés ci-dessous.

17.3.1 Le protocole Internet (IP)

Le rôle de l'Internet Protocol (**protocole IP**), indépendant de la plate-forme, est de transmettre des données d'un expéditeur à un destinataire en passant par plusieurs réseaux. IP se trouve sur la couche 3 et il est responsable de la coordination de la transmission des fragments de données que la couche 4 envoie à la couche 3. Un paquet IP est défini par une grandeur minimale de 576 octets et une longueur maximale de 65.535 octets. En raison de la variabilité et des différentes

définitions des structures de transmission et des longueurs de paquets pour chaque partie de réseau à traverser, il se peut qu'un paquet IP doive être divisé en parties plus petites au cours du trajet de transmission. Cette division est aussi appelée fragmentation. L'assemblage des différentes parties pour revenir à l'état d'origine est appelé rassemblement.

La structure fondamentale d'un paquet de données IP (aussi appelé datagramme) reste toujours la même, indépendamment de la fragmentation : les principales composantes d'un paquet IP sont dans l'ordre : l'en-tête avec les informations concernant le paquet lui-même, l'adresse de la source et celle du destinataire, de même que toutes les informations qui servent au contrôle de la transmission et à la correction des erreurs. L'en-tête est suivie d'informations optionnelles concernant l'expédition, comme par exemple des règles de sécurité pour la transmission des données. Les informations concernant les données qui doivent être transmises sont rattachées aux derniers bits.

La transmission IP est axée sur les paquets. La transmission se fait sans liaison et sans garantie. Si à un endroit du trajet de transmission un tampon vient à être saturé, le paquet IP sera repoussé quand il atteindra ce point surchargé. Cependant, grâce à la fonction de Frequency Check Sum et à la communication directement établie entre la source et le destinataire, en cas d'erreur une retransmission a lieu. Etant donné que les paquets ID ne sont pas transmis en tant qu'unité d'information mais sont considérés séparément, ils sont transmis de façon discrétionnaire, c'est-à-dire sans lien. Chaque paquet de données emprunte, entre la source et le destinataire, le chemin qui est pour lui optimal. Il revient au protocole TCP, basé sur le protocole IP, de remettre les paquets IP dans le bon ordre chez le destinataire.

17.3.2 Transmission Control Protocol (TCP)

Le **Transmission Control Protocol (TCP)** se trouve sur la couche 4 du modèle de référence OSI et il est responsable de la transformation du flux de données provenant des couches 5 à 7 en fragments que peut traiter le protocole IP de la couche 3. Selon des règles fixes, le protocole TCP partage le flot de données, par exemple d'un fichier, en paquets et les remet au protocole de transmission.

Le protocole Stack **TCP/IP (Transmission Control Protocol Internet Protocol)** défini par le ministère américain de la défense est disponible sur toute plate-forme d'ordinateur importante. Il n'a pas été conçu pour un système de transmission particulier, contrairement, par exemple, aux protocoles pour réseau LAN, mais pour être utilisé sur différents médias et ordinateurs. TCP/IP est donc le protocole Stack approprié aux réseaux hétérogènes. Des ordinateurs tournant sous Unix (et ses variantes SunOS, Digital Unix, HP-UX, AIX, Linux), OpenVMS, DOS ou Windows par exemple, peuvent être interconnectés. De nombreuses applications, normalement appelées protocole, reposent sur le protocole TCP/IP. Par exemple : **ftp** pour le transfert de fichiers, **telnet** et **rlogin** pour le contrôle à distance ou la connexion à distance, le courrier électronique, le navigateur Web etc.

17.3.3 User Datagram Protocol(UDP)

Le **User Datagram Protocol (UDP)** est, comme le TCP, situé sur la couche 4 selon le modèle de référence OSI et il est, comme le TCP, un protocole de transport qui repose directement sur le protocole IP. UDP est uniquement responsable du transport et a été développé pour permettre aux applications d'envoyer directement des datagrammes. UDP travaille sans liaison. UDP envoie des données vers le destinataire mais sans recevoir la confirmation que la transmission a réussi. UDP ne garantit donc pas la sécurité de la transmission, les paquets perdus ne sont pas à nouveau envoyés.

17.3.4 Les protocoles de routage

Les protocoles de routage sont responsables du déroulement et du choix du trajet de la transmission entre une source et un réseau de destination. La décision d'un routeur de faire suivre un message sur le WAN est basée sur la table de routage établie à partir du protocole de routage et sur la métrique qui en résulte. La métrique d'un protocole de routage est définie en tant que valeur sur laquelle un routeur se fonde pour prendre sa décision de réacheminement. Le calcul de la métrique varie selon les protocoles.

Parmi les protocoles de routage, on distingue les protocoles de routage statique et les protocoles de routage dynamique.

Les **protocoles de routage statique** ne sont en général utilisés que dans des petits réseaux ou pour des liaisons commutées car la mise à jour manuelle des tables de routage est fastidieuse. Chaque nouveau trajet doit être, de même que tout changement de trajet, inscrit à la main dans la table de routage.

Par contre les **protocoles de routage dynamique** se retrouvent souvent dans les grands réseaux en expansion. Le peu de travail que demandent les tableaux de routage de la part de l'administrateur en fait un outil prédestiné à cet emploi. Les protocoles de routage dynamique détectent les changements intervenus dans les réseaux et réagissent en modifiant leur table de routage en conséquence. Ces protocoles se trouvent modifiés par leurs voisins sur le réseau. Sur un WAN conçu sur la base d'un protocole de routage dynamique, chaque routeur diffuse ses informations concernant les stations du trajet, c'est-à-dire les adresses IP qu'il connaît, à ses voisins. Le choix du meilleur chemin à travers le réseau est fixé en fonction des informations spécifiques propagées par le protocole.

Il existe un deuxième critère de différenciation entre les protocoles de routage : il peut s'agir soit d'un protocole à vecteur de distance soit d'un protocole à état de liaison.

Les protocoles à vecteur de distance se caractérisent par une convergence relativement lente, une souplesse limitée mais une installation simple et un procédé d'exploitation confortable. Ils travaillent selon le principe du « routage par rumeur » et envoient périodiquement leur table de routage toute entière à leurs voisins directs. Ceux-ci traitent ces informations en remplaçant entièrement leur

propre table de routage par les nouvelles informations. Sur les grands réseaux, qui ont aussi des tableaux de routage très complexes, ce procédé entraîne un trafic excessif et les routeurs sont très sollicités. RIP, RIPv2 et IGRP sont des exemples de protocoles à vecteur de distance.

Par contre les protocoles à état de liaison supportent les mises à jour déclenchées, c'est-à-dire que les nouvelles informations de routage sont immédiatement diffusées en ne reprenant que les changements, et non pas toute la table de routage. Cela n'entraîne qu'une charge minime des liens et des routeurs pour l'actualisation des informations de routage. La diffusion d'un changement de topologie du réseau dès son apparition rend les réseaux basés sur les protocoles de routage à état de liaison nettement plus convergents que ceux basés sur des protocoles à vecteur de distance. OSPF et IS-IS sont des exemples de protocoles à état de liaison.

EIGRP réunit des caractéristiques des deux types de protocoles.

17.3.4.1 RIP

Le **Routing Information Protocol (RIP)** est un protocole à vecteur de distance dont la métrique repose uniquement sur le nombre de sauts. Un saut est le passage d'un composant de routage au composant suivant. Pour la métrique du RIP aucun autre critère de décision, tels que par exemple la largeur de bandes ou le délai de transmission, n'entre en ligne de compte. RIP est le plus ancien protocole de routage et son procédé est très simple. C'est un Classful Routing Protocol plat qui diffuse toutes les informations de routage dans le réseau tout entier. RIP ne supporte ni VLSM (Variable-Length Subnet Masking) ni la fonction de Route Summarization manuelle. La distance maximale pour un réseau qui travaille avec RIP est de 15 sauts.

17.3.4.2 RIPv2

RIPv2 est une version élargie de RIP qui supporte VLSM et peut, en dehors des mises à jour périodiques typiques pour les protocoles à vecteur de distance, diffuser également des mises à jour déclenchées, c'est-à-dire des changements inattendus de la topologie du réseau. RIPv2 est implémenté essentiellement dans de petits réseaux qui fonctionnent avec des liaisons point à point. Il est en outre utilisé pour des liaisons commutées parce que dans RIPv2, la table de routage peut être gelée jusqu'à ce qu'une liaison soit demandée et qu'intervienne alors l'échange des informations de routage.

RIPv2 comporte cependant deux points faibles qui existaient déjà dans RIP : la limitation du nombre de sauts à 15 et le critère de mesure de la métrique qui reste basée uniquement sur le nombre de sauts.

17.3.4.3 IGRP/EIGRP

IGRP, l'**I**nterior **G**ateway **R**outing **P**rotocol, est un protocole à vecteur de distance développé par Cisco, donc propriétaire. Comparé à RIP, le calcul de sa métrique est plus complexe parce qu'il y

ajoute la largeur de bande minimale et le délai de transmission sur une liaison. En raison de la fonctionnalité purement à distance de vecteur, il a des temps de convergence relativement longs et n'est utilisé que dans les petits réseaux.

Les faiblesses de IGRP ont été éliminées dans une version élargie, le **EIGRP**, **Enhanced Interior Gateway Routing Protocol**. EIGRP réunit certaines caractéristiques des protocoles à vecteur de distance et des protocoles à état de liaison. EIGRP supporte ainsi VLSM et les mises à jour déclenchées, c'est-à-dire la diffusion immédiate de changements imprévus dans la topologie d'un réseau. De plus les routeurs supportés par EIGRP construisent des tables de routage qui contiennent non seulement le meilleur trajet mais aussi toute la topologie du réseau. En outre la fonction manuelle IP-Address-Summarization est supportée. Pour le calcul de la métrique, EIGRP dispose des paramètres suivants : la largeur de bande, le délai, la fiabilité, le débit et le MTU. Mais en fonctionnement standard seuls la largeur de bande et le délai sont utilisés pour le calcul du trajet optimal.

Parce qu'ils sont propriétaires, les protocoles IGRP et EIGRP ne peuvent être implémentés que sur des réseaux basés sur du matériel CISCO. Seul leur matériel supporte ces protocoles.

17.3.4.4 OSPF

L'**Open Shortest Path First (OSPF)** est un protocole à état de liaison et a été développé pour le routage de IPv4. OSPF est optimisé pour l'utilisation dans de grands réseaux évolutifs pour lesquels les limites du RIP ne sont pas acceptables. OSPF présente de meilleures fonctions de convergence, supporte VLSM et la fonction manuelle IP-Address-Summarization. Dans OSPF le calcul de la métrique pour trouver le trajet optimal est basé sur les coûts des chemins et sur la somme des largeurs de bande disponible entre le premier et le dernier point du trajet.

Une connaissance très exacte des réseaux est indispensable pour pouvoir utiliser OSPF. Dans les environnements OSPF un segment fédérateur doit être défini comme aire 0 à laquelle toutes les autres zones doivent être directement connectées en tant que non segment fédérateur. Tout le trafic de routage entre les non segments fédérateurs doit passer par le segment fédérateur. Les routeurs situés à la frontière entre différentes zones sont appelés Area Border Routers. Ils peuvent réaliser des IP-Summaries de sorte que les tables de routage peuvent être relativement petites, ce qui minimise la charge des routeurs.

17.4 La diffusion de données sur le WAN

Les WAN transmettent des données soit en commutant des circuits soit en transmettant des paquets de données.

17.4.1 La commutation de circuits

Dans la commutation de circuits les commutateurs sont hiérarchisés. Les commutateurs peu élevés dans la hiérarchie sont subordonnés de façon linéaire à des commutateurs hiérarchiquement

supérieurs. Dans ces réseaux la transmission de données peut se faire sur toute la largeur de bande disponible parce que pour chaque communication entre la source et le destinataire une ligne propre passant par les différentes hiérarchies est connectée. Toute largeur de la bande qui n'est pas utilisée pour la transmission est perdue pour le temps que dure la communication, puisque la ligne ne peut être utilisée que pour cette communication. La connexion est réservée uniquement pour les deux partenaires en communication (pré-allocation).

Les avantages de la transmission par commutation de circuits sont une transmission presque sans délai, une transparence totale des protocoles et le routage simple demandant peu de calcul.

Le temps très long nécessaire à la connexion et à la déconnexion du circuit est un désavantage. De plus, aucune redondance des chemins n'est prévue et l'utilisation insuffisante de la largeur de bande est un inconvénient de la transmission par commutation de circuit.

17.4.2 La commutation par paquets

La transmission par paquets de données procède au découpage des informations à transmettre (les données) en différentes parties appelées paquets. Lors de la **transmission en paquets** ceux-ci reçoivent de l'expéditeur des marques précises concernant l'adresse, l'ordre d'expédition, le contrôle du débit et la correction d'erreurs afin que le destinataire puisse analyser toute la transmission d'informations et constater si une transmission est achevée et quand elle l'a été et comment les différents paquets doivent être agencés pour reconstituer la totalité de l'information. Les différents paquets sont expédiés par la source jusqu'au destinataire en passant par différents points du trajet (les nœuds) selon un procédé impliquant des mémoires intermédiaires : chaque nœud stocke les paquets, le contrôle et les transmet une fois contrôlés au nœud suivant. Ce procédé de réception, stockage intermédiaire, contrôle et transmission est aussi appelé **Store-and-Forward**.

Les procédés de transmission acheminant des paquets de données sont beaucoup plus rapides que les procédés de commutation de circuits, surtout en raison des temps plus courts de connexion et de déconnexion. De plus l'utilisation de la largeur de bande est optimisée et il est possible d'utiliser des chemins redondants. L'inconvénient est une plus grande sensibilité aux erreurs.

17.5 Les modes de transmission sur le WAN

17.5.1 Les modes de transmission synchrones

Les procédés de transmission synchrone acheminent les données dans des délais déterminés. Ces délais sont synchronisés à l'aide de signaux d'horloge. Chaque terminal de communication lit le signal d'horloge dans l'en-tête du paquet de données et s'y conforme. Les procédés de transmission synchrones sont plus rapides et plus efficaces que les procédés asynchrones dont le déroulement est comparativement désordonné.

17.5.2 Les modes de transmission asynchrones

Contrairement aux procédés de transmission synchrones, les procédés de transmission asynchrones n'ont pas de signal d'horloge prédéterminé. Dans la transmission asynchrone les paquets de données portent des bits de début et de fin qui servent à la détection d'erreurs. Une erreur de transmission se produit quand à l'arrivée chez le destinataire la différence entre un bit de début et un bit de fin est plus longue qu'elle ne l'était encore chez l'expéditeur.

17.6 Technologies du WAN

D'une manière générale les technologies du WAN reposent sur les trois couches inférieures du modèle de référence OSI : la couche physique, la couche de liaison de données et la couche réseau. En règle générale les services sont mis à disposition au moyen d'une des technologies suivantes :

- Sur des lignes louées (lignes permanentes)
- Sur des circuits commutés
- Sur des circuits commutés
- Par commutation de cellules.

Tous les procédés de commutation cités ont pour base des canaux virtuels et le fournisseur de services doit pouvoir, grâce aux informations contenues dans un paquet de données, reconnaître son appartenance à un canal.

17.6.1 Lignes louées

Les lignes permanentes sont des liaisons de point à point qui sont réservées de manière durable pour la transmission de données. Ces liaisons ne sont pas établies uniquement quand une transmission doit avoir lieu; elles sont toujours connectées, qu'il y ait ou non un flux de données. C'est pourquoi il est souhaitable, dans le cas de lignes louées, d'optimiser autant que possible l'utilisation de la largeur de bande afin de garantir un rendement rationnel des investissements. L'exploitant de la ligne louée établit une liaison soit au moyen d'une connexion matériel soit par l'intermédiaire de l'attribution d'un canal en se servant de la modulation de fréquence et du multiplexage temporel. En règle générale les lignes louées permettent une transmission synchrone de données.

17.6.2 Réseaux à commutation de circuit

Les réseaux de circuits commutés établissent pour la durée de la transmission une ligne spécialisée entre la source et le destinataire. C'est ainsi par exemple que des liaisons analogiques sur réseau téléphonique (PSTN) passent par des réseaux de circuits commutés. Pendant la durée de la connexion la ligne ne peut être utilisée pour d'autres liaisons, même si toute la largeur de la bande n'est pas utilisée. RNIS et les connexions sérielles asynchrones sont d'autres exemples de liaisons sur circuits commutés.

17.6.3 Réseaux à commutation par paquets et par cellules

Dans les réseaux à commutation par paquets et par cellules l'exploitant crée des circuits virtuels permanents (PVC) ou bien des circuits virtuels commutés (SVC). Dans ces réseaux les utilisateurs se partagent les ressources disponibles et utilisent pour la transmission de leurs données différents chemins à travers le réseau. Ceci permet à l'exploitant de réseau de mieux utiliser les ressources de son infrastructure que dans les connexions de point à point et d'optimiser pour tous le rendement des investissements. Cette structure est utilisée dans des réseaux devant utiliser X25, la commutation de trames ou SMDS (Switched Multimegabit Data Service).

ATM est une technologie utilisée uniquement dans les réseaux intégralement à commutation par cellules. ATM divise des données numérique en cellules de grandeur fixe et les transmet au moyen d'un support physique en utilisant la technologie des signaux numériques. Des cellules ATM peuvent être soit asynchrones, soit sur file d'attente, ou bien transmises par un procédé de multiplexage.

17.6.4 Digital Subscribe Line (DSL)

DSL est une technologie de transmission qui rend possible des hauts débits sur le câblage traditionnel du téléphone. Les quatre variantes de DSL sont l'Asymmetric Digital Subscriber Line (ADSL), la High-Data-Rate Digital Subscriber Line (HDSL), la Single-Line Digital Subscriber Line (SDSL) et la Very-High-Data-Rate Digital Subscriber Line (VDSL). Etant donné que DSL et la transmission téléphonique peuvent fonctionner avec des fréquences différentes, les deux flux de données peuvent être transmis parallèlement. La variante la plus courante de DSL est ADSL.

ATM et DSL sont décrits plus en détail dans un paragraphe ultérieur.

17.7 La transmission de données sur le WAN

17.7.1 La transmission analogique de données sur le WAN

Le réseau le plus étendu et le plus connu de tous est certainement le réseau téléphonique public. Ce réseau permet d'établir des communications vocales, via des liaisons établies par commutation. L'utilisation de ce réseau pour transférer des données par modem ou par télécopieur gardera son importance.

17.7.2 La transmission numérique de données sur le WAN

17.7.2.1 Réseau numérique à intégration des services - RNIS

RNIS permet l'utilisation de la parole, de textes, d'images et de données sur un seul et même réseau. Une unique connexion RNIS permet donc l'utilisation de plusieurs services de télécommunications,

comme le téléphone, le fax ou la transmission de fichiers. Ce réseau est particulièrement intéressant, non seulement pour les novices, mais aussi pour les utilisateurs de modem analogique. En effet, il séduit par sa vitesse de transmission et sa relative insensibilité aux perturbations, sa rapidité d'établissement des liaisons. RNIS peut utiliser les lignes téléphoniques existantes pour la connexion aux périphériques. A la différence du système conventionnel, le signal transmis sur le réseau RNIS est numérique du début à la fin de la transmission. Le transfert entre centraux téléphoniques de nombreuses villes s'effectue déjà entièrement en mode numérique.

17.7.2.1.1 Compatibilité

Lors de l'établissement d'une communication entre deux périphériques RNIS, ce sont d'abord des informations de contrôle qui sont transmises sur le canal de signalisation (canal D). Il s'agit par exemple du numéro de l'abonné, qui est reproduit sur l'écran d'affichage du téléphone, ainsi que du type de service désiré (par ex. vocal ou fax) ou d'autres informations nécessaires à l'établissement de la communication entre les deux postes RNIS.

Après l'introduction de RNIS se sont développés différents standards pour les protocoles, qui sont utilisés lors de la transmission d'informations de contrôle dans le canal D. En conséquence, deux protocoles pour canal D dans la communication RNIS sont disponible. D'une part, le protocole national 1TR6 et d'autre part, le protocole européen DSS1 ou aussi E-DSS1. On parle dans ce cas du protocole Euro-RNIS, bien qu'entre-temps il soit également utilisé dans beaucoup de pays non européens. Le nombre de réseaux dans le monde offrant les services Euro-RNIS est passé à plus de 30, dont 20 en Europe. La communication téléphonique ne doit pas poser de problème, si les protocoles locaux sont différents. Mais dans certaines circonstances, il faut s'attendre à des problèmes lors de transmissions de données ou lorsque certains services ou types de lignes utilisées ne sont disponible qu'au niveau national. Euro-RNIS s'est maintenant imposé en tant que standard dans de nombreux pays si bien que lors d'une nouvelle installation avec RNIS ce type de connexion est préférable.

17.7.2.1.2 Types de liaisons

On peut distinguer les types de liaison RNIS suivants :

Pour la **liaison automatique RNIS**, un canal B est réservé pour un service RNIS dès qu'un numéro est composé par l'utilisateur. Ce genre de liaison est également possible sur d'autres réseaux (téléphone, radiotéléphone, X.25).

Les **lignes fixes** numériques (ou lignes louées) mettent en permanence des canaux de 64 kbit/s à disposition de l'utilisateur, et ce, jusqu'à un maximum de 30 canaux B (PRI) par connexion. Ces liaisons louées exclusives peuvent être utilisées avec ou sans canal de signalisation.

17.7.2.1.3 CAPI

CAPI (Common ISDN Application Interface) a été développé dans le but de fournir une interface uniforme entre les applications et les périphériques RNIS (par exemple la carte RNIS). CAPI permet en principe d'utiliser chaque carte RNIS supportant CAPI avec chaque logiciel d'application RNIS, supportant également CAPI.

Deux versions de CAPI sont utilisées actuellement. Les versions CAPI 1.0 et 1.1 sont destinées aux solutions RNIS sur base de PC et sont supportées par pratiquement toutes les cartes RNIS de PC. La toute récente version CAPI 2.0 offre comme amélioration principale le support de toutes les plates-formes. Cette indépendance à l'égard des plates-formes est une des raisons pour lesquelles par exemple Windows NT utilise CAPI 2.0 pour ses services d'accès à distance (Remote Access Services).

17.7.2.1.4 Communication via RNIS avec des postes appelés analogiques

Si la station appelée se trouve sur le réseau téléphonique analogique, comme un modem analogique ou un accès analogique au réseau, la communication des données est plus délicate. En effet, la liaison à un poste analogique ne fonctionne que si le périphérique RNIS supporte ce genre de liaison. Quelques cartes ou adaptateurs de terminaux RNIS disposent à cet effet d'une puce modem intégrée ou d'un processeur numérique, qui permet l'utilisation d'un modem analogique. La communication avec des télécopieurs analogiques est cependant possible à l'aide de cartes RNIS, qui ne disposent pas de chip modem. Ce logiciel prépare les données numériques pour l'appareil fax analogique. Cependant cette méthode réclame un temps de calcul considérable et peut éventuellement affecter la fiabilité du transfert.

17.7.2.1.5 Communication via RNIS avec des postes appelés numériques

Que la station appelée soit un périphérique numérique, comme par exemple un PC muni d'une carte RNIS ou un télécopieur numérique (fax de groupe 4) ou qu'il s'agisse d'un accès RNIS à un réseau ou à un partenaire de services (BTX ou Minitel, CompuServe, fournisseur d'accès Internet), l'échange de données s'effectue sur le canal B du RNIS, selon les normes X.75 ou V.110.

Le protocole X.75 utilise au mieux la largeur de bande RNIS et fournit un taux de transfert de données de 64.000 bits/s par canal B du RNIS. Si la station appelée admet moins de 64.000 bits/s le débit doit être adapté. On parle alors d'adaptation du taux de bit. Pour ce faire, des bits de remplissage sont ajoutés entre le taux de transfert nécessaire et les 64.000 bits/s de la bande RNIS. Ce processus est défini dans la norme V.110 pour 2.400 à 38.400 bits/s.

Une flexibilité totale dans la communication RNIS vers des stations numériques ne peut être obtenue qu'en utilisant un matériel supportant les deux normes.

17.7.2.2 Hiérarchie numérique de multiplexage

17.7.2.2.1 Plesiochronous Digital Hierarchy (PDH)

La hiérarchie numérique plésiochrone (PDH) définit une technique de transmission numérique pour le transfert entre nœuds qui n'ont pas la même cadence, donc qui sont asynchrones. PDH a été normalisé en 1972 par le CCITT de l'époque et prévoit différents débits partent tous qui du taux de base de 64 Kbit/s. Ce taux de base, défini dans G.702 de l'UIT-T, est également appelé interface E0. La PDH est en passe d'être remplacée dans les nouvelles installations par la hiérarchie synchrone numérique (SDH).

La hiérarchie numérique européenne de multiplexage PDH fonctionne sur la base d'un taux de 64 Kbit/s par interface. Ce taux de base est aussi appelé interface E0. D'autres interfaces E-X se laissent définir grâce à une hiérarchie de multiplexage dans laquelle l'interface supérieure représente le quadruple du multiplexage de l'interface inférieure.

17.7.2.2.2 Normes PDH

G.703

La recommandation G.703 de l'UIT se rapporte à une interface de ligne utilisée pour des vitesses de transmission supérieures au 64 Kbit/s. Il s'agit d'une interface numérique bi-directionnelle pour la transmission de flux de données non structurés. Le G.703 non structuré sert en général à des transferts avec un débit maximal possible de 2 Mbits/s, ce taux n'étant pas forcément atteint. Non structuré signifie dans ce contexte que les 32 canaux de 64 Kbits/s disponibles sont regroupés en un canal de données de 2 Mbits/s. G.703 est le plus souvent associé à du matériel de communication tels que routeurs ou multiplexeurs. La transmission se fait soit par câble symétrique (120 Ohm paire torsadée) ou asymétrique (75 Ohm coaxial double). Le service le plus développé est le service symétrique. Les Pays-Bas et le Royaume-Uni constituent les exceptions.

G.704

G.704 est la version structurée de G.703 et G.704 fonctionne exactement comme G.703 mais les 32 canaux de 64 Kbits/s disponibles (créneaux temporels compris) peuvent être utilisés séparément. Le créneau temporel 0 est cependant réservé à la synchronisation.

17.7.2.2.3 Multiplexage PDH

Pour agrandir la largeur de bande il est possible de regrouper 32 lignes E0 en une interface E1. On parle alors de multiplexage. Le résultat du multiplexage est que les données de plusieurs liaisons peuvent être transmises sur une seule liaison sans réduction du débit. L'interface de transmission E-1 (aussi CEPT1) est l'interface de taux primaire (PRI, Primary Rate Interface) de la hiérarchie de

multiplexage numérique PDH en Europe, constituant ainsi le premier échelon du multiplexage. Elle fonctionne avec un débit atteignant 2.048 Kbits/s ou 2Mbits/s. Ces 2.048 Kbits/s réunissent 32 canaux E0 utiles de 64 Kbits/s pour la transmission de la parole et des données. Les augmentations suivantes comme variantes d'interfaces E sont possibles grâce à la technologie du multiplexage :

E-2 : Une ligne groupant quatre lignes E1 et ayant un débit de 8.448 millions de bits par seconde (Mbps)

E-3 : Une ligne groupant quatre lignes E2 et ayant un débit de 34.368 millions de bits par seconde (Mbps)

E-4 : Une ligne groupant quatre lignes E3 et ayant un débit de 139.264 millions de bits par seconde (Mbps)

E-5 : Une ligne groupant quatre lignes E4 et ayant un débit de 565.148 millions de bits par seconde (Mbps).

"Plesiochron" a la même signification que "quasiment synchrone". Cela porte à penser que dans les différents niveaux de multiplexage de PDH il se produit inévitablement certains écarts de cadences. Ces écarts de cadence sont compensés dans les niveaux supérieurs de la hiérarchie par des bits de remplissage.

