ISEIG
Institut Suisse d'Enseignement
de l'Informatique
de Gestion

Les bases des réseaux et des système

Microsoft Windows 2000

ISEIG - Institut Suisse d'Enseignement de l'Informatique de Gestion
Avenue des Boveresses 52, Case postale 99
CH - 1000 LAUSANNE 21
Tél. : 021/654.40.60, Fax : 021/654.40.69, E-Mail : info@iseig.ch

Microsoft Windows 2000 Network and Operating System Essentials. Référence : 2151

A l'issue du cours : A la fin de ce cours, les stagiaires seront à même d'effectuer les tâches suivantes : décrire les principales fonctionnalités de Windows 2000 et les notions fondamentales de la gestion de réseau avec Windows 2000 ; décrire les types de comptes d'utilisateur et les principales fonctionnalités de sécurité d'un réseau Windows 2000 ; identifier les outils utilisés pour effectuer diverses tâches administratives ; décrire les fonctionnalités des protocoles couramment utilisés dans un réseau Windows 2000 ; décrire les notions fondamentales du protocole TCP/IP (Transmission Control Protocol/Internet Protocol), y compris la résolution de noms, le routage et les différences entre l'adressage IP Classful et le routage CIDR ; décrire les modèles de communication réseau utilisés sur un réseau Windows 2000 ; distinguer les différents types d'architectures de réseau ; décrire les composants physiques couramment utilisés pour les communications réseau ; décrire les concepts et les protocoles utilisés pour l'accès distant ; décrire les technologies clientes et de serveur utilisées pour accéder aux services Web.
Connaissances requises : Expérience pratique de l'interface Windows pour rechercher, créer et manipuler des dossiers et des fichiers, et pour configurer l'environnement de bureau. Connaissances générales sur les composants matériels des ordinateurs, notamment la mémoire, les disques durs et les processeurs. Connaissances générales sur les concepts des réseaux, notamment les systèmes d'exploitation réseau, les relations client-serveur et les réseaux locaux (*LAN, Local Area Network*)
Plan du cours
1 : **Présentation de Windows 2000 et de la gestion de réseau**
Sujets étudiés : Systèmes d'exploitation Windows 2000 Présentation des réseaux Implémentation de la gestion de réseau dans Windows 2000
Compétences acquises : définir un système d'exploitation ; identifier les fonctionnalités de Windows 2000 ; définir un réseau et décrire les différents types de réseaux et de systèmes d'exploitation réseau ; définir les domaines, les arborescences et les forêts ; décrire l'implémentation des services d'annuaire Microsoft Windows NT avec le service d'annuaire Active Directory de Windows 2000.
2: **Administration d'un réseau Windows 2000**
Sujets étudiés : Aide Windows 2000. Tâches administratives. Outils d'administration
Atelier : Utilisation de l'aide Windows 2000, Identification des outils d'administration
Compétences acquises : utiliser l'aide en ligne ; décrire les outils utilisés pour effectuer des tâches administratives de routine : Panneau de configuration, Propriétés système, Informations système, Observateur d'événements. Gestionnaire des tâches Windows, Performances, Imprimantes, Dossiers partagés, Gestion de disque, Sauvegarde, Gestion de la sécurité, Réseau, Microsoft Management Console
3: **Sécurisation d'un réseau Windows 2000**
Sujets étudiés : Comptes d'utilisateur, Groupes Droits d'utilisateur, Autorisations
Atelier : Analyse des utilisateurs et des groupes, Analyse des droits d'utilisateur, Analyse des autorisations de fichier et de dossier
Compétences acquises : identifier deux types de comptes d'utilisateur, à savoir les comptes d'utilisateur locaux et les comptes d'utilisateur de domaine ; décrire le rôle des groupes dans l'administration de Windows 2000 ; décrire les droits d'utilisateur qui peuvent être octroyés et les autorisations qui peuvent être affectées pour accéder aux ressources.
4: **Analyse du réseau** Sujets étudiés : Étendue des réseaux , Composants de base de la connectivité, Topologies du réseau Technologies du réseau Expansion du réseau.
Atelier : Analyse de l'architecture du réseau. Compétences acquises : décrire l'étendue d'un réseau ; décrire les composants utilisés dans un réseau ; décrire les topologies utilisées dans les réseaux ; décrire les technologies utilisées dans les réseaux ; décrire les composants utilisés pour développer un réseau.

5 : **Élaboration d'une infrastructure Active Directory pour la prise en charge d'une stratégie de groupe**. Sujets étudiés : Présentation des protocoles, Protocoles et transfert de données, Protocoles couramment utilisés Autres protocoles de communication, Protocoles d'accès distant
Atelier : Identification des capacités des protocoles
Compétences acquises : définir un protocole et décrire les types de protocoles ; nommer les protocoles réseau couramment utilisés pris en charge par Windows 2000 et décrire leurs caractéristiques ; décrire les protocoles et les technologies de communication compatibles avec Windows 2000 ; décrire les protocoles utilisés pour l'accès distant, à savoir les protocoles d'appel distant et les protocoles de réseau privé virtuel (VPN).

6 : **Analyse de TCP/IP**
Sujets étudiés : Présentation de TCP/IP, Suite de protocoles TCP/IP ,Résolution de noms , Analyse du processus de transfert de données, Routage de données,
Atelier : Utilisation des utilitaires TCP/IP, Identification des processus et des protocoles dans TCP/IP. Compétences acquises : décrire le processus de communication TCP/IP ; décrire les protocoles de la pile de protocole TCP/IP et leur fonction ; décrire le processus de résolution de noms d'ordinateur conviviaux qui consiste à les mapper sur une adresse IP ; décrire le processus d'envoi de paquets de données d'un ordinateur à un autre ; décrire la façon dont le processus de routage transmet des informations entre deux segments du réseau afin d'élargir les moyens de communication entre les ordinateurs.

7 :**Analyse de l'adressage IP**
Sujets étudiés : Adressage IP Classful, Création d'un sous-réseau, Planification de l'adressage IP
Affectation d'adresses TCP/IP
Atelier : Détermination des classes d'adresses et des masques de sous-réseau.
Identification des adresses IP valides, Analyse de la configuration de TCP/IP
Compétences acquises : définir l'adressage IP Classful et décrire les fonctionnalités de chaque classe ; décrire la procédure de création d'un sous-réseau ; décrire les problèmes relatifs à la planification des adresses IP pour un réseau ; décrire la procédure d'allocation d'une adresse IP en utilisant les outils fournis par Windows 2000.

8. **Optimisation de l'allocation d'adresses IP**
Sujets étudiés : Routage CIDR, Adresses IP binaires, Masques de sous-réseau binaires Allocation d'adresses IP à l'aide du routage CIDR . Atelier : Utilisation de la calculatrice pour la conversion des nombres au format décimal et au format binaire, Détermination des destinations locales et distantes, Allocation d'adresses IP
Compétences acquises : décrire les fonctionnalités du routage CIDR ; convertir des adresses IP du format décimal au format binaire ; calculer l'identificateur de réseau d'un masque de sous-réseau afin de déterminer les hôtes locaux et distants ; décrire l'allocation d'adresses IP à l'aide du routage CIDR.

9 : **Analyse des services Web**
Sujets étudiés : Identification des concepts d'Internet, Utilisation des technologies clientes Connexion à Internet, Identification des concepts du serveur Web
Atelier : Accès à un site FTP à l'aide de Internet Explorer. Identification des concepts du Web
Compétences acquises : décrire Internet, un réseau intranet, l'espace de noms de domaine et une URL (*Uniform Resource Locator*) ; décrire les différentes technologies clientes disponibles permettant d'accéder aux informations disponibles sur Internet ; décrire les méthodes qui permettent de se connecter en toute sécurité à Internet à partir d'un réseau Windows 2000 à l'aide de traducteurs d'adresses réseau (NAT), de serveurs proxy et de pare-feu ; expliquer comment utiliser des technologies de serveur Web, telles que Microsoft Internet Information Services (IIS), pour héberger des services sur Internet.

Organiser les ressources du LAN

Les LAN fournissent des services de deux manières : par le partage de ressources point-à-point ou par le biais du serveur central. Quelle que soit la méthode utilisée par votre serveur, le problème reste de permettre aux utilisateurs de trouver les ressources disponibles. Cette section traite de quelques techniques qui ont été utilisées pour organiser les ressources du réseau : Les services autonomes, Services d'annuaire, Groupe de travail, Domaines.

Les services autonomes (stand alone)

La grande majorité des premiers LAN ne comprenait qu'un serveur : les utilisateurs avaient donc peu de difficultés à localiser les fichiers, imprimantes et autres ressources partagées. Netware 2.x et 3.x ont été pendant longtemps les systèmes d'exploitation dominant sur le marché des petits LAN. Et les statistiques indiquent que les réseaux Novell 2.x et 3.x moyens sont composés d'un serveur unique et de 30 postes de travail au maximum.
Il y a donc peu de besoins pour un service de gestion de ressources sophistiqué. Les fichiers peuvent être trouvés en utilisant les commandes DIR du DOS et les imprimantes sélectionnées facilement à partir d'une liste. Dans la plupart des cas, les environnements LAN sont entièrement préconfigurés pour eux par l'administrateur du LAN. On donne aux utilisateurs l'accès à des imprimantes spécifiques, l'accès aux fichiers est réglé à l'avance et les utilisateurs n'ont pas besoin d'une grande connaissance du LAN pour l'utiliser.
Ajouter un deuxième serveur peut cependant compliquer énormément les choses. Le problème survient parce que chaque serveur maintient sa propre liste d'utilisateurs et de ressources. Le serveur A héberge des applications telles que Wordperfect et Lotus 1.2.3. Le serveur B héberge la messagerie de l'entreprise, les applications de comptabilité et la base de donnée des ventes. Les utilisateurs qui ont besoin d'accéder à la base de données des ventes et d'utiliser les applications doivent avoir des comptes sur les deux serveurs. Chacun de ces comptes utilisateur doit être créé et géré séparément. Notez que certains utilisateurs ont un compte sur un seul serveur. Les serveurs peuvent facilement être désynchronisés lorsqu'ils sont mis à jour manuellement.
La situation complique également les choses du point de vue de l'utilisateur. il doit s'identifier et gérer un mot de passe sur chaque serveur. Les administrateurs de réseaux avec plusieurs serveurs autonomes sont habitués à recevoir des appels pour resynchroniser les mots de passe des utilisateurs sur les différents serveurs.
Deux serveurs, c'est le maximum que vous voudriez administrer de cette manière, mais deux c'est déjà un de trop. En admettant que tous les utilisateurs aient besoin d'accéder à toutes les ressources du serveur, un compte par serveur doit être attribué sur chaque serveur. Les utilisateurs ont aussi un problème avec les serveurs autonomes multiples. Pour utiliser une imprimante, l'utilisateur doit savoir quel serveur héberge l'imprimante. Pour accéder à un fichier ou un programme, l'utilisateur doit connaître le serveur où est le fichier. A moins qu'il ne dispose d'outils conviviaux, beaucoup de ressources du réseau seront difficiles d'accès pour l'utilisateur.
Etant donné ces limitations, les concepteurs de LAN ont réalisé d'énormes investissements pour rendre les grands LAN plus faciles à gérer et à utiliser. Deux outils sont utilisés : les services d'annuaire et d' exploration.

Les services d'annuaire

Un annuaire de réseau fonctionne plus ou moins comme les pages jaunes du téléphone. Les ressources peuvent être groupées logiquement pour les rendre plus faciles à localiser. Les utilisateurs peuvent chercher dans le répertoire les informations qu'ils veulent ou ils peuvent browser de façon intelligente. Les services d'annuaire peuvent être utilisés pour organiser les ressources dans les grands LAN. Plusieurs approches sont possibles :
X.500 est un standard international de service d'annuaire. Il n'est pour l'instant installé dans aucun produit LAN.

Netware Directory Services (NDS) est inclus dans la ligne de produits Novell's Netware 4.x. NDS est basé sur X.500 mais n'est pas totalement compatible avec le standard. A l'heure actuelle NDS ne peut être utilisé qu'avec les réseaux Netware 4.x.
Le concept de service d'annuaire est attractif. Au lieu de se connecter auprès de plusieurs serveurs, un utilisateur se connecte sur un réseau et l'accès aux ressources lui est accordé par le biais du service d'annuaire quel que soit le serveur fournissant le service. L'utilisateur voit un service d'annuaire sans indication de quel serveur supporte le compte utilisateur. Un service d'annuaire est un moyen très formel d'organiser les ressources du réseau. Mettre en place un tel service nécessite un planning précis qui implique tous les départements de l'organisation. Et les services d'annuaire fonctionnent mieux lorsqu'un seul service est responsable de la maintenance du répertoire. Certains services d'annuaire permettent à des départements d'être responsable pour une section du répertoire, mais un seul département doit prendre la responsabilité principale. Dans des organisations qui n'ont pas de département informatique centralisé, il peut être difficile d'identifier un responsable de répertoire principal.
Dans beaucoup d'organisations, des LAN ont été mis en place dans les départements bien avant d'être découverts par les départements informatiques. Les départements mettant en place des LAN sont souvent réticents à l'idée d'abandonner le contrôle et préfèrent garder la responsabilité de la gestion de leurs ressources LAN. Mettre en place un service d'annuaire dans une entreprise qui a des réseaux bien établis peut apparaître comme une menace pour l'autonomie du département et peut causer des difficultés dans les politiques d'entreprise. Dans la plupart des cas, les utilisateurs qui sont authentifiés auprès d'une structure de répertoire ne peuvent accéder à des ressources contrôlées par une autre structure de répertoire, ce qui rend la coopération inter-départements essentielle. Les administrateurs d'un service d'annuaire ont besoin de plus de compétences que les administrateurs de réseaux autonomes.

Les groupes de travail
Les groupes de travail sont les opposés conceptuels des services d'annuaire. Les annuaires sont formels et administrés de façon centrale ; les groupes de travail sont informels et gérés par des utilisateurs qui mettent en commun leurs ressources.
Avec une approche réseau point à point, les utilisateurs partagent les ressources de leur ordinateur avec d'autres utilisateurs. Ils peuvent autoriser les autres à imprimer sur leur imprimante, à accéder à leurs fichiers ou à partager un modem ou un cédérom. Les utilisateurs individuels gèrent le partage des ressources sur leur PC en choisissant ce qui sera partagé et qui aura une autorisation d'accès.
Le réseau point à point rencontre deux problèmes dans les grandes organisations :
Il y a tant de ressources disponibles que les utilisateurs peuvent avoir des difficultés à les localiser.
Les utilisateurs qui veulent partager des ressources ont souvent besoin d'un moyen facile de partager des ressources avec seulement un groupe limité de collègues.
Après l'arrivée de quelqu'un dans un groupe de travail, celui-ci doit pouvoir accéder à toutes les ressources qui sont partagées dans ce groupe de travail. Vous pouvez partager votre disque dur avec vos collègues de travail simplement en donnant à votre groupe de travail droit à votre imprimante. Une boîte de dialogue permet au propriétaire de l'imprimante d'attribuer un mot de passe qui peut être utilisé pour restreindre l'accès à des individus spécifiques. Sans mot de passe, n'importe quel membre du groupe de travail peut utiliser l'imprimante. C'est la seule sécurité offerte par Windows pour Workgroups. Pour localiser les ressources sur un réseau, Microsoft utilise les services d'exploration. Sous Windows NT 4.0 ou Windows 95, le voisinage réseau ou l'explorateur de Windows peuvent être utilisés pour naviguer sur le réseau et identifier les ressources auxquelles se connecter.
Les groupes de travail sont plus pratiques que quoi que ce soit d'autre. Ils rendent le partage des ressources plus efficace, mais ils n'organisent pas les services en annuaires. Ils ne facilitent pas non plus l'efficacité de la gestion des ressources partagées. Les mots de passe peuvent être utilisés pour limiter l'accès à des ressources, mais avec un mot de

passe pour chaque ressource, la prolifération des mots de passe est rapide. Lors du changement de mot de passe, toute personne qui utilise les ressources doit être avertie. Si chaque ressource a un mot de passe différent, les choses commencent réellement à se compliquer. Il est difficile de maintenir la sécurité dans de telles circonstances. Quand des mots de passe séparés sont attribués par des utilisateurs individuels, le nombre de mots de passe qu'un utilisateur individuel doit mémoriser peut augmenter rapidement. Pour faciliter les choses, les utilisateurs ont tendance à sélectionner des mots de passe qui sont facile à mémoriser, mais de tels mots de passe sont également faciles à deviner. Pour rendre les choses encore plus difficiles, imaginez que l'on puisse se connecter au réseau à distance et qu'un employé viennent de démissionner pour aller chez votre principal concurrent. Vous allez devoir changer tous les mots de passe pour que l'employé ne puisse pas pénétrer le réseau et obtenir des informations. Il est évident que changer tous les mots de passe et informer tout le monde du changement va être une lourde tâche.

Les Domaines

Les domaines empruntent leur concept à la fois aux groupes de travail et aux services d'annuaire. Comme les groupes de travail, les domaines peuvent être relativement informels et être administrés en utilisant un mélange de contrôles centralisés et locaux. Les domaines peuvent évoluer relativement facilement et peuvent être installés avec moins de planification que ce qui est généralement requis par un annuaire. Comme un annuaire, un domaine organise les ressources de plusieurs serveurs en une seule structure administrative. On attribue aux utilisateurs une autorisation d'accès à un domaine plutôt qu'à chaque serveur individuel. Parce que un domaine contrôle les ressources de plusieurs serveurs, c'est plus facile à administrer qu'un réseau avec plusieurs serveurs autonomes. Les serveurs à l'intérieur du domaine rendent public leurs services aux utilisateurs. Les utilisateurs qui s'authentifient auprès d'un domaine accèdent ainsi à toutes les ressources du domaine pour lesquelles ils ont l'autorisation d'accès. Ils peuvent explorer les ressources dans un domaine comme ils exploreraient les ressources dans un groupe de travail. Les domaines, cependant, sont hébergés par Windows NT Servers et peuvent être plus sécurisés que les groupes de travail. Quand les réseaux deviennent suffisamment grands pour nécessiter plusieurs domaines, les administrateurs peuvent établir des relations d'approbation (Trust relationships) entre les domaines. Les relations d'approbation simplifient l'administration parce que un utilisateur n'a besoin que d'un compte sur un domaine. Les autres domaines qui approuvent le domaine où se connecte l'utilisateur peuvent se fier à cette authentification. Les domaines Windows NT Server ne sont pas les mêmes que les domaines rencontrés sur les réseaux TCP/IP.

Domaines et relations d'approbation

Les domaines sont essentiellement des groupes de travail améliorés. L'accès aux ressources du domaine est contrôlé par un contrôleur de domaine. Il est attribué à l'utilisateur un unique compte sur le domaine et un mot de passe qui est utilisé pour contrôler l'accès à toutes les ressources du domaine. Les domaines de Windows NT Server supportent également l'utilisation de groupes ce qui permet aux administrateurs d'attribuer et de modifier les permissions pour de grands nombres d'utilisateurs plus efficacement.

Les domaines et les serveurs de domaines

Un serveur dans un domaine joue l'un des trois rôles suivants :
Contrôleur principal de domaine (PDC). Un serveur Windows NT stocke la copie de la base de données des utilisateurs et des groupes du domaine. Le PDC est responsable de la synchronisation de la base de données des comptes avec tous les BDC (Contrôleur secondaire de domaine).
Contrôleur secondaire de domaine (BDC). D'autres serveurs Windows NT peuvent stocker des copies de sauvegarde de la base de données des utilisateurs et groupes du domaine.
Serveur membre ou autonome. Les serveurs membres participent à un domaine sans être désignés comme contrôleurs principaux ou secondaires du domaine.