17.7.2.2.4 Procédés de multiplexage

Le multiplexage peut s'effectuer de cinq façons différentes : Multiplexage à répartition spatiale, de fréquence, temporel, par répartition de code, en longueur d'ondes.

17.7.2.2.4.1 Multiplexage physique

Avec le multiplexage physique (en anglais Space Division Multiplexing, SDM), les supports de transmission physiques sont regroupés dans un câble ou une bande de fréquence. Dans le cadre de la transmission numérique, le multiplexage physique est par exemple mis en œuvre pour le regroupement de plusieurs lignes RNIS à une centrale téléphonique locale dans une interface à taux primaire.

17.7.2.2.4.2 Multiplexage de fréquence

Dans le cas du multiplexage de fréquence (en anglais Frequency Division Multiplexing, FDM), une large bande de fréquence est divisée en plusieurs bandes plus petites pouvant transmettre des données en parallèle et indépendamment les unes des autres. Le FDM est par exemple utilisé dans les liaisons télégraphiques. De nos jours, le FDM n'est quasiment plus mis en œuvre car il a été remplacé par le multiplexage temporel.

17.7.2.2.4.3 Multiplexage temporel

Le multiplexage temporel (en anglais Time Division Multiplexing, TDM) traite les demandes de transmission indépendamment les unes après les autres. Chaque canal se voit affecté une fenêtre temporelle pour l'envoi de ses données. Si cette fenêtre est dépassée, la transmission est interrompue et le prochain canal reçoit le droit d'envoi pour la durée de sa fenêtre. Le TDM est divisé en deux catégories : Le multiplexage temporel synchrone (en anglais Synchronous Time Division Multiplexing, STD) et le multiplexage temporel asynchrone (en anglais Asynchronous Time Division Multiplexing, ATD).

Le processus STD définit des cadres de transmission composés d'un nombre déterminé de fenêtres de durée fixe. Chaque utilisateur se voit attribuer une fenêtre bien précise au sein du cadre de transmission pendant laquelle il peut envoyer ou recevoir des données. Le processus ASD effectue la transmission des données devant être envoyées de manière asynchrone sous forme d'unités d'informations de longueur fixe ou variable. L'affectation des unités d'informations a lieu par numéro d'identification de canal, le Channel Identifier, que chaque paquet reçoit. ATD est de ce fait aussi nommé Multiplexage d'adresses. Si, lors de la transmission, des paquets de données de longueur fixe sont utilisés, on parle de Cell-Switching. Si en revanche il s'agit de paquets de longueur variable, on parle alors de transmission de paquets de données.

17.7.2.2.4.4 Multiplexage de code

Le multiplexage de code (en anglais Code Division Multiplexing, CDM) permet d'envoyer simultanément des données de plusieurs expéditeurs par l'intermédiaire d'un seul médium (fréquence ou canal). Cela est rendu possible par un codage individuel des données par un bit échantillon pour chaque expéditeur, permettant ainsi au destinataire de recréer l'information originale à partir du mélange de données grâce à ce code. CDM trouve son application dans l'UMTS.

17.7.2.2.4.5 Multiplexage de longueurs d'onde

Le multiplexage de longueur d'onde (en angl. Wave Division Multiplexing, WDM) est mis en œuvre lors de la transmission via fibres optiques. Avec le WDM, plusieurs longueurs d'ondes lumineuses sont transmises en parallèle sous forme de courant lumineux. La transmission simultanée peut même avoir lieu en mode full duplex.

17.7.2.2.5 Synchronous Digital Hierarchy (SDH)

SDH, SONET en version américaine, est une structure de multiplexage flexible et transparente qui se distingue par sa haute disponibilité et sa sécurité. Sur SDH il est possible d'atteindre des débits de données atteignant 155 Mbits/s à 40 Gbits/s. Comparé à PDH, SDH a l'avantage de pouvoir regrouper plusieurs débits faibles (par ex. 2 Mbits/s) dans un cadre de transmission plus élevé. Pour

le transfert d'informations, SDH utilise les signaux STM (Synchronous Transport Module) qui sont transmis à 155 Mbit/s sur la base des caractéristiques STM1. Les débits plus importants sont réalisés par multiplexage. A la différence du signal d'horloge sur PDH, le signal d'horloge sur SDH est réglé uniformément par une cadence de réseau centrale. De ce fait tous les niveaux de la hiérarchie suivent la même cadence et il est possible d'accéder aux niveaux hiérarchiques inférieurs sans devoir passer par tous les niveaux de multiplexage. Cet accès direct se fait par les unités de transport STM.

17.7.2.2.5.1 Multiplexage SDH

Le cadre de données de base STM STM-1 permet d'atteindre un taux de transmission de données de 155 Mbits/s. Chaque augmentation de ce taux représente le quadruple du niveau inférieur dans la hiérarchie de multiplexage. Il en résulte les taux de transmission suivants :

STM-4 avec un taux de transmission de 622 Mbits/s en deuxième échelon de hiérarchie

STM-16 avec un taux de transmission de 2,5 Gbits/s en troisième échelon de hiérarchie

STM-64 avec un taux de transmission de 10 Gbits/s en quatrième échelon de hiérarchie

STM-256 avec un taux de transmission de 40 Gbits/s en cinquième échelon de hiérarchie.

17.7.3 Interfaces série sur le WAN

Dans les WAN les lignes permanentes sont souvent reliées par des interfaces série. Les plus courantes sont décrites ci-dessous.

17.7.3.1 V.24

V.24, développée par l'UIT, est une interface qui transmet 20 Kbit/s sur 15 mètres. Elle est vraisemblablement la technologie la plus répandue pour la connexion d'équipement terminal de transmission de données (ETTD), le premier mais aussi le dernier élément dans la communication, en général relié à un raccord de télécommunication (par ex. un modem). V.24 est indépendant du mode de transmission. Elle supporte aussi bien les transmissions synchrones que les transmissions asynchrones. L'interface physique est le connecteur miniature Sub-D à 25 broches.

17.7.3.2 RS-232

RS-232 est l'interface série et bidirectionnelle basée sur les caractéristiques fonctionnelles de V.24 transmettant des données asynchrones. RS-232 définit la transmission série aussi bien en mode half-duplex qu'en mode full-duplex. RS-232 est conçu pour deux canaux série fonctionnant indépendamment l'un de l'autre et pouvant envoyer et recevoir simultanément (full duplex). Dans la pratique, RS-232, qui s'appelle RS-232-C dans la version actuelle, est mis en œuvre pour la communication d'un ordinateur avec un autre ordinateur ou un autre appareil série. Etant donné

que l'ordinateur utilise en fonctionnement interne un flux parallèle de données, RS-232 spécifie comment ces flux parallèles de données sont transformés sur l'équipement terminal de transmission de données (ETTD) par le chip de l'Universal Asynchronous Receiver/Transmitter (UART) en un flux série de données, qui est ensuite transmis en série, un bit après l'autre, à un autre ordinateur. En tant que ETTD de l'ordinateur, l'UART communique également avec d'autres appareils séries, qui ont ensuite le pendant de l'ETTD comme interface de communication : le matériel de transmission de données (Data Communication Equipment, DCE) qu'utilisent par exemple les modems et les routeurs.

17.7.3.3 X.21

X.21 est la norme de l'UIT-T pour l'accès aux réseaux numériques. Elle vaut pour tous les réseaux de transmission par paquets et par circuits, mais aussi pour les lignes permanentes avec accès numérique. X.21 est valable aussi bien pour les lignes symétriques que pour les lignes asymétriques. X.21 permet d'atteindre des débits de 10 Mbit/s, mais en général X.21 sert pour des lignes permanentes ayant un débit de 2 Mbit/s. L'interface normalisée pour X.21 est un connecteur à 15 broches.

17.7.3.4 V.35

V.35 fonctionne sur des largeurs de bande de plus de 19,2 Kbit/s et il est également utilisé comme interface entre des réseaux de transmission par paquets et l'équipement d'accès à ces réseaux. V.35 permet de regrouper plusieurs lignes téléphoniques.

17.7.4 X.25 et commutation de trames

17.7.4.1 X.25

La norme la plus connue pour les procédés de transmission par paquets est certainement **X.25**. X.25 a été développée par l'UIT-T. L'UIT-T décrit dans sa recommandation concernant X.25 le fonctionnement synchrone d'une station finale de transmission par paquets sur un réseau public. Elle décrit aussi le déroulement et le format des transmissions effectuées avec X.25. La recommandation de l'UIT-T est orientée sur les trois couches inférieures du modèle de référence OSI. Dans la couche 1 de X.25 se produit la connexion physique et la transmission des bits proprement dite. La couche 2 est celle de la sécurisation de la ligne et des schémas de contrôle pour le filtrage et la détection d'erreurs de transmission. Dans la couche 3 pour transmissions X.25 sont définies la connexion et la déconnexion de la liaison de même que la connexion des terminaisons du système pour les couches supérieures d'application. Cette interface entre la troisième couche et la couche supérieure dans le modèle OSI s'appelle Network Service Access Point (NSAP). Avec X.25, jusqu'à 4.096 liaisons virtuelles réparties sur maximum 16 canaux logiques sont créées entre les stations connectées.

Ces liaisons sont soit permanentes (Permanent Virtual Circuit) soit commutables dynamiquement (Switched Virtual Circuit). X.25 est idéal pour relier des réseaux locaux à l'aide de routeurs X.25. Les avantages essentiels résident dans la rapidité de la liaison, qui est établie en une seconde, et dans la bonne qualité de la transmission. Et ce, à des vitesses de 300 à 64.000 bits/s. En vue de la transmission de données avec X.25, il existe des réseaux propres de données par exemple Datex-P en Allemagne, Telepac en Suisse, Datanet 1 aux den Pays-Bas ou ISTELE de British Telecom.

17.7.4.2 Commutation de trame

La commutation de trames (Frame Relay) est une méthode de transmission similaire à X.25. Contrairement à X.25, la commutation de trames tourne sur les niveaux 1 et 2 du modèle ISO/OSI. Le protocole ne se charge plus lui-même de l'attribution correcte des paquets de données, mais transmet cette tâche aux périphériques.

La transposition de la correction d'erreur sur les couches supérieures du protocole permet de contourner les difficultés apparaissant parfois au niveau de l'efficacité de X.25. De ce fait, elle n'ajoute pas de bits supplémentaires pour le contrôle, ce qui autorise des débits beaucoup plus rapides. Toutefois, cela suppose des terminaux suffisamment intelligents pour effectuer les contrôles d'erreurs, lesquels se trouvent donc reportés à des couches supérieures du modèle OSI. La commutation de trames est idéale pour l'amélioration du débit dans le WAN. Par rapport aux lignes permanentes, Frame Relay représente des avantages lorsque les connexions Point-to-Point ne sont pas surchargées. Suivant le pays, la technique de la commutation de trames peut être utilisée dans différents réseaux privés ou publics, comme par ex. dans le service Datex-M de Deutsche Telekom. Pour l'accès au réseau, **SNI (Subscriber Network Interface)** est utilisée en tant que terminaison du réseau. La connexion "Small-Entry" commence avec 64 Kbits/s, la catégorie suivante avec 2 Mbits/s (E1). L'interface standard pour les routeurs et les ponts est l'interface X.21. Actuellement, la vitesse la plus élevée est de l'ordre de 34 Mbits/s (E3).

Même si la commutation de trames présente des avantages par rapport à X.25, elle ne peut convenir à des applications aussi "chronophages" que la transmission vocale ou vidéo, par exemple. Cet inconvénient était jusqu'à présent négligeable, les réseaux pour les transferts de voix ou d'images étant construits séparément. Pourtant, avec l'apparition des applications multimédia sur les réseaux LAN et WAN, l'intégration d'informations audio et vidéo est devenue réalité. C'est dans ce contexte qu'intervient le nouveau procédé de transmission de paquets ATM (Asynchrone Transfer Mode).

Plusieurs fournisseurs de services offrent les liaisons de commutation de trames. Les différences se font sentir nettement au niveau du prix, mais dans certains cas, plus encore au niveau de la performance. En aucun cas, il n'est de règle dans ce marché que le CIR (Committed Information Rate) confirmé ne soit réellement disponible ou que les Round Trip Delays ne soient dans des

limites raisonnables. Avant de se décider pour un fournisseur d'accès de Frame Relay, il serait judicieux de contrôler la qualité du réseau que celui-ci offre et de confirmer par écrit les conséquences en cas de non respect des attentes.

17.7.5 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM), mode de transfert asynchrone) est une technologie de transmission de paquets asynchrone, rapide qui a été mise au point principalement pour une fonctionner dans les réseaux d'WAN. ATM a cependant trouvé sa place dans quelques réseaux locaux.

17.7.5.1 Transfert de données sur des réseaux ATM

L'exacte vitesse de transmission d'un fichier n'est en général pas un facteur déterminant. Il en va autrement pour les données dont le temps de transmission est un facteur critique, citons par exemple les données audio ou les animations. Le plus petit retard de transmission d'un signal audio provoque une discontinuation ou une interférence et lors d'informations vidéo on obtient un déroulement de l'image irrégulier. Si l'on veut donc intégrer les données de type multimédia dans le réseau, il faut que les composants matériels et logiciels soient capables de transmettre en temps réel. ATM propose ce service et s'avère donc être la technologie la mieux adaptée à des applications multimédia. La clé du succès d'ATM réside dans la vitesse de transmission qui est de l'ordre de grandeur du Gigabit. Les administrateurs de réseaux se tournent avec insistance vers les fournisseurs et intégrateurs de systèmes, afin que ceux-ci trouvent la solution à leurs problèmes concernant la largeur de bande. ATM représente à cet égard un investissement à long terme et passera bientôt du statut de technologie haut de gamme à celui d'application du quotidien. Les entreprises devraient s'informer sur le marché et sonder les possibilités de migration pour amener l'utilisateur à se tourner vers ATM. En plus de la vitesse vient s'ajouter la variabilité de ATM, par laquelle on entend la possibilité d'échelonner la largeur de bande disponible. La génération actuelle de commutateurs ATM supporte 155 Mbits/s ou 622 Mbits/s par port. Cela ne constitue pas loin s'en faut la limite maximale. Des vitesses de l'ordre du multi-gigabits sont réalisables en ATM. ATM est la première technologie à même d'intégrer sans problème les réseaux LAN et WAN. Cela rend superflues des passerelles supplémentaires convertissant des protocoles LAN en protocoles WAN.

Avec ATM, tous les types d'information, audio, vidéo et données sont transmises par paquets d'une longueur déterminée (53 octets), qui sont aussi appelés "cellules" (cell relay). 48 octets sont à la disposition des données elles-mêmes, et 5 octets sont réservés à l'information de contrôle. Le principal intérêt d'ATM réside dans cette structure de données. La longueur homogène de toutes les cellules permet de calculer un retard de transmission de n'importe quelle information. Cela permet d'attribuer, pour des applications individuelles, des largeurs de bande garanties, ceci même en présence de plusieurs courants de données. Le problème bien connu dans les autres topologies de trames plus longues, qui apparaissent lors de transfert de fichiers et qui bloquent dès lors les

autres applications, est évité grâce à la structure en cellule de ATM. Les très petits blocs conviennent pour les transmissions de la voix et de vidéos, les grands blocs pour la transmission de données et les images animées. Le format ATM des cellules a permis de trouver un compromis, qui devrait satisfaire tous les services. Etant donné que la plupart des informations ne sont pas consignables dans une seule cellule ATM, le mécanisme d'adaptation **SAR** (**S**egmentation and **R**eassembly) de l'adaptateur ATM émettant distribuera les paquets de longueurs différentes des couches supérieures du réseau sur des cellules ATM. Les paquets seront de nouveau assemblés lorsqu'ils arriveront à destination.

La transmission repose sur le principe de la liaison virtuelle, qui est aussi sous-jacent aux réseaux transmettant des paquets, tel X.25. Ce principe ne fait pas intervenir des canaux fixes entre les périphériques concernés. Bien plus, les cellules d'une liaison déterminée seront transportées suivant un trajet fixé à l'avance. Ainsi les moyens d'exploitation dans les éléments du réseau peuvent être utilisés plus efficacement pour plusieurs liaisons. ATM supporte aussi bien des liaisons fixes (**PVCs**, **P**ermanent **V**irtual **C**ircuits) que des liaisons commutées (**SVCs**, **S**witched **V**irtual **C**ircuits). Dans ce cas, il peut s'agir de liaisons point à point ou de liaisons point à multipoint.

Les liaisons peuvent être établies sur base d'une certaine qualité de fonctionnement **QoS** (**Q**uality **o**f **S**ervice). A chaque périphérique connecté, ATM attribue, grâce aux PVC et SVC déjà évoqués, de manière statique ou dynamique la bande passante requise, celle-ci n'étant limitée que par la capacité du matériel ATM. Après l'établissement de la liaison, on a dès lors la certitude de pouvoir utiliser seul le canal de transmission, sans être dérangé ou même interrompu par d'autres stations désireuses d'émettre.

Ce faisant, il convient de répondre le mieux possible aux exigences particulières. ATM propose essentiellement trois catégories de services : les services garantis, les services prévisibles ou les services utilisant au mieux un taux de bit disponible. Un service garanti est nécessaire pour supporter un taux constant de bits (**CBR**, **C**onstant **B**it **R**ate), toutes les cellules seront transmises de manière sûre avec un retard minime, comme pour les applications vocales. Il existe aussi d'autres applications ayant un taux de bits variable, par exemple le transfert de fichiers ou le courrier électronique, pour lesquelles un service utilisant au mieux le taux de bits disponible peut suffire. Mais il n'y a aucune garantie. Dans ce cas, les cellules sont simplement portées sur la bande passante demeurée libre après la transmission des informations prioritaires. Dans la spécification du forum ATM, ces services sont répertoriés sous l'appellation "Traffic Management".

17.7.5.2 Interfaces

Un grand nombre d'interfaces de transmission ATM est défini aussi bien pour les WAN que pour les LAN. Les vitesses de transmission pour les moyens physiques atteignent de 1,5 à 622 Mbits/s. Les différences de spécification entre les LAN et les WAN résident principalement dans les moyens de

transmission. Si dans le domaine WAN des fibres Single Mode et des câbles coaxiaux sont prévus en priorité, ce sont des câbles paire torsadée et des fibres Multi Mode qui sont utilisés principalement dans le domaine LAN.

17.7.5.3 Disponibilité et standardisation

Le moteur du processus de normalisation est le forum ATM, déjà cité plus haut : un groupement d'intérêt composé de fabricants ATM, faisant des suggestions à ITU (International Communication Union - organisme prescrivant notamment les normes pour les modems) successeur de la CCITT (Consultative Committee for International Telephony and Telegraphy). La définition des cellules est depuis longtemps établie. La manière dont le matériel des systèmes ATM doit fonctionner est aussi définie, ainsi que l'établissement et le contrôle des liaisons et de là les interfaces logiques utiles. ATM comporte toutefois encore d'autres spécifications. Selon les données du fabricant, les produits peuvent être adaptés à divers standards sans problème au moyen de mises à niveau logicielles. Si l'on ne met en œuvre les produits que d'un seul constructeur, on est assuré d'être en conformité avec toutes les spécifications du forum ATM. Cependant, si des produits ATM de différents constructeurs doivent fonctionner ensemble dans une même installation, il est de bon ton que la compatibilité des produits entre eux soit assurée.

17.7.5.4 Migration dans les réseaux existants

Les différences importantes existant entre le réseau ATM et les réseaux déjà en place, nécessitent une intégration flexible des produits ATM afin de continuer à utiliser au mieux les investissements déjà consentis. Ce procédé d'adaptation est appelé migration. La migration d'ATM se déroulera en plusieurs étapes. Les commutateurs ATM peuvent être utilisés dans les grands réseaux comme support principal. Les câbles de segments fédérateurs en topologie de type anneau ou bus peuvent être transformés pour former une topologie de type étoile via le commutateur ATM auquel doivent être reliés tous les segments et appareils du réseau. A partir de là, d'autres commutateurs ou composants ATM peuvent être raccordés au commutateur ATM d'origine. Le raccordement de topologies de réseau déjà constituées à un réseau ATM s'effectue aujourd'hui essentiellement par l'intermédiaire de solutions ATM faisant appel à des routeurs. La plupart des fabricants de gros concentrateurs offrent des modules pour réaliser des connexions ATM.

L'établissement d'une connexion continue avec un terminal est la dernière étape de ce processus. Il faut s'attendre à ce que ce processus fasse encore baisser le coût total par port dans les réseaux ATM. L'utilisation de l'ATM est cependant déjà une alternative intéressante pour certaines applications (stations de travail haut de gamme, serveurs, traitement d'images ou Virtual Reality). Mais comment est-il possible d'intégrer des applications actuelles dans un réseau ATM ? La solution la plus simple consisterait à échanger l'interface LAN existante par une carte ATM et à installer un pilote ATM à sa place. Ce n'est malheureusement pas aussi simple, car contrairement aux LAN,

ATM ne supporte pas les messages “broadcasts”, “multicasts” ni l’utilisation des adresses MAC. Ceci constitue cependant une condition préalable à l’utilisation de la plupart des protocoles réseau tels TCP/IP ou IPX. La solution proposée par le forum ATM pour cette problématique s’appelle **LAN Emulation LANE 2.0**. LANE comprend 4 composants logiciels.

Les **LAN-Emulation-Services (LES)** comprenant 3 composants seront affectés à un ou plusieurs ordinateurs reliés au réseau ATM en tant qu’application ATM ou en tant que partie intégrée d’un commutateur ATM. Le **LAN-Emulation-Client (LEC)** en tant que quatrième composant sera installé sur tous les autres terminaux. Services Emulation LAN :

Le LECS (**LAN Emulation Confirmation Server**) coordonne tous les LES et LEC.

Le LES (**LAN Emulation Server**) traduit les adresses MAC en adresses ATM et vice versa.

Le BUS **B**roadcast and **U**nknown **S**erver transmet les paquets “Broadcast” et “Multicast” à l’aide de connexions Point-to-Multipoint ATM à des ordinateurs inconnus jusqu’à ce que l’adresse cible soit trouvée. En début de transmission, le LEC contacte le LECS en utilisant une adresse réseau unique afin de garantir l’échange d’informations LANE. Le LECS transmet l’adresse correspondante LES au client. Ensuite le LEC contacte le LES. Les adresses ATM, MAC ainsi que l’importance de l’environnement et le type du LAN sont définis. Les “Broadcasts” et les paquets dont la destination est inconnue sont transmis par le LEC au BUS qui lui se charge de la transmission.

Les caractéristiques des niveaux MAC manquants sont émulées pour les clients. ATM apparaît finalement à ces derniers comme un réseau 802.3 (Ethernet) ou 802.5 (Token-Ring), par exemple. La communication entre un LAN conventionnel et un réseau ATM est ainsi parfaitement réalisable.

17.7.6 Digital Subscribe Line (DSL)

DSL est une technologie de transmission qui rend possible de hauts débits sur le câblage téléphonique. Les traditionnelles quatre variantes de DSL sont l’Asymmetric Digital Subscriber Line (ADSL), la High-Data-Rate Digital Subscriber Line (HDSL), la Single-Line Digital Subscriber Line (SDSL) et la Very-High-Data-Rate Digital Subscriber Line (VDSL). Si l’on évoque DSL dans toutes ses variantes, le terme **xDSL** est aussi souvent utilisé. Etant donné que DSL et la transmission téléphonique peuvent fonctionner avec des fréquences différentes, les deux flux de données peuvent être transmis parallèlement.

17.7.6.1 Asymmetric Digital Subscriber Line (ADSL)

ADSL est la norme DSL la plus répandue et la plus utilisée. ADSL est un procédé de transmission asymétrique de données sur larges bandes qui est connecté sur les traditionnels chargeurs doubles en cuivre. Pour une communication ADSL il faut que des deux côtés de la ligne soit installé un modem ADSL, aussi bien sur le réseau local que chez l’abonné. Dans le procédé ADSL la ligne en cuivre est séparée en trois canaux. Le canal Downstream du fournisseur de services au client final, le canal Upstream dans le sens opposé et un canal via lequel les communications PSTN et

RNIS peuvent avoir lieu simultanément grâce à l'intervention d'un diviseur. En fonction du processus, le signal devant être transmis est décomposé en divers signaux partiels pouvant être transférés sur diverses fréquences porteuses. En dehors de la modulation multiporteuse spécifiée dans la norme ADSL on utilise aussi le procédé CAP/QAM. Il est possible d'atteindre avec l'ADSL des taux de transmission de 6 Mbits/s avec des câbles téléphoniques normaux. Pour la transmission bidirectionnelle, une deuxième bande de fréquence est disponible avec des taux de transmission de l'ordre de 640 kbits/s.

L'ADSL peut aussi bien être mis en œuvre pour des services de répartition que pour des services vidéo interactifs comme par exemple pour les applications Pay-per-Channel-, Pay-per-View-, Video-on-Demand- et Information-on-Demand. Pour des vitesses de transmission supérieures à 1,5 Mbit/s la distance jusqu'au prochain nœud peut être de 4 km et jusqu'à 6 km pour des vitesses inférieures.

17.7.6.2 High-Data-Rate Digital Subscriber Line (HDSL)

HDSL est idéal pour la connexion d'installations avec postes supplémentaires et comme alternative à la commutation de trames sur réseaux locaux. Il peut en outre remplacer des liaisons E-1 ou des liaisons renforcées par amplificateur. Avec l'HDSL, des taux de transmission de 2 Mbits/s max. sont possibles sur des distances pouvant atteindre 5 kilomètres.

17.7.6.3 Symmetric Digital Subscriber Line (SDSL)

SDSL est comme HDSL un procédé pour transmissions en full-duplex avec des vitesses symétriques situées entre 64 kbit/s et 2 Mbit/s (ligne E 1). Mais contrairement à HDSL la transmission nécessite seulement une ligne à deux fils. La distance maximale pour SDSL se situe vers 3,5 km.

17.7.6.4 Very High-Data-Rate Digital Subscriber Line (VDSL)

VDSL est utilisé partout où il s'agit de transmettre des flux de données symétriques ou asymétriques à grande vitesse sur de courtes distances. Cette variante du DSL fonctionne aussi bien avec câble en cuivre qu'avec câble en fibre de verre.

Avec le VDSL, il est possible d'atteindre en transmission symétrique des taux de transmission de 72 Mbits/s selon la classe. Au niveau des classes on distingue la transmission asymétrique et la transmission symétrique. La classe en mode de fonctionnement asymétrique a des taux de 8 Mbit/s, 16 Mbit/s et 28 Mbit/s et la classe symétrique a des taux de 12, 24, 48 et 72 Mbit/s.

Elle peut donc être aussi utilisée pour la transmission de la télévision à haute définition. VDSL permet d'atteindre en downstream, donc du nœud vers l'utilisateur, des vitesses de transmission allant de 13 Mbit/s à 52 Mbit/s sur des lignes à deux fils de cuivre. En upstream, les vitesses de transmission se situent entre 1,5 Mbit/s et 2,3 Mbit/s.

En ce qui concerne la portée de VDSL, il faut distinguer trois catégories : La longue distance entre un kilomètre et 1,5 km, la moyenne distance entre 300 et 500 mètres et la courte distance

en-dessous de 300 mètres.

17.8 Sécurité sur les WAN

Ajoutons encore la sécurité des réseaux comme condition incontournable pour le succès d'une entreprise. La savoir faire sur lequel repose le succès d'une entreprise doit aussi rester la propriété exclusive de cette entreprise. Si des tiers viennent à prendre possession d'informations et de données de cette entreprise, celle-ci court le risque de devoir partager son chiffre d'affaire et ses profits avec ces tiers, voire de perdre la totalité du chiffre d'affaire à leurs profits. Les attaques malveillantes destinées à perturber le bon déroulement des processus internes à l'entreprise doivent aussi être considérées comme un danger pour la sécurité. C'est pourquoi il est nécessaire de s'assurer, dans le domaine des WAN, que la communication sur base WAN ne puisse pas être piratée, que personne ne puisse pénétrer dans le réseau interne de l'entreprise via le WAN, obtenant ainsi un accès aux ressources du réseau qui pourraient éventuellement être modifiées.

17.8.1 Attaques et cibles

Pour les entreprises le plus grand danger provient des menaces contre la confidentialité et l'intégrité. On parle de menaces pour l'intégrité des données quand un agresseur essaye de modifier des données appartenant à l'entreprise sans avoir l'autorisation d'y accéder ou de les éditer. Un agresseur peut par exemple essayer d'accéder à des données d'une entreprise, de les modifier ou de les effacer. Il se peut que le propriétaire ne remarque pas cette intervention avant qu'il ne soit trop tard et que toutes les données soient perdues. Un autre exemple est celui d'une attaque sur un serveur Web et les modifications dans la présentation de l'entreprise sur Internet. Les préjudices subis par la réputation de la victime d'une telle attaque sont incalculables ! Beaucoup d'entreprises considèrent que les menaces contre l'intégrité sont le danger le plus grave parce qu'il est très difficile de détecter des modifications éventuelles et de les annuler. Dans le cas de la suppression de données, c'est même la base du succès de l'entreprise qui peut être détruite.

Les menaces pour la confidentialité visent à obtenir l'accès à des données secrètes ou confidentielles afin d'en prendre connaissance. Ces attaques sont encore plus difficiles à repérer parce qu'il n'y a pas trace de l'agresseur une fois que celui-ci a quitté le réseau. Même les cas où l'agresseur copie les données secrètes sont très difficiles, voire impossibles, à déceler. Une autre attaque du même type consiste à capturer, modifier puis remettre en circuit des données circulant sur le WAN, comme par exemple entre une filiale et la maison-mère.

Les attaques de refus de service (DoS) constituent un danger supplémentaire visant à rendre inutilisables des services ciblés. Lors d'une attaque de refus de service l'agresseur envoie tellement de données et de demandes à la cible qu'elle est trop occupée pour pouvoir s'acquitter de son service proprement dit ou même tellement dépassée qu'elle cesse de l'exercer. Des serveurs ouverts au public comme les serveurs Web ou WWW sont par exemple inondés de messages électroniques ou de demandes et leurs utilisateurs sont ainsi contraints à s'avouer vaincus. Les liaisons Internet

peuvent également faire l'objet d'attaques de refus de service. L'agresseur envoie par exemple tellement de paquets à un routeur que celui-ci ne peut plus accepter ni traiter les demandes de ses propres utilisateurs.

Des composants actifs de réseau peuvent également être pris pour cibles. Si un agresseur parvient par exemple à accéder à un commutateur ou à un routeur, il a de multiples possibilités de mettre à profit cet accès illégal pour procéder à des opérations nuisibles :

- La capture de données
- L'attaque de services de sécurité installés fonctionnant selon le principe de la confiance entre composants réseaux
- La modification de configurations.

L'agresseur peut par exemple copier et capturer les données circulant sur un commutateur de segment fédérateur. Si un serveur d'accès à distance est victime d'une attaque, l'attaquant peut par exemple y lire des mots de passe et les utiliser pour d'autres attaques en se connectant sur le réseau comme utilisateur autorisé. Lors d'une attaque sur un firewall l'agresseur peut par exemple modifier la configuration de telle façon qu'il soit à l'avenir identifié comme utilisateur autorisé. Un routeur d'accès peut être reconfiguré de telle manière que l'accès à Internet ne soit plus disponible pour le service lui-même.

Des réseaux complets deviennent alors la cible d'agresseurs qui espèrent ainsi obtenir des informations utiles pour des attaques futures spécifiques. Un réseau peut être examiné à la recherche de cibles potentielles non protégées. L'agresseur essaye de se faire une idée de tout le réseau, y compris sa topologie générale, les services utilisés et les applications utilisées. Cette analyse lui permet de détecter des points faibles qui lui serviront pour des attaques spécifiques ultérieures. Ces attaques spécifiques peuvent concerner des hôtes, des applications ou la disponibilité du réseau. Toutes ces attaques se font dans les mêmes intentions : accéder sans autorisation à des données secrètes pour les lire ou les modifier ou encore rendre des services indisponibles.

17.8.2 Stratégies et mesures de protection

Tous ces dangers potentiels constituent pour tout exploitant de réseau un risque presque incalculable si des mesures de sécurité adéquates ne sont pas adoptées. Pour pouvoir protéger de manière effective un réseau contre des attaques extérieures, il faut d'abord en connaître les points faibles, les classer et prendre les mesures nécessaires à leur protection. La définition des dangers potentiels et la manière dont l'entreprise y fera face sont déterminées dans une charte de sécurité interne. Une charte de sécurité documente les risques auxquels un réseau est exposé et la manière dont il convient d'y faire face. Son élaboration et sa mise en application sont un processus continu. Les chartes sont en général segmentées par secteurs afin de minimiser les risques identifiés. La charte de sécurité détermine les mesures spécifiques prises pour chaque domaine. Une telle charte peut s'appliquer par exemple aux sujets suivants:

- Définition d'un contrôle d'accès au réseau. Qui a accès à quelles données et comment ?
- Définition d'une hiérarchie des données. Quelle importance ont quelles données pour l'entreprise et qui peut y accéder ?
- Définition d'une politique des utilisateurs. Comment les utilisateurs doivent-ils se comporter quand ils ont accès au réseau ?

Un autre exemple :

Dans le cadre de sa charte de sécurité exhaustive, une entreprise souhaite mettre au point des directives concernant l'accès à Internet. La charte de sécurité veut que l'accès à Internet soit réservé à certains utilisateurs pour des services nécessaires précis, qu'aucun utilisateur n'installe lui-même des applications et les utilise ensuite, et que toutes les transactions qui contreviennent aux directives de sécurité soient intégralement documentées par un audit. En application de ces directives pour l'accès à Internet l'entreprise a implémenté les mesures suivantes :

- Les Firewalls ne laissent passer que les Emails et les échanges http
- L'accès à Internet ne doit plus avoir lieu que pour le travail
- Le réseau protégé ne permet pas le téléchargement de programmes exécutables depuis des sources externes
- Les composants réseau rédigent des journaux répertoriant tous les échanges Internet.

17.8.3 Contrôles d'accès aux réseaux

Un contrôle d'accès bien étudié permet avant tout d'assurer l'intégrité et la confidentialité des données. Un contrôle d'accès repose sur les directives par exemple d'une charte de sécurité qui définit quel utilisateur peut accéder à quelles ressources. Le contrôle d'accès à un réseau est basé sur deux mesures : l'authentification et l'autorisation.

17.8.3.1 Authentification

L'authentification contrôle et établit l'identité d'un utilisateur. Les administrateurs peuvent après authentification accéder aux composants du réseau, aux hôtes et aux installations de gestion du réseau ; les utilisateurs peuvent accéder au réseau et aux ressources pour lesquelles ils sont admis. Cette authentification est particulièrement importante quand des possibilités d'accès public, comme par exemple des points d'accès, sont implémentés dans le réseau. Il est impératif de pouvoir séparer à ces points d'accès les utilisateurs avec autorisation d'accès de ceux dont l'accès n'est pas autorisé. L'identification d'un utilisateur est effectuée au moyen d'une clé précise :

- Que l'utilisateur connaît, par exemple, un mot de passe ou un pin
- Que l'utilisateur possède, par exemple, un dongle ou une SmartCard
- Qui fait partie entière de l'utilisateur, par. ex. une empreinte digitale.

Un contrôle d'accès efficace réunit au moins deux des critères mentionnés ci-dessus : il s'agit de

l'identification à deux facteurs. Ces méthodes, souvent utilisées pour les systèmes de traitement de données, constituent la base de toute une série d'autres possibilités d'identification d'utilisateurs et d'autorisation. Les différents procédés sont présentés dans le chapitre suivant qui mentionne également leurs avantages et inconvénients respectifs.

17.8.3.1.1 Procédés d'authentification

Les méthodes les plus courantes d'identification d'utilisateurs sont de nos jours :

- Les mots de passe indépendants
- Le système de rappel (dial back)
- L'autorisation par un système de questions/réponses
- Le dongle logiciel
- La méthode fondée sur le facteur temps.

17.8.3.1.1.1 Mots de passe réutilisables

L'utilisation de mots de passe présente certains inconvénients :

- Les mots de passe peuvent être manipulés
- Dans la pratique ils ne sont pas modifiés à intervalles réguliers
- Ils peuvent être en la possession de plusieurs utilisateurs
- Ils dépendent de diverses composantes sociales
- Ils peuvent être décodés par des programmes spéciaux.

Il faut de plus prendre en compte que leur parcours et leur utilisation ne peuvent être que difficilement contrôlés et suivis.

17.8.3.1.1.2 Systèmes de rappel

Utilisés en parallèle avec la technique des mots de passe, les systèmes de rappel permettent d'assurer une protection accrue : l'utilisateur demandant l'accès doit, après identification, attendre d'être rappelé par téléphone. Un contrôle d'accès au système est possible via la liste des appels téléphoniques. L'avantage supplémentaire de la prise en charge du coût par le demandeur appelant (la centrale de l'entreprise dans la plupart des cas) est certes indiqué, mais non pertinent au niveau de la sécurité. Cette technique a cependant d'autres inconvénients :

- C'est l'appareil et pas l'utilisateur qui est autorisé
- Il n'est que rarement possible de procéder au rappel d'utilisateurs mobiles
- Les utilisateurs autorisés n'utilisant pas un appareil précis peuvent être exclus
- Le système peut être manipulé avec des transferts d'appel
- Il est compliqué pour l'utilisateur et implique une perte de temps
- Il ne peut être mis en œuvre que par protocole de support (autrement dit pas de protection pour les accès X.25 ou l'accès via Internet)

- Il n'y a pas de protection au niveau application ou protocole.

En bref, les systèmes de rappel sont difficiles à contrôler et n'offrent pas encore un degré de protection totale.

17.8.3.1.1.3 Systèmes de question-réponse

De telles solutions sont basées sur deux sous-systèmes. Le premier est installé chez l'utilisateur et le second au niveau de l'ordinateur hôte. Lors d'une demande d'accès de l'utilisateur, l'ordinateur hôte émet des informations en direction de l'utilisateur. Ces informations doivent être traitées par un algorithme installé côté utilisateur qui doit, le cas échéant, compléter les données ainsi transformées. L'ensemble de ces informations est alors renvoyé à l'ordinateur hôte. Si les informations reçues correspondent bien à ce qu'elles doivent être, l'ordinateur hôte autorise l'accès. Pour augmenter encore la sécurité, ce système peut être répété plusieurs fois. Les systèmes "Dongle" (clé matérielle) courants pour certains produits logiciels fonctionnent également selon le même principe. La sécurité proposée par ces systèmes est substantielle. Mais ils ne sont pas non plus dépourvus d'inconvénients, suivant le type de système :

- L'utilisateur peut, le cas échéant, subir plusieurs cycles de contrôle
- Certains systèmes sont d'usage assez difficile
- Le PIN est sauvegardé selon une suite de caractères, qui sont intervertis, un second PIN est nécessaire pour l'ordinateur hôte
- Les systèmes d'autorisation peuvent être empruntés ou volés
- L'exportation de fichiers est problématique.

17.8.1.1.4 Dongle logiciel

Si la protection d'accès est implémentée dans le système d'exploitation ou dans une application, un appareil externe n'est plus nécessaire. Ceci constitue l'avantage principal du dongle logiciel. Là comme ailleurs, les inconvénients existent :

- Dépendance vis-à-vis du périphérique ou du système d'exploitation
- Le dongle logiciel peut être copié ou modifié
- PIN, clé et algorithme sont enregistrés dans le programme
- La gestion est problématique.

Le contrôle et la recherche de voies sont très difficiles et peuvent mener à la mauvaise personne. On ne peut contrôler de manière fiable leur utilisation.

17.8.3.1.1.5 Dongle en fonction du temps

Les solutions qui calculent une séquence de chiffres ou de lettres en fonction d'un temps déterminé sont extrêmement satisfaisantes. Le matériel nécessaire prend place sur une carte de dimension réduite (carte de crédit). Les avantages en sont :

- Indépendance vis-à-vis du périphérique, un lecteur de cartes n'est pas nécessaire
- La connexion s'opère en une seule étape, pas de procédure de questions/réponses
- La sécurité repose sur deux facteurs indépendants (le PIN de l'utilisateur et le dongle)
- Seule une personne à la fois peut être en possession de la carte contenant la séquence, et la combinaison peut immédiatement être désactivée en cas de vol. C'est pourquoi l'accès lui-même est contrôlable lorsque PIN et carte tombent dans de mauvaises mains.

17.8.3.1.2. Protocoles d'authentification

17.8.3.1.2.1 Password Authentication Protocol (PAP, protocole d'authentification de mot de passe)

Le PAP est un système d'authentification simple servant à authentifier une personne pénétrant dans le réseau par reconnaissance de l'utilisateur et mot de passe. Il est un composant du protocole de tunnelisation PPP. PAP est un processus d'authentification à deux étapes avec lequel le client envoie son identification d'utilisateur et son mot de passe sans codage au serveur qui procède à l'authentification. En cas de concordance, le serveur répond avec une confirmation et libère l'accès à Internet. En cas de saisie erronée, la connexion est interrompue.

17.8.3.1.2.2 Challenge Handshake Protocol (CHAP)

Le Challenge Handshake Protocol (CHAP) sert à l'authentification des systèmes entre eux et est mis en œuvre par des liens utilisant le protocole de tunnelisation PPP. Il s'agit d'un processus d'authentification à trois étapes. Au cours de la première étape, l'utilisateur s'identifie, au cours de la seconde, le mot de passe est exigé par la station appelée, laquelle met aussi à disposition la clé pour le codage et au cours de la troisième étape l'utilisateur externe transmet son mot de passe codé et obtient son autorisation d'accès.

17.8.3.1.2.3 Terminal Access Controller Access Control System (TACACS)

TACACS est un protocole d'authentification mis au point par Cisco permettant à un serveur d'accès à distance de transmettre les données d'authentification à un serveur d'authentification spécial. Les mots de passe pour l'authentification des utilisateurs sont gérés dans une banque de données centrale.

17.8.3.1.2.4 TACACS+

Bien que les noms soient extrêmement similaires, TACACS+ n'est pas comparable avec TACACS. TACACS+ est un protocole d'authentification tout nouveau fonctionnant avec une fonction de Message-Digest pour les mots de passe. TACACS+ peut supporter l'authentification PAP et CHAP.

TACACS+ exploite le Transmission Control Protocol (TCP).

17.8.3.1.2.5 Remote Authentication Dial-In User Service (RADIUS)

RADIUS est un protocole client/serveur permettant à un serveur d'accès à distance de communiquer avec un serveur central pour authentifier les utilisateurs entrants. Pour ce faire, une banque de données contenant tous les profils d'utilisateurs dont l'accès est autorisé est mise à jour sur le serveur central. Comme avec RADIUS la banque de données utilisateurs est centrale, celle-ci peut aussi être gérée de manière centrale, ce qui facilite la tâche de l'administrateur. Il est en outre ainsi possible de mettre facilement en oeuvre une charte de sécurité propre à l'entreprise. Cette centralisation permet aussi une surveillance et des analyses statistiques plus simples ainsi qu'en cas de besoin une facturation simplifiée des services.

17.8.3.1.2.6 Secure Shell (SSH)

SSH est un protocole de sécurité protégeant l'authentification et la communication même lorsqu'un utilisateur s'identifie sur un ordinateur Unix. L'authentification d'un utilisateur peut aussi être effectuée en plus avec un codage lors de la vérification du mot de passe. La clé publique utilisée dans ce procédé est enregistrée sur le système cible, la clé privée est utilisée par l'utilisateur pour l'authentification.

17.8.3.2. Autorisation

Une autorisation définit les prérogatives de tout utilisateur dans un réseau. Partant des droits impartis à chacun utilisateur, les mécanismes d'autorisation limitent l'accès aux ressources et définissent ce que chaque utilisateur est en droit de faire avec ces ressources. Pour qu'une protection soit efficace il faut que chaque utilisateur n'ait accès qu'aux ressources dont il a absolument besoin pour accomplir sa tâche. Il faut également prévoir une redondance dans les questions d'autorisation. Un mécanisme de sécurité devrait être confirmé par un second avant que l'accès à une ressource ne soit définitivement accordé. Pour être vraiment efficace le contrôle de l'autorisation doit être centralisé. L'autorisation peut être réalisée en implémentant, par exemple, les mesures de sécurité suivantes :

- Les adresses IP sont attribuées aux clients demandant un accès par un poste central crédible
- Les filtres d'adresse limitent l'accès aux ressources
- Les filtres d'application ne permettent que la transmission d'applications autorisées.

17.8.3.3 Détection d'intrusion

Les systèmes de détection d'intrusion fonctionnent sur la base d'utilisation de signatures d'attaque. On entend par là des schémas caractéristiques d'une attaque ou d'un mode d'agression. Ces signatures définissent des conditions précises devant être remplies avant que l'échange de données ne soit identifié comme une agression. Il existe deux technologies de détection d'intrusion qui se complètent. Le système de détection d'intrusion basé sur le réseau (Network Intrusion Detection System, NIDS) surveille tous les paquets qui traversent un domaine de collision. Dès que le NIDS reconnaît un paquet ou une série de paquets correspondant à un schéma prédéfini ou suggérant qu'il s'agit d'une agression, une alarme est déclenchée et/ou la session est interrompue. Avec un système de détection d'intrusion sur base d'hôte (HIDS), les agents correspondants sont positionnés sur l'hôte à protéger. Cette technologie est opérante quand l'attaque est dirigée directement contre cet hôte. Une alarme est également déclenchée et l'accès à l'hôte est supprimé ou refusé.

17.8.4 Protection de la transmission de données

La protection de la transmission de données est nécessaire quand elle passe par des réseaux non protégés. Le danger d'une telle transmission réside dans le fait qu'un agresseur peut écouter, lire ces données et en faire mauvais usage. Une protection n'est réalisable que par un cryptage des données. Des données cryptées peuvent être lues par un tiers mais il ne peut pas en reconstituer le contenu, pour autant que le cryptage a été fait de manière efficace. Le décryptage des données ne peut être effectué que par des utilisateurs autorisés, c'est-à-dire qui sont en possession du code de décryptage. L'algorithme de cryptage IPSec, qui est très souvent employé, permet un cryptage efficace du contenu des paquets IP ; dans la pratique il est envoyé dans un tunnel VPN de la source, qui crypte les données, en passant par le réseau non protégé, par exemple Internet, jusqu'au destinataire qui décrypte les données.

17.8.4.1 Virtual Private Networks (VPN, réseaux privés virtuels)

La mise au point des **Virtual Private Networks (VPN, réseaux privés virtuels)** offre à l'utilisateur mobile et aux bureaux externes la possibilité de se connecter au siège de l'entreprise par le biais d'un réseau public non sécurisé. Un VPN correspond, du point de vue de la sécurité, à des lignes louées ou appartenant à l'utilisateur mais il présente une plus grande flexibilité et, quand il est correctement utilisé, un avantage de coûts puisqu'un VPN n'est établi que quand des données doivent être transmises. Les VPN peuvent être utilisés avec des accès par ligne commutée dans le réseau téléphonique analogique ou dans le réseau RNIS tout comme dans le réseau GSM et en cas de grandes quantités de données avec des lignes permanentes.

Le VPN est en règle générale un réseau fermé logique, se fondant majoritairement sur les couches 2 ou 3 du modèle de référence OSI et établi pour un groupe déterminé d'utilisateurs. Pour le trafic IP les VPN utilisent les mécanismes de tunnelisation.

17.8.4.1.1 Tunnelisation

La tunnelisation désigne un processus dans lequel deux protocoles différents sont encapsulés sur la même couche. Les données d'un protocole sont enveloppées dans les paquets de données du deuxième protocole. Ce procédé est utilisé lors du passage d'un protocole à un autre. Il sert à transporter des données entre un Gateway VPN central et un client VPN à distance en passant par un réseau public non sécurisé, comme l'Internet. Une connexion virtuelle est établie entre les deux stations finales. Cela entraîne la construction d'un tunnel dans lequel chaque paquet de données reçoit une en-tête IP supplémentaire et une ou plusieurs cellules initiales. Le tunnel commence là où l'en-tête IP est ajoutée et s'arrête là où elle est enlevée. L'authentification et le cryptage se font à l'intérieur du tunnel. La tunnelisation peut être réalisée sur les couches 2 et 3.

17.8.4.1.1.1 Normes et protocoles de tunnelisation

17.8.4.1.1.1.1 Generic Routing Encapsulation

Avec GRE, une norme dans laquelle un processus de tunnelisation est décrit de manière plus précise, il est possible de créer des tunnels indépendamment du protocole. Le pack tunnel GRE est composé de l'en-tête GRE et tunnel et de la charge utile (angl. : Payload). L'en-tête de tunnel contient les données d'adresse. Les informations concernant le protocole de tunnel encapsulé se trouvent quant à elles dans l'en-tête GRE, les algorithmes de codage et la charge utile incluent l'en-tête de protocole et les données purement utiles.

17.8.4.1.1.1.2 Point to Point Protocol (PPP)

Le Point to Point Protocol (PPP) : Protocole point à point) a été conçu pour l'encapsulation de diagrammes de données via connexions séries et supporte la transmission de tous les protocoles LAN courants. Le protocole PPP supprime les limites de l'interopérabilité provoquée par la technique d'encapsulation utilisée par les ponts et les routeurs pour la transmission via liaisons éloignées. Le protocole PPP permet la transmission de données via lignes permanentes et lignes commutées synchrones et asynchrones. Il est de ce fait en mesure de fonctionner en totale indépendance de toute interface physique. La seule condition préalable indispensable à la mise en œuvre du protocole PPP consiste en une ligne de données absolument transparente et à capacité full duplex.

17.8.4.1.1.1.3 Point to Point Tunnelling Protocol (PPTP)

Le protocole de tunnelisation point à point leader développé par Microsoft a été proposé en 1996 par l'IETF comme protocole standard pour la tunnelisation Internet. PPTP est une extension de PPP. PPTP encapsule des paquets PPP dans des paquets IP, ce qui permet de transmettre des protocoles comme IP, IPX et NetBEUI tunnelisés via Internet. PAP et CHAP sont utilisés pour contrôler l'accès.

Généralement, les algorithmes de codage Data Encryption Standard (DES) avec des clés de 56 (DES) à 168 (3DES) bits sont utilisés. Le contrôle du point final d'un tunnel réside chez l'utilisateur avec PPTP.

17.8.4.1.1.1.4 Layer 2 Forwarding (L2F)

Le Layer 2 Forwarding (L2F), développé par Cisco Systems, est spécialement conçu pour l'intégration d'ordinateurs indépendants. Avec PPTP, il forme le fondement du protocole Layer 2 Transport Protocol (L2TP), une révolution combinant deux systèmes. L2F supporte divers protocoles et plusieurs tunnels parallèles indépendants. L'identification des utilisateurs est toutefois plus faible qu'avec PPTP et un codage supplémentaire des données n'est malheureusement pas prévu.

17.8.4.1.1.1.5 Layer 2 Tunneling Protocol (L2TP)

Le protocole Layer 2 Tunneling ne se différencie que par quelques caractéristiques de PPTP. D'une part L2TP supporte plusieurs tunnels, comme L2F, d'autre part le contrôle du point final d'un tunnel ne réside pas comme avec PPTP chez l'utilisateur mais est imposé par prestataire d'accès à Internet.

17.8.4.1.1.1.6 IP Security Protocol (IPSec)

Le protocole IP Security Protocol (IPSec) a spécialement été mis au point pour la connexion entre deux réseaux locaux. IPSec protège les paquets de données du protocole IP contre des éventuelles modifications ou copies. IPSec n'influence ni les protocoles de communication ni les programmes d'application, de telle sorte que le routage n'est pas touché. Les processus d'authentification créés avec IPSec peuvent différencier les données issues de partenaires admis ou non admis. Les processus d'autorisation se fondent sur les algorithmes MD5-Hash avec 128 bits, le codage sur l'algorithme DES avec 56 ou 168 bits. Avec IPSec, il est possible de protéger tous les échanges de données IP. Ipv6 peut aussi être transmis avec IPSec.

17.8.4.1.1.1.7 Layer 2 Security

Le protocole Layer 2 Security (L2Sec) a pour fonction d'éliminer les points faibles dont IPSec est affecté pour les solutions d'accès à distance. Avec L2Sec, tous les paquets de données sont empaquetés dans un tunnel et celui-ci est sécurisé dans son ensemble.

17.8.4.1.2 Normes de codage

17.8.4.1.2.1 Data Encryption Standard (DES)

Le Data Encryption Standard (DES) est un chiffrement de bloc codant les données en blocs de 64 bits. Il est fourni à l'algorithme un bloc de 64 bits de texte clair et celui-ci livre en sortie un texte chiffré 64 bits. DES est un algorithme symétrique : le codage et le décodage utilisent le même algorithme et la même clé. La longueur de la clé est de 56 bits. La clé est de fait généralement imprimée en nombre 64 bits, mais tous les huit bits se trouve un bit de contrôle de parité qui est ignoré. Ces huit bits de parité sont toujours les bits ayant le moins de valeur de chaque octet de la clé. La clé peut être n'importe quel nombre de 56 bits. Il est de plus possible de modifier la clé à tout moment. La norme DES a été remplacée en 2001 par une version améliorée, l'AES, car des pirates DES avaient fait perdre l'intégrité de la clé.

17.8.4.1.2.2 Triple Data Encryption Standard (3DES)

La clé DES triple est un codage multiple sur base de DES. L'algorithme de codage symétrique 3DES utilise deux clés et trois processus DES. 3DES fonctionne ainsi avec une longueur de clé de 168 bits et 56 bits par processus DES.

17.8.4.1.2.3 Secure Socket Layer (SSL)

SSL a été développé spécialement pour le codage d'informations sur Internet et se fonde sur TCP/IP. SSL code avec des clés publiques confirmées en standard par un tiers. Le fait que la clé pour le déchiffrement sera une nouvelle fois déterminée de manière individuelle et qu'elle n'est enregistrée que chez l'utilisateur et de ce fait n'est pas transmise sur Internet constitue un gage de sécurité élevée. Les développeurs de SSL ont créé le protocole sur deux niveaux : niveau est responsable du codage des données. Il permet l'utilisation de divers algorithmes, entre autres DES et 3DES et impose en condition préalable que les deux partenaires de communication possèdent une clé secrète commune générée à chaque fois pour une connexion. L'authenticité des données est en outre vérifiée par un contrôle des sommes. Au deuxième niveau à lieu l'échange des clés privées. Les participants d'une connexion de communication s'authentifient, définissent un algorithme de codage et s'envoient mutuellement la clé de session.

17.8.4.1.2.4 Advanced Encryption Standard (AES)

La norme Advanced Encryption Standard a été mise au point en 2001 en réaction aux problèmes de sécurité du DES. L'AES repose sur la clé Rijndael et dispose de trois dimensions de clé avec 128, 192 ou 256 bits. L'AES permet 10 puissance 21 fois plus de clés 128 bits que le DES ne permet de clés 56 bits, ce qui démontre son niveau de sécurité.

17.8.4.1.3 Configurations VPN

Le chapitre suivant concerne la configuration et la constitution de VPN pour divers domaines d'application.