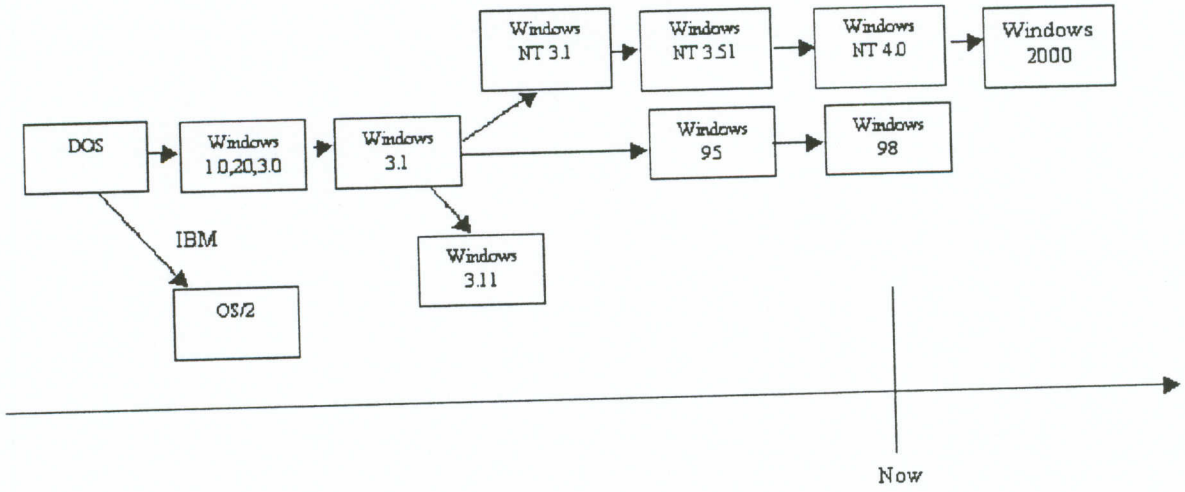
Le contrôleur principal de domaine.
Le premier serveur Windows NT est configuré en tant que contrôleur principal de domaine (PDC). L'utilitaire gestionnaire d'utilisateur de domaine (User Manager for Domains) est utilisé pour gérer l'information utilisateur et groupe pour le domaine. Cette information est stockée dans une base de données de sécurité du domaine située sur le contrôleur principal de domaine.

Les contrôleurs secondaires Windows NT de domaine
D'autres serveurs Windows NT dans le domaine peuvent servir de contrôleurs secondaires de domaine (BDC). Chaque BDC stocke une réplique de la base de données sur le contrôleur principal de domaine qui est répliquée périodiquement pour distribuer les changements opérés sur la base de données principale sur le PDC. La réplication de la base de données a plusieurs avantages. Si le contrôleur principal de domaine a un problème matériel, l' administrateur peut promouvoir un contrôleur secondaire au rang de contrôleur primaire. Chaque domaine Windows NT devrait avoir au moins un BDC. Lorsqu'un utilisateur se connecte à un domaine, la requête de connexion peut être gérée par tout contrôleur principal ou secondaire du domaine. Cela répartit la charge de connexion entre les serveurs disponibles et améliore les performances.
Des modifications ne peuvent être apportées à la base de données du domaine que si le PDC fonctionne. Si le PDC tombe en panne ou est arrêté pour maintenance, vous pouvez utiliser un BDC en tant que PDC. La promotion doit être faite par un administrateur.

Les serveurs
Les ordinateurs faisant tourner Windows NT Server peuvent aussi fonctionner comme des serveurs autonome dans un Workgroup ou membre d'un domaine. Ces serveurs ne fonctionnent pas comme des contrôleurs. Ils peuvent cependant tirer parti des bases de données utilisateurs et groupe qui sont gérées pour un domaine et vous pouvez attribuer des permissions utilisateurs et groupe pour le serveur avec le gestionnaire d'utilisateur pour les domaines.
Le serveur peut également gérer sa propre base de données d'utilisateurs et les utilisateurs peuvent se connecter au serveur indépendamment du domaine. Dans ce cas là, le serveur ne peut utiliser la base de données utilisateur et groupe d'un domaine et le serveur gère les comptes de la même manière que des ordinateurs faisant tourner Windows NT Workstation.
Vous pouvez choisir de configurer un serveur membre autonome Windows NT pour plusieurs raisons. Le serveur peut être administré par différents membres de l'équipe. Beaucoup de serveurs Windows NT sont utilisés comme serveurs d'applications, telles que les bases de données SQL. Si vous configurez un serveur de base de données comme serveur indépendant, vous pouvez désigner un membre de votre équipe en tant qu'administrateur de serveur. Gérer les requêtes de connexion peut utiliser une part importante des capacités du serveur. Si vous configurez le serveur en tant que serveur indépendant, il peut se concentrer sur une seule tâche, telle que fournir des services d'applications.

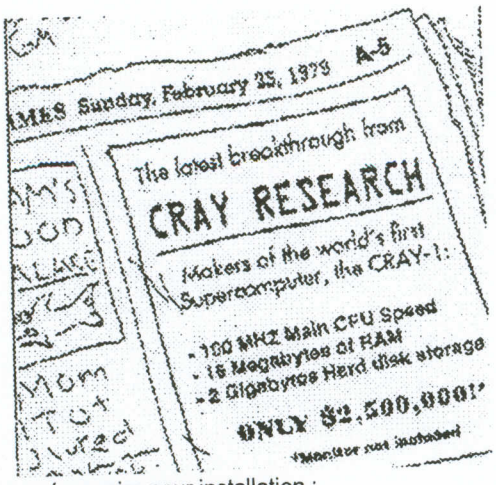
Synchroniser la base de données de l'annuaire de domaine
Tous les changements sur la base de données de l'annuaire de domaine NT sont effectués d'abord sur le PDC, et ensuite distribués au BDC par un processus appelé synchronisation. Dans un domaine Windows 2000 tous les contrôleurs de domaine Windows 2000 sont des PDC. Le service NetLogon se charge de la synchronisation de la base de données du domaine. Par défaut, le service NetLogon synchronise les BDC à 5 minutes d'intervalle.

Windows 2000 Professional et Windows 2000 Server



Configuration minimale suivante pour Windows 2000 Serveur:
Microprocesseur Pentium 166 MHz ou supérieur. Une nouvelle installation de Windows 2000 Server prend en charge des ordinateurs équipés d'un ou de deux microprocesseurs. (Si vous mettez à niveau un ordinateur qui exécutait Windows NT Server avec quatre microprocesseurs au maximum, ceux qui étaient pris en charge auparavant continueront à l'être par Windows 2000 Server.)
Windows 2000 Advanced Server prend en charge quatre microprocesseurs au maximum.
64 mégaoctets (Mo) de mémoire vive au minimum ; 128 Mo recommandés, 8 gigaoctets (Go) au maximum.
2 Go d'espace disque avec au moins 850 Mo d'espace libre. Il est possible que davantage d'espace soit nécessaire, en fonction des critères suivants :
Les composants installés : plus leur nombre est élevé, plus l'espace disponible doit être important.
Le système de fichiers utilisé : le système FAT nécessite 100 à 200 Mo d'espace disque libre supplémentaire, car il stocke les fichiers moins efficacement que FAT32 ou NTFS.
Si l'ordinateur dispose de plus de 64 Mo de mémoire vive : 1 Mo d'espace disque supplémentaire doit être prévu pour chaque Mo de mémoire au-dessus des 64 Mo.
Une installation via le réseau exige 100 à 200 Mo d'espace supplémentaire.
Une mise à niveau peut demander beaucoup plus d'espace qu'une nouvelle installation, car la taille de la base de données des comptes d'utilisateur augmentera sensiblement durant la mise à niveau, avec l'ajout de l'annuaire Active Directory.
Écran VGA ou de résolution supérieure. Clavier. Souris (facultatif).
Pour une installation à partir d'un CD-ROM :
Lecteur de CD-ROM (12x ou plus rapide recommandé).
Lecteur de disquette haute densité 3,5 pouces, sauf si votre lecteur de CD-ROM est amorçable et prend en charge le démarrage du programme d'installation à partir d'un CD-ROM.
Pour une installation en réseau :
Une ou plusieurs cartes réseau compatibles Windows 2000 Server, avec les câbles appropriés (consultez la Liste du matériel compatible (en anglais) Hcl.txt dans le répertoire \Support du CD-ROM de Windows 2000 Server).
Consultez la Liste du matériel compatible de Windows 2000 Server — le fichier Hcl.txt dans le répertoire \Support du CD-ROM de Windows 2000 Server ou http://www.microsoft.com/hwtest/hcl (Notez que le bus microchannel n'est plus pris en charge.)

Windows 2000 Professionnel et 2000 Serveur



	2000 Professional	2000 Server
Minimum nécessaire pour installation :	Pentium 166 32 Mb	Pentium 166 64 Mb
Taille du disque / espace libre	2Go / 650 Mb	4Go / 850 Mb
Mise a jour possible depuis :	Windows 95 et 98 Windows NT Workstation 3.51, Windows NT Workstation 4.0	Windows NT Serveur 3.51, Windows NT Serveur 4.0
Protection exhaustive contre les arrêts inopinés des applications 16 bits par exécution de ces dernières dans des espaces adresse distincts	Oui	Oui
Tolérance de panne disque : (Miroir, Duplexing, RAID5	Non	Oui
Profils utilisateurs sécurisés pour la maîtrise de l'accès aux machines, aux applications et aux fichiers de configuration système	Oui	Oui
Support de systèmes de fichiers	FAT, FAT32, NTFS NTFS5 (Cryptage) Oui	FAT, FAT32, NTFS NTFS5 (Cryptage) Oui
Protection des données grâce au système de fichiers transactionnel	Non	Non
Exécution de toutes les applications MS-DOS	Oui	Oui
Support de systèmes de fichiers FAT, FAT32 et NTFS	10	Illimité
Nombre des clients supporté	NON : seulement Protocole Appletalk	OUI : Services pour Macintosh
Services for Macintosh	Client seulement	DNS, WINS,DHCP
Serveur DNS, WINS, DHCP	Poste à poste	Internet Information Server
http. ftp,	1 client seulement	256 clients
Nombre des clients RAS (Serveur d'accès distant distant) supportés :	Non	Non
Exécution des gestionnaires de périphériques MSDOS ou 16 bits	2	2 (mais 4 si mise à jour)
Support des configurations **multiprocesseur**		

Préparation de l'installation

- supprimer toutes les partitions avec la commande FDISK
- créer une partition principale de 2 Go.
- activer et formater cette partition avec la commande FORMAT C : /S

(La partition active est appelé PARTITION SYSTEME sous Windows NT)

- est-il possible de créer une 2e partition principale a l'aide du FDISK ?
  Réponse _____

Deux méthodes peuvent être utilisées :

1. **Installer 2000 depuis un répertoire déjà partagé sur un Serveur** (réseau compatible DOS comme: Novell ou NT). Dans ce cas une disquette de démarrage réseau doit être crée a l'aide de l'Administrateur client réseau. L'installation peut être automatisé. Remarques :
WINNT est un exécutable d'installation destiné aux machines Dos et Windows 3.x.
WINNT32 est destiné pour effectuer une mise a jour sur les machines fonctionnant déjà sous Windows NT ou Windows 9x
Smartdrv peut accélérer l'installation d'une façon spectaculaire pour les machines MSDOS.

2. **Booter sur le CDROM** permet de créer une partition FAT16 de moins de 2 GO, FAT32 de moins de 32 GO ou NTFS
(Windows NT 4 n'est pas compatible avec FAT 32 de OSR2 et Windows 98 !)
Pour savoir sur quelle type de FAT Windows 9x est installé : Poste de travail, Cliquez du bouton droit sur le disque C : et sélectionnez Propriétés. Dans l'onglet Général, le champ type précise FAT 16 ou FAT 32.

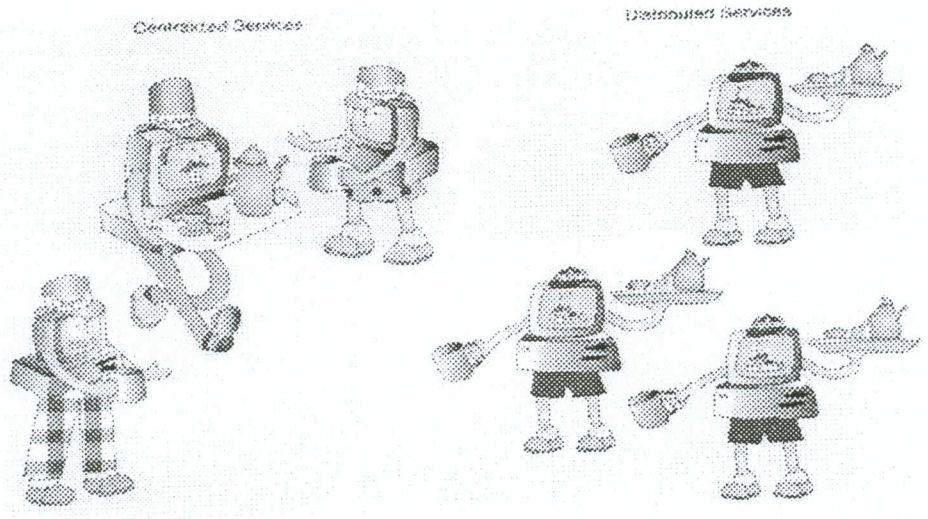
Taille de partition	FAT 16 16 bits = 65636 Clusters taille des clusters :	FAT 32 Win 95OSR2, 98 Windows 2000	NTFS Windows NT et 2000 taille des clusters :
65 à 128 Mo	2 Ko	2 Ko	512 octets
129 à 255 Mo	4 Ko	4 Ko	512 octets
256 à 511 Mo	8 Ko	4 Ko	512 octets
512 à 1023 Mo	16 Ko	4 Ko	1 Ko
1024 à 2047 Mo	32 Ko	4 Ko	2 Ko
2048 à 4095 Mo	64 Ko NT	4 Ko	4 Ko
4 à 8 Go	Impossible	4 Ko	8 Ko
8 à 16 Go	Impossible	8 Ko	16 Ko
16 à 32 Go	Impossible	16 Ko	32 Ko
Au-delà de 32 Go	Impossible	Impossible	64 Ko

Windows 95OSR2, Windows 98 et Windows 2000 utiliseront le même format de FAT ou FAT32. Windows 95 et Windows NT4.0 peuvent cohabiter seulement sur une partition FAT16 de maximum 2048 Mb.
Windows 2000 formate :
Un contrôleur de domaine Windows 2000 nécessite une partition NTFS.
Pour faire une mise a jour insérez le CDROM dans le lecteur de CDROM et suivez les instructions.

Réseaux Locaux

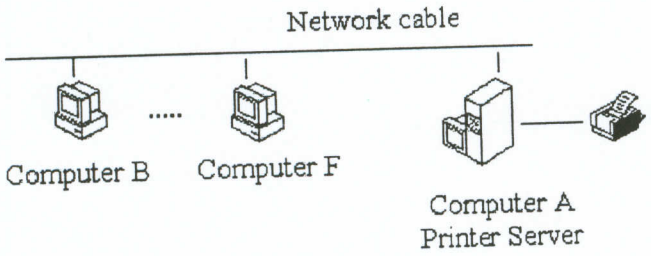
Réseau organisé autour de serveurs
Les rôles sont strictement définis.

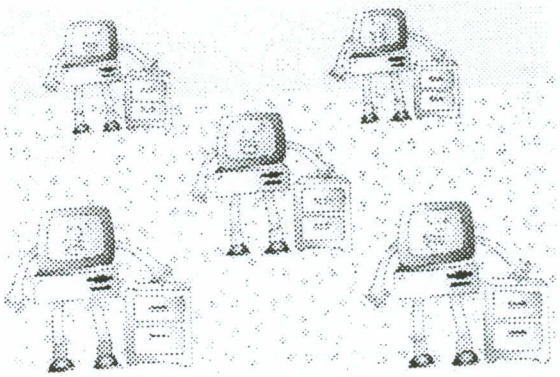
Réseau d'égal à égal, d' homologues
ou Peer to Peer

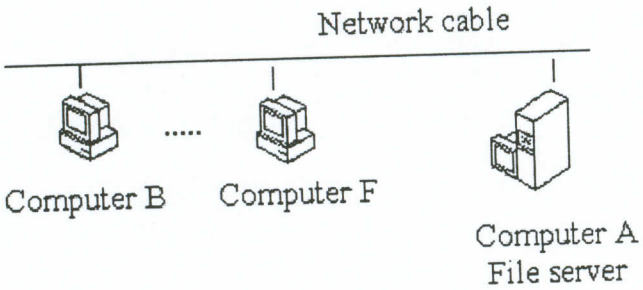


Chaque client est serveur en même temps
Gestion des utilisateurs et de la sécurité centralisé
Mise à disposition des ressources, Sauvegarde facile
Un serveur dédié est nécessaire

Chaque utilisateur défini sa propre sécurité
Aucune personne responsable du système
n'est nécessaire pour administrer le réseau.