17.8.4.1.3.1 VPN de bout en bout

Les VPN de bout en bout forment une connexion directe entre plusieurs ordinateurs de postes de travail. Ce type de VPN peut être mis en œuvre, par exemple, pour connecter de manière sûre des clients avec un magasin en ligne ou pour faciliter à plusieurs employés répartis en des lieux différents le travail sur un projet commun. Il faut, avec les VPN de bout en bout, prendre en compte le fait que le protocole VPN correspondant doit être installé sur chaque ordinateur car les postes de travail sont directement connectés les uns avec les autres et non pas via des serveurs VPN. L2F, L2TP et IPSec sont des protocoles particulièrement appropriés pour le montage de VPN de bout en bout. IPSec est spécialement adapté pour les applications requérant le plus haut niveau de sécurité.

17.8.4.1.3.2 VPN de bout en site

Les VPN de bout en site (ou VPN d'accès à distance) sont utilisés en premier lieu pour la connexion des commerciaux au réseau central. L'avantage principal d'un tel réseau réside dans le fait que les employés peuvent se connecter au réseau via n'importe quel POP du fournisseur de services de la société. Avec les VPN de bout en site, il est possible de réduire les coûts généralement élevés des communications à distance, car il n'est pas nécessaire de mettre des pools grands de modems à disposition des employés.

17.8.4.1.3.3 VPN de site en site

Les VPN de site en site représentent la variante de VPN classique. Plusieurs LAN de lieux différents sont reliés les uns aux autres. Cette configuration est adaptée par exemple pour connecter les réseaux d'entreprise ou les institutions publiques. Tous les protocoles énumérés peuvent servir à un accès sécurisé sur un réseau d'entreprise, par exemple l'accès à distance.

17.8.4.2 Accès à distance

Accès à distance signifie que l'on peut accéder aux applications ou aux données se trouvant sur un ordinateur à partir d'un système n'étant pas directement relié sur le même réseau local. Pour l'accès à distance les éléments décrits ci-dessous sont incontournables. La condition préalable à remplir est une **connexion réseau** entre le calculateur cherchant l'accès et le système sur lequel se trouvent les données ou applications. Dans le cas le plus simple, la connexion se fait via deux modems branchés chacun à une interface série d'un des deux systèmes. Il est également possible d'utiliser

des serveurs de communication avec des modems y étant connectés. Si RNIS doit servir de service de transmission il convient d'utiliser des contrôleurs RNIS internes ou des adaptateurs de terminaux série RNIS. Tous les autres types de connexion comme GSM, X.25 ou FrameRelay, décrits aux paragraphes précédents, peuvent être utilisés. Internet a pris de plus en plus de poids en tant que medium de transport économique pour les connexions via PPTP. PPTP permet d'installer des tunnels pour des réseaux appelés Virtual Private Dial-Up Networks (VPDN). La seconde condition à remplir est le **protocole de communication** grâce auquel les données peuvent être transportées entre les systèmes mais aussi sur le réseau. Le PPP joue ici le rôle le plus important. PPP est un protocole dédié aux connexions WAN via lignes série. Il permet le transfert de protocoles LAN comme TCP/IP, IPX ou DECnet suivant le procédé asynchrone ou synchrone. Nous verrons plus en détail dans un autre chapitre le fonctionnement et la structure du PPP. Les protocoles plus anciens comme SLIP et CSLIP (Compressed Serial Line Internet Protocol) ne jouent plus un rôle important. Le protocole Low Bandwidth X Protocol (LBX) a été conçu pour les systèmes basés sur X-Window. La compression de données de ce protocole entraîne une accélération de la transmission si la bande passante disponible est minime, comme c'est le cas pour les connexions série.

On classe habituellement les applications d'accès à distance selon les trois catégories suivantes :

Remote Control, Remote Node et transfert de données. Bien entendu toutes ces applications peuvent tourner sous divers systèmes, mais comme dans la plupart des scénarios imaginés, le système d'accès fonctionne sous Windows, nous ne prenons en considération dans les paragraphes suivants que ce dernier système d'exploitation. Les explications valent en principe aussi bien pour tout autre système.

17.8.4.2.1 Contrôle à distance

Le contrôle à distance est une fonctionnalité consistant à piloter un ordinateur par un ordinateur extérieur via connexion WAN. Un ordinateur externe peut être un appareil isolé ou également une station de travail dans un réseau local. Suivant qu'il s'agit d'un système utilisateur unique ou multi-utilisateurs, la commande à distance est exclusive (comme par ex. pour Windows 9x) ou peut s'effectuer en parallèle (comme par ex, pour Unix). Lorsque les données transférées entre les deux ordinateurs se limitent à celles du clavier et de l'écran, il est tout à fait possible, avec un accès à distance, d'obtenir une vitesse de travail élevée, pour autant qu'on ne travaille pas avec une application nécessitant de fréquents rafraîchissements complets de l'écran. Le domaine d'application principal du "remote control" réside dans la maintenance d'un ordinateur isolé ou d'un réseau local (LAN), via la connexion WAN. Il devient ainsi possible de régler à distance les problèmes occasionnés par des logiciels, tout en évitant le déplacement onéreux d'un spécialiste.

17.8.4.2.2 Remote Node

Remote Node est une solution spécialement conçue pour l'intégration de PC distants. Comme dans le LAN, la communication se fait via protocole de support. Le PC distant dispose d'une propre adresse réseau. Cette adresse est soit définie lors de la connexion dans le réseau ou fixée préalablement. Dans une solution "Remote Node" toutes les applications tournent sur le calculateur. Pour éviter de charger les programmes d'application au travers des lignes quelquefois lentes, il est judicieux de maintenir une copie locale de ceux-ci.

Les protocoles LAN comme TCP/IP, IPX ou DECnet ne peuvent pas être directement transmis via une connexion série, un protocole spécial de communication ou de support est demandé. Le protocole le plus couramment utilisé est le protocole **"Point-to-Point" (PPP)**. La tâche du protocole PPP est de transporter les données avec le protocole LAN. PPP n'est pas un protocole LAN à proprement parler mais avant tout un protocole de support pour les protocoles LAN existants. Lors du transport, PPP prend en charge différentes tâches comme par exemple l'accord sur les paramètres de connexion, la compression, la définition de la taille des blocs, la surveillance de la qualité de la ligne, la validation du mot de passe via PAP (Password Authentication Protocol) et CHAP (Challenge Handshake Authentication Protocol). Plusieurs protocoles réseau comme TCP/IP, IPX ou AppleTalk peuvent être utilisés simultanément via PPP. Via une liaison PPP, il est aussi possible de faire exécuter simultanément plusieurs tâches, par ex. une fenêtre telnet pour un système Unix et une fenêtre de navigation Internet via TCP/IP.

17.9 Matériel informatique pour le WAN

17.9.1 Modems analogiques

Les modems sont utilisés pour la transmission analogique des données à travers les lignes téléphoniques. Les modems garderont leur importance dans la transmission de données aussi longtemps qu'un grand nombre des connexions installées dans le monde mais passeront par le réseau analogique du téléphonique.

L'appellation modem est une création provenant de **Modulation** et **Démodulation**. Les modems actuels offrent des fonctions supplémentaires, telles que le contrôle d'erreurs, la compression de données et la fonction fax et répondeur, pour autant que le PC dispose d'un logiciel adéquat. Un modem reçoit des données numériques en provenance de l'ordinateur et les convertit en signaux analogiques adaptés aux lignes téléphoniques. A l'autre extrémité de la ligne, un second modem sert à la « démodulation » des données et les restaure dans leur format numérique initial. Pour la connexion des modems, une distinction est faite entre ceux qui sont essentiellement connectés au PC, sous forme de carte enfichable, et les modems externes qui sont connectés à l'aide de l'interface série RS232. Les modems équipés de l'interface PCMCIA sont également très répandus, car presque tous les portables sont équipés de ce type d'interface.

Les modems actuels sont également capables d'envoyer et de recevoir des fax, et ont ainsi évincé les cartes fax du marché.

Le jeu d'instructions compatible Hayes s'est imposé comme moyen de configuration et de contrôle des modems. Il est aussi appelé jeu d'instructions AT, car toutes les commandes commencent par AT.

17.9.1.1 Modes de transmission

La plupart des modems disponibles aujourd'hui ont pour différences principales leur mode (asynchrone ou synchrone) et la vitesse de transmission.

En transmission asynchrone, les caractères sont transmis les uns après les autres. Chaque caractère transmis est encadré par un bit initial et un ou deux bits terminaux. En transmission synchrone, tous les bits de données sont envoyés les uns à la suite des autres. La synchronisation se fait suivant le top d'une horloge séparée.

Le taux de transfert d'un appareil est mesuré en bit par seconde. L'unité Baud donne la vitesse sur le trajet de transmission. Par les récents procédés de transmission, l'information n'est plus codée uniquement suivant la fréquence, mais aussi suivant l'amplitude et la phase, ce qui permet de transférer plusieurs bits par Baud. L'investissement plus important pour un modem rapide s'amortit déjà par les coûts d'exploitation minimisés.

La norme de transmission V.34+, qui permet un taux de transfert de 33.600 bits/s n'utilise pas la capacité maximale d'une ligne téléphonique, même si les experts avaient déjà prévu la limite à 28.000 bits. La vitesse de 56.000 bit/s est reprise sous la norme V.90, avec laquelle 56 kbit/s peuvent être transmis dans la direction du téléchargement. Pour cela il faut un serveur 56k. Ces taux de transmission élevés sont réalisables en éliminant la conversion analogique du signal entre le serveur 56k et le médiateur numérique. La connexion analogique persiste uniquement sur le côté utilisateur.

Les plus anciens protocoles spécifiques comme PEP, HST, V.32turbo ou V.Fast ont perdu de leur importance car le standard V.90 permet une vitesse de transmission supérieure à tous ces protocoles.

17.9.2 Adaptateurs RNIS

La communication entre différentes applications s'effectue en général sur la base de modems analogiques maîtrisant les jeux d'instructions AT. Si l'on désire néanmoins passer par RNIS, l'usage d'un adaptateur de terminaux RNIS avec interface série est conseillé. Comme il s'agit d'un périphérique externe muni d'une interface série (RS232), il peut être directement utilisé à la place d'un modem analogique. Le pilotage se fait à l'aide d'un large jeu d'instructions AT. Les adaptateurs de terminaux RNIS sont donc appropriés partout où des données doivent être transmises à travers RNIS par l'interface série. Ce seront, par exemple, les stations de travail ne disposant pas de contrôleur RNIS interne ou encore les ponts et routeurs à distance dotés d'une interface série. Combinés avec les

serveurs de communication série, les serveurs de terminaux RNIS sont également appropriés aux structures d'applications accès à distance via RNIS. N'importe quelle interface série n'est cependant pas conçue pour supporter les transferts à 64.000 bits/s (jusqu'à 256.000 bits/s ou plus pour des couplages de canaux/compression de données) du RNIS. Pour plus de détails, l'utilisateur doit se reporter aux spécifications techniques des interfaces. Dans tous les cas il est préférable d'avoir une interface avec tampon de données intégré (Interfaces compatibles avec UART 16550). Il faut ajouter que la plupart des adaptateurs de terminaux RNIS peuvent être contrôlés au choix avec le jeu d'instructions AT ou une interface CAPI. Vous trouverez plus de détails sur CAPI dans le paragraphe correspondant.

Les téléphones analogiques, les répondeurs automatiques, les télécopieurs du groupe 3 et les modems sont des périphériques analogiques ne pouvant pas être connectés directement sur RNIS. Il faut alors utiliser un adaptateur de terminal RNIS muni d'une interface a/b, qui convertit les données analogiques dans le format numérique RNIS. Des petites stations RNIS secondaires munies de 16 raccords de stations secondaires analogiques, correspondent en principe à un adaptateur pour 16 terminaux. La qualité et la vitesse de transmission sont affectées par la puissance inférieure de la liaison analogique.

Les contrôleurs RNIS constituent une solution économique et performante pour la transmission de données sur le réseau RNIS. Ils sont disponibles pour la plupart des bus et des plates-formes. Selon les cartes, les transmissions sont possibles aussi bien sur BRI que par PRI. La forme la plus courante est la carte PCI enfichable pour PC.

17.9.3 Routeurs

Contrairement aux ponts, les routeurs peuvent relier, sur la couche 3 du modèle ISO, des réseaux de topologies différentes. Ils constituent le pont central dans des réseaux LAN et WAN. Une utilisation optimale de la capacité ainsi qu'une excellente gestion du trafic sont possibles grâce à la capacité de ces routeurs à travailler sur différents types de réseaux et de protocoles. Un routeur n'est nécessaire que lors de communications entre stations de réseaux différents.

Ils doivent être capables de reconnaître tous les protocoles, puisqu'ils traduisent les trames d'informations en fonction du protocole requis. Ceci signifie que tous les protocoles doivent être routables, ou du moins pouvoir être transposés en un autre protocole qui réponde aux exigences de routage. Comme tous les protocoles ne sont pas routables, la plupart des routeurs sont en mesure de bridger des paquets.

Les ponts assurent une meilleure isolation du trafic de données que les commutateurs parce qu'ils ne transmettent par exemple pas automatiquement les broadcasts. Cependant le transfert de données est généralement ralenti. Dans une connexion ramifiée de réseaux, les routeurs peuvent amener une meilleure organisation du transfert sur des réseaux WAN. Les routeurs sont plus

onéreux que les ponts, il sera donc important de faire le bon choix. En cas de besoin, une analyse détaillée déterminera la solution pertinente.

Afin de trouver le meilleur trajet d'un émetteur à un récepteur, les adresses logiques sur un réseau peuvent être analysées par les routeurs moyennant des tables de routage internes. Les routeurs ont la capacité d'optimiser la longueur des messages selon le segment de réseau et modifient donc le message en passant d'Ethernet à X.25. Les routeurs ne modifient pas seulement la longueur des paquets ; ils opèrent aussi un ajustement des vitesses lors du passage d'un réseau local (LAN) à un réseau étendu (WAN). Il leur faut à cet effet un tampon de grandeur adéquate qui dans la plupart des modèles est librement configurable.

Les routeurs existent sous différentes formes. Par exemple **les routeurs locaux**, lesquels sont surtout utilisés pour des raisons de sécurité, lorsque dans un réseau local seule la communication entre certains nœuds est autorisée. Ils sont aussi employés pour réduire la quantité de données qui sature un réseau, c'est-à-dire quand des domaines de collision et donc le nombre et le domaine d'extension de broadcast doivent être minimisés. Il existe des routeurs locaux pour toutes les vitesses Ethernet.

Les routeurs RNIS sont souvent utilisés comme **routeurs d'accès à distance** en raison du grand nombre de connexions RNIS disponibles et de la structure avantageuse des coûts. Mais DSL est également utilisé en tant que routeur d'accès à distance avec des techniques de transmission allant jusqu'à 2 Mbit/s quand la quantité des données est en conséquence. Afin d'assurer une redondance et donc une haute disponibilité, des connexions RNIS servent de Backup pour les routeurs d'accès à distance à grande vitesse de transmission

Les routeurs décrits jusqu'ici sont tous basés sur une combinaison entre logiciel et matériel mais il existe aussi des solutions logicielles qui tournent sur des serveurs, des stations de travail ou des PC. Il faut peser le pour et le contre de chaque solution avant de se décider pour l'une ou l'autre.

Les composants essentiels et les caractéristiques techniques des routeurs sont présentés ci-après.

17.9.3.1 Interfaces LAN

La plupart des routeurs sont munis d'une ou plusieurs interfaces LAN, suivant la topologie pour Token Ring, Ethernet, 100BASE-T Fast Ethernet, FDDI ou ATM. La connexion aux différents moyens se fait soit à l'aide de ports (par exemple Ethernet AUI, BNC, RJ45), soit sous forme d'insertion et peut alors être adaptée.

17.9.3.2 Interfaces WAN

Des liaisons WAN de vitesses différentes sont proposées par plusieurs fabricants, ce qui entraîne des différences au niveau du prix et des interfaces.

Pour de petites intégrations, par exemple des groupes de travail, des liaisons avec une vitesse de transmission de 64 kbits/s sont conseillées. Il existe naturellement des applications pouvant se contenter d'un taux de transfert moindre. Pour des applications réclamant un taux de transfert plus élevé, on dispose en Europe de la liaison E1 avec 2048 Kbits/s ou des connexions DSL.

Les routeurs sont équipés d'un ou plusieurs ports WAN, qui peuvent soit être fixes, soit être équipés dans le modèle modulaire de modules d'interfaces. Les interfaces physiques courantes pour le fonctionnement en mode synchrone sont les RS449, V35 et X21, et RS232 pour le mode asynchrone. L'interface SO est utilisée pour la connexion au RNIS.

17.9.3.3 Support de protocole

Les routeurs routent un ou plusieurs protocoles de réseaux. Le protocole de réseau le plus souvent supporté par les routeurs est le protocole IP. Les réseaux hétérogènes gagnant en importance, les routeurs développent de plus en plus des capacités multiprotocoles. En plus d'IP et IPX, suivant le type, un routeur peut aussi supporter DECnet, AppleTalk, OSI, XNS, VINES et Apollo Domain. Tous les protocoles non routables (par exemple LAT et NetBIOS) « pontés », si le routeur supporte les fonctionnalités des ponts.

17.9.3.4 Logiciels

Les logiciels de routage sont en général inscrits dans les « Flash PROM », ce qui offre des avantages pour la mise à niveau. Lors du démarrage du routeur, le logiciel est chargé dans la mémoire RAM et mis en route. Les fabricants ont différentes stratégies quant à la conception des logiciels.

17.9.4 Firewalls

Les firewalls sont des ordinateurs qui travaillent comme passerelles de sécurité entre les réseaux et qui sont destinés à accroître la sécurité dans l'entreprise par divers mécanismes. Ils assurent le contrôle central des accès de l'entreprise à Internet en authentifiant les utilisateurs et en ne laissant passer que les services autorisés. Les critères selon lesquels les firewalls bloquent ou laissent passer des données sont définis dans des règles propres. Si une de ces règles n'est pas respectée, le flux de données est interrompu et, selon les configurations, une alarme peut être déclenchée en cas de manquement grave.

Un firewall est constitué en règle générale de plusieurs composants logiciels et matériels que l'administrateur adapte aux besoins de ses services et de sa sécurité. La concentration de l'accès sur un seul composant simplifie la gestion de la sécurité ainsi que les fonctions de surveillance et de contrôle.

17.9.4.1 Technologies du firewall

17.9.4.1.1 Filtre de paquets

Les filtres de paquets contrôlent au niveau IP si un paquet est recevable ou non. Pour cela les adresses de la source et du destinataire ainsi que les services sont contrôlés. Les exigences matérielles des filtres de paquets sont relativement modestes si bien qu'ils sont généralement implémentés avec les routeurs.

17.9.4.1.2 Stateful Inspection

Sous Stateful Inspection on trouve une technique d'inspection des paquets qui consiste à analyser les données des paquets en prenant en considération l'état de la connexion. Les paquets de données sont analysés sur la couche de transfert et stockés dans des tables d'état dynamiques. La suite de l'acheminement des paquets dépend de la comparaison entre plusieurs paquets de données et de la corrélation entre les paquets de données d'une transmission. Dans les applications décisives pour la sécurité les firewalls possédant la technique de la stateful inspection sont supérieures aux firewalls à filtre de paquets.

17.9.4.1.3 Passerelles de niveau circuit

Les passerelles de niveau circuit imputent les paquets aux connexions TCP existantes. Elles fonctionnent avec un sous-réseau, un routeur externe et un routeur interne et avec un hôte comme partenaire de connexion. Toute communication passe par cet hôte. Le concept des passerelles de niveau circuit est comparable à celui des filtres de paquets mais il tourne sur un niveau plus élevé de la pile des protocoles. Un ordinateur qui veut établir une liaison doit passer par l'hôte et prouver qu'il a une autorisation d'accès. En raison de la séparation entre réseau interne et réseau externe, les adresses IP internes ne peuvent pas être lues de l'extérieur.

17.9.4.1.4 Application Gateways

Les Application Gateways sont les formes de firewall les plus sûres mais aussi les plus coûteuses. Dans ces applications les mécanismes de sécurité sont répartis sur plusieurs couches. Ils peuvent déconnecter des circuits logiquement et physiquement et exigent de tout utilisateur une identification et une authentification préalables.

Dans les applications gateways les paquets de données sont interceptés aux ports. Si un seul service est autorisé sur le port, un logiciel est activé sur le serveur d'application (proxy serveur) qui transfère le paquet de données d'un côté du réseau à l'autre. L'utilisateur connecté a l'impression de communiquer avec le serveur du service de l'ordinateur destinataire. Mais en fait il communique avec le proxy server, son remplaçant, qui se présente dans les deux directions en tant qu'intermédiaire si bien qu'il n'y a jamais de connexion entre l'ordinateur destinataire et le visiteur.

18. LAN solutions de noyau

18.1 Introduction

Il devient de nos jours de plus en plus difficile de communiquer rapidement et d'avoir accès ensemble à des informations, des idées ou des ressources. C'est pourquoi les réseaux de données constituent la base décisive de la réussite commerciale.

La situation économique exige d'une entreprise moderne qu'elle devance la concurrence et qu'elle améliore sa productivité. Dans ce contexte, l'optimisation de la circulation des données à l'intérieur de l'entreprise toute entière est d'une importance primordiale. La mise en place de données réclamant de grandes largeurs de bandes et des applications multimédias complexes exige une utilisation efficace. Ce qui implique la nécessité d'une infrastructure de réseau stable.

En raison de ces nouveaux impératifs les réseaux sont conçus de telle façon à servir les activités actuelles de l'entreprise mais se préparent également à une croissance ultérieure. L'augmentation du nombre de réseaux commutés représente pour les entreprises, quelle que soit leur dimension, une évolution importante. La complexité des réseaux s'en trouve considérablement réduite. La technologie de routage autrefois prépondérante passe de plus en plus à l'arrière-plan. Les réseaux commutés fournissent, avec leur LAN-Traffic puissant, une base avantageuse pour la mise en place d'applications de la génération suivante, entre autres pour le streaming vidéo et les services optimisés du Web.

Les commutateurs de couche 3 actuellement disponibles remplissent toutes les fonctions d'un routeur traditionnel. Ils peuvent être installés à n'importe quel endroit du noyau ou du segment fédérateur d'un réseau et travaillent sur la couche réseau du modèle de référence OSI (Open Systems Interconnection). La transmission des données s'accroît de ce fait considérablement. La nouvelle génération des commutateurs a été spécialement conçue pour fonctionner dans les couches supérieures de l'OSI. Elle possède même des fonctions encore plus flexibles et s'accommode ainsi des modes de transfert de données les plus divers. Elle permet en outre une meilleure administration du réseau. Les derniers commutateurs sont encore plus intelligents et atteignent un débit supérieur. Dans le même temps, ils apportent à tous les types de réseaux des avantages appréciables, comme par exemple l'authentification de l'utilisateur et Quality of Service (QoS). Les commutateurs de couche 4, qui identifient et transmettent les données en circulation à l'aide des informations multicouches concernant les paquets permettent une gestion des données au niveau du réseau et non pas uniquement dans le noyau central.

L'avantage : des réponses plus rapides et une rationalisation de l'utilisation et de la disponibilité du serveur. Ils permettent l'identification et la transmission prioritaire de données critiques d'applications.

Au cours des dix dernières années les entreprises ont sans cesse implémenté de nouvelles possibilités de création et de gestion de réseaux. Cette évolution se poursuit avec pour objectif de répondre aux exigences vitales des entreprises. Les réseaux commutés sont importants pour assurer un accès

optimal aux données et aux services. Ils sont de plus les garants d'un haut niveau de sécurité, de mobilité, de disponibilité de données et de cette collaboration si importante dans l'économie actuelle. Ce chapitre a pour but de faire connaître les techniques actuellement disponibles.

18.2 Nouvelles stratégies pour réseaux

Une entreprise part aujourd'hui du principe que le réseau est adapté aux exigences des affaires courantes. Acquérir des clients, traiter les affaires et fournir des avantages dans la lutte contre la concurrence. Mais comment un réseau peut-il suffire aux impératifs de la croissance quotidienne du volume des affaires, surtout en ne dépassant pas les moyens financiers?

Beaucoup d'administrateurs de réseaux se voient aujourd'hui confrontés à ces exigences. Et ils doivent y répondre en respectant le budget imparti. Ceci n'est cependant possible que si le réseau envisagé peut être élargi sans que cela n'entraîne de coûts importants. Les futures extensions de réseau doivent être possibles sans grandes restructurations qui sont à coup sûr toujours beaucoup plus chères. Pour y parvenir le choix du noyau du réseau est déterminant.

18.2.1 Construction d'un noyau de réseau

Tout changement dans la structure d'une entreprise, qu'il s'agisse d'une fusion, d'une reprise ou simplement de croissance, exige beaucoup du segment fédérateur du réseau. Un besoin accru en circulation de données en raison de nouveaux sites ou de nouveaux utilisateurs devrait dans le meilleur des cas être couvert par le budget, sans cependant limiter une extension future. Un tel besoin se présente le plus souvent de façon absolument imprévue ; comme par exemple lorsque beaucoup de fournisseurs doivent coopérer à de grands projets, les flux de données augmentent. Ces brèves pointes de débit ne doivent pas nuire à la stratégie de développement du réseau sur le long terme. L'exploitant doit en outre être en mesure de mettre en place de nouvelles technologies pour un coût avantageux. Et malgré l'extension continue ou la création de LAN virtuels la sécurité des liaisons et le contrôle des coûts doivent demeurer prioritaires.

Quels sont les facteurs économiques décisifs dans le développement et le choix des technologies de noyau ? Il faut ici prendre en considération les exigences propres à chaque entreprise.

18.2.2 Contrôle des coûts

Les exigences sont les suivantes : progresser et prendre de l'extension en utilisant des ressources restreintes. C'est pourquoi des prix d'achat avantageux sont un facteur déterminant. Dans le contexte économique actuel il est tout aussi important de concevoir le réseau dans une perspective à long terme. Les coûts d'exploitation doivent jouer un rôle essentiel dans les calculs. S'il est possible d'économiser sur ce plan tout en assurant une sécurité contre les pannes, cela se répercute de façon sensible sur le rendement des investissements. Les entreprises disposent alors d'un meilleur contrôle de leurs dépenses.

18.2.3 Extension et flexibilité

La flexibilité des réseaux est une composante substantielle du capital d'exploitation. Si un accroissement de fonctionnalité s'avère nécessaire, il faut peser avec soin les demandes spécifiques et les besoins financiers. De ce fait l'avenir d'un réseau est immédiatement optimisé. Dans beaucoup d'entreprises les demandes en capacités supplémentaires sont dynamiques et imprévisibles. C'est la raison pour laquelle la flexibilité de la configuration du réseau est un facteur important. Par la création d'un réseau évolutif les entreprises assurent au mieux leurs investissements.

18.2.4 Sécurité

Même si les réseaux commutés sont avantageux, ils augmentent le risque de sécurité, justement à l'endroit exact où le réseau n'est pas protégé. La sécurité de bout en bout est devenue de nos jours un domaine critique de l'administration de réseau. Et ceci est d'autant plus vrai quand on intègre les effets secondaires du e-business, l'utilisation d'extranets et la circulation accrue de données dans les réseaux privés. Aujourd'hui plus que jamais les réseaux doivent protéger les utilisateurs, les systèmes et le capital intellectuel. Cela suppose avant tout une authentification et un contrôle renforcés.

18.2.5 Disponibilité

Le poste de travail est de nos jours tout à fait différent de ce qu'il était il y a seulement quelques années. Quand le réseau ralentit ou même tombe en panne, cela n'est plus simplement ennuyeux ; cela peut au contraire constituer un danger sérieux pour des opérations vitales de l'entreprise. La plupart des entreprises emploient aujourd'hui très peu de personnel informatique formé à l'administration des systèmes. Un panne de réseau a de ce fait des conséquences catastrophiques. Une infrastructure de réseau résiliente est indispensable pour assurer une communication sans problème et un fonctionnement ininterrompu. Le réseau doit cependant également être en mesure de se régénérer lui-même, il doit être performant et supporter un grand nombre d'applications et une quantité considérable de données. Un haut degré de disponibilité et de tolérance aux erreurs dépend de la configuration et des fonctions des appareils répartis sur l'ensemble du réseau. Des commutateurs montés dans des boîtiers et des configurations empilables sont utiles pour garantir l'accès aux applications critiques du réseau.

18.3 Solutions actuelles

Dans les très grandes entreprises la capacité du réseau est en règle générale prévisible ou statique. Le noyau n'est alors concerné que par de petites modifications ou des changements prévus. Généralement ceux-ci requièrent la souplesse, la disponibilité et la performance d'un segment fédérateur de noyau centralisé. De grands réseaux exigent des fonctions de commutation multicouche afin de supporter des applications complexes et de prioriser la circulation de données en

temps réel comme, voix et la vidéo. Les commutateurs centraux de noyau hauts-de-gamme offrent à l'entreprise la fonctionnalité d'exécution, la densité de ports et la capacité de stockage requises. C'est certainement aussi la meilleure solution pour les réseaux qui requièrent un support pour les protocoles de routage (par ex. IPX et Appletalk).

Dans une entreprise de grandeur moyenne à croissance rapide dont les besoins en capacité ne sont pas prévisibles, il est possible qu'un segment fédérateur de réseau traditionnel, aujourd'hui insuffisamment utilisé, soit demain déjà surchargé.

Considérons l'exemple suivant. L'installation montée dans des boîtiers comprend une infrastructure de routeurs avec plusieurs emplacements de connexion pour des modules interfaces. Quand le nombre d'utilisateurs augmente, il vous suffit d'ajouter au boîtier des modules supplémentaires. Vous devez prévoir exactement l'augmentation de capacité du réseau afin de choisir le boîtier adéquat. Etant donné que toute la capacité n'est pas utilisée, le prix de revient augmente. Si toutefois après une nouvelle extension le réseau dépasse les capacités du commutateur, il vous faut un deuxième commutateur de configuration analogue.

Si par contre dans une entreprise l'augmentation de capacité est exactement prévisible et qu'un appareil réseau comportant le nombre exact de ports répondant à la demande est disponible, alors le boîtier est la bonne solution. Il est important que le type de réseau choisi soit adapté de façon optimale à la demande. La plupart des entreprises devraient se fixer comme objectif une stratégie de disponibilité de bout en bout qui s'applique à tout le réseau. Pour les entreprises en expansion il est important d'avoir une architecture de réseau dynamique afin d'arriver à un équilibre réaliste entre le support des affaires du moment et la croissance future. Ce qui suit explique comment y arriver.

18.4 Réseaux avec noyau distribué

De nouvelles générations d'appareils arrivent sur le marché, en même temps qu'une demande d'évolutivité et de diversité. Des fonctions importantes, qui autrefois n'étaient possibles qu'avec le commutateur du noyau, se déplacent maintenant vers les extrémités du réseau. Des commutateurs flexibles, des points d'accès sans fil et autres appareils intelligents situés à l'extrémité du réseau assurent désormais la priorisation de la voix ou de la vidéo et la performance de bout en bout. L'information se propage ainsi de plus en plus sur tout le réseau et permet à chaque utilisateur d'accéder partout immédiatement aux données souhaitées. Les entreprises peuvent de cette façon administrer plus facilement leurs filiales. En même temps elles supportent ainsi des programmes destinés aux télétravailleurs et proposent un accès à distance sécurisé.

Dans cette nouvelle approche il s'agit de réseaux à noyau distribué. Un réseau distribué ne repose plus sur un point de contrôle central. Il repose sur le principe de l'agrégation et non plus sur celui de la hiérarchie. Les administrateurs peuvent ainsi ajouter des appareils quand une argumentation des performances ou des ports supplémentaires sont nécessaires. Ils exécutent dès lors une extension étapes! Dans un réseau extrêmement distribué toutes les commutations et tout le routage sont administrés par différents appareils.

Si on retire l'intelligence, la fonctionnalité et la performance du noyau d'une unique plate-forme de noyau centrale Highend pour la répartir sur plusieurs commutateurs on peut garantir que le noyau ne présente pas de Single Point of Failure. Une configuration flexible du noyau se passe de fonctions redondantes onéreuses et complexes. De plus le danger d'une panne totale du réseau s'en trouve considérablement diminué.

La technologie XRN (eXpandable Resilient Networking) de 3Com est une nouvelle approche basée sur ce concept d'une Distributed Fabric. Les caractéristiques de performance et la fonctionnalité des commutateurs compatibles XRN offrent aux administrateurs de réseaux une flexibilité idéale pour la conception de segments fédérateurs performants à haute disponibilité qui présentent des liaisons redondantes, des protocoles et des routeurs. La souplesse de la technologie XRN signifie : Extension uniquement en cas de besoin ! Cela réduit le prix d'achat et vous garantit vos investissements de réseau.

Plusieurs commutateurs Gigabit reliés entre eux se comportent dans la technologie XRN comme une Distributed Fabric avec administration centrale. Cette dernière grandit avec le réseau et ne connaît pas les limites techniques d'un noyau central. Les fonctions du noyau telles que QoS et authentification sont réparties dans la Distributed Fabric et assurent ainsi une performance de haut niveau. Dans la Fabric chaque commutateur constitue une unité rapide de commutation de couches 3 et 4. La performance augmente parallèlement à l'agrandissement du réseau étant donné que chaque commutateur de la Fabric contribue au transfert matériel des données. Les processeurs ne sont pas obligés de se charger de toute la procédure de routage. Il en découle un degré de performance et de résilience encore jamais atteint.

Etant donné que la technologie XRN supporte l'agrégation de liens dans toute la Distributed Fabric (Distributed Link Aggregation), les performances et la disponibilité augmentent. La technologie de routage résilient distribué permet de plus un acheminement performant entre les commutateurs reliés les uns aux autres. Cela garantit une redondance de routeurs pour le segment fédérateur du noyau. Les commutateurs reliés entre eux forment une unité, ce qui simplifie considérablement la gestion de tout le réseau. De précieuses ressources informatiques se trouvent ainsi libérées et au total la charge administrative diminue.

18.4.1 Composants XRN

18.4.1.1 Distributed Link Aggregation (DLA)

DLA offre la possibilité d'implémenter sur des ports des agrégations de liens qui actuellement dans la Distributed Fabric XRN se répartissent sur deux unités. DLA permet de configurer des commutations d'étages avec des chemins vers les deux commutateurs du noyau.

DLA supporte IEEE 802.3ad.Link Aggregation. Les appareils qui supportent cette norme sont directement reliés à la Distributed Fabric XRN et profitent immédiatement de l'amélioration de la performance et de la résilience.

18.4.1.2 Distributed Resilient Routing (DRR), Routage résilient distribué

DRR est une implémentation de routage éprouvée. Deux commutateurs reliés entre eux dans une Distributed Fabric XRN se comportent alors comme une seule unité active de routage. DRR répartit intelligemment la charge de routage sur les deux commutateurs de la Distributed Fabric avec une utilisation maximale de la performance de routage et une optimisation de la capacité de la largeur de bande. De toutes nouvelles possibilités d'architecture de réseau pour des administrateurs de réseaux ayant des exigences en terme d'évolution dynamique. Si une unité devait tomber en panne, l'autre commutateur se charge automatiquement de ses fonctions. Les interruptions dans le fonctionnement du réseau et la reconfiguration de la station finale qui en résultaient sont supprimées. Etant donné que chaque commutateur de la Fabric peut prendre lui-même les décisions de transfert de couche 3 pour les appareils qui lui sont reliés, cela apporte des avantages considérables en terme de performance.

18.4.1.3 Distributed Device Management (DDM), Administration distribuée des périphériques

DDM est le système de commande de la technologie XRN. Il est responsable de la répartition des informations concernant la gestion et la commande de la Distributed Fabric XRN. Indépendamment des appareils reliés, DDM rend possible, à l'aide de SNMP, TELNET ou de l'administration du Web, l'administration de toute la Distributed Fabric XRN en tant qu'unité logique avec une seule adresse IP. Toutes les tâches administratives, comme par exemple les mises à jour de logiciels, la configuration du VLAN, les modifications des paramètres dans le spanning tree, le filtrage multicast et la configuration QoS, sont effectuées pour toute la Distributed Fabric. Cela réduit la complexité et contribue à diminuer les coûts administratifs. De plus les deux unités utilisent en commun l'adresse d'administration IP. La gestion et le contrôle continus des appareils sont ainsi assurés, même si l'un des commutateurs devait tomber en panne.

18.5 Création d'une Distributed Fabric dans un réseau

L'implémentation d'un réseau avec Distributed Fabric ouvre aux administrateurs de réseaux qui ont des exigences en terme d'évolution dynamique de nouvelles possibilités d'architecture de réseau.

18.5.1 Réseau de base

Les réseaux de base ne demandent le plus souvent qu'un minimum en gestion de réseau et en ressources administratives. Dans le même temps ils proposent une solution de réseau performante, très extensible et redondante qui permette un élargissement des activités. Les utilisateurs spécialisés et les applications vitales demandent des liaisons redondantes avec le commutateur du noyau et les

serveurs critiques pour l'entreprise. Des coûts de faible importance constituent un autre facteur décisif.

Un exemple typique d'une architecture de ce genre serait une infrastructure de couche 2 et une architecture de réseau sur deux niveaux - couche 2. Couche 2 (c'est-à-dire commutateur de groupe de travail avec commutateur de noyau), souple et extensible en un réseau complet de routage IP sans la complexité habituelle.

Dans les réseaux de base l'implémentation d'une Distributed Fabric offre une meilleure garantie de disponibilité du réseau. Lors d'une nouvelle extension de l'entreprise et de l'augmentation du nombre des utilisateurs ou d'une nécessaire répartition des utilisateurs dans différentes divisions, le logiciel de commutation de couche 3 est facilement activé sur les commutateurs du noyau, ce qui garantit des interruptions minimales de fonctionnement. Les composants qui viennent s'ajouter au réseau en raison de l'agrandissement de la surface des bureaux, que ce soit temporaire ou durable, peuvent être gérés à moindres frais. De plus il est possible d'authentifier les utilisateurs avant qu'ils n'aient accès aux ressources du réseau.

Avantages :

- Fournit à un prix avantageux le niveau de performance adéquat pour les applications
- Supporte en cas de besoin la téléphonie du réseau
- Besoin limité en ressources pour la gestion et l'entretien du réseau
- Grande disponibilité du réseau, de la périphérie au noyau
- Forte résilience grâce à l'utilisation de groupes de travail appropriés et de commutateurs de noyau
- La fonctionnalité Dual Home Trunking veille à une mise en réseau complète.

18.5.2 Réseau normalisé

Les réseaux normalisés sont habituellement basés sur le protocole IP. Souvent ils doivent passer sur Gigabit Ethernet en préservant les investissements faits dans le noyau ou sur les points d'agrégation. Plus l'utilisation d'Internet est conséquente, plus la redondance/résilience standard et une gestion intuitive du réseau jouent un rôle important. Les réseaux normalisés s'étendent souvent sur plusieurs bâtiments proches les uns des autres de même que sur des sites à distance. Une topologie de réseau courante est une architecture à trois niveaux, couche 2 - couche 3 - couche 2, composés d'une agrégation de groupes de travail, d'une connectivité de noyau et d'une agrégation de serveurs. Une solution Gigabit Ethernet de couche 3 à trois niveaux se compose d'une agrégation de groupes de travail, d'une connectivité de noyau et d'une agrégation de serveurs.

Avantages :

- Performance avantageuse câblée de la périphérie au noyau avec blocking 2:1.
- Supporte en cas de besoin la téléphonie du réseau.
- Besoin limité en ressources pour l'administration et le maintien du réseau.
- Grande disponibilité du réseau, de la périphérie au noyau.
- Forte résilience grâce à l'utilisation de groupes de travail appropriés et de commutateurs de noyau.

- Sur le réseau les applications peuvent facilement être priorisées et bloquées. La fonctionnalité Dual Home Trunking veille à une mise en réseau complète.

18.5.3 L'extension du réseau

Les réseaux élargis requièrent une fonctionnalité de réseau de haut niveau pour tout ce qui touche à la commutation de couche 3. Ces réseaux d'entreprise peuvent être utilisés pour toutes les applications relatives au fonctionnement de l'entreprise (voix, données et vidéo) par l'intermédiaire d'une infrastructure commune. Le support de plusieurs protocoles (de même qu'un support multicast) et un grand nombre de VLAN sont souvent nécessaires.

Pour les réseaux élargis, la disponibilité, la résilience et la redondance sont d'une importance extrême. Car une panne, si petite soit-elle, peut entraîner une perte considérable de chiffre d'affaire. La performance est également un point important. Elle comprend aussi l'aptitude à supporter des applications complexes, comme le streaming vidéo, CRM, ERP et la communication unifiée. Les possibilités qui s'ouvrent grâce à l'installation sur plusieurs sites de réseaux élargis et l'intégration d'un grand nombre d'utilisateurs à distance renforcent le besoin d'avoir un service VPN sécurisé et résilient. Le support de routage multiprotocole et la possibilité de commander la circulation des données grâce à la priorisation, à la classification et aux listes d'accès sont des facteurs importants. Pour des réseaux élargis la solution adéquate est un réseau Gigabit Ethernet de couche 3 sur quatre niveaux qui se compose d'une agrégation de groupes de travail, de connectivité de noyau et d'une agrégation de serveurs. Ce réseau assure la reprise de protocoles Legacy et le passage sans difficulté à une infrastructure IP.

Avantages :

- Une redondance totale de la périphérie, du groupe de travail, du noyau et sur le serveur exclut un Single Point of Failure
- Stacking Resilience
- Liaison au niveau de la mémoire à liste inversée (double liaison avec les groupes de travail)
- DLA (Distributed Link Aggregation) assure la résilience de XRN
- Des Switching Fabrics redondantes assurent une redondance complète et permettent une commutation rapide
- Disponibilité client grâce au support VRRP dans le noyau
- La double liaison des serveurs avec les commutateurs de l'agrégation de serveurs assure une disponibilité intégrale de la ferme de serveurs
- La performance de bout en bout procède à la priorisation des applications du commutateur du desktop.
- La téléphonie de réseau est immédiatement exécutable
- Utilisation efficace de la largeur de bande du WAN, les commutateurs du desktop et des groupes de travail détournant automatiquement la circulation des données du Web vers un cache Web, ce qui fait baisser les dépenses totales du WAN.

18.6 Une nouvelle orientation pour les réseaux d'entreprise

Le développement de réseaux commutés bat son plein parce que la demande en bande passante augmente fortement. Il faut de ce fait répondre au besoin d'élargissement des fonctions de réseau. Les liaisons de réseaux continuent à être câblées ou sans fil. La flexibilité et la mobilité doivent être assurées sans que la sécurité ou la convivialité en soient affectées. L'utilisateur peut alors accéder au réseau à partir de sites à distance.

La fonction de roaming sans fil est également à disposition sur le site de l'entreprise. Un accès sécurisé et rapide à toutes les applications et tous les services est aisément possible.

Afin de faire baisser les coûts d'exploitation 3Com favorise une nouvelle orientation des réseaux d'entreprise. Autrefois l'intelligence du réseau était uniquement intégrée aux appareils du noyau. Aujourd'hui chaque commutateur, chaque access point sans fil et autres équipements nouvelle génération peuvent s'y connecter. De cette façon les fonctions telles que priorisation du trafic, authentification et cryptage peuvent se rapprocher de leurs utilisateurs.

De cette intelligence répartie sur les composants du réseau résulte une structure des coûts qui répond au principe "Pay as You Grow". Elle est le symbole d'un meilleur contrôle des coûts, d'une meilleure gestion et de la mise en place ciblée de nouveaux services et de nouvelles fonctions. L'amélioration de l'interpolarité entre les différents appareils du réseau permet d'utiliser plus efficacement les investissements déjà réalisés et d'y ajouter quand cela est nécessaire les éléments pour la voix, des données et de la radio. Diverses applications, dont Voice over IP (VoIP), la messagerie unifiée et une série d'outils spécifiques aux entreprises peuvent bénéficier à bon marché de la performance du design des réseaux distribués.

18.7 Résumé

Un réseau doit constituer une base solide pour les applications et les services très variés qui apportent des avantages stratégiques et contribuent au succès de l'entreprise. Les réseaux nouvellement commutés doivent leur développement à de véritables défis en ce qui concerne l'extension, le QoS élargi et la sécurité, une gestion simple et des frais d'exploitation modérés.

Grâce à la répartition de l'intelligence du réseau sur des commutateurs à des points d'accès sans fil et autres appareils intelligents sur la périphérie du réseau, vous avez la possibilité de construire des réseaux souples, faciles à gérer, qui permettent une croissance à peu de frais et sans entraver la performance et la disponibilité.

Depuis plus de deux décennies 3Com Corporation développe des réseaux innovants et propose sans cesse des solutions innovatrices. De cette façon vous répondrez à la demande croissante de nouveaux services et de fonctions intensifiant la productivité tout en obtenant un meilleur contrôle des coûts et en réduisant la complexité de la gestion.

19. Périphériques de saisie

19.1 Claviers

Dans un environnement normal, un clavier se doit de répondre à différents critères : longue durée de vie, robustesse, ergonomie et simplicité d'utilisation.

La durée de vie d'un clavier est liée à la robustesse mécanique de ses touches. En règle générale, les claviers possèdent des contacts métalliques en or, ce qui garantit une longue durée de vie pour un usage intensif. À l'opposé, les claviers simples utilisent un film de contact très fin, qui est très sensible et finalement moins durable.

Les claviers ergonomiques, le Microsoft Natural Keyboard par exemple, assurent une position saine des mains et des articulations et réduisent les dangers de fatigue et de blessure (syndrome du tunnel métacarpien ou tendinite, par exemple). Ils contribuent à créer des conditions de travail saines et efficaces. Dans ce contexte, il convient de ne pas oublier que le siège, la surface de travail et le clavier doivent toujours se trouver dans une bonne disposition, les uns par rapports aux autres. Les claviers ayant des fonctions supplémentaires intégrées ont tous l'avantage qu'une seule interface est occupée sur l'ordinateur, bien que plusieurs fonctions soient disponibles sur le clavier. Il existe des claviers lisant les cartes chip, les codes-barres, en les cartes magnétiques. Les claviers librement programmables pour la lecture de cartes de crédit, de cartes Eurochèque et de codes-barres constituent une variante supplémentaire. Pour le contrôle d'accès, des claviers lisant les cartes chip avec un lecteur d'empreintes digitales intégré peuvent être installés.

19.2 Souris et trackballs

Généralement, une **souris** est constituée d'une boule sphérique et d'un capteur mécanique/électronique, qui saisit les mouvements de la boule, les transforme en un flux de données et les transmet à l'ordinateur. Les modèles les plus récents travaillent sans boule. Les mouvements de la souris ne sont plus saisis par un élément mobile, mais par un capteur optique. Le cœur de cette technologie est une petite puce, contenant un capteur optique et un processeur numérique de signaux (DSP Digital Signal Processor). Le capteur traite, à partir de la surface de travail, plusieurs centaines d'images par seconde et le processeur numérique de signaux en déduit les mouvements. Comme les parties mobiles retenant la poussière, la saleté et la graisse ne sont plus indispensables, il n'est pas nécessaire de nettoyer les souris optiques. De plus, ces souris se déplacent sur presque n'importe quelle surface de travail, ce qui rend un tapis de souris inutile.

Ces souris disposent en plus, sur leur partie supérieure, d'un certain nombre de boutons dont les fonctions sont définies soit par l'application mise en oeuvre, soit par l'utilisateur lui-même.

Les générations actuelles de souris (Genius, Logitech ou Microsoft) sont également munies d'une molette ou d'une touche à bascule, qui permettent dans certaines applications de faire un zoom ou de faire défiler l'écran sans bouger la souris. Le contrôle des fenêtres en est plus confortable et

la navigation sur Internet (via Microsoft Explorer ou Netscape Navigator, par exemple) plus rapide que jusqu'à présent.

Les souris sans câble offrent une liberté de mouvement illimitée sur la surface de travail. Pour ces souris, la technologie sans fil a depuis remplacé la technique à infrarouge. L'avantage de cette solution est qu'aucun contact visuel direct avec le récepteur n'est nécessaire, la souris sans fil peut travailler dans un rayon d'environ 2 m.

L'utilisation d'un **trackball** est judicieuse lorsque la place sur le bureau est réduite : les commandes se transmettent en faisant tourner la boule par le dessus et en utilisant les différentes touches. On peut comparer un trackball à une souris « renversée » elle remplit les mêmes fonctions que cette dernière, mais nécessite moins de place.

Ces périphériques désormais standard, tels que souris et trackball, ne sont pas particulièrement adaptés aux applications 3D, car elles ne permettent de contrôler simultanément que deux dimensions. De nombreuses applications en 3 dimensions (par ex. programmes de réalité virtuelle et autres logiciels de modélisation) exigent pourtant la maîtrise complète des 6 degrés de liberté de l'espace tridimensionnel. Des souris 3D spéciales ont été développées pour répondre aux exigences spécifiques de ces applications. Elles associent les fonctions d'une souris classique à celle de dispositifs de pilotage d'objets graphiques 3D.

19.3 Scanners

Les scanners sont devenus un moyen important d'acquisition de données. Ces données initialement disponibles sous la seule forme papier, peuvent être des textes imprimés, des manuscrits, des photos ou des dessins. Le principe de fonctionnement d'un scanner est le suivant : une cellule CCE (Charge Coupled Device) sensible à la lumière est déplacée pas à pas par un moteur sur la surface du document éclairée par une lampe. Sur chacun des points de la surface qu'il examine, l'élément CCD reconnaît les différentes intensités de couleur et traduit ses différences en signaux électriques. Un convertisseur analogue/numérique se charge alors de transformer le signal analogique en une information numérique pouvant être transmise à l'ordinateur.

En fonction de la méthode appliquée, la tête de lecture CCD peut être passée sur l'original une seule et unique fois (one pass) ou bien en trois fois (une passe pour chacune des couleurs de base : rouge, jaune, bleu). Dans le groupe des scanners "one-pass", on peut encore différencier deux grandes méthodes. Dans la première, un rayon lumineux blanc est dirigé sur une cellule CCD, qui le filtre immédiatement en distinguant les couleurs rouge, jaune et bleu. Dans la seconde, le rayon lumineux traverse un prisme, qui le disperse en trois couleurs (R, J, B), elles-mêmes dirigées séparément sur les trois cellules CCD distinctes. La première méthode s'est imposée pour le scanner.

La technologie CCD dont le développement a été poursuivi exclusivement par HP permet une haute résolution associée à une vitesse élevée. Elle est composée de deux capteurs (CDD) en

un : capteur CCD linéaire de 600 dpi pour les scans de haute qualité à grande vitesse et un capteur CCD 2400 dpi pour les scans à résolution plus élevée. En général, une résolution supérieure à 600 dpi n'est pas nécessaire, et dans ce cas le CCD 600 dpi est utilisé. Pour les transparents, les négatifs et les agrandissements, une résolution de 2400 dpi s'avère toutefois indispensable. Dans ce cas, il est fait appel au capteur CCD 2400 dpi pour assurer entre autres un fort agrandissement sans perte de qualité.

Lors du choix d'un scanner, il convient de prendre un certain nombre de critères en considération. La **résolution** d'un scanner s'exprime en dpi (dots per inch), et la règle d'or est la suivante : plus la résolution est élevée, meilleur est le rendu du document lorsqu'il est à nouveau imprimé. La valeur dpi correspond en fait au nombre de pixels par pouce (un pouce = 2,54 cm) pouvant être distingués par la cellule CCD du scanner. Une résolution de 100 dpi signifie donc que chaque pouce de document est décomposé en 100 pixels. Puisque l'on travaille sur une surface, cela signifie que chaque pouce carré du document fournit $100 \times 100 = 10.000$ pixels. Une résolution de 200 dpi permet de décomposer un pouce carré de document en 40.000 pixels.

Cependant, le doublement de la résolution se traduit par un volume de données quatre fois plus grand. La résolution à laquelle il est fait référence dans les paragraphes précédent est en fait la résolution purement physique du scanner. Elle détermine le balayage effectif des points de l'image. En parallèle à cela, une résolution est calculée mathématiquement, c'est ce qu'on appelle la résolution interpolée d'un scanner. En effet, à l'aide d'un logiciel, il existe la possibilité de calculer, par **interpolation**, d'autres valeurs intermédiaires entre deux points connus. L'ordinateur dispose ainsi d'informations supplémentaires sur les points d'image, qui conduiront à une meilleure impression du document scanné.

Un autre facteur décisif en matière de scanner constitue la **profondeur de couleur ou de bit**. Cette caractéristique indique le nombre de couleurs ou de niveaux de gris pouvant être reconnus par le scanner. Un scanner avec une profondeur d'1 bit ne peut faire la distinction qu'entre le noir et le blanc. Avec une profondeur de couleur de 8 bits, il différencie jusqu'à 256 niveaux de gris et de couleur (2 à la puissance 8). Une profondeur de 24 bits augmente le nombre de couleurs possibles pour atteindre 16,7 millions de niveaux de couleurs. Une profondeur de couleur de 48 bits est le standard actuel.

Pour les scanners, l'interface logicielle standard **Twain** s'est imposée. Derrière le nom de Twain (Toolkit **w**ithout **a**n **i**mportant **n**ame) se cache en fait un standard d'interface logicielle, émanant de constructeurs leader de périphériques. Ce standard permet, à partir d'une seule application, d'utiliser les scanners de différents fabricants. Lorsqu'un scanner possède un pilote Twain, tous les programmes supportant Twain peuvent accéder au scanner. Twain est constitué d'une interface **API** (Application Programming Interface, servant à la programmation de programmes d'application) et d'un protocole spécifique dont le rôle est d'établir la liaison avec le scanner et de piloter le déroulement des opérations.

Avec Twain apparaît également la nécessité de disposer d'un logiciel puissant pour pouvoir scanner. En effet, un scanner livre à l'ordinateur ce qu'il voit uniquement sous forme de données numériques. Ce que l'ordinateur fait de ces données et la manière dont elles sont traitées est du ressort du logiciel fourni avec le scanner. Le problème particulier est celui de la **reconnaissance des caractères ou la reconnaissance de texte**. Les textes scannés doivent d'abord être traités par un programme spécial de reconnaissance de texte ou un programme OCR (Optical Character Recognition) pour pouvoir être ensuite reconstitués un fichier texte.

Un progiciel standard est généralement inclus dans la livraison du scanner. Il faut cependant noter que les différents logiciels "scan" se distinguent en partie par les performances proposées. Souvent, seule une version limitée gratuitement du logiciel est fournie.

Bien entendu, le logiciel joue aussi un rôle prépondérant dans la convivialité de l'appareil. HP offre avec le logiciel HP ScanSoftware et les touches de service "Copier, Email, Faxer ou Archiver" une solution simple pour la lecture et le traitement de longs textes dans le PC. En outre, des présentations et des courriers sont plus élégants lorsqu'ils sont accompagnés d'images scannées - sans pour autant impliquer un travail fastidieux ou une manipulation complexe du logiciel ou de l'appareil.

L'option **transparence** est importante pour pouvoir scanner les supports transparents (par ex. films, diapos, ...). Les constructeurs font généralement appel à un support transparent doté d'une lampe fluorescente qu'il suffit de poser sur le lit du scanner.