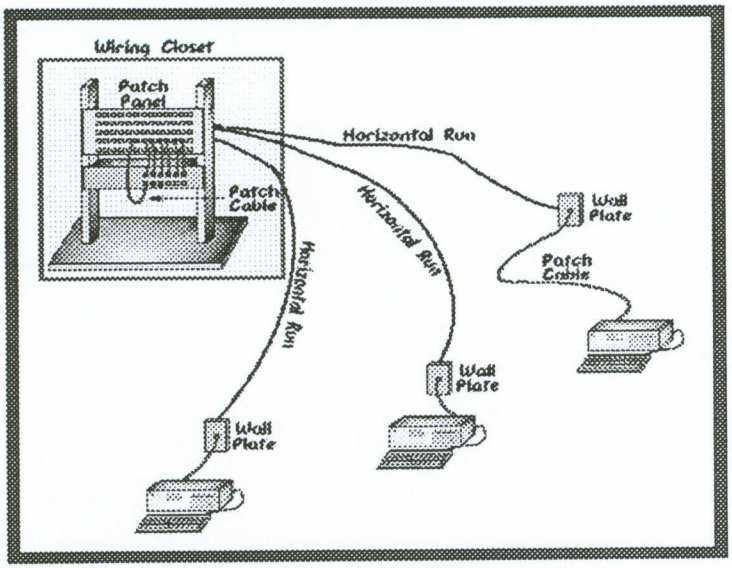


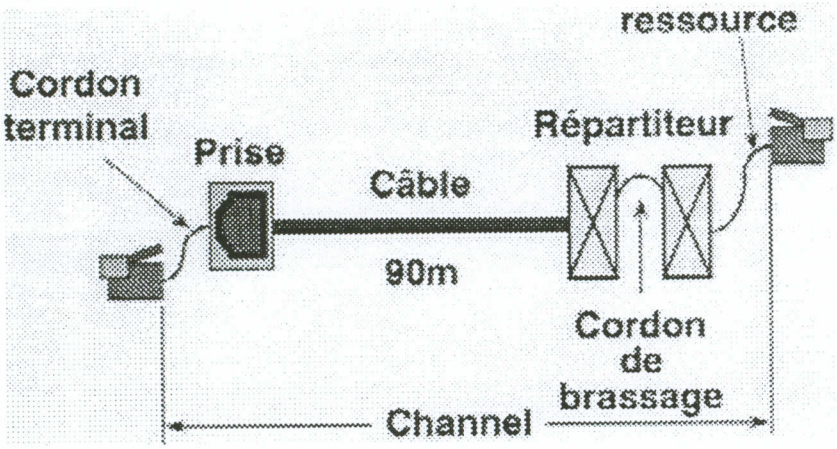




Câblage réseau

STRUCTURED CABLING





Cordon de brassage

Principaux types de câbles

Cables

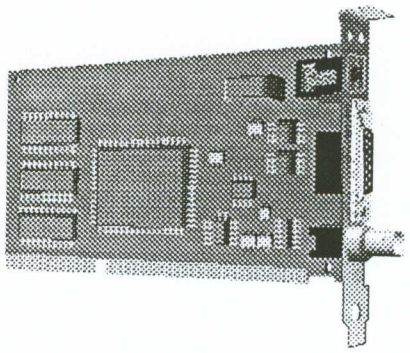
	Twisted-pair cable	Fiber-optic cable	Stacking cable	Thin (fin) coaxial cable	Thick (gros) coaxial cable
Description du câble	Copper, 4 or 25 twisted pairs	Glass, 2 fibre	Propriétaire	Cuivre, 2 conducteurs, 5-mm diamètre	Cuivre, 2 conducteurs, 10-mm diamètre
Connector type	RJ-45 or 50-pin telco	ST or SC	Propriétaire	BNC	N-series
Maximum segment length	10Base-T, Cat 3, 4, 5:100 m, 100Base-TX, Cat 5: 100 m, 100VG, Cat 3, 4: 100 m, 100VG, Cat 5: 200 m	10Base-F: 1000 m 100Base-FX: 2000 m 100VG fiber: 2000 m	Depends on product, usually around 30 cm	10Base2: 185 m	10Base5: 500 m
Maximum connections per cable	2	2	Switching Hubs: 8	30	100
10-Mbit/s operation	Oui*	Oui	Oui	Oui	Ouis
100-Mbit/s operation	Oui*	Oui	Oui	Non	Non
Noise immunity	Good	Excellent	Good	Good	Very Good
Security	Moderate	Excellent	Good	Moderate	Moderate
Reliability	Good	Good	Good	Moderate**	Good
Ease of installation	Excellent	Good	Excellent	Good	Poor
Ease of troubleshooting	Excellent	Excellent	Excellent	Good	Good
Ease of administration	Excellent	Excellent	Excellent	Poor	Poor
Cost per connection	**Très faible**	High	Included with hub: none	Lower	Moderate
Meilleur usage	Câblage des groups de travail	Long backbone, between wiring closets, between buildings	workgroup cabling	Backbone in wiring closet	Existing installations

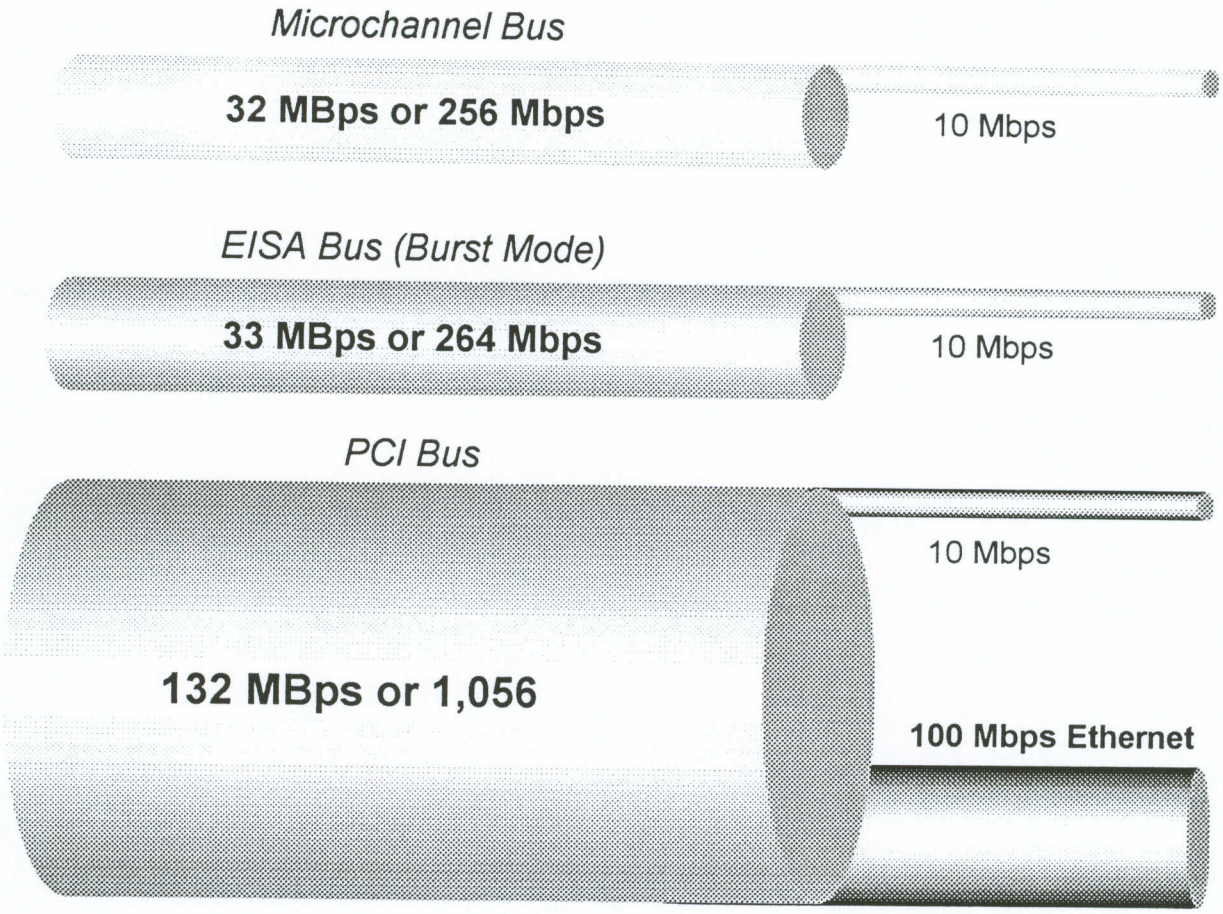
***10Base-T (10 Mbit/s) and 100VG-AnyLAN (100 Mbit/s) signals should not be transmitted within the same 25-pair bundled cable.**

****Le câble Ethernet fin est fiable mais pas les connecteurs sont très difficiles a installer..**

Le câble UTP Catégorie 5 est le moins cher de tous les câbles !

Cartes réseau
Rôle de la carte réseau
Options et paramètres de configuration, compatibilité
Performances du réseau
Cartes réseaux spécialisées





1 Megabyte (MBps) = 8 Megabits

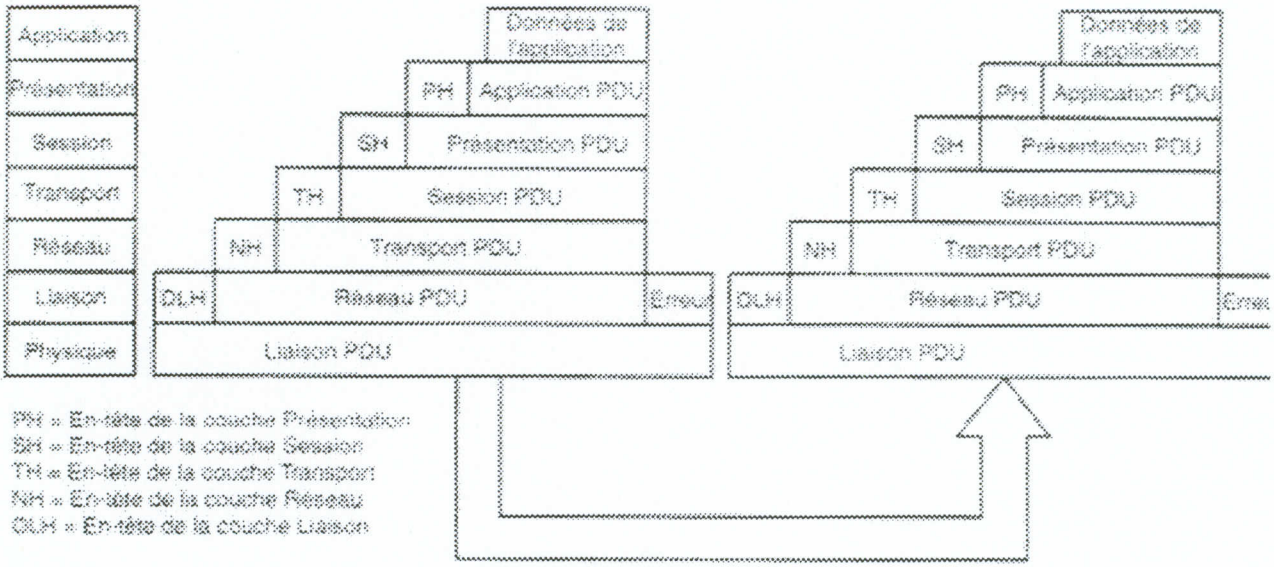
IRQ	Périphérique XT	Périphérique AT
0	Compteur (Timer)	Compteur (Timer)
1	Clavier	Clavier
2	Libre	Cascade en ligne depuis IRQ9
3	COM2	COM2. COM4
4	COM1	COM1. COM3
5	Disque dur	LPT2
6	Lecteur de disquettes	Lecteur de disquettes
7	LPT1	LPT1
8	Non-disponible	Horloge en temps réel
9	Non-disponible	Libre
10	Non-disponible	Libre
11	Non-disponible	Libre
12	Non-disponible	Souris BUS ou PS/2. sinon libre
13	Non-disponible	Coprocesseur
14	Non-disponible	Disque IDE 1 et 2. sinon libre
15	Non-disponible	Disque IDE 3 et 4. sinon libre

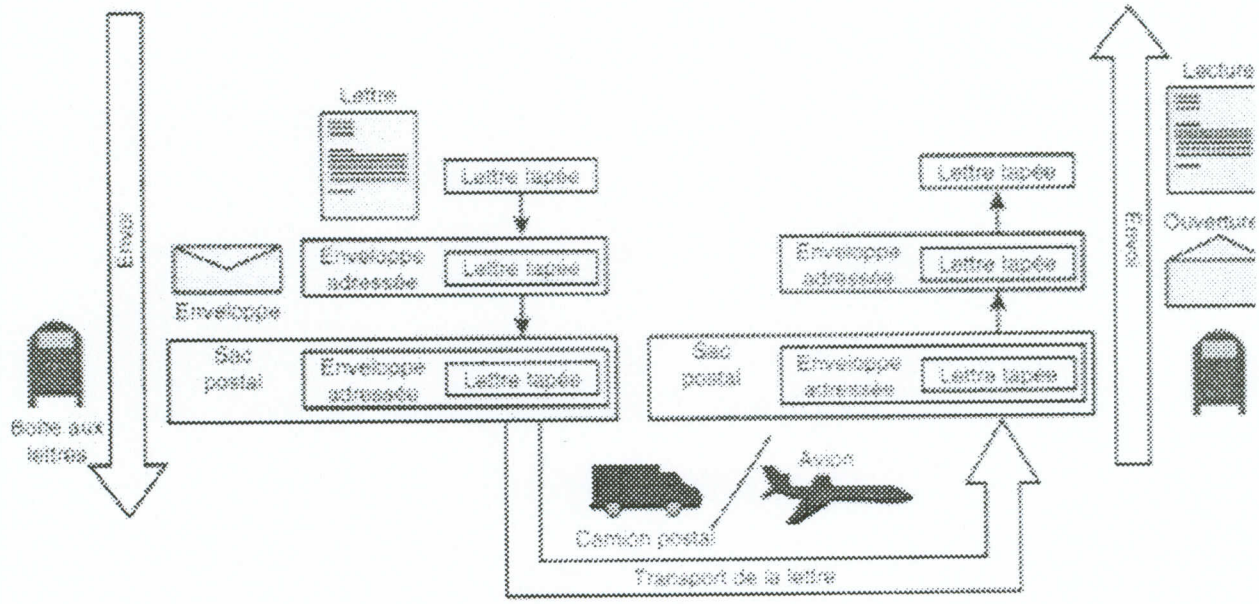
Canal DMA	Largeur	XT	AT
0	8	Rafraîchir la mémoire	Rafraîchir la mémoire
1	8	Libre	Libre
2	8	Lecteur de disquettes	Lecteur de disquettes
3	8	Disque dur	Libre
4	16	Non-disponible	Cascade en ligne des chips DMA
5	16	Non-disponible	Disque dur des PS/2, sinon Libre
6	16	Non-disponible	Libre
7	16	Non-disponible	Libre

Adresses de ports XT/AT	XT	AT
Contrôleur DMA no.1 (8237A-5)	000-00F	000-01F
Contrôleur d'interruption no.1	020-021	020-03F
Temporisateur/Compteur (Timer. 18.2 fois/sec)	040-043	040-05F
Interface périphérique programmable (PPI 8255A-5)	060-063	-----
Clavier (8042)	-----	060-06F
Horloge en temps réel (MC 146818)	-----	070-07F
Registre de page DMA	080-083	080-09F
Contrôleur d'interruption no.2	080-083	080-09F
Contrôleur DMA no.2 (8237A-5)	-----	0C0-0DF
Coprocesseur mathématique	-----	0F0-0F1
Coprocesseur mathématique	-----	0F8-0FF
Contrôleur de disque dur	320-32F	1F0-1F8
Manette de jeux	200-20F	200-207
Unité d'extension	210-217	-----
Carte de son	-----	220-22F
LPT2	-----	278-27F
COM4	-----	2E8-2EF
COM2	2F8-2FF	2F8-2FF
Carte de prototype	300-31F	300-31F
Interface MIDI sur carte de son	-----	330-33F
LPT1	378-37F	378-37F
LPT1 sur carte vidéo MDA	3B0-3BF	3B0-3BF
Carte vidéo couleur	3D0-3DF	3D0-3DF
COM3	-----	3E8-3EF
Contrôleur de disquettes	3F0-3F7	3F0-3F7
COM1	3F8-3FF	3F8-3FF

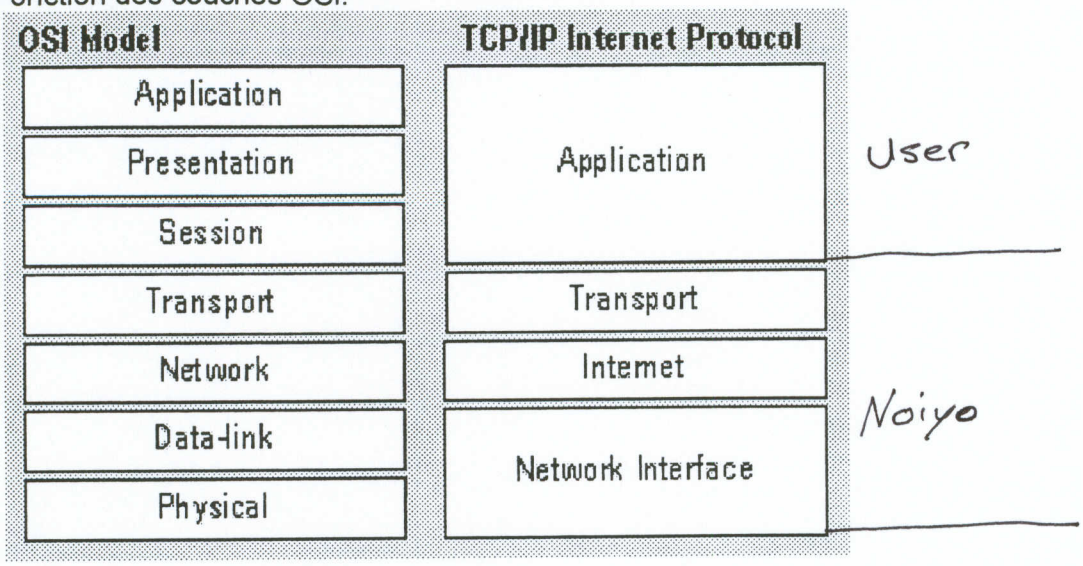
Fonctionnement d'un réseau
Modèles OSI et IEEE 802

Les couches de l'architecture OSI

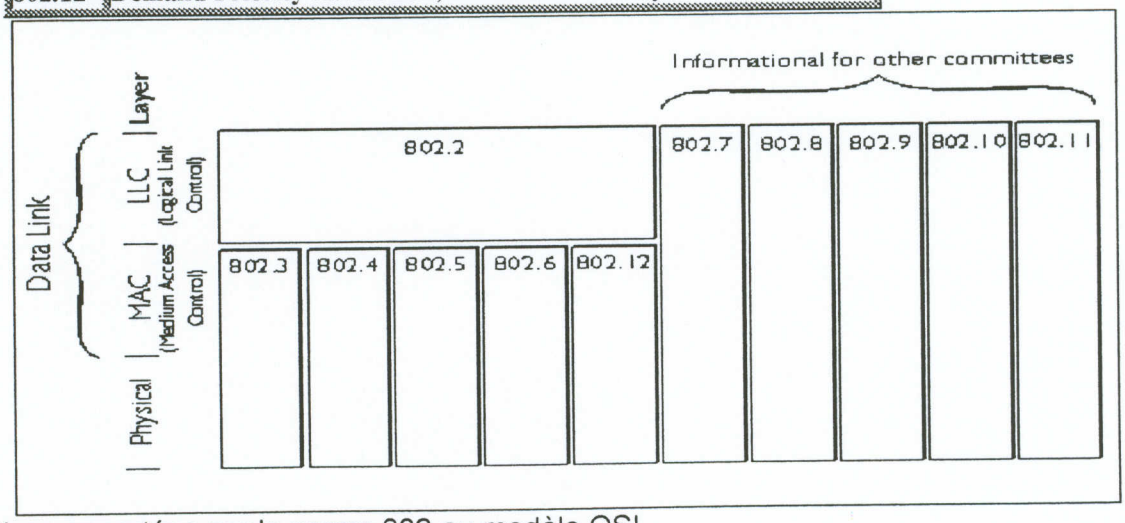




Modèle 802, Fonction des couches OSI.



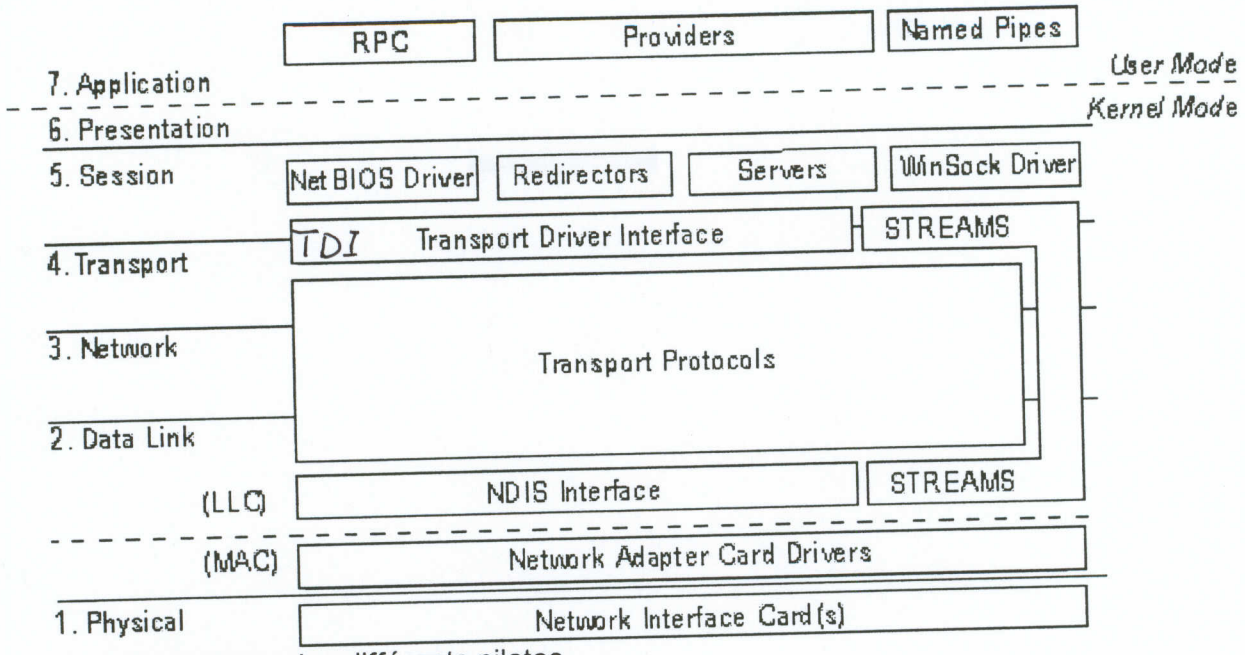
802.1	Internet working (802.1p =QoS)
802.2	Division of Data Link Layer into sublayers • LLC (Logical Link Control) • Media Access Control (MAC)
802.3	CSMA/CD - **Ethernet**
802.4	Token Bus LAN (ARCnet)
802.5	**Token Ring** LAN
802.6	MAN (Metropolitan Area Network)
802.7	Broadband Technical Advisory Group
802.8	Fiber-Optic Technical Advisory Group
802.9	Integrated Voice/Data Networks
802.10	Network Security
802.11	Wireless Networks
802.12	**Demand Priority** Access Lan, 100 Base VG - AnyLAN



Améliorations apportées par la norme 802 au modèle OSI.