19.4 Lecteurs de codes-barres

Les codes-barres sont utilisés partout dans l'industrie. Leur lecture permet de transmettre de manière rapide et fiable des informations vers un ordinateur où elles peuvent être traitées.

Il existe une multitude de codes pour des applications différentes. Un code-barres est constitué d'une succession de tirets et d'espaces plus ou moins larges. Lorsque le faisceau laser d'un lecteur balaie ces codes-barres, une cellule optique capte les différentes réflexions des barres foncées et des espaces claires et convertit le tout en impulsions électroniques. Ces impulsions sont à leur tour numérisées par un microprocesseur puis transmises.

Les plus répandus sont les lecteurs de codes-barres se branchant sur le câble du clavier d'un ordinateur (entre le clavier et l'unité centrale ou le terminal). L'avantage de cette configuration est qu'elle ne nécessite ni une interface spéciale, ni une alimentation électrique supplémentaire. Les données fournies par le lecteur de codes-barres étant parfaitement identiques à celles fournies par le clavier, toute modification logicielle ou matérielle est inutile. L'unité centrale ne fait pas la différence entre les données provenant du lecteur de codes-barres et celles provenant du clavier. La commutation de la saisie des données à partir du décodeur ou du clavier se fait automatiquement.

Les appareils hertziens sont constituent une alternative intéressante, car ils suppriment la manipulation fastidieuse de marchandises volumineuses (par exemple : palettes d'écrans). Ils sont constituer d'un scanner et d'une station de base. La station de base est positionnée entre le clavier et l'ordinateur et le pistolet permet une lecture et transmission des codes barres jusqu'à 30 m de le base.

Les lecteurs codes-barres se différencient par leur aptitude à lire différents types de codes, par leur fonction de reconnaissance de code (automatique/réglable), la distance de lecture et le type de lecture. Il existe les lecteurs manuels (crayons), les lecteurs à cellule CCD et les pistolets laser. Les crayons se prêtent idéalement à la lecture de quantités de données minimes. Une diode LED rouge est utilisée comme source lumineuse. Pour reconnaître correctement le code, le crayon doit être en contact direct avec le code à relever.

Les lecteurs codes-barres équipés d'une cellule CCD effectuent des lectures à une distance minime. La distance de lecture est soit de quelques centimètres, soit un contact direct. Par contre, un lecteur laser codes-barres saura lire un code jusqu'à une distance de 70 cm sur une surface aussi bien variable que chiffonnée par exemple. Il est fait appel à une diode laser comme source lumineuse.

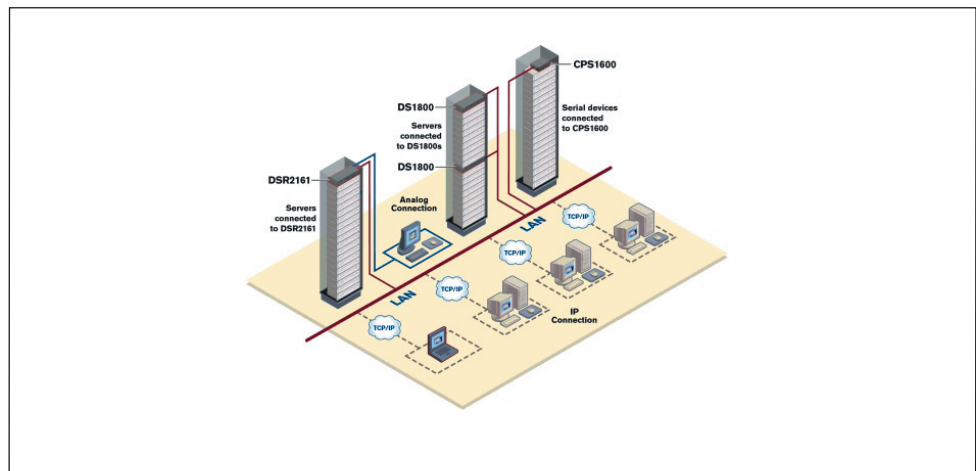
20. Communication des données

20.1 Commutation CVS (Clavier, Vidéo, souris)

Le fonctionnement de tout **commutateur CVS (Clavier, Vidéo, Souris)** est fondé sur un principe simple : plusieurs serveurs peuvent être commandés et contrôlés depuis un ou plusieurs postes de travail comme si on se trouvait directement devant chaque poste. Pour ce faire, uniquement les signaux de clavier, de souris et de vidéo sont directement repris de l'ordinateur et transmis à un poste de travail central. Depuis ce dernier, un administrateur système peut par exemple modifier les réglages de BIOS, procéder à des diagnostics de système ou redémarrer ses ordinateurs y compris si les protocoles de réseau ou les systèmes d'exploitation ne fonctionnent plus.

Cette technologie, qui était analogique à l'origine, a déjà contribué à supprimer de nombreux postes de travail avec écran qui n'étaient pas indispensables, à gagner de l'espace dans les centres informatiques et à réduire les coûts d'exploitation.

Ces systèmes montraient vite leurs limites au niveau du nombre de serveurs administrés et des possibilités réduites de rajout de postes. Les **commutateurs Matrix** sont ici d'assistance : grâce à leur conception modulaire, le nombre de serveurs successif et la quantité d'utilisateurs peuvent être augmentés. Un accès ne reste toutefois possible qu'avec un câblage analogique dans un rayon de quelques centaines de mètres autour du centre informatique. Le **Digital Datacenter-Management over IP** (administration numérique de centre de données par IP) représente le nec plus ultra de la technologie actuelle : les limitations de distance disparaissent lors de l'accès à distance des liaisons IP. Il est possible d'administrer autant de serveurs et d'appareils série qu'on le souhaite. Et le nombre d'utilisateurs n'est pas limité non plus.



21. Terminaux

Rares sont les postes de travail modernes qui peuvent aujourd'hui se concevoir sans PC ou sans station de travail. Les terminaux conventionnels reliés à un ordinateur central via une interface série, soit directement soit par un serveur de terminal, ne sont plus utilisés que dans les domaines sans représentation graphique, sans traitement intensif et pour lesquels, le prix de revient par poste de travail est important. C'est surtout dans le monde Unix que ces terminaux sont de plus en plus souvent mis en concurrence directe avec des stations de travail ou des PC plus puissants : ceux-ci sont capables de traiter localement les données, mais sont sensiblement plus onéreux et réclament une maintenance plus régulière que pour ces terminaux écrans. De par leur fonctionnalité et leur connexion, les terminaux X-Window se situent approximativement à mi-chemin entre les terminaux écrans et les stations de travail.

Les Network Computer (NC) ne se sont pas imposés, puisqu'il existe une alternative avec les terminaux basés sur Windows (Windows Based Terminals-WBT).

Dans un premier temps, on peut avoir l'impression que ces systèmes nous replongent quelques années en arrière : comme pour les terminaux X, les données sont centralisées et les applications sont représentées via une interface homogène. Lorsque l'on y regarde de plus près, les avantages de cette architecture décentralisée apparaissent finalement très clairement.

Vu l'importance des investissements initiaux et des coûts pour le suivi, la maintenance et les frais de fonctionnement (consommation d'énergie, etc.), la décision pour ou contre tel appareil, pour ou contre tel système est toujours extrêmement importante.

21.1 Les terminaux alpha

Les terminaux alpha conviennent aux postes de travail ne nécessitant aucune fonctionnalité graphique, et s'utilisent, par exemple, pour consulter uniquement des banques de données. Chaque terminal doit simplement supporter les protocoles qui lui permettent de communiquer avec l'ordinateur central. Chaque constructeur a, au fil des ans, développé ses propres protocoles et des terminaux compatibles avec les ordinateurs de son environnement propre. Les terminaux alpha sont disponibles en deux versions : les terminaux mono-session et les terminaux multi-sessions.

21.2 Les terminaux X-Window

Les terminaux X-Window ont été développés dans le but d'avoir une interface commune pour les différents environnements d'ordinateurs. La nécessité d'un tel système, qui permet indépendamment du constructeur comme du matériel, de distribuer des informations à travers un réseau, a été perçue et analysée dès le début des années 80 par le MIT (Massachusetts Institute of Technology) de Boston (U.S.A.). Fondé sur ces exigences, le système X-Window a été développé et la version X10 fut distribuée gratuitement en 1986. Un grand nombre de constructeurs saisirent cette opportunité et utilisent la version actuelle **X11R6** comme protocole graphique et comme protocole de terminal.

pour leurs propres produits. Entre temps, les solutions Thin Client prennent de plus en plus souvent la relève sur les terminaux classiques X-Window. Dans ce cas, les PC ou même les NetPC possédant le logiciel adéquat (Exceed de Hummingbird) sont étendus par les fonctions de terminal X-Window. Ces applications Xware peuvent être installées sous Windows 3.1/95/98/ME et Windows NT/2000/XP.

Le système X-Window s'utilise pour faire communiquer entre eux des systèmes et des applications fonctionnant sous des architectures et des systèmes d'exploitation différents. A partir de n'importe quel terminal X-Window ou Thin Client, muni du logiciel Xware, et grâce à l'interface graphique utilisateur, il est désormais possible d'ouvrir simultanément plusieurs applications sans devoir quitter les programmes déjà ouverts. L'utilisateur peut ainsi importer des informations d'une application vers une autre (avec les fonctions Copier/Collier), une fonctionnalité particulièrement appréciée sur les postes de travail où l'on saute souvent d'une application à l'autre. Grâce à X-Window, le réseau apparaît à l'utilisateur comme un seul et unique gros ordinateur.

Le **concept de terminal X-Window** repose sur le modèle client-serveur. Dans ce cas, le terminal X-Window est désigné comme **serveur**, tandis que le **client** est une application X, qui tourne par exemple sur le processeur d'un ordinateur hôte Unix. Le serveur, en tant que composant représentatif, est en charge de représenter et de traiter des entrées et sorties via l'écran, le clavier et la souris. Sur le composant fonctionnel, c'est-à-dire le client, c'est l'application proprement dite qui fonctionne. Client et serveur peuvent opérer sur des systèmes différents tant que ces systèmes sont reliés l'un à l'autre via un réseau. Pour se comprendre mutuellement, le serveur et le client doivent seulement utiliser le même protocole réseau (en règle générale TCP/IP).

Comparés à des stations de travail, les terminaux X-Window représentent une alternative avantageuse : l'administration du système s'opère de manière centralisée, ce qui en réduit considérablement le coût. Cependant, les problèmes de saturation du réseau, susceptibles de se produire avec un système de terminaux X-Window, peuvent généralement être évités par le choix d'un segment fédérateur (backbone) rapide. Les performances des terminaux X-Window sont régulièrement déterminées par des bancs d'essais comparatifs et indiquées dans les fameuses XStones. Les besoins en mémoire vive varient avec le nombre de fenêtres et d'applications graphiques ouvertes. Il est impossible de donner une indication définitive.

On assiste à des efforts visant à élargir les performances et les domaines d'application des terminaux X-Window. En raison de la grande diversité de logiciels à vocation commerciale ou technique fonctionnant sous les systèmes d'exploitation Microsoft, les informaticiens tentent d'intégrer aussi ces applications aux terminaux X. Configuré de cette manière, un terminal X est alors en mesure de faire traiter et de représenter à l'écran des **applications Windows** d'un serveur Windows tout en traitant des applications X tournant sur un serveur Unix. Il est également très facile, par la fonction copier & coller, d'échanger des informations entre les applications X et les applications Windows. Le marché offre actuellement plusieurs solutions logicielles qui varient beaucoup au niveau de

leurs performances et de leur système minimum requis. Grâce au logiciel Xware, déjà brièvement décrit ci-dessus, on est en présence de méthodes divergentes concernant l'extension des PC aux fonctions X-Windows.

21.3 PC et stations de travail

Lorsqu'un utilisateur désire accéder aux applications d'un ordinateur hôte, il peut aujourd'hui utiliser des **PC** équipés d'émulation de terminaux en lieu et place de terminaux écran. L'avantage de cette solution tient à ce que l'ordinateur central peut être complètement déchargé des tâches simples (les travaux de traitement de texte, par exemple) et que le PC peut également être mis à profit pour d'autres travaux. Le revers de la médaille se situe au niveau de l'augmentation des travaux d'administration du système : certaines données sont uniquement disponibles sur le PC et les mises à jour doivent être réalisées individuellement sur chaque machine. Parallèlement au nombre de PC connectés dans le réseau, la maintenance du système s'alourdit considérablement.

L'autre inconvénient des PC est le temps consacré par l'utilisateur à apprendre non seulement le fonctionnement de l'ordinateur central, mais en plus celui des différents PC. Cet inconvénient peut être évité par la mise en oeuvre de stations de travail disposant de la même architecture d'unité centrale ou du moins du même système d'exploitation que l'ordinateur hôte (exemple : SPARCservers et SPARCstations sous Solaris). Grâce à leurs capacités de traitements propres, de telles stations de travail sont en mesure de décharger le serveur. Contrairement aux terminaux X-Window, les stations de travail peuvent libérer de l'espace sur leur disque dur. Par rapport aux PC, elles présentent les avantages d'une utilisation uniforme et d'une administration plus simple.

21.4 Windows Based Terminals (WBT)

Un terminal WBT est un matériel Thin Client qui travaille avec le système d'exploitation Windows CE.NET et qui est raccordé à un Windows Terminal Server (pour Windows NT 4.0 et Windows 2000) ou à un MetaFrame Server. Pour communiquer avec le serveur, un WBT fait appel soit au protocole **Remote Desktop Protocol** (RDP, auparavant aussi appelé T.SHARE) développé par Microsoft, soit au protocole **Independent Computing Architecture** (ICA) de Citrix. Les deux protocoles sont généralement supportés.

La particularité des Windows Based Terminals est qu'ils s'accordent entièrement, comme leur nom l'indique, aux caractéristiques de la plate-forme Windows. Pour fonctionner, une version multi-utilisateurs de Windows 2000 ou Windows NT est absolument nécessaire, car ils ne peuvent pas coopérer avec d'autres systèmes. L'interaction, par exemple avec des applications Java ou avec un logiciel spécifique à l'entreprise, doit être réalisée à l'aide d'un explorateur.

Dans un WBT, toutes les applications sont exécutées sur le serveur et même la sauvegarde centrale des données s'effectue sur le serveur. Les données ne sont disponibles localement à aucun moment.

Les WBT offre de ce fait une sécurité, aussi bien contre la perte de données, que contre le vol des données.

La licence joue ici un rôle prépondérant. **Chaque Client** doit posséder en premier lieu une licence Server Client Access (CAL). Une licence Terminal Service CAL est en plus nécessaire sur le client. Les systèmes dotés de Windows 2000 Professional et Windows XP Professional reçoivent automatiquement cette licence et ne doivent donc plus l'acquérir en sus.

Afin de pouvoir également travailler avec des matériels ne fonctionnant pas sous Windows, Citrix propose **MetaFrame**. Ce successeur de WinFrame étend les possibilités de Windows Terminal Server, aussi bien du côté serveur que du côté client. En faisant appel au protocole ICA, il est notamment possible de travailler avec des ordinateurs basé sur Java, des MAC, des ordinateurs Unix ou des WBT ICA.

La technologie ICA comprend 3 composants essentiels :

Les **composants serveur** : ces composants logiciels installés sur le serveur travaillent en étroite collaboration avec le système d'exploitation multi-utilisateurs correspondant. Les systèmes d'exploitation suivants sont supportés : La gamme des Windows 2000 Server, Windows NT 4.0 Terminal Server Edition, HP-UX, IBM AIX, Sun Solaris. Le système d'exploitation installé sur le serveur se charge d'exécuter l'application, pendant que les composants serveur ICA se chargent de séparer la logique d'application de l'interface d'application. Les composants **protocole** : ces composants se chargent de transporter via le réseau la séparation d'application vers l'appareil final, de transmettre les saisies du clavier et de la souris vers le serveur et de retourner la réponse du serveur à l'appareil final. Dans la technologie ICA de Citrix, les applications n'occupent environ qu'un dixième de la largeur de bande du réseau, dont elles auraient normalement besoin dans une architecture client/serveur. Les **composants client** : ces composants ICA installés sur l'appareil final (ce qu'on appelle le client ICA), indiquent à l'utilisateur l'interface d'application et lui permet dès lors d'interagir avec l'application exécutée sur le serveur. Les clients ICA existent pour quasiment tout type d'appareil final. Ils autorisent un travail au-delà de la plate-forme avec des technologies autrement incompatibles entre elles.

Les clients ICA peuvent être téléchargés gratuitement : <http://www.citrix.com/download>

21.5 Network Computer (NC)

Le **Network Computer** est un système Thin Client doté d'une technologie reposant sur Java. Dans cette configuration, les applications peuvent tourner sur le serveur et la configuration Java-Applet les exécute même sur le client.

Ces configurations sont conçues pour l'Intranet et l'Internet. Elles ne reposent donc pas sur les protocoles ICA et RDP spécifiques à la plate-forme Windows (voir Windows Based Terminals), mais sur le protocole d'usage sur Internet. En revanche, cela ne signifie pas que les NC ne conviennent

pas pour les environnements ICA et RDP.

Dans cette architecture, le client ne nécessite plus un PC haut de gamme, un NC suffit. Les caractéristiques suivantes s'appliquent aux NC :

- Les NC ne nécessitent pas de disque dur
- Les NC sont préparés à une utilisation Intranet
- Utilisation de processeurs CISC ou RISC performants
- Utilisation graphique et audio très complète.

Par rapport à un PC, un NC présente des avantages importants qu'il convient de considérer avant l'achat. Citons les arguments suivants :

- Baisse considérable des coûts d'administration
- Sécurité et intégrité du système nettement plus élevées (mot-clé : sauvegarde centrale des données)
- La maintenance du client ou du logiciel client s'avère superflue, les fonctions "Helpdesk" PC ne sont plus requises
- Une gestion centrale des applications, ce qui signifie que l'entreprise est toujours équipée de la même version
- Les modules correspondants ne sont chargés que sur le serveur, ce qui permet une mise à disposition des versions logiciels les plus récentes sans travaux d'installation ou de maintenance
- Les explorateurs Web sont disponibles en tant que logiciel client et sont économiques
- Besoins minimes de formation.

Pour conclure : **Les Thin Clients permettent d'abaisser considérablement le coût total de propriété (Total Cost of Ownership : TCO).**

Les sociétés Apple, IBM, Netscape, Oracle et Sun ont mis en place ce qu'on appelle un "Network Computer Reference Profile" définissant exactement les exigences minimales d'un NC. Entre temps, le profil a été repris par **"The Open Group (TOG)"**. Cette organisation internationale est chargée de garder un standard actuel pour ce profil. Pour plus d'informations sur le TOG et ses membres, consultez la page d'accueil : www.opengroup.org

Les NC de fabricants tels que NCD (NCD NC), Tektronix (Netstation), IBM (Network Station), Neoware (Workstation) ou Sun (JavaStation) répondent tous à ces exigences, mais diffèrent quelque peu de par leurs accessoires et fonctionnalités supplémentaires.

21.6 Network PC

Contrairement aux NC, principalement équipés de processeurs Intel i960 et PowerPC (NCD, IBM, Neoware) ou de processeurs MicroSparc-II (Sun), les Network PC (de Microsoft par ex.) sont munis de processeurs Intel Desktop. En quoi diffèrent les NC ou les WBT ? Le système d'exploitation ainsi que l'équipement matériel typique des NetPC restent tout aussi importants (par ex. les lecteurs locaux et les disques durs), et bien entendu, il s'ensuit des coûts d'investissement et des coûts de propriété plus élevés. Le concept de la gestion centrale des données et de l'administration n'est pas tout à fait au point dans cette catégorie de produits. Les Network PC se situent plutôt entre les PC et les "Thin Clients" et forment une catégorie supplémentaire d'ordinateurs de travail.

Ce qu'on peut dire : les PC, NC et WBT garderont leur domaine d'application et influenceront de plus en plus d'applications grâce à Internet. Le développement des Internet Appliances a pour but de développer les appareils d'usage commun en appareils autonomes et communiquant entre eux. Les Internet Appliances sont reliés entre eux et peuvent échanger des données. Entretemps, ce développement présente des résultats intéressants, comme par exemple la mise en réseau d'appareils à usage privé dans le but de commander et de contrôler chaque appareil sans devoir tenir compte de la localisation de son propriétaire. De cette manière, tout le domaine électronique privé ou à domicile peut être commandé à partir de presque chaque terminal Internet. La technologie de base est reléguée ainsi à l'arrière-plan, la convivialité d'utilisation s'adapte aux besoins de l'utilisateur.

22. Périphériques de sortie

22.1 Ecrans

22.1.1 Unités de mesure et notions

La **résolution** d'un écran correspond au nombre de points élémentaires (on parle également de pixels) formant chaque image représentée. Un pixel est la plus petite entité adressable de l'écran.

La **fréquence de rafraîchissement** de l'image définit le nombre de fois, par seconde, que l'image est complètement redessinée sur l'écran. Plus cette fréquence est élevée et plus l'image apparaît stable à l'observateur. Le domaine de valeurs optimales commence autour de 73 Hz, seuil de fréquence à partir duquel l'œil humain ne détecte plus aucun scintillement. Un travail de longue durée devient alors possible sans que l'utilisateur ne soit fatigué par l'écran. La valeur de fréquence de rafraîchissement recommandée aujourd'hui se situe autour de 85 Hz.

La **fréquence de balayage** horizontal correspond au temps nécessaire à la construction d'une ligne d'écran. Cette fréquence, exprimée en kHz, se calcule à partir de la fréquence de rafraîchissement de l'image et du nombre de lignes du mode vidéo utilisé. Elle dépend aussi de la résolution et de la fréquence de rafraîchissement de l'écran.

La **largeur de bande vidéo** indique la qualité de l'amplificateur vidéo. Lorsque la largeur de bande vidéo est étroite, des lignes verticales claires sur fond noir peuvent engendrer la formation d'ombre.

Le **contraste** : Le réglage du contraste permet d'obtenir la « clarté d'image » souhaitée. Le contraste doit être réglé de telle sorte que l'image soit suffisamment claire, mais toutefois sans surmodulation. Une surmodulation s'observe par des bords d'image droits décousus et colorés.

La **focalisation** indique la forme du faisceau d'électrons, qui lors de l'impact avec le phosphore devrait être le plus circulaire possible sur toute la zone visible de l'écran, et ce pour n'importe quelle résolution ou fréquence. Une mauvaise focalisation entraîne le brouillage des signes et des lignes représentés, particulièrement dans les coins de l'écran. Pour obtenir une meilleure précision d'image, il est donc recommandé de prendre en compte également la largeur de bande vidéo, la convergence et la résolution d'écran.

La **stabilité d'image** : Pour maintenir la haute tension d'un écran stable, dans diverses conditions de fonctionnement, il faut en avoir une utilisation importante. Une mauvaise stabilité s'observe principalement lors du passage du clair au foncé. Une faible stabilité de haute tension provoque alors une modification constante de la largeur d'image, ce qu'on appelle le « pompage » de l'image.

L'**effet de traînée** désigne le phénomène, selon lequel un objet mouvant sur l'écran n'est plus délimité bien clairement, mais au contraire laisse derrière lui une « traînée de comète ». Cet effet survient particulièrement dans les écrans LCD passifs (STN, DSTN) et est provoqué par l'inertie du cristal liquide utilisé. En présence d'images mouvantes rapides présentant de grandes différences de contraste, les cristaux liquides ne sont plus capables d'adopter suffisamment rapidement la nouvelle position. Ces effets sont rarement observés dans les écrans TFT ou les moniteurs à tubes cathodiques. (Pour les tubes cathodiques, il faut toujours trouver le compromis, pour le phosphore utilisé, entre rapidité de réaction et diminution du scintillement en choisissant une durée suffisante de réflexion du phosphore.)

Le **réglage de luminosité** permet de choisir la luminosité de base (fonds) et la proportion du foncé de l'image (le réglage de la « luminosité » se fait par l'intermédiaire du contraste). Si la luminosité est trop élevée, certains éléments d'image apparaissent en gris.

La **convergence** indique la position des trois rayons d'électrons l'un par rapport à l'autre pour le rouge, le vert et le bleu. L'idéal est la superposition directe de ces rayons, pour obtenir un point d'image propre et blanc. Si ce n'est pas le cas, des bords de lignes ou de signes apparaissent colorés, voir même imprécis.

Par la notion de **moiré**, on entend le déroulement de raies d'interférence en forme d'arc sur tout l'écran, qui se modifie avec la largeur et la hauteur de l'image, et qui n'apparaissent qu'avec certaines résolutions. Elles proviennent d'interférences entre le signal vidéo et le masque d'écran et sont visibles surtout en présence de modèles à lignes ou à points. Malheureusement, la formation de moiré s'accroît souvent en présence d'une très bonne focalisation. Les modèles à lignes ou à points sont d'excellentes images test, qui se déroulent sur l'ensemble de l'écran.

22.1.2 Types d'écran

22.1.2.1. Ecrans CRT

22.1.2.1.1 Principe de fonctionnement :

Sur les écrans **CRT** (Cathode **R**ay **T**ube), l'image se forme grâce à l'impact d'un faisceau d'électrons sur la face interne de l'écran qui est elle-même recouverte d'une pellicule de matière électroluminescente. A chaque couleur de base (rouge, vert, bleu) correspond une matière électroluminescente différente. L'obtention d'une couleur quelconque s'effectue par le phénomène de superposition des couleurs de base. Lorsque le faisceau d'électrons frappe l'une des substances électroluminescentes, apparaît automatiquement la couleur correspondante. La combinaison des trois couleurs de base peut créer ainsi des couleurs de luminosité différente.

Pour que les faisceaux rencontrent la substance lumineuse exacte, un masque est posé devant la substance.

Actuellement, trois types de tubes cathodiques sont disponibles sur le marché; ils se distinguent par le type de masque utilisé :

22.1.2.1.2 Les masques à trous, à fentes et à lignes

Le **masque à trous** consiste en principe en une plaque métallique ou en céramique percée de trous ronds, à travers lesquels le ou les faisceaux d'électrons sont dirigés, pour qu'il/ils rencontre(nt) le point correct sur l'écran. La distance la plus courte entre deux points de même couleur définit la finesse du crible et est ainsi indirectement liée au nombre de points constituant l'écran. Plus le crible est petit, plus l'image est nette.

Les trous du **masque à fentes** sont carrés. Dans le domaine des moniteurs, ce type de masque n'est plus répandu, seuls les fabricants d'appareils TV utilisent encore cette technologie.

Le **masque à lignes** par contre, consiste seulement en des fils verticaux, soumis à une haute tension, et à travers lesquels le faisceau d'électrons est dirigé.

Les avantages et inconvénients des différents types de masque :

Les **tubes avec masques à trous et à fentes** sont peu sensibles aux chocs en raison de la « plaque trouée » mais n'ont pu reproduire encore jusqu'ici le contraste et la brillance des couleurs qu'offre le masque à lignes. En outre, en raison de la surface plus grande, ils tendent au phénomène de « dooming ». C'est ainsi qu'on nomme l'effet qui se produit à la suite d'un réchauffement important par le faisceau d'électrons. Le réchauffement provoque une déformation du masque. Le faisceau d'électrons ne peut donc plus percer librement le masque à trous. Il s'ensuit des impuretés de couleur, spécialement dans les coins de l'écran, ainsi qu'une mauvaise répartition de la luminosité. Grâce à leur insensibilité aux chocs, les écrans avec masque à trous conviennent particulièrement bien pour les environnements industriels.