Pilotes

Mise en place
Rôle des pilotes dans un environnement réseau, y compris leur place dans le modèle OSI.



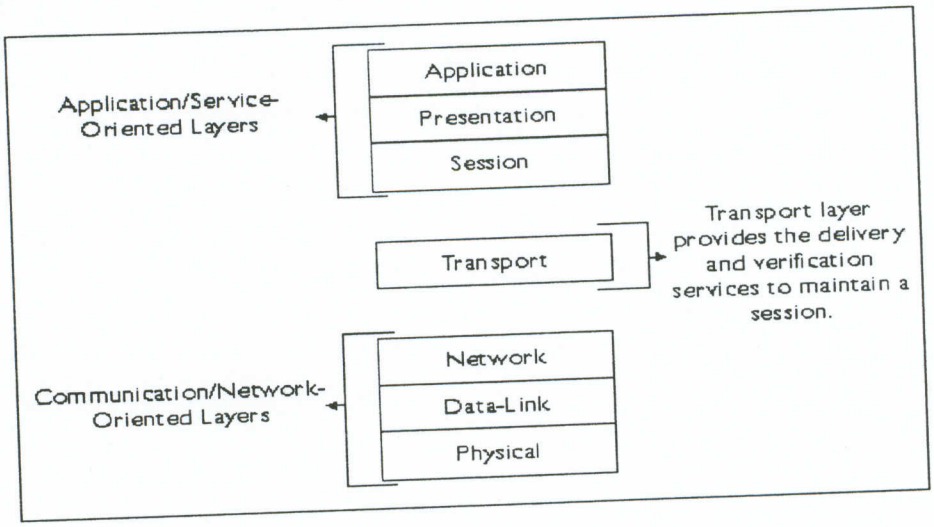
Identifier les sources des différents pilotes.

Sélection et mise en place de pilotes pour un réseau donné.

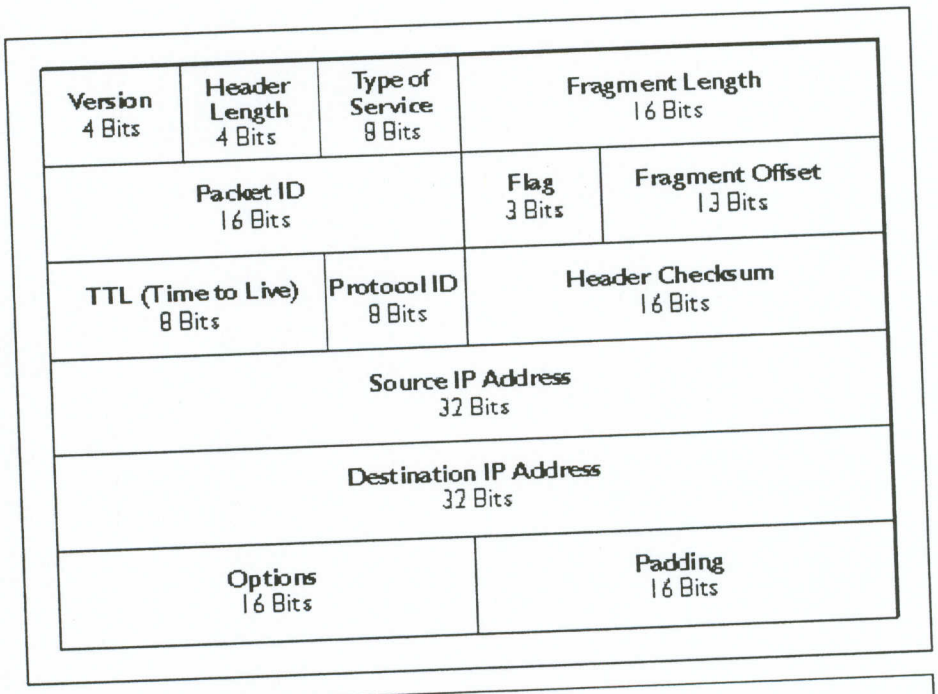
Installer, mettre à jour et retirer des pilotes.

Envoi de données sur le réseau

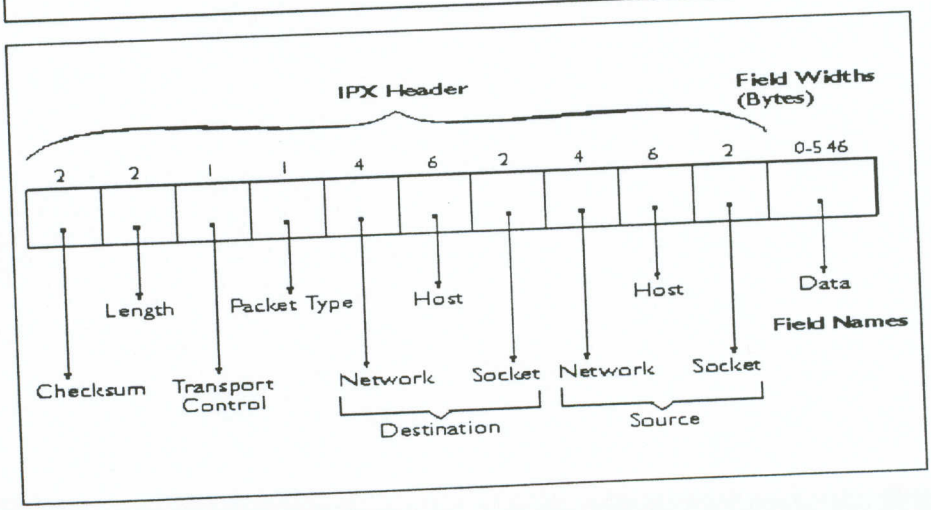
Fonction des paquets



La structure de l'entête IP

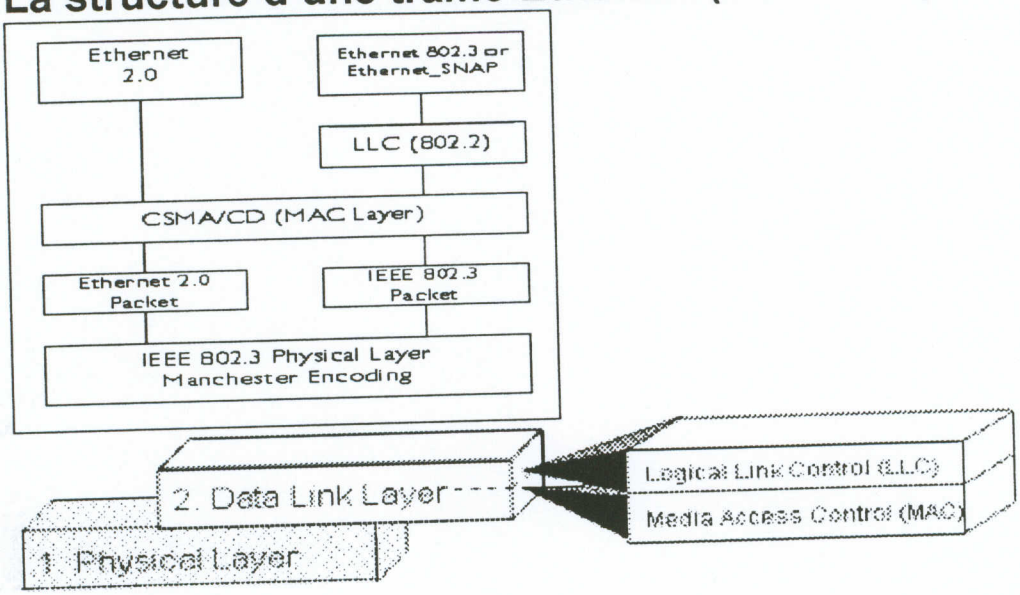


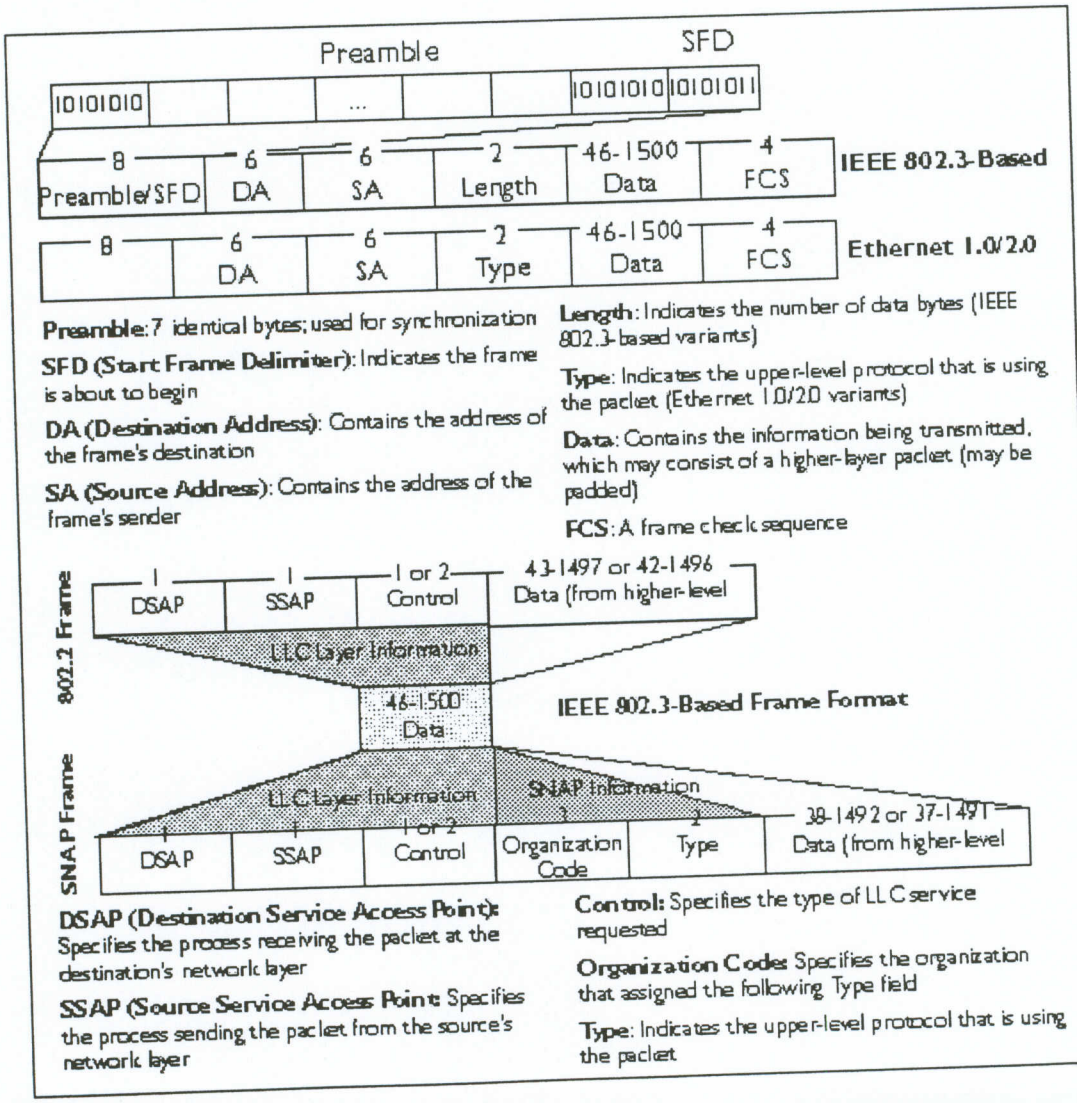
La structure d' un paquet IPX



Types de trames

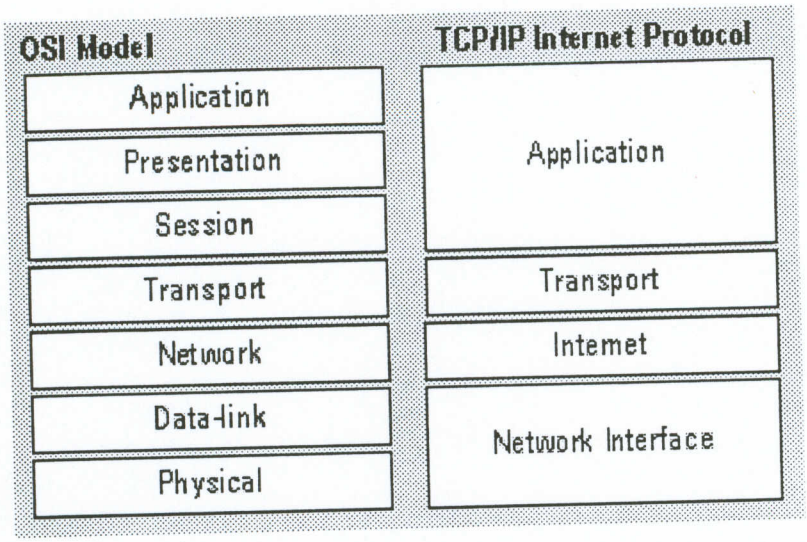
La structure d'une trame Ethernet (60-1514 bytes)





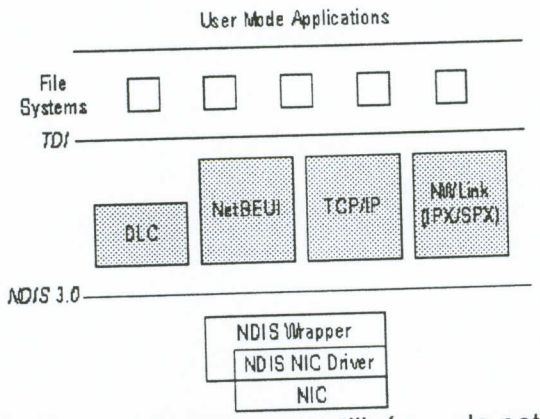
Protocoles

Fonction des protocoles et fonctionnement dans une architecture en couches



Caractéristiques	TCP/IP	NWLink	NETBEUI
Industry acceptance and experience	Most popular, especially in non-PC networks	Primary protocol in PC networks	Limited to IBM & Microsoft PC networks.
Open vs. proprietary specifications	Open	Proprietary	Proprietary, but published
Interoperability	Available on nearly every platform	Available on many platforms	Limited to IBM & Microsoft networks
Simplicity of client configuration	Can be difficult	Simple	Simple
Simplicity of administration	Can be difficult	Simple	Simple
Network segmentation			
Differentiates between networks	Yes	No	No
Hierarchy of subnets within networks	Yes	Yes	No
Routing capabilities	Natively routable	Natively routable	Not routable
Name resolution requirements			
Application Layer to Network Layer	Resolves host or NetBIOS name	Resolves NetBIOS name to IPX address	Uses NetBIOS natively
to IP address			
Network Layer to Data Link Layer	Resolves IP address to MAC address	IPX address contains MAC address.	Resolves NetBIOS name to
MAC address			
Network traffic			
NetBIOS Name Registration	WINS, Broadcast,	Broadcast	Broadcast
NetBIOS Name Resolution	Cache, WINS, WINS Proxy,	Cache,Broadcast	Multicast
LMHOSTS, Broadcast, HOSTS, DNS			
Router Broadcasts	Dynamic routers	Dynamic routers ¬Netware. File servers	N/A
issue RIP broadcasts every 30 seconds	issue RIP broadcast every 60 secondes		
SAP Broadcasts	N/A	IPX servers issue SAP broadcasts every 60 seconds	N/A
DHCP Broadcasts	Client IP configuration negotiated via broadcast	N/A	N/A
WINS Replication	Replication traffic when	N/A	N/A
using multiple WINS servers	Yes	No	No
Network status reporting			
Performance			
Small LANs	Fast	Fast	Fastest
File and Print Operations	Fast	Fastest	Fast
Application Services	Fastest	Fast	Fast

Les protocoles réseau courants sont les suivants :



- **NetBEUI.** Ce protocole est généralement utilisé sur de petits réseaux locaux (LAN) de la taille d'un service, comprenant de 1 à 200 clients. Il n'est pas routable !

- **NWLink** Transport compatible IPX/SPX. Il gère le routage mais le protocole de routage RIP ne supporte pas plus de 15 routeurs. Peut prendre en charge des applications client-serveur NetWare, où des applications utilisant des sockets et connaissant NetWare communiquent avec des applications IPX/SPX utilisant des sockets. Installez NWLink si votre ordinateur est connecté à ou communique avec un réseau NetWare.

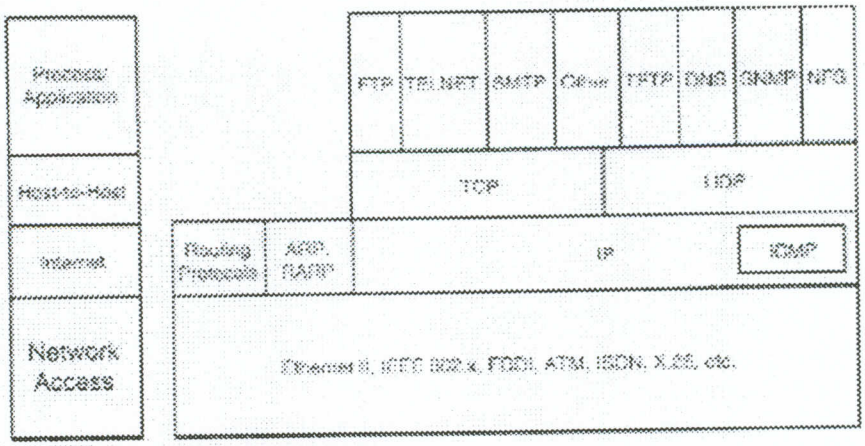
Les serveurs NetWare 2.xx et **3**.xx utilisent le type de trame 802.**3** X

Les serveurs NetWare **4**.xx utilisent le type de trame 80**2.2** X

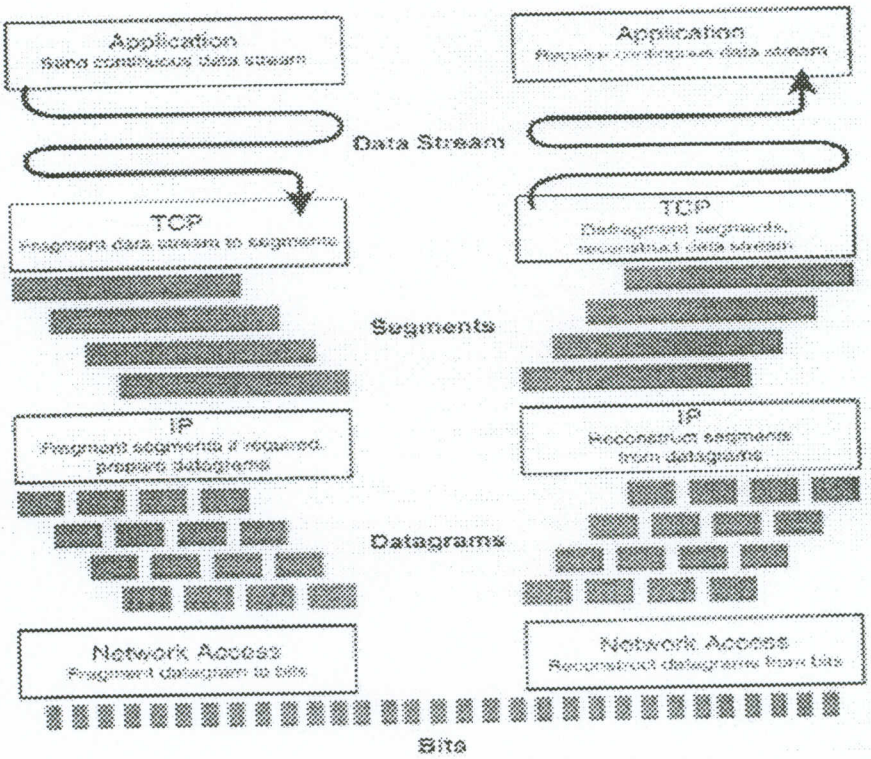
- **TCP/IP**. Cette suite de protocoles de gestion de réseau permet les communications entre réseaux interconnectés. Activez cette case à cocher si votre ordinateur se trouve sur un réseau interconnecté comportant différents matériels et systèmes d'exploitation, ou si vous souhaitez communiquer avec des systèmes non-Microsoft, tels que UNIX. TCP/IP est nécessaire pour les communications Internet.