En raison de sa construction, le **masque à lignes** convertit en chaleur seulement une faible partie de l'énergie contenue dans les faisceaux d'électrons. Il provoque ainsi moins d'altération des couleurs et atteint un contraste et une brillance plus élevés. Par contre, il est un peu plus sensible aux chocs et est renforcé par deux fils de stabilisation, qui pour un expert apparaissent comme de faibles lignes d'ombre. De plus, un moniteur Trinitron (Trinitron est une marque déposée de Sony Co.) présente l'avantage d'une surface d'écran plus plate. Les systèmes traditionnels d'écran à crible ont une forme sphérique difficile à aplatir, même en employant les techniques modernes les plus sophistiquées (écran Flat Screen Tube). Un écran avec masque à lignes, par contre, est de forme cylindrique. L'écran apparaît comme une fenêtre sur ce cylindre. L'augmentation du rayon du cylindre se traduit par un aplatissement relatif de la surface de l'écran. Rappelons ici que plus un écran est plat et moins il est sujet aux distorsions d'image. Les lignes droites sont représentées comme des droites, ce qui qualifie ces écrans pour les applications de CAO et FAO et autres

applications graphiques haut de gamme. En outre, le verre teinté monté sur les écrans Black Trinitron permet d'absorber une grande partie de la lumière extérieure incidente (rayonnement du soleil ou d'un système d'éclairage).

22.1.2.2 Ecrans LCD

22.1.2.2.1 Principe de fonctionnement :

Pour ce type d'écran, on se sert des propriétés spéciales d'un groupe d'éléments chimiques, à savoir les cristaux liquides (**Liquid Crystal**), qui sont transparents et dont les molécules sont altérées. La distorsion des molécules modifie la polarisation de la lumière traversante. En appliquant un champ électrique, les cristaux s'orientent de manière correspondante. Ces propriétés sont utilisées dans les écrans LCD, pour réguler le passage de la lumière à travers l'écran. La lumière est générée par des sources lumineuses, situées au dos de l'écran, et orientée par un filtre de polarisation.

Tant qu'un champ électrique n'est pas appliqué, la polarisation est modifiée le long des molécules distordues. Ensuite, cette lumière frappe un deuxième filtre de polarisation, qui est positionné à angle droit par rapport au premier. En raison de la distorsion par les cristaux liquides, la lumière peut pénétrer ce filtre. Si un champ électrique est appliqué au cristal, l'angle de distorsion des cristaux ainsi que de la lumière est modifié, et seule une partie de la lumière peut passer l'écran.

De cette manière, on peut régler la luminosité, pour obtenir le nombre nécessaire de degrés de gris pour un affichage de qualité. L'écran est divisé en éléments d'image (pixels), qui composent l'ensemble de l'image. Pour obtenir un affichage couleur, trois pixels sont utilisés par point d'image, dont les couleurs rouge, vert et bleu sont créées par un filtre de couleurs. L'image est créée par une matrice de pixels.

Il existe deux types d'écrans LCD :

22.1.2.2.2 Les écrans LCD à matrice active et à matrice passive

La commande de la luminosité de chaque pixel, aussi appelée « adressing », est la principale différence entre les deux types disponibles d'écrans LCD.

Contrairement à l'affichage passif de cristaux liquides, la commande des écrans TFT à **matrice active** est active comme son nom l'indique. Cela signifie, que pour chaque point d'image, trois commandes électroniques, une pour chaque couleur rouge, vert et bleu, sont utilisées pour réguler les cellules. Ces commandes sont généralement des transistors à film fin (Thin Film Transistor = TFT), qui protègent également le pixel contre l'influence d'un pixel voisin et qui empêche ainsi la transmodulation. La commande par des transistors présente l'avantage, que la cellule peut garder

son état aussi longtemps, jusqu'à une commande renouvelée. Cela permet d'utiliser des cristaux liquides plus rapides et d'éviter l'effet de traînée. Ces transistors à film fin sont produits selon un procédé semblable à celui de la fabrication de chips semi-conducteur. En raison des taux élevés de rebut inhérent à la production, les coûts de fabrication et donc le prix des appareils restent encore élevés (par exemple, pour fabriquer un écran avec une résolution de 1024 par 768, il faut prévoir $1024 \times 768 \times 3 = \sim 2,36$ millions de transistors).

Sur le plan technologique, les écrans à affichage LCD numérique ne présentent naturellement aucun défaut, tels que distorsions géométriques, différences de convergence ou flous, puisque chaque point d'image, constitué de trois pixels rouge, vert et bleu, se trouve dans une position fixe. Il faut plutôt s'attendre aux imperfections suivantes, selon la technologie utilisée :

- Pixels manquants (Missing Dots)
- Traînée (Smearing) en présence d'images mouvantes
- Réflexion irrégulière en raison de l'éclairage de fonds.

Matrice passive (STN, DSTN) : Avec ce type d'affichage à cristaux liquides, la commande de chaque cellule s'effectue par ligne, tout comme pour un écran. Les cristaux sont orientés par la courte application d'un champ électrique, et ensuite perdent à nouveau cette orientation. Pour diminuer cet effet, des cristaux liquides inertes sont utilisés. Ceux-ci ont le désavantage de provoquer des effets de traînée en raison de l'inertie des cristaux.

22.1.3 Exigences pour les écrans

22.1.3.1 Diagonale d'écran et application

Un point important pour la **diagonale d'écran** nécessaire est le type d'application pour lesquelles un écran est destiné. Une tendance nette est observée dans le passage des écrans traditionnels à tubes vers les écrans couleur plats, de plus en plus performants et avantageux. Avec leurs nombreux menus déroulants et autres barres d'outils, les applications actuelles imposent une résolution graphique d'au moins 1074×768 pixels pour une diagonale d'écran de $38,1 \text{ cm} = 15''$. Les capacités d'un tel écran et de l'utilisateur sont cependant très vite dépassées dès que plusieurs fenêtres (applications) doivent être simultanément ouvertes. Dans ce cas, les écrans couleur plats de $17''$ sont recommandés, car ils présentent couramment une résolution de 1280×1024 pixels. Pour des applications réclamant un plus large champ de vision, l'utilisateur a le choix, outre les écrans de $18''$, entre des écrans de $19''$ et $20''$. Pour les écrans de $20''$, une résolution de 1600×1200 dpi est déjà disponible en standard. Les écrans couleur plats de cette taille, pouvant atteindre une résolution supérieure par extrapolation, conviennent suffisamment pour des applications de courte durée. Cependant, chaque extrapolation entraîne une perte de qualité, il est donc recommandé d'acheter un écran doté de cette résolution, qui supporte physiquement la résolution de 1600×1200 . **Inter-/Extrapolation** : procédé pour agrandir ou réduire les images en ajoutant ou éliminant des pixels. L'avantage du procédé par interpolation se profile par la qualité d'image

qui en résulte.

Particulièrement dans le domaine graphique, pour les applications CFAO et toutes celles réclamant une authenticité absolue des couleurs et une certaine brillance, un écran CRT avec masque à lignes est préférable aux écrans couleur plat.

Dans un environnement industriel où des chocs et des coups sont inévitables, il est recommandé de faire appel à des écrans CRT avec masque à trous (se référer aux avantages et désavantages des différents types de masque).

Pour les applications de CAO et PAO, de design graphique, les écrans de 48 cm ou 50 cm (19"), 50,8 cm (20") ou 53 cm et 55 cm (21"), possédant une résolution de 1280 x 1024 pixels sont tout à fait appropriés. Pour des applications plus complexes, il faut disposer d'une résolution de 1600 x 1200 pixels.

22.1.3.2 Ergonomie

Exigences d'ergonomie pour les écrans :

Exigence minimum : MPR II angle bleu ou label TCO.

Significatif : Taille et qualité d'image, sans scintillement, contraste suffisant, bonne précision de l'image, focalisation dynamique, réglage de la convergence, taille suffisante des caractères, libre d'interférence et de réflexion, orientable et inclinable librement et légèrement.

Organisation du poste de travail : un agencement correct de l'emplacement de travail est un élément important pour un travail en toute détente et le respect de la santé. transtec peut vous fournir de plus amples informations à ce sujet.

22.1.3.3 Rayonnement

Un autre aspect essentiel dans le choix d'un écran est sans nul doute la puissance de rayonnement émanant de l'écran. Des valeurs indicatives ont été définies par différents instituts. Une norme importante est la norme **MPR-II** relative aux champs électriques, magnétiques et électrostatiques pulsés, publiée en 1990 par l'institut de contrôle suédois. Les écrans, dont les spécifications sont inférieures à cette norme, sont aujourd'hui couramment considérés comme peu rayonnants.

Depuis janvier 1999, il existe la norme **TCO99** qui est une extension des précédentes TCO92 et TCO95. Pour être conforme à cette directive, les écrans doivent satisfaire à des exigences de qualité et d'ergonomie encore plus sévères. En premier lieu, la fréquence de rafraîchissement minimale de l'écran est définie en fonction de la résolution et des dimensions de l'appareil (exemple : 85 Hz pour un écran de 17" et 1024 x 768 pixels). Cette recommandation introduit également d'autres nouveautés : consommation de 15 Watt uniquement encore en mode d'économie d'énergie (auparavant 30 Watt), interdiction de matières comportant du brome ou du chlore, éviter les matériaux lourds et respecter les normes légales de recyclement en vigueur dans chaque pays.

Adoptée depuis fin 2002, début 2003, et encore peu connue, norme **TCO03** repose sur la norme courante TCO99 et prévoit des exigences encore plus sévères pour les écrans à tubes et les écrans plats. Cette norme définit par exemple le réglage en hauteur, les exigences en matière de câble, de boîtier et de recyclage.

22.1.4 Standards graphiques

Dans le domaine des ordinateurs personnels (PC) différentes normes régissant la compatibilité entre cartes graphiques, écrans et logiciels, ont été développées. Les deux normes graphiques aujourd'hui les plus répandues sont indéniablement les standards **VGA** (Video Graphics Array) et Super-VGA. La résolution du standard VGA est égale à 640 x 480 pixels. 16 couleurs parmi une palette globale de 256 peuvent être simultanément présentes sur une représentation VGA. Un mode supplémentaire peut afficher 256 couleurs, mais seulement 320 x 200 pixels.

Super-VGA (**SVGA**) et **XGA** correspondent à des résolutions plus élevées atteignant 1024 x 768 pixels. Pour représenter une image faisant appel à 16 couleurs parmi 256, il convient de disposer d'une mémoire d'écran de 512 ko. Moyennant une extension de la mémoire d'écran de 1 Mo, il devient possible de construire des images utilisant 256 couleurs extraites d'une palette de 16,7 millions.

Les normes graphiques des PC n'ont pu s'imposer dans le domaine des stations de travail. Les cartes graphiques mises en œuvre dans les environnements Compaq/Digital, HP, IBM ou SGI proposent des résolutions de 1024 x 768 et 1280 x 1024 voire 1600 x 1280 pixels maximum sous différentes fréquences de rafraîchissement d'écran. Les cartes graphiques mises en œuvre sur les stations SPARC disposent généralement d'une résolution de 1152 x 864 sous une fréquence de rafraîchissement de l'écran de 66 Hz ou 76 Hz. On trouve aussi des cartes graphiques à la norme VGA ou disposant des résolutions 1024 x 768 voire même 1600 x 1280 pour stations SPARC.

22.2 Projecteurs LCD

Pour des présentations devant un large public il est recommandé que tous les participants puissent voir la représentation de l'écran, et ce grâce à un projecteur. Si le temps de préparation est assez long pour une présentation à l'aide d'un projecteur de transparents (impression de transparents, photocopies, etc.), par contre il est nettement réduit avec un projecteur LCD. En effet, des modifications peuvent être faites jusqu'à la dernière minute, et même en cours de présentation, qui peut s'agrémenter d'animations interactives, ce qui rend l'événement encore plus intéressant. Le développement de la génération actuelle de projecteurs tend à des appareils toujours plus maniables et silencieux pour une utilisation en salles de conférence, mobile ou lors de manifestations de toutes ampleurs. Des niveaux sonores inférieurs à 30 dB, des lampes extrêmement modernes d'une durée de vie de 6.000 heures et des poids inférieurs à 2 kg sont maintenant chose courante. Une utilisation dans des salles aussi lumineuses qu'en plein jour est tout à fait possible grâce à

l'indice toujours plus important de lumen ANSI. Les projecteurs de Philips sont dotés par exemple de la technologie appelée Limesco (**L**ine **M**emory **S**can **C**onverter). Un chip intégré permet au projecteur de présenter des standards graphiques plus élevés, dépassant sa propre résolution graphique.

22.2.1 Les technologies

La technologie la plus répandue est la **technique LCD**. La lumière est fragmentée dans les couleurs de base rouge, vert et bleu. A travers de chacune d'elle est conduit un écran LCD en tant que clapet lumineux, ensuite, chacune des couleurs est ajoutée à la fin de ce processus. Chaque point d'image et chacune des trois couleurs de base disposent donc d'un écran LCD.

La **technologie DLP** utilise de nombreux miroirs, de forme carrée et extrêmement petits, qui sont déposés sur un chip DMD. La lumière est réfléchiée vers l'écran uniquement par des miroirs inclinés. L'œil humain ne peut discerner cette haute fréquence d'activation/désactivation des points lumineux. La bande de couleurs, créant les couleurs à partir des trois couleurs de base, permet la représentation des gradations.

22.2.2 Avantages et désavantages des deux technologies

Un haut degré de saturation des couleurs et une réflexion homogène sont les avantages de la technologie LCD. L'investissement des appareils de type LCD présente également l'avantage d'être peu onéreux.

L'authenticité des couleurs dans la représentation et l'absence d'éventuelles erreurs de pixel sont quant à eux les avantages nets des appareils DLP, un peu plus coûteux, dont les arguments de poids sont un important rendement lumineux et une excellente qualité d'image.

22.3 Imprimantes

Quand on aborde les différentes technologies d'impression, les deux techniques qui se profilent au premier plan sont l'impression à jet d'encre et l'impression laser, tandis que les impressions à aiguilles et à transfert thermique ont quant à elles moins d'importance.

22.3.1 Les technologies

22.3.1.1 Impression jet d'encre

Pour les imprimantes à jet d'encre, diverses technologies ont été développées. On fait la distinction entre jets d'encre compacte et jet d'encre liquide, ainsi qu'entre les techniques « Drop on demand » et « Continuous flow ».

Les **imprimantes jet d'encre compact** sont utilisées pour l'impression couleur. Une masse de

couleur, sous la consistance de gel, à la température ambiante est réchauffée et projetée en fusion sur le papier, où elle se refroidit immédiatement. En raison de la modification de la consistance de la matière colorée (dur, liquide, dur), on parle également d'imprimante à jets d'encre « Phase-change ». L'image imprimée est excellente, cependant l'investissement et l'entretien de ces appareils sont relativement onéreux. C'est la technique employée qui rend ces appareils peu abordables : pour chaque couleur est prévue une chambre de fusion, dans laquelle la masse est liquéfiée et mise à disposition du réservoir d'encre pour impression. Après déconnexion de l'imprimante, cette masse de couleur se refroidit à nouveau. Il s'ensuit un nettoyage fastidieux du système d'impression et une attente plus ou moins longue lors du rebranchement de l'appareil, pour atteindre la bonne température de service et la bonne consistance de chaque substance colorée. Les résultats d'impression, tout comme dans le procédé à transfert thermique, sont un usage quotidien sujets à quelques conditions : ils sont très délicats et réclament dès lors beaucoup de précaution dans leur manipulation.

Les imprimantes à jets d'encre à flux continu perdent toujours plus de terrain, et seules quelques imprimantes fonctionnent encore avec cette technologie. L'encre coule continuellement dans un champ électrostatique, à partir d'un réservoir vers un récipient de réception. Lors de l'impression, quelques gouttes de ce flux d'encre sont déviés sur le papier. Cette technologie permet, tout spécialement pour l'impression couleur, d'atteindre un haut degré de qualité, mais elle est très onéreuse.

Les imprimantes à transfert thermique

Cette technologie développée par HP s'est établie en leader sur le marché. Les imprimantes, fonctionnant selon ce principe, sont rapides, atteignent une excellente qualité d'impression et l'entretien et reste acceptable. Ces appareils constituent des systèmes robustes, dans lesquels la mécanique et les têtes d'impression à haute précision sont indépendantes l'une de l'autre. L'ensemble de la tête d'impression est logée dans une cartouche d'encre interchangeable. Elle est fabriquée selon une technique identique à celle utilisée pour produire les micro-chips. La technique de fabrication microlithographique permet une production en série économique pour une qualité constante. La matière de base est une gaufre monocristalline ronde de silicium. Par corrosion de cette gaufre, on obtient les structures nécessaires pour le mécanisme de transport d'encre, les buses d'encre et bien entendu les liaisons et les divers éléments électriques. Lorsqu'une cartouche d'encre est vide, l'utilisateur reçoit une nouvelle cartouche, équipée automatiquement d'une nouvelle tête d'impression, ce qui garantit une qualité constante d'impression, même après plusieurs années. Et ceci, pour un prix comparablement assez bas.

Dans ce procédé, la tête d'impression voyage horizontalement au-dessus du papier, dans un traîneau de transport. Après impression, le traîneau avance d'une ligne pour commencer l'impression de la ligne suivante. L'opération d'impression s'effectue sans aucun contact. A chaque point d'impression souhaité, la buse de la tête d'impression dépose une goutte infime d'encre. C'est pourquoi on parle également de procédé « drop on demand » (goutte à la demande), différent

de la technologie en flux continu. Ce procédé à la demande garantit la consommation de la seule quantité d'encre effectivement nécessaire à l'impression. Dans le cœur de la mécanique se déroulent entre temps d'autres opérations très complexes.

La buse, délivrant l'encre, est une petite chambre, sur le sol de laquelle se trouve une résistance. Cette résistance est chauffée par amenée de courant. L'encre est introduite grâce à une force capillaire au travers de canaux du réservoir vers la chambre de buse. Là, elle est réchauffée à 300° en quelques fractions de seconde. La bulle de vapeur se formant au sol de la chambre exerce une pression sur le reste de l'encre s'y trouvant et la dirige vers l'ouverture de la buse. A l'ouverture de la buse, qui est plus fine qu'un demi cheveu humain, la bulle de vapeur éclate. Cette éclatement libère des forces (ondes de choc), qui propulsent les gouttes d'encre à une vitesse d'environ 100 km/heure. Une fois que les gouttes d'encre ont quitté la buse, une sous-pression se forme dans la chambre. Et cette sous-pression permet un nouveau écoulement d'encre à partir du réservoir vers la chambre. Cette opération peut se répéter quelques milliers de fois en une seconde.

La formation de bulle et l'éjection sont aujourd'hui étudiés à l'aide de simulations complexes par ordinateur. Le développement du procédé est ainsi continuellement amélioré. Ceci est un facteur important pour l'aspect dynamique du procédé, car en cours d'impression, une tête d'impression est en effet continuellement en mouvement. La goutte d'encre ne coule pas selon une trajectoire linéaire, mais bien selon une trajectoire en forme d'arc, calculée avec précision, en direction du papier. Ces paramètres techniques sont pris en compte lors de la configuration de l'imprimante, pour améliorer en conséquence tout le procédé.

L'ingénieur pousse même son intérêt jusqu'à la grosseur de la goutte d'encre. Actuellement déjà, les gouttes d'encre atteignent des diminutions de l'ordre de 10 milliardième de litre. Ceci permet un meilleur dosage de la quantité d'encre, en poussant plusieurs gouttes les unes sur les autres. Dans la pratique, on obtient les avantages suivants : plusieurs couleurs par point d'impression peuvent être représentées, la qualité d'impression est élevée même sur du papier normal et la vitesse d'impression est en constante progression.

22.3.1.2 Imprimantes laser

Alors que les technologies d'impression, décrites ci-dessus, reposent sur le fameux principe de la ligne - un fichier d'impression qui a été créé dans l'ordinateur - la technologie laser repose elle, sur le principe de la page. Les imprimantes laser travaillent selon le principe électrographique, un procédé physique d'impression, au cours duquel aucune opération chimique n'a lieu, et donc aucun produit révélateur liquide n'est nécessaire. Lors de l'impression le cylindre photosensible est chargé électriquement. Par un système de miroir, l'image est transmise par laser sur ce cylindre. L'imprimante déconnecte le laser pour chaque point qui ne doit pas être imprimé et, au point de rencontre avec le rayon laser, le chargement électrique du cylindre est neutralisé. Le cylindre absorbe le toner sur tous les points neutralisés ; celui-ci est transféré sur le papier où il est alors fixé par chauffage et application d'une pression mécanique élevée.

Ce procédé convient aussi bien pour les imprimantes monochromes que couleur laser. Dans les

imprimantes couleur laser uniquement, toute l'opération est répétée pour chaque mélange de couleur (C, J, M et N). Par contre, ce n'est pas le papier à imprimer qui passe quatre fois dans la machine, mais une bande spéciale sur laquelle sont stockées les pages à imprimer. Cette image d'impression est transmise en une seule opération par le cylindre sur le papier ou le transparent. Quelques fabricants ont développés des méthodes, qui améliorent nettement l'image d'impression, grâce à des tailles réglables de point ou des positions variables de point. HP par exemple, a nommé son procédé : **Resolution Enhancement Technology (RET)**. Indépendamment d'un logiciel, et seulement par l'amélioration de la taille et point et de son positionnement par rapport aux points voisins, cette fonction intégrée produit de meilleurs courbes arrondies, des lignes/arêtes plus vives et des croisements plus uniformes.

L'argument en faveur des imprimantes laser repose principalement sur l'excellente qualité d'impression, l'aptitude au graphisme et la faible émission de bruit en cours d'impression. En raison de leur prix plus élevé que celui des imprimantes à jet d'encre, ces imprimantes sont surtout proposées pour les grandes quantités d'impression.

23.3.1.3 Imprimantes matricielles

Il y a quelques années encore, on trouvait les imprimantes matricielles à côté de chaque PC. Elles permettaient d'imprimer des signes et des graphiques, même mélangés sur une même page. Outre le fait que les signes composés de plusieurs points ne sont pas particulièrement esthétiques, les imprimantes matricielles sont également très bruyantes. Quelques imprimantes matricielles peuvent produire aussi des impressions couleur, en utilisant une bande à trois voire quatre couleurs au lieu de la seule bande noire. Outre une vitesse d'impression particulièrement lente, les coûts d'utilisation sont élevés. En effet, l'impression fréquente de couleur foncée projette celle-ci sur la bande de couleur et la salit. Cependant, les imprimantes matricielles sont de nos jours encore indispensables dans certains domaines, particulièrement dans les entreprises de logistiques, où l'on doit imprimer des documents en plusieurs copies.

22.3.1.4 Imprimantes à transfert thermique

Sous la notion de transfert thermique, on distingue surtout deux technologies : les imprimantes à transfert thermique et à sublimation thermique. Les quelques imprimantes thermiques, qui rendent visible la matière colorée déposée sur le papier par réchauffement (comparable aux appareils fax), ne jouent plus qu'un rôle limité sur le marché.

Pour des impressions couleur de qualité, ce sont les **imprimantes à sublimation thermique** qui sont proposées. Elles réchauffent de la cire colorée, qui se trouve sur un film porteur et la pressent sur le papier. La cire se réchauffe à tel point qu'elle dégage de la vapeur et s'imprègne sur le papier.

L'impression à sublimation thermique réalise également de fines gradations de couleur dans une qualité, qui est suffisante pour l'impression d'essai dans l'industrie graphique. Dans ce contexte,

il est également intéressant que ces imprimantes réalisent des rendus photographiques de qualité dans une résolution comparablement faible, inférieure même à 200 dpi.

Ceci est une preuve supplémentaire, que la qualité d'impression couleur ne dépend pas que de la résolution sélectionnée mais bien du type de mélange des couleurs. Toutefois, les coûts d'investissement et d'utilisation (film de couleur, papier spécial) sont tellement élevés, que les imprimantes à sublimation thermique n'entrent pas en ligne de compte pour usage bureautique ou privé. Une variante beaucoup plus simple est celle des **imprimantes à transfert thermique**. Elles fonctionnent également avec un film de cire. Cependant la cire n'est réchauffée à une température lui permettant de fonder pour être portée sur le papier comme point colorié. Le rendu couleur est suffisamment bon, mais les impressions sont sensibles aux plis et aux griffes. Seuls des papiers et des films spéciaux peuvent être utilisés, et les films de cire nécessaires sont coûteux. Même si quelques imprimantes sont offertes dans un segment inférieur de prix, les coûts élevés des consommables parlent en défaveur de leur utilisation. Elles sont surtout utilisées par des graphistes professionnels, pour qui elles représentent une sérieuse alternative, et surtout avantageuse, par rapport à l'impression par sublimation thermique.

22.3.2 Protocoles d'imprimantes

La plupart des imprimantes laser maîtrisent les protocoles **HP PCL** et/ou **PostScript**. PostScript est un langage de description de page, indépendant de l'imprimante, pour lequel le type d'écriture (les fontes) sont définies par des courbes mathématiques (courbes de Bézier). En raison de sa grande performance et de sa structure flexible de commande, le protocole PostScript est utilisé dans de nombreux domaines.

HP PCL (**P**rinter **C**ommunication **L**anguage) est un langage de description de page développé par HP, pour commander les imprimantes, et plus particulièrement les traceurs, et qui est également utilisé par de nombreux autres fabricants. HP PCL 6 est le perfectionnement de HP PCL 5 et est compatible avec celui-ci. Les nouveautés au niveau de PCL 6 résident surtout dans l'impression accélérée de graphiques complexes, l'amélioration de la qualité d'impression ainsi que dans un débit réseau plus élevé grâce à l'utilisation de commandes plus petites et plus compactes. De nettes améliorations de performance sont surtout attendues sous Microsoft Windows, en effet, les commandes PCL 6 supportent l'interface GDI (Graphical Direct Interface).

Certains appareils dominent également le langage pour traceurs HP-GL (HP **G**raphics **L**anguage). Le protocole HP-GL/2 intégré dans HP PCL est un développement de HP-GL. HP-GL est un langage vectoriel, qui garantit une parfaite qualité d'impression.

Une implémentation du langage pour traceur HP-GL ou HP-GL/2 vers les imprimantes laser présente l'avantage que les commandes pour traceur peuvent être traitées par l'imprimante laser et peuvent donc être transposées dans une représentation graphique correspondante. Un traceur peut être remplacé par une imprimante supportant HP-GL ou HP-GL/2 sans pour autant devoir procéder à une adaptation au niveau du pilote. L'impression de graphiques dure souvent longtemps lorsque l'on se sert d'un traceur. Sur une imprimante laser, l'impression se fait en quelques secondes.

23. Multimédia

Si le **Multimédia** est à la mode, il est également devenu une réalité dans de nombreuses applications.

Le terme multimédia décrit la **combinaison de différentes formes de médias : illustrations (par ex. avec utilisation d'appareil photo numérique), sons, animations, textes et graphiques.**

Beaucoup d'ordinateurs accomplissent bien plus. On peut également écouter des CD musicaux, envoyer des e-mail sonores, téléphoner ou transférer des appels, ainsi que de mettre en oeuvre des fonctions de répondeur téléphonique.

Les systèmes de conférence vidéo gagnent de plus en plus d'importance, car on peut retransmettre bien plus qu'une image vidéo normale. Il est possible d'établir des conférences avec plusieurs participants et d'échanger rapidement et économiquement, entre distances importantes, des documents. Les médias tels que les lecteurs de CD et de DVD, ainsi que les Jukebox sont aussi de plus en plus souvent mentionnés en association avec les multimédia. En effet, le volume des données est en général très élevé et requiert ainsi des supports de données économiques, rapides et de capacité importante.

23.1 Appareils photos numériques

Avec la croissance exponentielle du marché des applications multimédia, celui des appareils photos numériques se développe à un rythme non moins vertigineux. Avec un matériel photographique traditionnel, le traitement d'une photo via un ordinateur devra d'abord passer par le développement du film puis par le passage au scanner de la diapo ou d'un tirage papier. Avec un appareil photo numérique, les images sont déposées sous format numérique dans une mémoire interne et transmises à l'ordinateur par une interface, une disquette ou un CD/DVD.