DLC ne peut pas être utilisé pour la communications entre deux ordinateurs Windows. Il peut être utilisé pour :
-Connexion a partir d'un ordinateur Windows 2000 a un AS400
-Connexion a partir d'un ordinateur Windows a un périphérique d'impression qui a une carte réseaux intégré.
Toutefois l'utilisation de ce ce protocole non-routable doit être évité.

DLC :



La suite des protocoles TCP/IP



Pour identifier un processus dans un environnement TCP/IP un socket est utilisé comme identifiant :

Un Socket est composé de:

- **Le protocole de transport (TCP ou UDP)**
- **L'adresse IP**
- **Le No de port (un no de 0 à 65535)**

Les premiers 1024 ports sont réservées (80 pour http, 21 ftp, etc)

Numéros de ports réservés par des applications "standard"

TCP utilise des ports pour les principaux services qu'il gère.
Un Socket est composé d'une adresse IP, d'un protocole de transport et d'un port.

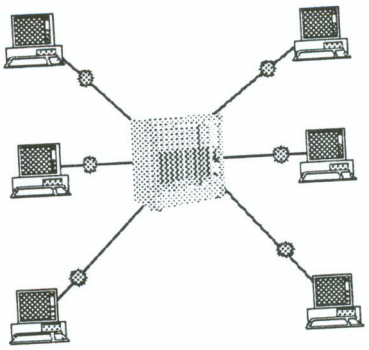
ftp-data	20/tcp		FTP, données
ftp	21/tcp		FTP. contrôle
telnet	23/tcp		
smtp	25/tcp	mail	Format SMTP (Simple Mail Transfer Protocol)
domain	53/tcp		Serveur de nom de domaine
domain	53/udp		Serveur de nom de domaine
bootps	67/udp	dhcps	Serveur de protocole d'amorçage
bootpc	68/udp	dhcpc	Serveur de protocole d'amorçage
tftp	69/udp		Transfert de fichiers trivial
http	80/tcp	www www-http	World Wide Web
kerberos	88/tcp	krb5 kerberos-sec	Kerberos
kerberos	88/udp	krb5 kerberos-sec	Kerberos
hostname	101/tcp	hostnames	Serveur de nom d'hôte NIC
pop3	110/tcp		Protocole Bureau de poste - Version 3
nntp	119/tcp	usenet	Protocole de transfert de nouvelles par Internet
ntp	123/udp		Protocole d'heure du r,seau
RPC	135		Mise en correspondance de ports RPC
netbios-ns	137/tcp	nbname	Service de nom NETBIOS WINS
netbios-ns	137/udp	nbname	Service de nom NETBIOS WINS
netbios-dgm	138/udp	nbdatagram	Service de datagramme NETBIOS
netbios-ssn	139/tcp	nbsession	Service de session NETBIOS
imap	143/tcp	imap4	Protocole d'accés de messagerie Internet
pcmail-srv	158/tcp		Serveur PCMail
snmp	161/udp		SNMP
snmptrap	162/udp	snmp-trap	Piege (trap) SNMP
ldap	389/tcp		Protocole all,g, d'accés aux répertoires
https	443/tcp	MCom	
https	443/udp	MCom	
microsoft-ds	445/tcp		
microsoft-ds	445/udp		
kpasswd	464/tcp		Kerberos (v5)
kpasswd	464/udp		Kerberos (v5)

Consultez le fichier : winnt\system32\drivers\etc\services qui contient la liste complète des ports.

Dépôt de données sur le câble
Principales méthodes d'accès, leurs caractéristiques et leur fonction : CSMA/CD, CSMA/CA, passage de jeton et priorité de la demande

La topologie des réseaux :

Les réseaux en étoile *(star)*
Un noeud central servant de commutateur et concentrateur établit des circuits entre paires d'utilisateurs.
Avantages : une station défectueuse peut facilement être déconnectée de l'étoile sans entraver le fonctionnement des autres machines. noeud central se voit parfois doté de diodes LED indiquant l'activité et les erreurs de chaque station. facilite la localisation d'éventuels problèmes.
Inconvénients : l'établissement d'un réseau en demande une quantité non négligeable de noeud. Si un problème survient au noeud central, il se répercute sur le réseau entier. Enfin, le prix d'un tel réseau demeure souvent plus élevé qu'un autre, de par la présence du commutateur central.

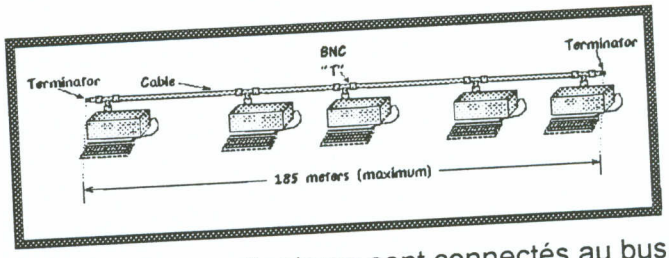


Le

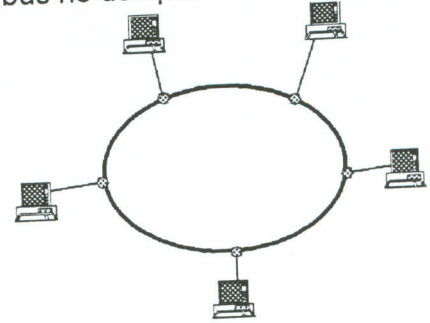
Ceci

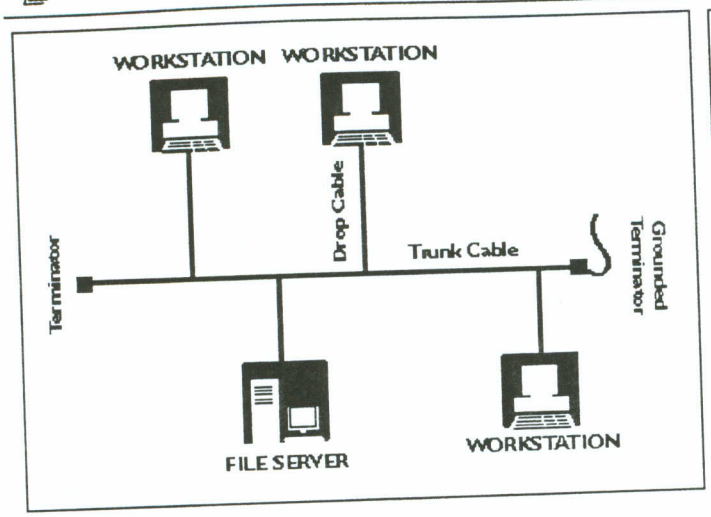
étoile

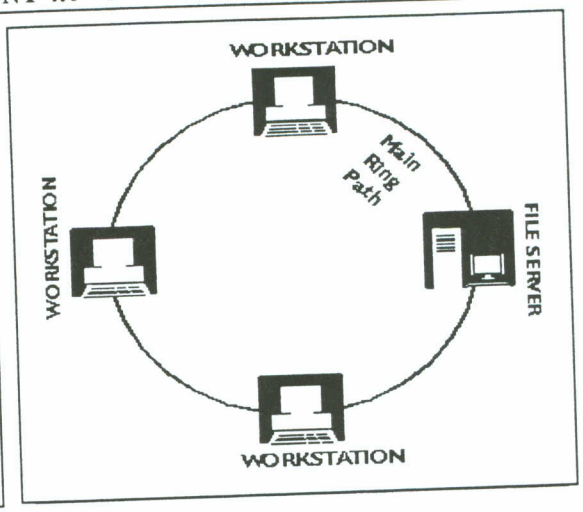
Les réseaux en bus
C'est la topologie la plus courante. L'ensemble des stations est raccordé sur une liaison physique commune. Cela suppose des algorithmes de contrôle d'accès appropriés. Le câble doit, à chacune de ses extrémités, être terminé par une charge adaptée. Les ordinateurs sont connectés au bus à l'aide d'un T. La topologie logique peut être en anneau, comme c'est le cas dans les réseaux ARCNET et Token Bus pour lesquels chaque DTE n'a besoin de connaître uniquement les adresses de son prédécesseur et de son successeur sur l'anneau logique. En outre, dans ce cas, où l'accès s'effectue par jeton, tous les DTEs ne doivent pas nécessairement être connectés à l'anneau logique, ce qui signifie que ces derniers ne peuvent que recevoir de l'information sans posséder le jeton.
Inconvénients : un problème mobilisera l'ensemble du réseau et sera difficile à localiser; de même, une interruption du câble posera problème à l'entièreté du réseau de par l'absence de résistance de terminaison. La longueur maximale du bus ne doit pas excéder 200 mètres; le nombre de terminaux est limité à une trentaine.



Les réseaux en anneau *(ring)*
L'information circule dans une direction le long du support. Chaque terminal est connecté à celui qui le précède et à celui qui le suit.
Avantages : peu de câble, la méthode d'accès en jeton permet d'associer une priorité aux trames.
Inconvénients : la moindre défaillance de connexion entraîne la panne de tout le réseau. Chaque station agissant comme un répéteur, le risque de corruption des données est sensiblement accru. Un réseau de type Token-Ring est assez coûteux et difficile à entretenir.
Token-Ring et FDDI constituent des exemples de réseaux en anneau. Rappelons cependant que ces réseaux ont la plupart du temps une topologie *physique* en étoile,

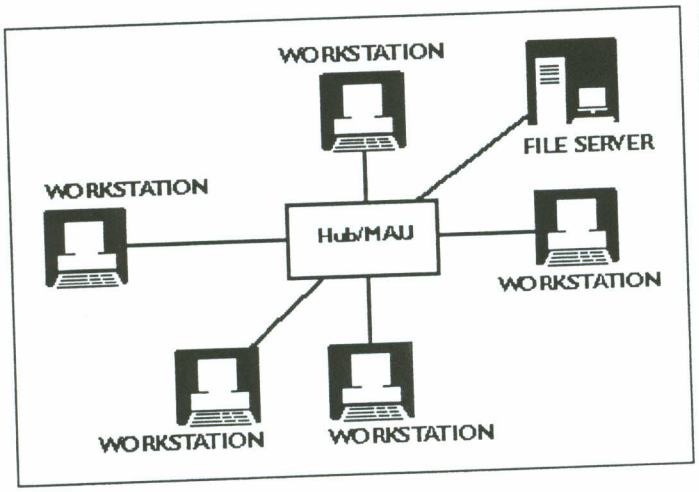


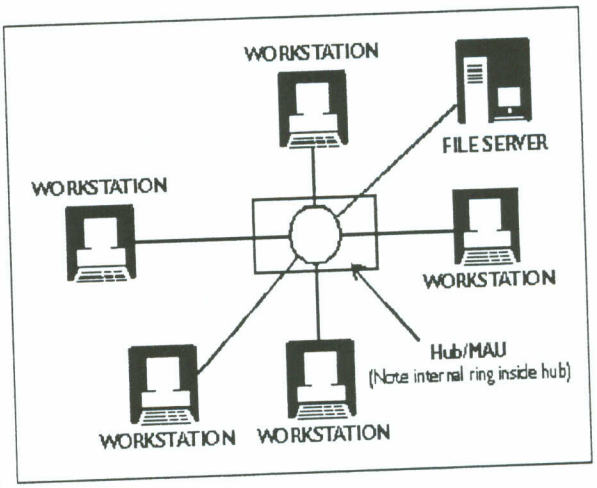




____Câblage : BUS_____ ___Câblage : RING_____

____Circulation du Signal : BUS_____ ___Circulation du Signal : RING_____



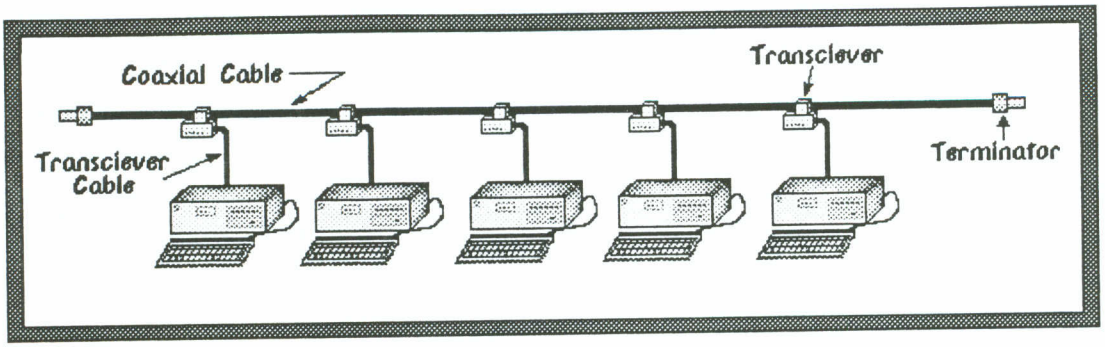


___Câblage : ETOILE (STAR)_____ _Câblage : ETOILE (STAR)_____

___Circulation du Signal : BUS_____ _Circulation du Signal : RING_____

THICK ETHERNET

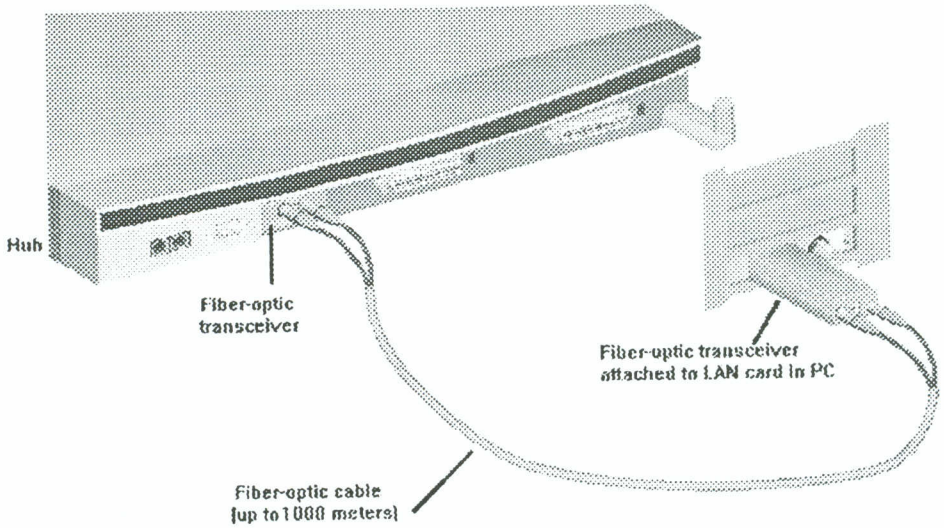
10 Base 5



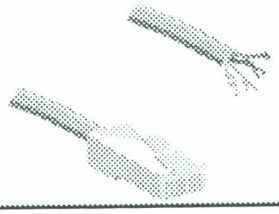
10 BASE-FL

Fiber Link

Câble Fibre optique	10 Base-FL	100 Base-FX	100VG-AnyLAN	FDDI
Longueur maximale du segment	1000 m repeateur to end node 2000 m switch to switch	412 m, half-duplex multimode switch to Hub 2000 m, full duplex multimode switch to switch	2000 m	2000 m node to node



10 BASE-T



Catégories de câbles torsadés non blindées			Nécessaire pour			Longueur		
Catégorie	Bande	Désignation	10Base-T	100Base-TX	100VG-AnyLAN	10Base-T	100Base-TX	100VG-AnyLAN
Category 3	15 MHz	Voice Grade	2 paires	Impossible	4 paires	100 m	Impossible	100 m
Category 4	20 MHz	None	2 paires	Impossible	4 paires	100 m	Impossible	100 m
Category 5	100 MHz	Data grade	2 paires	2 paires	4 paires	100 m	100 m	200 m
Category 6	250 MHz	Data grade	2 paires	2 paires	4 paires	100 m	100 m	200 m

Fast Ethernet, ATM, GigaEthernet, des technologies de transmission dont les débits de 100 Mbit/s a 1 Gbit/s réclament des fréquences élevées.
D'ou les réponses apportées par les fabricants de systèmes de câblage, avec la catégorie 5 améliorée, 5+ *(enhanced cat. 5),* la catégorie 6 on le niveau 7 (Level 7).
Attention a ne pas confondre Megabit par seconde et Megahertz, on la catégorie et la classe.
Pour l'Ethernet a 100 Mbit/s, les fréquences de 100 MHz définies par les normes Iso 11801, EN 50173 ou EIA/TIA 568A sont suffisantes.
L'Ethernet rapide nécessite 62,5 MHz avec codage NRZE mais se contente de 31,25 MHz avec un codage plus complexe de type MLT3, tandis que l'ATM a 622Mbit/s exige du 350MHz, donc la catégorie 5 amélioré. En dépit de l'absence de norme pour ces fréquences les industriels lancent déjà leurs nouveaux câbles AMP, le FutureLan 350; Belden, le MediaTwist 350; BICC. le Millenium 155; Lucent, le Gigaspeed...

Pour la catégorie 6, Un projet de norme allemande
D'autres encore proposent la catégorie 6, s'appuyant sur le projet de norme allemande Din 44312-5, et présentent même sur le marche français des câbles qualités de 600Mhz. Leur constitution est de type écranté **et blinde par paire (S/STP, *Screened-shielded twisted pairs*** ou, en allemand, PiMF, *Individuell abgeschimte adem paare in metal folie)*
La confusion s'installe avec la classification largement diffusée par Anixter. qui nomme **Level 6 la catégorie 5 améliorée, laquelle devient a' l'occasion la catégorie 6**, on qualifie Level 7 de catégorie 6, qui se transforme ainsi en catégorie 7

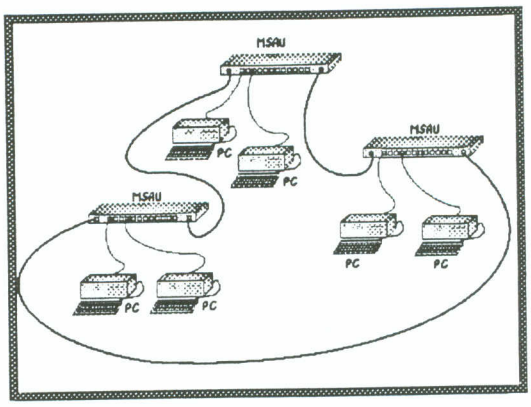
Ces niveaux ou catégories ne définissent cependant que les câbles. Il est donc préférable de parler de lien, c'est-à-dire de la liaison de cent mètres au maximum entre le poste de travail et le sourepartiteur. L'Iso 11801 détermine le lien de classe D comme étant composé d'un câble de distribution horizontale, de 3 cordons, d'un point de transition optionnel, et avec un affaiblissement de 23dB a 100 MHz. Le projet DIN 44312-5 propose un lien de classe E réduit a un câble de distribution et 2 cordons, avec un affaiblissement de 19,2dB a 100 MHz. Ainsi, les fabricants sont amenés à élaborer des systèmes complets avec câble, connecteurs, cordons et panneaux de brassage.
Toutefois, ces solutions sent onéreuses: par rapport a un système de câblage en catégorie 5, le coût d'un système en catégorie 5 améliorée est supérieur de 10% et celui d'un système en catégorie 6 de type Din 44312-5, de 25 à 35%.
Anixter impose une nouvelle classification des câbles non blindés*(UTP,Unshielded twisted pair)* en trois niveaux: Level 5, 6 et 7.
La plus notable des différences entre ces niveaux concerne le rapport le rapport affaiblissement- para diaphonie (ACR, Atténuation crosstalk ratio).Plus il est faible, plus la détérioration de la qualité du signal est importante., Anixter propose un ACR de 10dB aux fréquences de 100 MHz pour Level 5, de 155 MHz pour Level 6 que deviendrait la catégorie 6, et de 200 MHz pour Level 7, qui prendrait le nom de catégorie 7.

Token Ring

Fonctions et caractéristiques de Token Ring

Eléments matériels, concentrateurs, câblage et cartes réseau

Caractéristiques d'un réseau Token Ring.
Principaux éléments d'un réseau Token Ring.
Les éléments nécessaires à la mise en œuvre d'un réseau Token Ring sur un site donné.

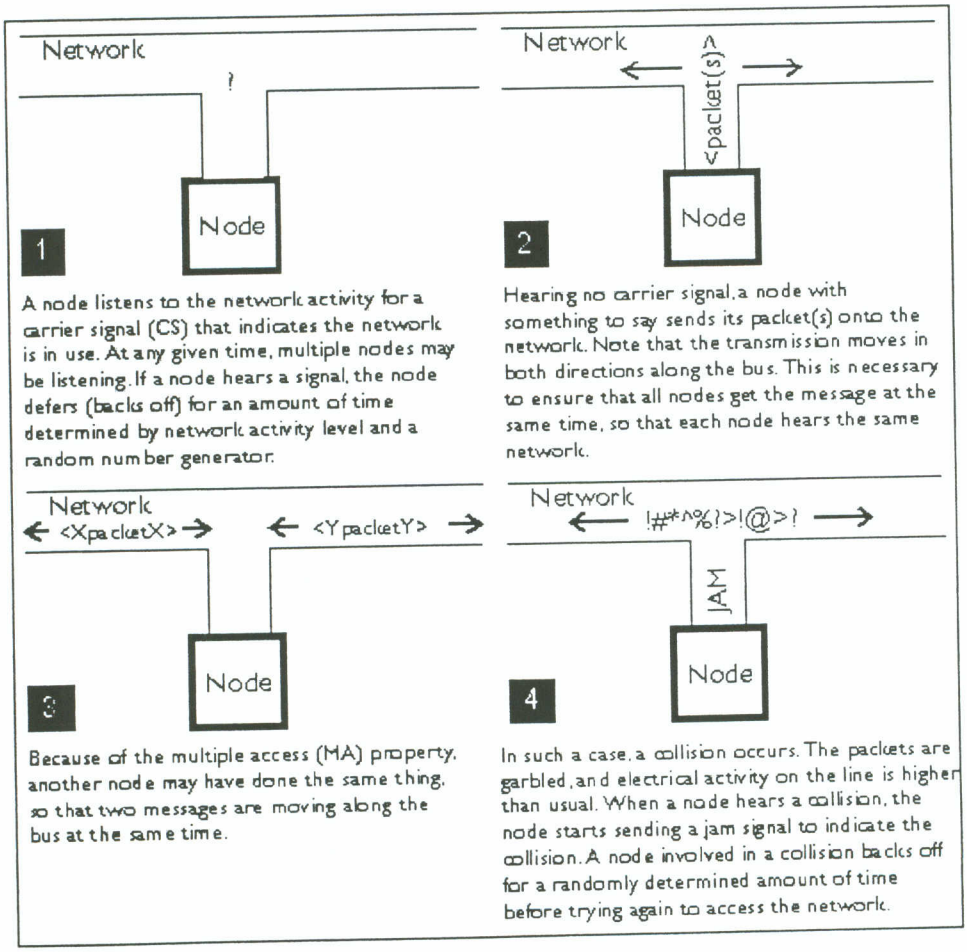


AppleTalk

Présentation de l'environnement AppleTalk, y compris LocalTalk et Appleshare
Les éléments et les caractéristiques d'AppleTalk.

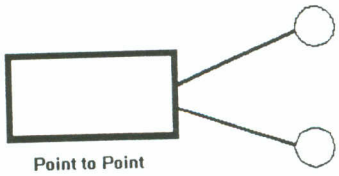
ETHERNET

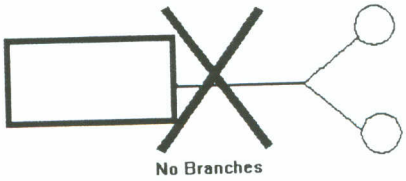
CSMA/CD Accès multiple avec écoute de la porteuse et détection de collisions

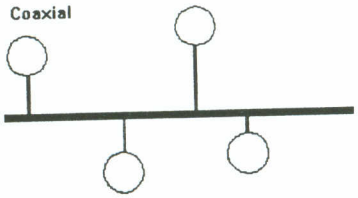


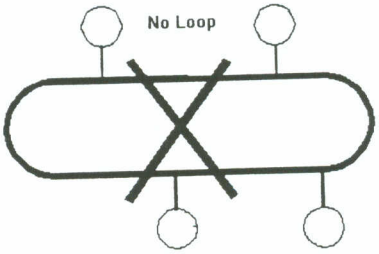
Les Règles de l'Ethernet/802.3 :

Règle 1: Tous les segments doivent être linéaires, sans boucles ni branches.









Règle 2: A un moment donné, un seul chemin doit exister entre n'importe quels 2 nodes.

(Among other things, this keeps packets from colliding with themselves.) Note that it is permissible, however, to have multiple paths as long as no more than one path is active at any one time. This allows for redundant connections in which a backup path can be activated and continue the flow of information when a primary path fails. These types of connections can be made using the backup links available with HP AdvanceStack hubs, and using the Spanning Tree Protocol available with certain bridge and switching products.

Règle 3: Dans un seul LAN (local area network) (Ethernet collision domain) le nombre maximal de nodes est de 1024.

Cette règle n'est pas explicitement prévu dans les standards; elle est plutôt le résultat d'un algorithme qui détermine le temps maximum d'attente des nœuds avant de retransmettre après une collision. Beaucoup d'administrateurs pour des raisons de performances limiter le nombre des nœuds a 200.

Règle 4: Entre 2 nodes dans un réseau il doit y avoir pas plus que 7 bridges or switches.

Il y a une recommandation imposé par le protocole Spanning Tree IEEE 802.1, et il est important de l'utilisé même pour les réseaux qui n'ont pas implémenté le Spanning Tree, a cause du retard introduit par les switch et bridges store-and-forward".

Règle 5: Les longueur des segments :

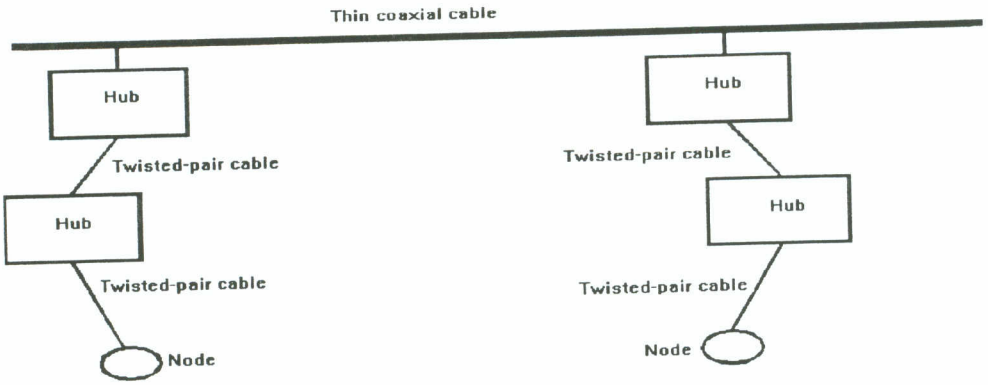
	Twisted-pair cable	Thin coaxial cable	Thick coaxial cable	Fiber-optic cable
Maximum segment length	Cat 3, 4, et 5: 100 m	185 m	500 m	1000 m
Minimum section length	none	0.5 m	2.5 m	none
Connection interval	none	none	2.5 m (at markings)	none
Terminators	not applicable	At each end	At each end	not applicable
Maximum connections per segment	2	30	100	2

Règle 6: Pour un domaine de collisions, les règles qui déterminent les topologies sont :

These rules are based on round-trip collision delay times and interpacket gap shrinkage.

Règle 5-4-3 :
Un réseau Ethernet fin (10 Base2) peut combiner jusqu'à cinq segments de câble connectés par quatre répéteurs, mais seulement trois segments peuvent être attachés à des stations.

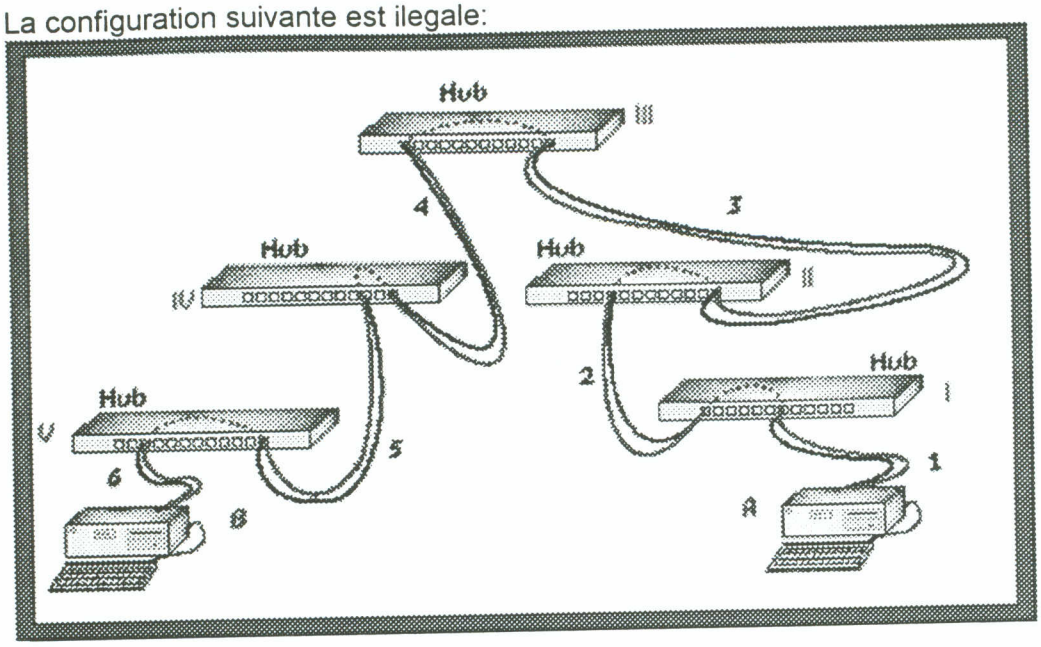
La configuration suivante est correcte



Un ensemble de hubs reliées par un câble spécial (Stacking câble) se comporte comme un simple hub.

Il peut y avoir 4 repeteurs/Hub 10 BaseT entre le switch et n'importe quelle station ou serveur.
Seulement 3 Hubs peuvent avoir des stations attachées.
2 Segments ne peuvent pas avoir des PC et sont donc utilisés seulement pour des liaisons.
5 segments a 100m par segment=500m
Un domaine de collision peut avoir maximum 1024 stations.
Le switch ne doit pas être compté comme un repeteur

La configuration suivante est ilegale:

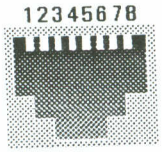


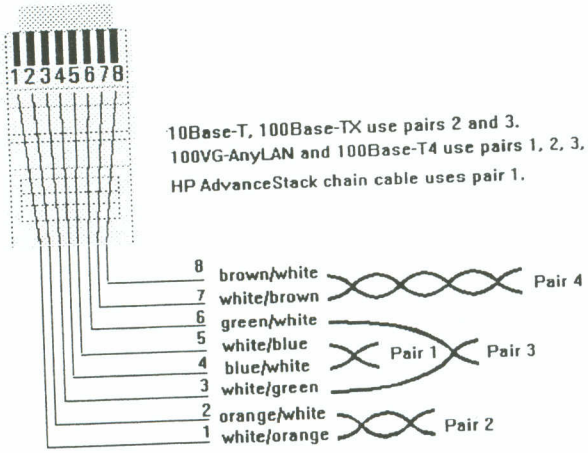
Transmission Mode	Signals on Wire Pairs in Category 3 Cable	Link Capacity
Half-Duplex	10 Mbit/s Transmit OR 10 Mbit/s Receive	10 Mbit/s
Full-Duplex	10 Mbit/s 10 Mbit/s Simultaneous Transmit and Receive (Collision Free)	20 Mbit/s

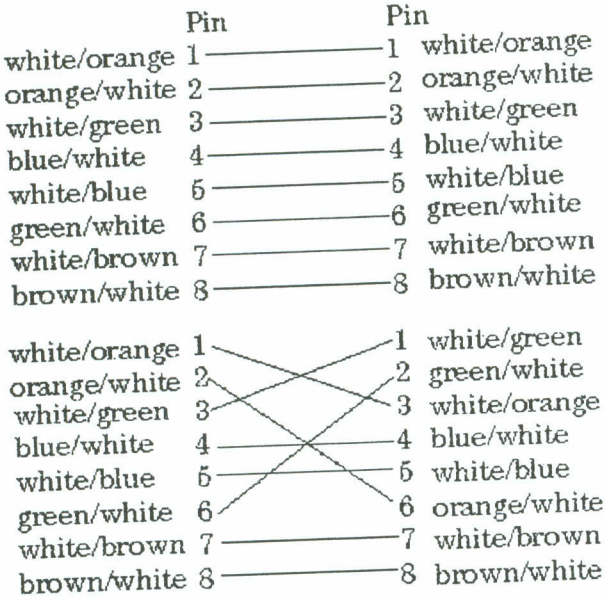
FULL-DUPLEX= mode de communication entre deux équipements capables de transmettre et de recevoir simultanément des données.

Full-duplex possible entre des commutateurs ou entre commutateurs et serveurs ou postes de travails. Le FULL-DUPLEX est impossible avec des hubs.

HALF DUPLEX : Une paire pour la transmission et une autre pour la détection des collisions.







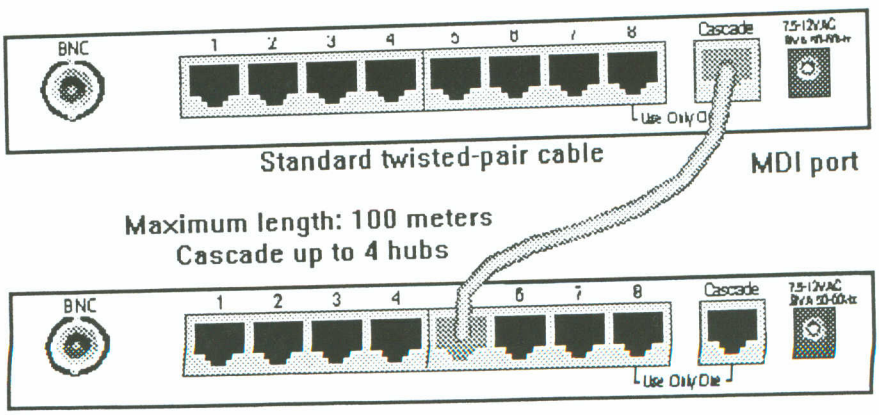
Straight-Through Cable
(for connecting node to hub)

All conductors are wired to the same RJ-45 connector pins on each end of the cable. All color pairs (such as white/blue and blue/white) are kept twisted together.

Crossover Cable (except 100VG)
(for connecting hub to hub or transceiver to transceiver)

Pairs 2 (pins 1 and 2) and pair 3 (pins 3 and 6) are crossed (note the different color assignments at each connector). All color pairs are kept twisted together.

- Sur un Hub ou Switch chaque port est inversé sauf le port Cascade.



Caractéristiques des différentes technologies.

	FDDI (Fibre Multimode)	100VG-AnyLAN (Cat 3, 4, or 5)	100Base-T (TX-FX-T4)	ATM (25/155 Mbps)	Gigabit Ethernet (802.3z)
Max Segment Distance	2000 m	100 m	100 m Cat 5, 412 m fiber, 2000 m full duplex	200 m Cat 5, 2000 m OC 3 fiber	25 to 100 m Cat 5, 550 m to 2000 m fibre
Network Diameter with Repeater(s)	100 km	200 m to 6000 m	205 m to 320 m	N/A	To be determined by the standard
Current Bandwidth	100 Mbps	100 Mbps	100 Mbps(33 MhzTX)	25-155 Mbps	1 Gbps
Media Access method	Token passing	Demand Priority	CSMA/CD	PVC/SVC	CSMA/CD
Maximum Number of Nodes Per Domain	500 (1000 actual connections)	1024 (250 max recommended)	Limited by the hub's stacking capabilities and port count.	N/A	To be determined by the standard
Frame Type	802.5	Ethernet and Token Ring	Ethernet	53-byte Cell/Ethernet with LANE	Ethernet
Full Duplex Capable	YES (point-to-point only)	NO	YES (point-to-point only, except T4)	YES	YES
Multimedia support	Limited to FDDI II	YES	NO	YES	YES (with 802.1p)
Legacy 10BT LAN integration	YES via routers and switches	YES via bridges, switches and routers	YES via switches	YES via routers or switches	YES via 10/100 Mbps switching
Relative Cost/Average Cost per Port	Medium/$2000 (fiber) $800 (cuivre)	Low/$200 (shared), $700 (switched)	Low/$200 (shared), $700 (switched)	High/$4000 (fiber) $750 (cuivre)	Mediium/$920 to $1400
Relative Complexity	Medium	Low	Low	High	Low
Best Application	backbone in the wiring closet	multimedia, video conferencing	high speed access to servers	backbone between buildings	high speed access to servers

Fast Ethernet est utilisé sur paires torsadé non blindées (unshielded twisted-pair) et cable fibre-optique :

Abréviation	Description of Media
100Base-T	Nom générique pour Fast Ethernet
100Base-TX	Fast Ethernet sur des paires unshielded(non blindé) or shielded(blindé) twisted(torsadé) câble, Category 5 ou plus
100Base FX	Fast Ethernet sur multimode, deux strand fiber- optic câble
100Base-T4	Fast Ethernet sur twisted pair cable, 4 pairs Category 3, 4, or 5.