L'utilisateur peut agrandir ou réduire l'image, l'intégrer au sein de documents ou les expédier via Internet. Des publications Desktop, des présentations ainsi que des brochures simples de marketing peuvent rapidement et simplement, sans scanner, être complétées d'image. Il faut en outre disposer d'une imprimante couleur adéquate, par ex. une imprimante HP. Le processus de travail **"photographier - visionner - traiter - imprimer"** peut être complètement bouclé.

23.2 Applications linguistiques

Tout comme la musique, la parole est un signal analogique. Il suffit de la digitaliser en un format que l'ordinateur peut traiter et ensuite retransformer en signal analogique par le biais d'une carte audio. L'entrée et la sortie, ainsi que le traitement de séquences sonores s'effectuent via une carte d'interface audio, appelée simplement carte audio dans le monde PC.

Le signal analogique en provenance d'un microphone ou d'un câble de réenregistrement est

échantillonné par la carte audio plusieurs milliers de fois par seconde (Sampling). Durant cette phase, la qualité du balayage dépend de la résolution du convertisseur numérique/analogique utilisé (8, 10 ou 16 bits, par exemple) et de la fréquence d'échantillonnage (nombre de mesures par secondes). Ce procédé est appelé "**Puls-Code-Modulation**" (**PCM**). Si l'on désire transmettre des séquences de parole sur de longues distances via E-Mail par exemple, il faut veiller à ce que le volume de données ne soit pas trop important. Avant d'être envoyés, les signaux sont comprimés via **ADPCM** (**A**daptive **D**ifferential **PCM**) et décomprimés à la réception.

23.3 Traitement des signaux vidéo

Les cartes vidéo sont désormais utilisées dans les applications les plus diverses. Indépendamment de la réalisation de vidéo-clips numériques pour des formations ou des présentations, ces cartes sont de plus en plus souvent utilisées pour la représentation de vidéos en direct (Live-Video) ou de vidéos sur demande (Video-On-Demand). La fonctionnalité **Live-Video** permet à l'utilisateur de suivre le journal télévisé sur son écran tout en laissant ses autres applications ouvertes.

La transmission d'images vidéo comprimées en temps réel via le réseau constitue un autre champ d'application de ces cartes. Les vidéos peuvent être stockées sur un serveur de vidéos équipé d'une telle carte. Un utilisateur distant, ayant accès au serveur de vidéos via le réseau, peut, grâce à la fonction **Video-On-Demand**, visionner les films sur sa station de travail. Il peut aussi les enregistrer s'il désire les retraiter.

Pour la réalisation de **présentations**, les séquences vidéo enregistrées par un magnétoscope ou un caméscope peuvent être récupérées sur la station de travail. Les séquences vidéo entières ou des sélections d'images fixes peuvent être retouchées et être insérées à l'intérieur de vidéos de démonstration.

Pour fabriquer un vidéo-clip, il convient de disposer d'une carte vidéo capable d'enregistrer sur disque dur les séquences vidéo ou autres images fixes fournies par un magnétoscope, un caméscope ou un poste de télévision relié au poste de travail. A l'aide de programmes vidéo, on peut ainsi manipuler le matériel vidéo. Etant donné que les données vidéo se laissent copier et couper à volonté, sans perte de qualité perceptible, le montage d'une séquence n'est plus l'affaire que de quelques commandes couper-coller. Le traitement des vidéos sur ordinateur offre un avantage considérable : l'accès à une image quelconque de la séquence enregistrée est quasiment instantané. Les fastidieuses opérations d'embobinage et réembobinage disparaissent.

Le transfert d'images fixes ou de séquences vidéo entières vers l'ordinateur ou la station de travail peut s'effectuer via des cartes vidéo à caractéristiques multiples, dont de plus amples explications suivent ci-après.

La restitution de séquences vidéos ou d'images de télévision sur l'écran d'un ordinateur en temps réel exige de disposer d'une carte de superposition (**Overlay Card**). Une telle carte élude le fastidieux travail de numérisation des données vidéo. Ce type de carte ne dispose souvent que de fonctionnalités de grabbing très limitées. Elle n'est utilisée que comme récepteur de télévision ou

comme caméra de surveillance. Le signal vidéo est transmis de la carte de superposition à la carte graphique, de telle sorte que la représentation à l'écran n'exige aucune durée de calcul. L'image vidéo apparaît à l'écran dans une fenêtre séparée.

Outre la carte vidéo et la carte de superposition, certaines cartes vidéo possèdent une **carte graphique** intégrée. L'installation d'une carte graphique séparée est donc parfaitement superflue. L'avantage est qu'un emplacement reste libre sur le PC. Les cartes vidéo disposant d'un **TV-Tuner** vont encore plus loin. Avec ce tuner, le PC ou la station de travail est en mesure de recevoir un programme de télévision et de l'afficher en direct (Live-TV) à l'écran dans une fenêtre séparée. Pour numériser et faire défiler à l'écran une séquence vidéo complète, il faut faire appel à des **digitaliseurs en temps réel** chargés de transformer le signal vidéo (analogique) d'entrée en une suite d'images numériques.

La difficulté principale à laquelle on se voit confronté lorsque l'on désire enregistrer une séquence vidéo est toujours la même : le volume gigantesque de données généré par la numérisation d'une image et à fortiori par celle d'une séquence vidéo. La numérisation d'une image vidéo disposant d'une résolution couleur de 24 bits nécessite environ 1,2 Mo. Un signal PAL constitué de 25 images par secondes génère donc un flux de données équivalent à 30 Mo par seconde. Ces chiffres illustrent bien la nécessité de disposer d'une carte vidéo dotée d'un **module de compression** des données dès lors que l'on envisage l'enregistrement des séquences vidéo sur son disque dur. Les procédures de compression de données réduisent les besoins de mémoire de masse et augmentent simultanément la vitesse de traitement des images vidéo. La compression permet par ailleurs de réduire la bande passante nécessaire au transfert de ces données sur le réseau.

Une compression sans perte de qualité en un temps de traitement raisonnable n'est possible que sous un rapport de 1:2. Toutes les procédures de compression de données vidéo doivent cependant en pratique atteindre des performances beaucoup plus élevées. Acceptant une perte minime de la qualité des images, certains logiciels de compression utilisent des algorithmes qui atteignent des taux de compression de 1:20. C'est la raison pour laquelle la plupart des digitaliseurs de signaux vidéo font appel au standard de compression **JPEG**. Les circuits intégrés spécialisés montés sur les cartes vidéo permettent de traiter en temps réel un signal vidéo (à savoir 25 images au minimum par seconde) avec un facteur de compression/décompression égal à 1:10. L'algorithme de compression n'est cependant pas sans conséquence sur la qualité, surtout lorsqu'on impose un taux de compression élevé. En effet, on ne peut tout simplement plus distinguer l'original de l'image comprimée, et en plus on ne peut plus reconstituer l'original à partir de l'image comprimée. Il apparaît ce qu'on appelle des effets de cubes. Le grain de l'image grossit au cours de la compression. Le taux de compression est modulable à volonté. Dans la pratique, il faut faire un compromis. Toute exigence de qualité supplémentaire se paie chèrement en Mo qu'il faut ensuite traiter et enregistrer.

La procédure **Motion-JPEG** ne fait jamais que traiter, elle aussi, des images isolées. Il en résulte en principe un fichier comprenant plusieurs images JPEG.

MPEG prend en compte des changements d'une image à la suivante (en général très minimes). La procédure élimine les informations redondantes que transportent les images qui se suivent. L'information correspondant à toute l'image d'origine n'est plus présente que sur deux images par seconde. Toutes les images intermédiaires ne contiennent plus que les modifications de l'image qui la précède. L'opération consistant à déterminer la partie d'image qui reste constante d'une image à l'autre exige une puissance de calcul colossale. C'est aussi la raison pour laquelle les cartes de numérisation vidéo avec compression MPEG sont extrêmement chères.

Afin d'obtenir une **qualité de restitution finale** satisfaisante, il convient de ne numériser que des signaux vidéo analogiques de première qualité. Quiconque tentera de numériser des vidéos VHS se heurtera rapidement à des problèmes de qualité de l'image. Les vidéos S-VHS ou mieux encore Bétacam sont ici beaucoup plus adaptées. Il serait fatal de considérer qu'en raison de la perte inéluctable de qualité inhérente à la compression, la qualité de l'image vidéo d'entrée ne joue plus qu'un rôle secondaire. Après la compression, les défauts d'image tels que les drops-out ou les parasitages ressortent davantage. La compression MPEG en particulier réagit de manière très sensible aux parasitages étant donné que ces défauts correspondent à des modifications d'information considérables d'une image à l'autre.

Une fois enregistrées sur un disque dur, les images vidéo peuvent être traitées et manipulées à loisir via les logiciels appropriés. L'utilisation de fondus enchaînés électroniques ou d'autres effets spéciaux peut contribuer à valoriser le matériel vidéo dont on dispose.

A l'aide de bibliothèques et d'interfaces de programmation appropriées comprises dans la livraison, il est possible d'écrire ses **propres programmes** de traitement de l'image vidéo sur son PC ou sur sa station de travail. Lors de formations ou de séances de présentation, on peut dès lors définir à volonté l'ordre d'apparition des séquences et associer des sous-titres.

Les programmes d'apprentissage peuvent être conçus de manière à ce que l'élève puisse choisir le chapitre et le rythme de progression qui lui conviennent. Une fois ces choix définis, le programme cherche les images et séquences vidéo appropriées.

Pour les présentations de produits, il est très pratique de pouvoir visualiser les données numérisées via un magnétoscope ou un téléviseur. Cette opération suppose que la carte vidéo possède une sortie vidéo propre. Cela permet de bénéficier du fait qu'à diagonale égale un téléviseur est bien meilleur marché que l'écran grand format correspondant. Moyennant un projecteur vidéo, le film numérique réalisé peut aussi être présenté à un public beaucoup plus important. Citons enfin la possibilité de réaliser des copies sur bandes vidéo du résultat obtenu. Sous cette forme, le film considéré peut à son tour être distribué et visualisé via un poste de télévision à partir de n'importe quel magnétoscope.

23.4 Systèmes de conférence vidéo

Les **systèmes de conférence vidéo** permettent de réaliser des économies considérables et gagnent ainsi de plus en plus d'importance au sein des entreprises. Une communication dotée de son et d'image, améliore et facilite sensiblement la compréhension entre quelques interlocuteurs ou tout un groupe d'interlocuteurs. La diffusion de plus en plus large de la norme RNIS permet d'installer facilement des systèmes de conférence vidéo. La plupart des systèmes disponibles de nos jours se composent d'une carte graphique, d'une caméra vidéo, d'un microphone, d'une carte RNIS ainsi que d'un logiciel. Les standards industriels ITU H.323 (LAN), H.320 (RNIS) et T.120 (accès commun aux données) garantissent une communication avec des systèmes de conférence vidéo d'autres fabricants.

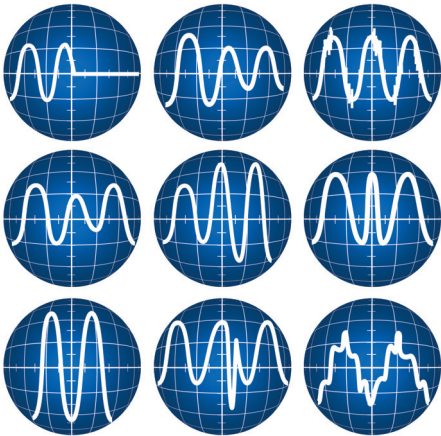
24. Onduleurs

Les onduleurs fournissent à l'ensemble des consommateurs le courant nécessaire à partir d'une batterie, si l'alimentation secteur venait à faire défaut. Une panne inattendue du secteur peut provoquer la perte de données et de programmes, et les coûts et les dommages qui en résultent sont incalculables. Elle provoque également la dégradation du disque dur lorsqu'elle intervient au cours d'un processus d'écriture ou lorsque le contenu de mémoire cache n'a pas été transféré sur le disque dur avant la panne. Il est donc important de pouvoir fermer les applications proprement avant, la déconnexion de l'ordinateur en cas de panne.

En matière de perturbations du secteur, il ne faut pas penser uniquement à une panne de courant. Les problèmes peuvent en effet avoir plusieurs causes, et apparaître sous différents cas de figure.

24.1 Problèmes, causes et effets

Problèmes	Causes	Effets
Panne de secteur	Tempête, panne du transformateur, panne du générateur, travaux	Panne des appareils reliés au secteur, perte de données
Interruption de courant	Tempête, courts-circuits, manipulations sur les appareils de courant	Connexions défectueuses, plantage du système, perte de données
Sous-tension, surtension, variation de tension	marche, déconnexion de l'appareil, coupure du moteur	système, symptômes d'erreur non définissables
Variation de fréquence	Générateurs diesel	Pannes de matériel et de logiciel, pannes du système
Distorsion de tension	Harmoniques, circuits cadencés, courts-circuits, perturbations du secteur	Dégâts matériel et logiciel, instabilités (symptômes partiellement définissables)
Crêtes de commutation, surtensions transitoires	DC-AC, champs magnétiques, transformateurs	Dégâts matériel et logiciel, instabilités (symptômes partiellement définissables)



24.2 Technologies

24.2.1 La technologie Offline

Les utilisateurs sont alimentés par le secteur directement par un filtre sans régulation de tension et de fréquence. Après un temps de commutation inférieur à 10 ms, les utilisateurs sont alimentés par la batterie à partir du redresseur de courant. Les modèles Offline fonctionnent comme un groupe électrogène de secours, ne s'enclenchant que lorsqu'il y a effectivement une panne de courant. En général, pour un PC, la durée de commutation est suffisamment courte pour ne pas encourir de dommages au niveau du calculateur. Par contre, dans d'autres systèmes, ce court laps de temps peut déjà engendrer des pertes de données.

24.2.2 La technologie Line-Interactive

Tout comme dans la technologie Offline, les utilisateurs sont ici aussi alimentés en courant directement par le secteur au travers d'un filtre. Dans la technologie Line-Interactive, la régulation de tension est toutefois possible. Une boucle d'asservissement, installée parallèlement à l'alimentation électrique de l'onduleur, fait en sorte que les fluctuations de tension soient tolérables pour l'utilisateur et que les ressources réseau soient utilisées de manière optimale, puisque la batterie ne s'enclenche pas directement lors de chutes de tension. Ce qui a pour effet de préserver la longévité de celle-ci. Si la tension réseau tombe, les utilisateurs sont alimentés, après un laps de temps inférieur à 10 ms, par la batterie à partir du redresseur de courant. C'est pourquoi, même cette version améliorée de la technologie Offline n'est parfois pas suffisante pour protéger les périphériques sensibles contre les variations de phases découlant de la commutation. C'est le cas par exemple pour de nombreux appareils de télécommunication.

24.2.3 La technologie Online

Ces modèles assurent une plus grande sécurité des données, mais en raison de leur technique complexe, ils sont aussi plus onéreux que les modèles de technologie Offline ou Line-Interactive. L'entrée de courant secteur est entièrement isolée d'un point de vue galvanique puis démodulée. La tension démodulée est aplanie, stabilisée et transformée à nouveau en courant alternatif propre. Ce procédé représente pour l'utilisateur la meilleure protection contre les variations de tension, les interruptions, les parasites ou les espions.

La recharge de la batterie s'effectue en cours de fonctionnement normal. Lorsque l'alimentation électrique tombe complètement en panne, la batterie constamment chargée prend immédiatement le relais doucement et sans interrompre le flux d'énergie. Cette technologie fournit une alimentation nouvelle, sûre et pour ainsi dire indépendante de l'alimentation secteur. Outre les temps de commutation qui sautent, les appareils Online présentent l'avantage d'assurer une tension constante et de filtrer le réseau. L'inconvénient de cette technologie se situe au niveau des

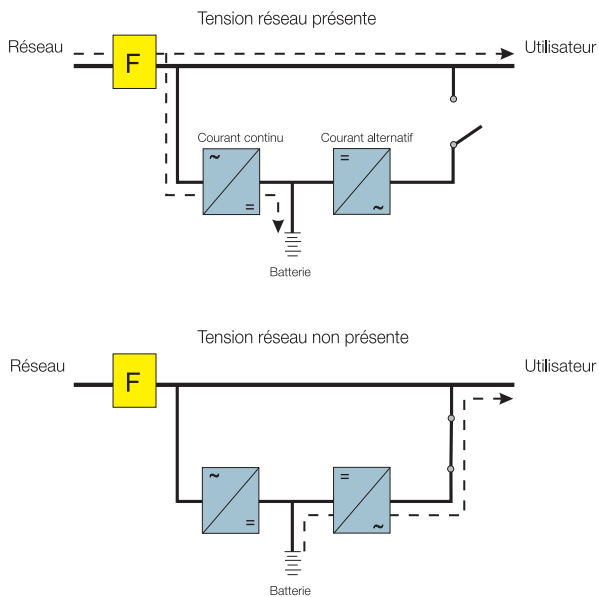
dépertitions d'énergie plus élevées qu'exige l'alimentation permanente fournie par le redresseur de courant. Le dégagement de chaleur important nécessite la présence de ventilateurs, qui sont source de bruit. Il est donc préférable d'installer les onduleurs dans des locaux informatiques.

Pour conférer à l'utilisateur toute indépendance par rapport au réseau et même par rapport à l'onduleur, les modèles courants disposent en plus d'un bypass. En cas de panne du redresseur de courant, l'appareil est coupé et l'utilisateur est ainsi directement alimenté en énergie à partir du secteur.

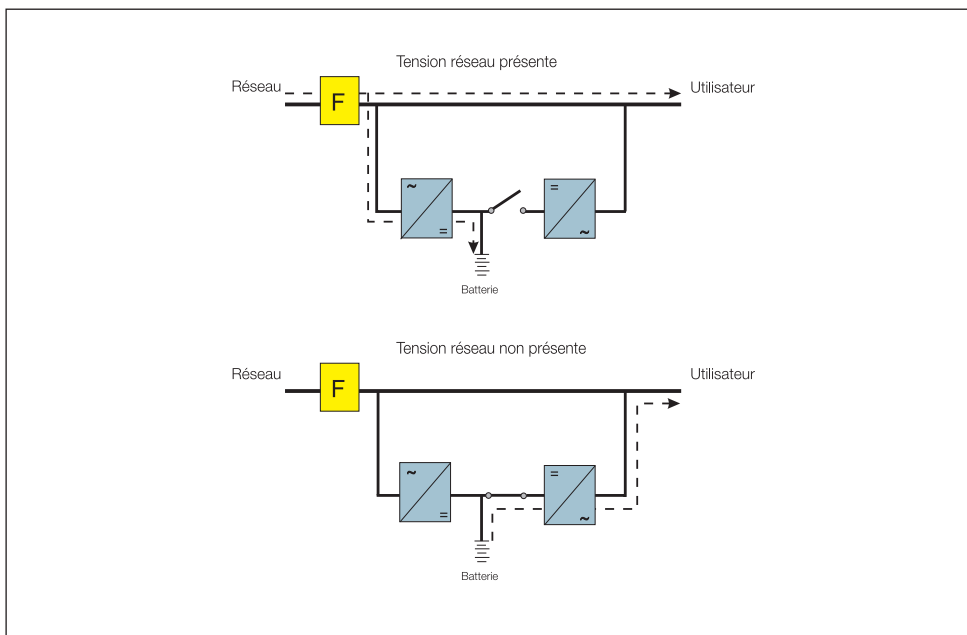
En outre, les appareils disposent d'une poignée. En effet, par simple renversement d'un bouton, ce dispositif permet d'effectuer l'échange et la maintenance de la batterie, en cours de fonctionnement, sans pour autant influencer les utilisateurs.

Faisons ici une comparaison sous forme structurée :

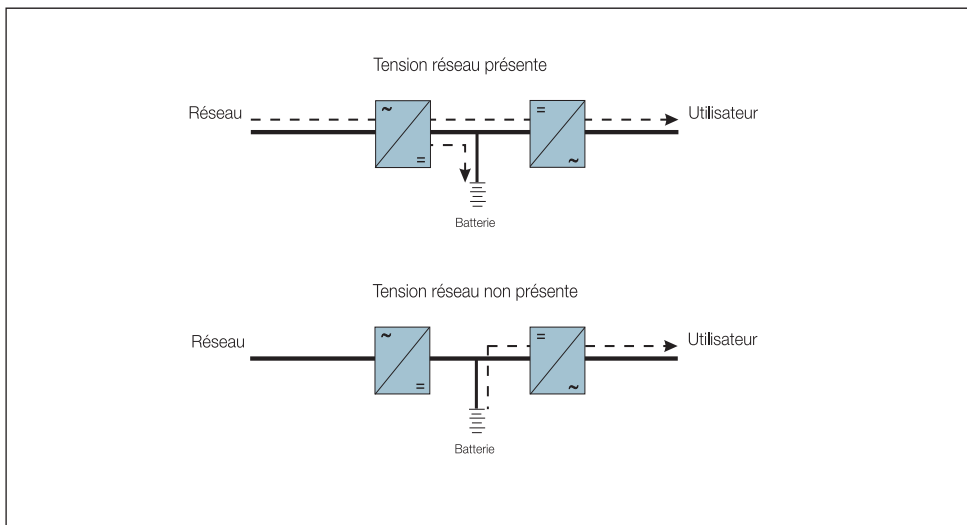
Caractéristiques	Offline (ou standby)	Line-interactive (ou conversion Delta)
Durée d'autonomie	Quelques minutes	Quelques heures
Régulation de tension	Uniquement en mode batterie	Limité
Filtrage	Limité	Limité
Régulation de fréquence	Non	Non
Coefficient d'efficacité	> 98%	> 98%
Emission de bruit	Aucune	Aucune ou très faible
Application typique		Salles informatiques



La technologie Offline



La technologie Line-Interactive



La technologie Online

24.3 Dimensionnement des onduleurs

Le dimensionnement correct s'effectue suivant la puissance en VA (VoltAmpère) indiquée sur la plaquette signalétique ou suivant le calcul de la puissance apparente pour des charges non linéaires.

Si la plaquette

signalétique indique la puissance en VA, il suffit d'additionner la puissance des différents appareils, dont notamment celle des écrans, des terminaux, des mémoires externes et des périphériques.

Si l'indication est donnée en Watt, la puissance apparente doit être calculée mathématiquement, c'est-à-dire multipliée par une constante. Pour les composants actuels les plus courants, on prend le facteur de 1,4.

Exemple de calcul : pour une plaquette signalétique indiquant une valeur de 150 W
La valeur en VA est de $150 * 1,4 = 210$

Si une extension de l'installation est prévue ou prévisible, il est judicieux de prendre tout de suite en compte les nouveaux éléments pour réajuster la capacité de l'onduleur. Il est recommandé de manière générale d'acquérir un onduleur d'une puissance supérieure de 20% à la puissance réellement nécessaire. En effet, si en raison d'une extension ultérieure la consommation en courant des appareils connectés dépasse la capacité de rendement de l'onduleur, on ne peut plus garantir une extinction normale du système. Les onduleurs sont dotés de ce qu'on appelle simplement un mécanisme d'auto-protection. En cas de surcharge importante, ce mécanisme coupe tout simplement l'appareil, avant qu'il ne puisse subir un quelconque endommagement.

Il est donc recommandé de tester à intervalles réguliers la fonctionnalité des onduleurs par rapport à tous les appareils connectés.

Comme l'onduleur ne permet généralement qu'une sécurité provisoire du système, les ordinateurs et les périphériques connectés ne peuvent être alimentés par le courant de la batterie que pour une courte durée. Cette **autonomie** de l'accumulateur doit être définie de manière à garantir la sauvegarde des données et l'arrêt des programmes en cas de défaillance complète de l'alimentation secteur. Pour des applications complexes, qui doivent tourner en permanence, il existe aussi des appareils ayant un temps d'autonomie de plusieurs heures.

L'élément essentiel de chaque onduleur est la batterie, dont la durée de vie moyenne de 3 à 5 ans est largement influencée par la température de la batterie. Les tests des constructeurs ont pu montrer qu'une augmentation de la température de service de 5 degrés Celsius suffisait à faire baisser la durée de vie des accumulateurs jusqu'à 25%.

24.4. Alarme, interfaces, communication sur le réseau

L'émission d'une alerte fournissant des informations sur les états critiques, tels qu'une panne de courant ou une défaillance de l'onduleur lui-même, doit pouvoir avoir lieu aussi bien par réseau, e-mail, pager, fax ou que téléphone GSM. Si l'onduleur émet une information, l'exécution automatique de scripts, de routines ou de séquences d'instructions prédéfinies (*.exe, *.bat, *.com, *.cmd, etc.) doit être garantie. De nombreuses options de communication permettent l'accès direct (avec restrictions selon les utilisateurs) via Internet.

Le contrôle d'un dispose onduleur devient alors possible à partir de chaque station de travail connectée au réseau. Si un réseau dispose de plusieurs onduleurs, ceux-ci peuvent être gérés sur l'ensemble du réseau par n'importe quel poste de travail autorisé.

Les messages générés par un logiciel de gestion d'onduleur peuvent être émis à des participants du réseau prédéfinis selon une grille horaire définie. Ces messages peuvent être édités et les modifications de chaque poste sont directement actives, de telle sorte qu'un redémarrage du logiciel Shutdown ou même de l'ordinateur n'est plus nécessaire. Les fonctions critiques (modifications des paramètres, redémarrage du réseau, etc.) sont protégées par mot de passe.

Si plusieurs utilisateurs réseau (serveurs, stations de travail, passerelles, concentrateurs, routeurs, etc.) d'un même système réseau sont connectés à un onduleur, il est possible de former des groupes logiques. Un calculateur relié via une interface série à l'onduleur peut ainsi faire office de contrôleur de groupe. Il met alors les informations onduleur à disposition des autres membres du groupe sur le réseau. Le logiciel Shutdown doit être installé sur tous les autres composants du réseau, ayant été définis comme membres du groupe. Le comportement des membres du groupes peut cependant être défini indépendamment du contrôleur. Ceci garantit par exemple une déconnexion séquentielle de tous ces composants du réseau.

Le test de tous les onduleurs se trouvant dans le réseau doit aussi pouvoir être initié par l'utilisateur, à partir de n'importe quelle station de travail.

Tous les événements sont enregistrés dans le fichier journal. Il est absolument nécessaire de générer un fichier journal séparé pour la batterie. En effet, la batterie étant un élément important en tant que réserve d'énergie du dispositif onduleur, il faut pouvoir analyser clairement et séparément son statut.

En général, les onduleurs sont pourvus d'une interface RS232 et très souvent aussi d'une interface USB, qui assure la connexion à l'ordinateur. Tous les onduleurs sont généralement livrés avec un logiciel Shutdown et de gestion tournant sous tous les systèmes d'exploitation courants. Les mises à jour peuvent être téléchargées gratuitement à partir de la page d'accueil de chaque constructeur. L'installation est très simple à réaliser grâce à un guidage de l'utilisateur .

24.5 Déconnexion

Les caractéristiques suivantes s'appliquent à une déconnexion réalisée par un logiciel de gestion d'onduleur :

1. Sauvegarde du contenu du cache sur le disque dur
2. Sauvegarde de l'état actuel de toutes les données ouvertes (Windows)
3. Arrêt correct de toutes les applications en cours
4. Exécution des éventuelles commandes de fond (sauvegarde de sécurité et sauvegarde de la base de données, par exemple)
5. Exécution d'un arrêt correct du système
6. Coupure correcte de l'alimentation de l'onduleur.

Il est possible dès lors de définir exactement une grille horaire de mise en route/d'arrêt des onduleurs.