Distances

	Hub to End Node	Hub to Hub Switch to Switch half *duplex*	Switch to Switch Using Full Duplex
twisted-pair	100 mètres	100 mètres	100 mètres
fiber-optic	150 mètres	412 mètres (half duplex)	2000 mètres (full duplex)

FAST ETHERNET

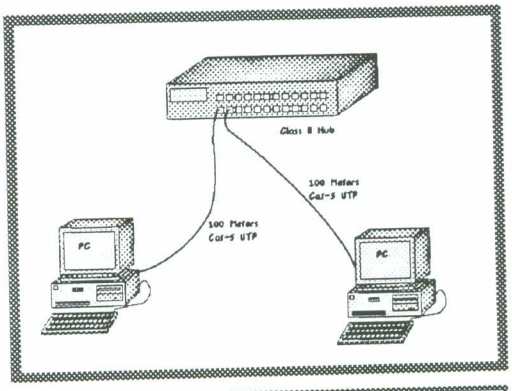
Les règles pour la topologie réseau 100 Base Tx (IEEE 802.3u)

Les règles et les recommandations pour la topologie 100Base-TX (twisted-pair) et 100Base-FX (fiber) network sont basées sur le standard IEEE 802.3u.
La topologie de votre réseau doit être en étoile physique , sans branches ni boucles.

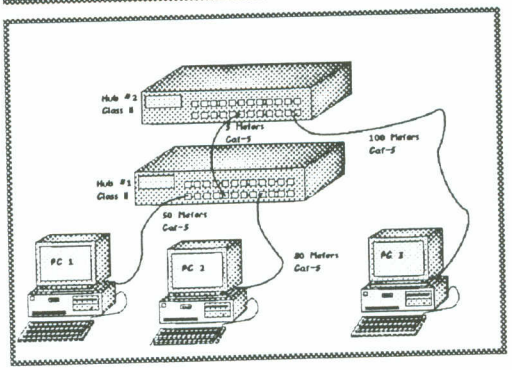
Toutes les quatre paires doivent être câblés dans un câblage UTP. Donc, n'utilisez pas les autres 2 paires dans 100Base-TX pour rien d'autre.

Vous devez utiliser du câble de Catégorie 5. (1.112.bit time/metre round trip delay)
La longueur maximale d'un câble UTP est de 100 mètres, Un hub peut être connecté a un switch avec un câble UTP de 100 m maximum, Un hub peut être connecté a un switch avec un câble fibre qui ne doit pas dépassé 160 mètres. Un switch connecté a un autre switch avec full-duplex le câble fibre ne doit pas dépassé 2 kilomètres.
Les répéteurs doivent être organisés:

Class I: Un seul répéteur entre deux nodes (pas de cascade).

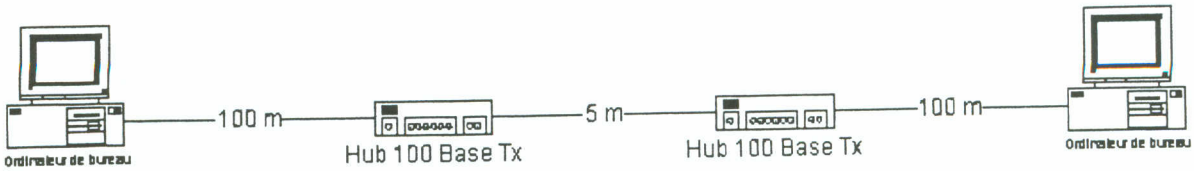


Class II: Utiliser un maximum de deux répéteurs entre deux nodes reliés avec un câble de 5 mètres au maximum.



Chaque hub de classe II produit un retard de 92 bit time (round-trip delay).
Le diamètre du réseau ne peut pas dépasser 205 mètres.
Round-trip delays ne peut pas dépasser 512 bit times. 2 DTE delay is 100 bit time (50 bit time each)
The delay est en Bit time qui est équivalent a 10 ns par bit.

50 +1.112*100 +92 +1.112*5 +92 +1.112*100 +50
<512



GIGABIT ETHERNET 1000 Base X

Couches physiques définies :
Ethernet 10 Mbps 802.3g et Ethernet 100 Mbps 802.3u
Token Ring 4 Mbps et Token Ring 16 Mbps
100 VG AnyLAN
FDDI
ATM jusqu'à 622 Mbps
Couches physiques de demain :

IEEE 802.3z

Le standard IEEE 802.3 z se décline en trois versions :

1000 Base-SX qui supporte la fibre multimode seulement.
260 mètres sur fibre multimode 62.5/125 et 525 mètres sur multimode 50/125

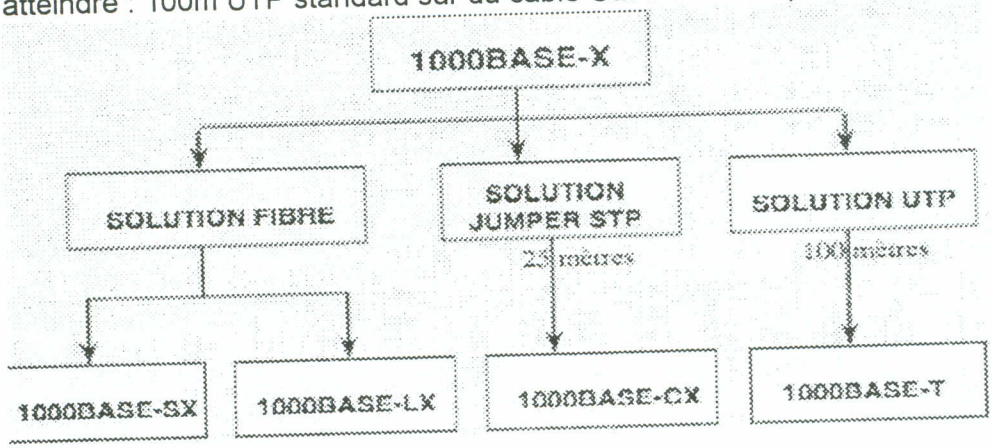
1000 Base LX qui permet de travailler a la fois avec monomode et multimode
3Kilometres en monomode et 525 mètres sur multimode 62.5/125

1000 Base CX Gigabit Ethernet sur cuivre (paires torsadées blindées) 25 m

IEEE 802.3ab

1000 Base TX Gigabit Ethernet sur paires torsadées non blindées
est en développement. 2Gbits par seconde en full duplex (1Gbps dans chaque sens)

Fonctionne avec 4 paires (4x250Mbps dans les 2 directions)
But a atteindre : 100m UTP standard sur du câble Cat 5 Délai de propagation 50 ns



Mise à jour ISO SC25 WG3

Câble Catégorie 6/Class-E : Sera aligné sur les performances du câblage UTP de classe mondiale. Il constituera une version améliorée de Catégorie 5 (incluant RJ-45) Il supportera une .largeur de bande jusqu' à 250 Mhz sur les 4 paires en full duplex.

Câble Catégorie 7/Class-F : Sera aligné sur les performances du câblage de l'an 2000 utilisant les paires blindées individuelles.. Il exigera la mise au point d'un nouveau connecteur. Il supportera une largeur de bande de 750 Mhz. 25 mètres. Pas de support de IEEE et ATM
Pas de support de fournisseurs de composants actif car pas de compatibilité en aval donc pas de débouchés sur le marché.

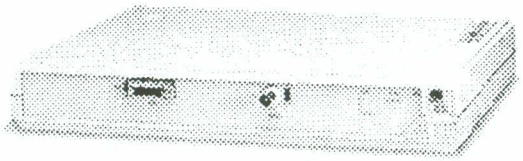
ETHERNET commuté

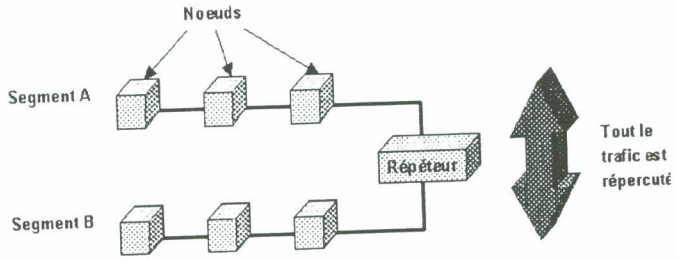
Un réseau commute s'obtient en coupant le réseau Ethernet d'origine en des domaines de collisions autonomes relies entre eux par des ponts en essayant de bien garder un trafic local. Les ponts ne sont ici que des commutateurs Ethernet mémorisant les trames et les re-emettant vers d'autres réseaux Ethernet. L'ultime solution est de découper le réseau de telle facon a n'avoir qu'une seule station par port du commutateur Ethernet. C'est ce qu'on appelle la ***commutation Ethernet.*** L'autre appellation est Ethernet FDSE (Full Duplex Switched Ethernet)

Avantages : Pas de limitation de distance
Possibilité de réaliser des réseaux en commutation au niveau mondial

Inconvénients : Techniques de contrôle a mettre en place (QoS)

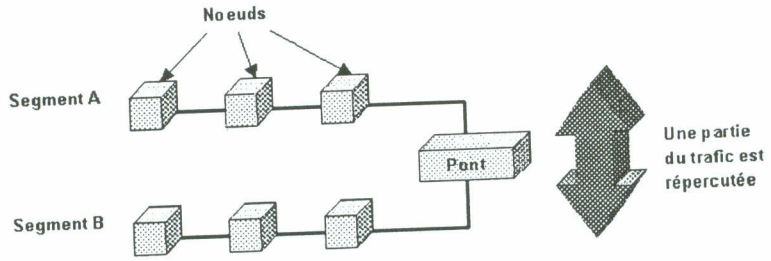
1. Le répéteur *(repeater)* est un dispositif permettant d'étendre la distance de câblage d'un réseau local. Son rôle consiste à répéter, amplifier et régénérer les signaux qui lui parviennent. Le répéteur fonctionne au niveau 1 du modèle OSI.





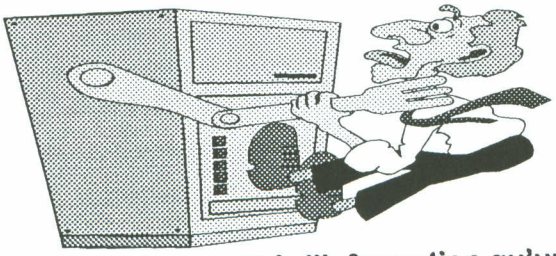
Le Concentrateur (Hub) est un répéteur multiports.

2. Le pont *(bridge)* permet d'interconnecter des réseaux locaux. Tandis que les répéteurs relient des LANs au niveau hardware le plus bas, les ponts les rattachent au niveau hardware, appelé MAC *(Media Access Control)*. Sa fonction est de faire passer des trames d'un réseau à un autre. Se situant au niveau 2 de l'OSI, le pont demeure indépendant du protocole réseau utilisé mais dépend des adresses physiques. **Le pont est donc utilisé pour interconnecter des réseaux de même type (Ethernet à Ethernet, Token-Ring à Token-Ring, etc....).** De par sa simplicité, il supporte des débits relativement élevés: entre 20.000 trames par seconde pour Ethernet et 200.000 trames pour FDDI. Concrètement, si un pont doit relier un LAN A à un LAN B, il connaîtra, par apprentissage, les adresses appartenant au réseau A et celles faisant partie de B. Le pont aura construit une table avec ces informations. Tous les paquets provenant d'un réseau et destinés à ce même réseau seront ignorés. En effet, la transmission au sein d'un réseau peut s'effectuer sans l'aide du pont. Par contre, il transmettra les informations inter-réseau. Les ponts construisant leur table par apprentissage l'actualiseront automatiquement si des terminaux s'ajoutent ou sont enlevés du réseau. Les ponts permettent de diviser le réseau en plus petits segments. Ils offrent également la possibilité d'étendre la taille physique du réseau. Bien que les segments individuels soient toujours limités par le délai de propagation, les ponts permettent d'étendre la distance entre segments. Cependant, au-delà d'une certaine taille, l'utilisation d'algorithmes (et non plus de simples tables) s'impose. D'où l'emploi de routeurs.

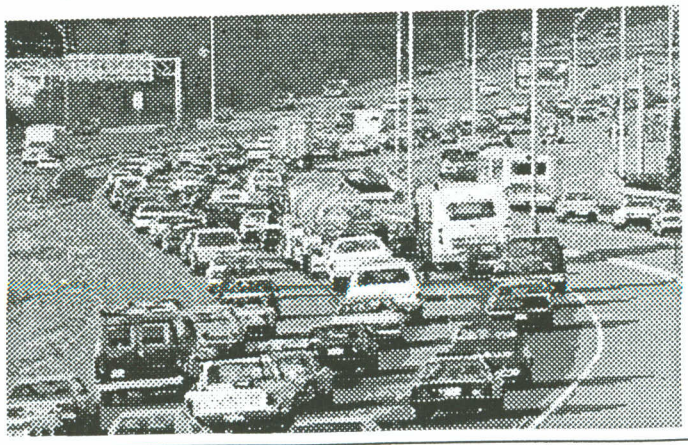


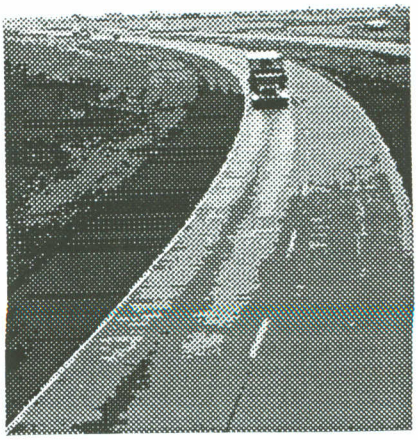
Le commutateur *(switch)*, est un pont (brige) multiport plus performant.

Quand aurez-vous suffisamment de bande passante ???

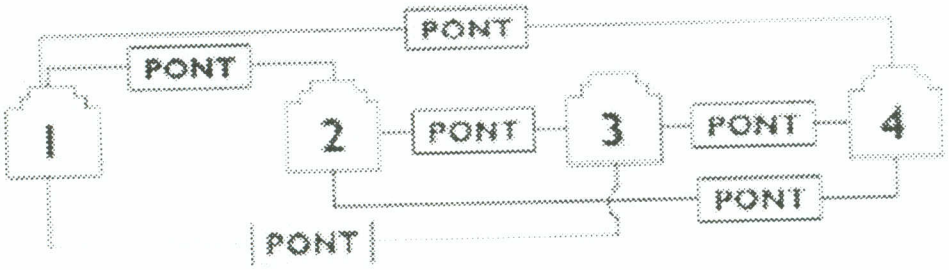


La bande passante représente la quantité d'information qu'un système peut transporter



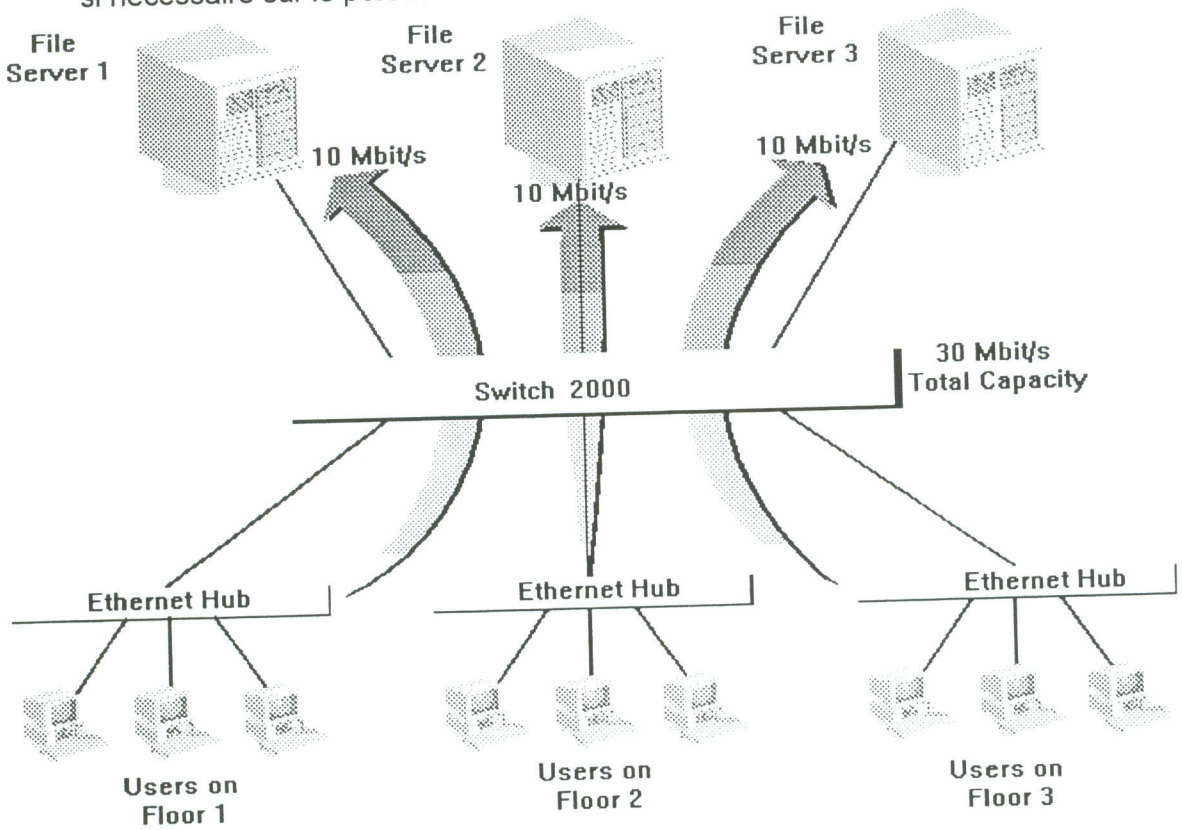


-Le switch établit une connexion entre un port d'entrée et un port de sortie en fonction des adresses physiques (MAC)
-Les adresses de niveau 2 (MAC) sont apprises sur chaque port
-Les tables d'adresses MAC sont construites
-Trafic de diffusion (broadcast) copié sur chaque port
-Divers méthodes de commutation (switching)
-Ports haute vitesse pour serveurs



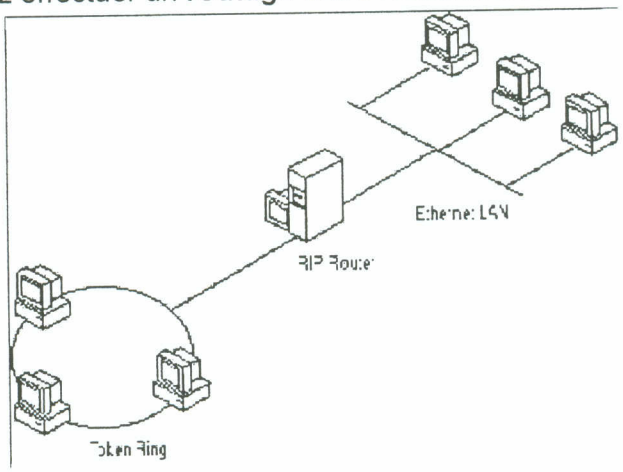
Le switch fonctionne comme un pont local multiport. Il permet de scinder un réseau en autant de sous-réseaux qu'il y a de ports. Un switch est nettement plus rapide qu'un pont, il y a 2 principes de fonctionnement :

1. CUT THROUGH (On the fly) :récupère la trame, analyse les adresses MAC et renvoie si nécessaire sur le port concerné du switch.
2. STORE & FORWARD (95% des switches): stocke la trame en mémoire flash, analyse les analyse les adresses MAC et vérifie l'intégralité des données et renvoie si nécessaire sur le port concerné du switch.



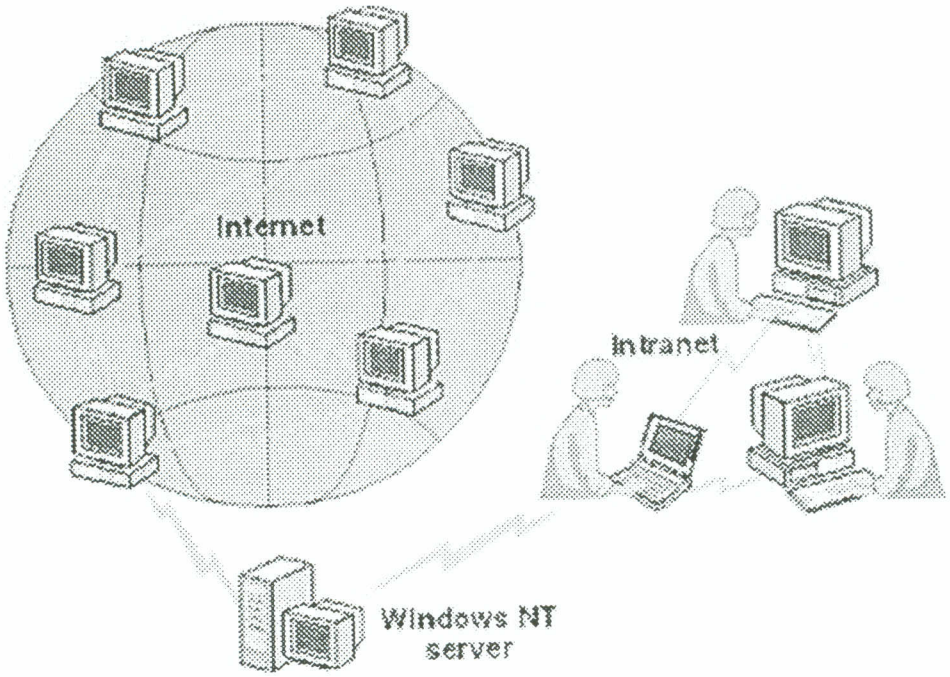
3. Le ROUTEUR

Le routeur *(router)* (plus évolué) se situe au niveau 3 du modèle OSI. Il réalise donc une fonction d'adressage et doit connaître la topologie des réseaux à interconnecter. Il est naturellement dépendant du protocole réseau utilisé. **Les routeurs peuvent relier des LANs de types différents (ex.: Ethernet et Token-Ring).**
Avec Windows 2000 Server, vous pouvez effectuer un **routage** entre réseaux locaux, comme illustré sur la figure suivante :



Routage entre deux réseaux locaux

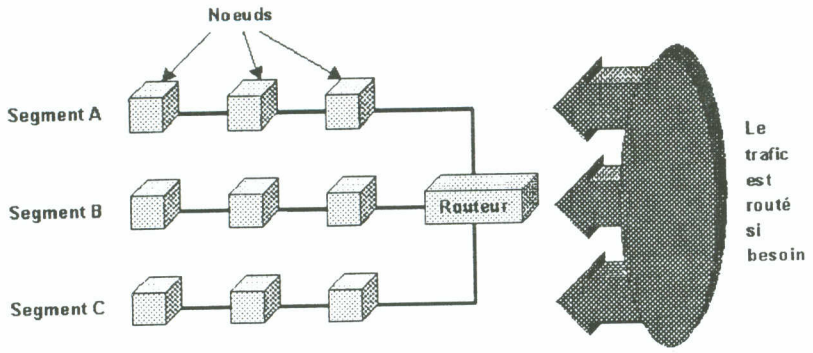
Vous pouvez utiliser RRAS pour effectuer un routage entre réseaux WAN



Routage entre INTRANET et INTERNET

Si le réseau local utilise des adresses réservées pour les intranets vous pouvez ajouter au routeur Windows 2000 RRAS le protocole de routage NAT

Les routeurs utilisent des algorithmes qui déterminent le chemin le plus efficace pour l'acheminement de l'information. C'est pourquoi ils sont fréquemment utilisés pour interconnecter un LAN à un WAN, les WANs possédant généralement des chemins multiples. Un routeur est donc plus "intelligent" qu'un pont, donc plus cher. Il est aussi moins rapide. Il existe également sur le marché des routeurs plus perfectionnés pouvant router plusieurs protocoles réseau.



-Les **B-routeurs**, ou ponts-routeurs, intègrent les trois premières couches du modèle OSI tout en agissant sur le niveau 2 lorsqu'ils ne reconnaissent pas le protocole réseau (protocoles non routables).

Protocoles routables : IP, IPX, OSI, DDP(Apple talk), XNS, DECnet

Protocoles nonroutables : NetBEUI, LAT, DLC

Enfin, les routeurs - tout comme les ponts - peuvent être asynchrones ou synchrones. Dans le mode de transmission asynchrone, les données sont transmises en un flot continu de bits. Chaque caractère est entouré d'un start bit et d'un stop bit. En cas d'erreur de transmission, des flux entiers de données doivent être retransmis.

En transmission synchrone, chaque bloc de données est précédé de caractères de synchronisation. Après l'envoi de ceux-ci, le pont (ou le routeur) récepteur, accepte tous les bits transmis jusqu'à ce que de nouveaux caractères de synchronisation soient envoyés, indiquant la fin de la transmission précédente et le début de la nouvelle. La correction d'erreurs est beaucoup plus aisée en transmission synchrone. En mode asynchrone, elle prolonge les temps de réponse. Ce mode s'avère relativement inefficace par rapport à son opposé. Par contre, il s'implémente facilement sur les lignes téléphoniques standards.

L' utilisation des routeurs pour interconnecter des réseaux a également l'avantage éviter les « orages de diffusions » (broadcast storm). Les routeurs sont configuré pour interdire les diffusions (broadcast)

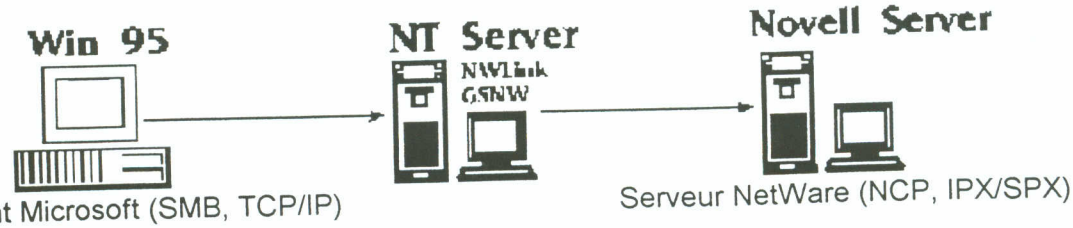
Un routeur Windows 2000 RRAS peut utilise les protocoles de routage :

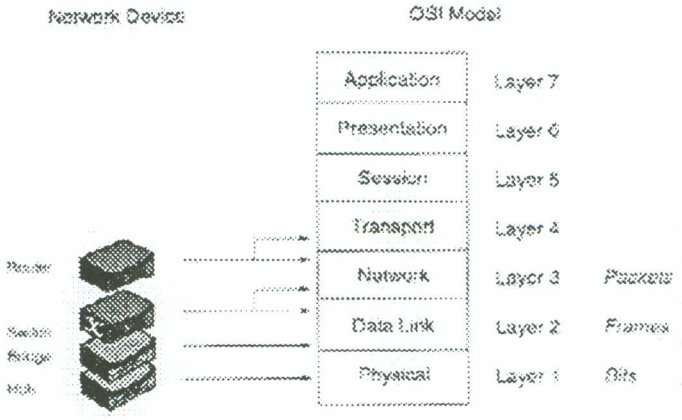
-RIP version 2 et

-OSPF. (Open Shorted Path First)

-NAT (Network Address Translation)

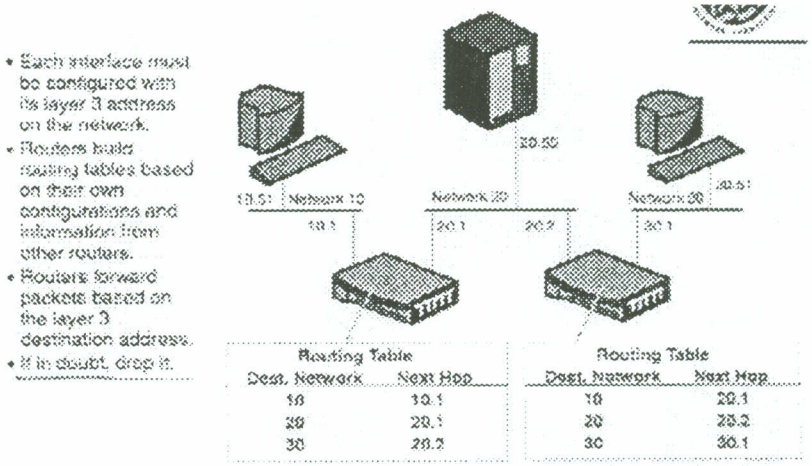
4. La passerelle *(gateway)* est un dispositif permettant d'interconnecter des architectures de réseaux différentes. Elles offrent donc la conversion de tous les protocoles, au travers des 7 couches du modèle OSI.



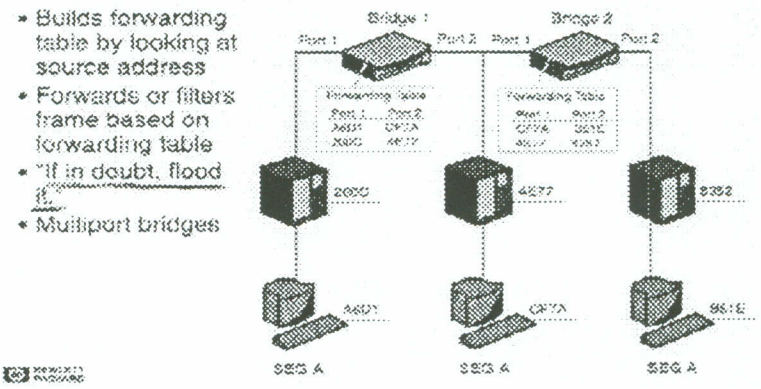


OSI model	Device
Application	Gateway
Presentation	Gateway
Session	Gateway
Transport	Gateway
Network	Router, Gateway
Data Link	Bridge, Gateway
Physical	Repeater, Gateway

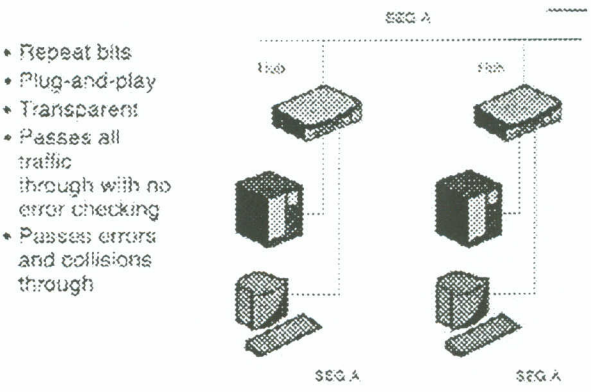
3. Routeur



2.Bridges(ponts), Switches(commutateurs)



1. Hubs (Concentrateurs)



Impression réseau
Processus d'impression réseau y compris le partage d'une imprimante et la connexion à une imprimante

Gestion d'une imprimante partagée

Les étapes de l'installation et de l'utilisation d'une imprimante partagée.
Enumérer les tâches de gestion d'une imprimante partagée.
Déterminer si un service de télécopie partagé convient à un site donné.

Mise en œuvre d'applications de réseau

Messagerie électronique

Applications de planification

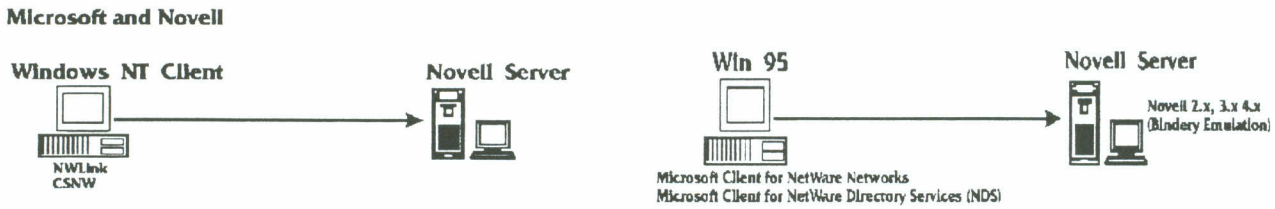
Applications de productivité de groupe

Applications de réseau partagées, telles que les bases de données

Les fonctionnalités et les applications de la messagerie électronique.
Déterminer les stratégies et les procédures appropriées à la mise en œuvre et à la gestion d'un système de messagerie électronique.

Réseaux dans des environnements multifournisseurs

Mise en œuvre de solutions multifournisseurs du point de vue client et serveur



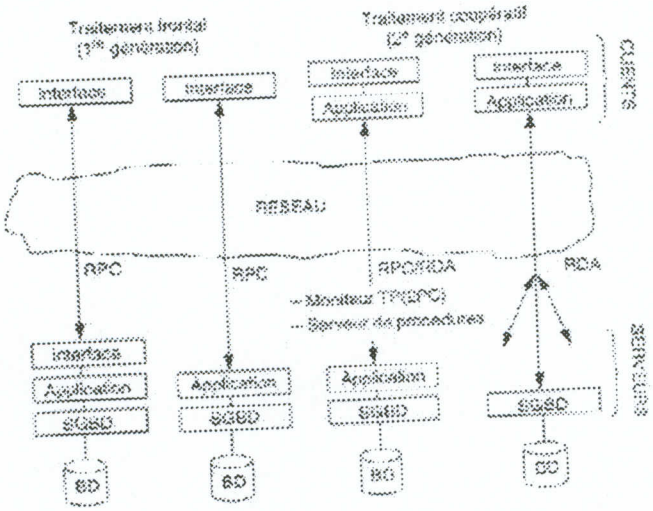
Définir une solution client et une solution serveur pour l'interopérabilité.
Identifier les méthodes utilisées par les fournisseurs pour intégrer leurs produits à ceux d'autres fournisseurs.
Déterminer les systèmes d'exploitation de réseau et les redirecteurs appropriés à un site donné.

Environnement client-serveur
Modèle client-serveur y compris les fonctions client et serveur, l'architecture et les avantages de l'informatique centralisée. **Les trois générations d'architecture client – serveur**

1. Le traitement frontal
"Revamping" Le *revamping* correspond à un ré-habillage graphique d'applications existantes. Un environnement de travail graphique, plus convivial que le mode d'affichage caractère initial, est fourni, mais le gain de performance est réduit.
Terminal x. Les terminaux en mode caractères sont remplacés par des terminaux X . La puissance de traitement local du poste de travail n'est pas exploitée au-delà du mode d'affichage graphique. Les terminaux X-Window permettent d'afficher autant de fenêtres d'applications provenant d'autant de serveurs que l'utilisateur le désire. Toute la logique de l'interface est maintenant déportée sur le poste client (X-Window, etc.) l'application et la gestion des données demeurent sur le serveur. Le poste client gère l'interaction (graphique) avec le serveur distant.

FRONTAL
Front end

DORSAL
Back end



2. Le traitement coopératif
La deuxième génération correspond à l'architecture client-serveur type avec plusieurs variantes
• répartition partielle de l'application entre le client et le serveur.
• localisation complète de l'application sur le poste client ; c'est le cas, par exemple, de l'accès à des données distantes (gérées par un serveur SQL) dans un applicatif bureautique type comme un tableur ou un traitement de texte, situé sur le poste client, etc.
• accès possible, mais explicite par l' applicatif à plusieurs serveurs distants.
3. Le traitement réparti et les données réparties

Les étapes du processus client-serveur.
1. Le client demande des données.
2. La requête est traduite en langage SQL
3. La requête SQL est envoyée au serveur par l'intermédiaire du réseau.
4. Le serveur de base de données effectue une recherche sur l'ordinateur contenant les données.
5. Les enregistrement demandés sont renvoyés au client.
6. Les données sont présentées à l'utilisateur.

Identifier les fonctions du client et du serveur : Déterminer si l'approche client-serveur est appropriée à un environnement de mise en réseau donné.

Industry standards for SCSI hard disks:

Standard	Bit Width	Cable Name	Pin Count	Max. Rate	x-fer MB/sec	Max SCSI Devices	Description
SCSI-1	8	A	50	5	8		Asynchronous
SCSI-2	8	A	50	10	8		Fast
SCSI-2	16	A+B	50+68	20	8		Fast+wide **
SCSI-2	32	A+B	50+68	40	8		Fast+wide **
SCSI-3	8	A	50	10	8		Fast
SCSI-3	16	P	68	20	16		Fast+wide *
SCSI-3	32	P+Q	68+68	40	32		Fast+wide **

* = with 1 cable
** = with 2 cables

Standard: The name of the SCSI standard as defined by ANSI.
Bit width: The number of bits that are transferred by the SCSI bus during the data transfer phase.
Cable Names: A is most common, P is becoming more popular, A+B is currently not popular due to cost and space issues.
Pin Count: The number of pins in the cable.
Max Transfer Rate (MB/sec): Number of bits transferred over the SCSI bus in one second.
Max SCSI Devices: The maximum number of devices that can be connected to the SCSI bus with one host adapter installed.
Descriptions
Asynchronous: A handshaking protocol that requires a handshake for every byte transferred. (Synchronous transfers a series of bytes before handshaking occurs, increasing the data transfer rate.)
Fast:Fast SCSI is an option that doubles the synchronous data transfer speed. The speed is achieved by removing excess margins from certain times and delays. To use the fast SCSI option, high quality cables are required. This option is compatible with normal synchronous SCSI and has:
- Up to 10 MB/second over an 8 bit bus.
- Synchronous data transfer negotiation required.
- Single-ended implementation recommendations: maximum cable length of 3 meters and active terminators.

Wide: Wide SCSI is an option that adds a second SCSI cable of 68 conductors. This cable provides a data path for 16- or 32-bit data. This path has separate handshake signals and is for data transfer only. The transfer rate is two or four times the present transfer rate of SCSI-1. With the second cable, SCSI-2 remains compatible with the 8-bit SCSI.

Systèmes à tolérance de pannes

Tolérance de panne disque :

Windows NT supporte RAID Levels 0, 1, et 5.

-L' agrégat par bande avec parité a des meilleures performances en lecture que le disque miroir.
-Les données et les informations de parité sont enregistré sur des disques différents.
-Sector Sparing - Automatically adds sector-recovery capabilities to the files system while the computer is running.
-Disponible uniquement si une méthode RAID est utilisé.
-Uniquement sur disques SCSI drives.

RNIS-ISDN

RNIS signifie Réseau Numérique avec Intégration de Services. C'est un réseau comparable à celui du téléphone analogique classique qui permet une liaison entièrement numérique entre deux abonnés. Il permet d'accéder à une large gamme de services tels que téléphonie, base de données, messagerie électronique, etc. Il existe plusieurs types de connexion :

L'accès de base (BRA) : permet une connexion "2B+D" qui est constituée de deux canaux de communication à 64 kbits/s (B1 et B2) et d'un canal de services a 16 kbits/s. Il est plutôt réservé à un usage domestique ne demandant qu'une seule ligne. Cette ligne permet de raccorder jusqu'a 8 terminaux (RNIS Light = 3) dont deux pourront être utilisés simultanément (par exemple : envoyer un fax par le canal B1 pendant que l'on discute au téléphone par l'intermédiaire du canal B2.

L'accès primaire en Europe **E1** (PRA) 2,048 Mbits/s: permet une connexion "30B+D" qui est constituée de 30 canaux à 64 kbits/s (B) et de canaux de services.

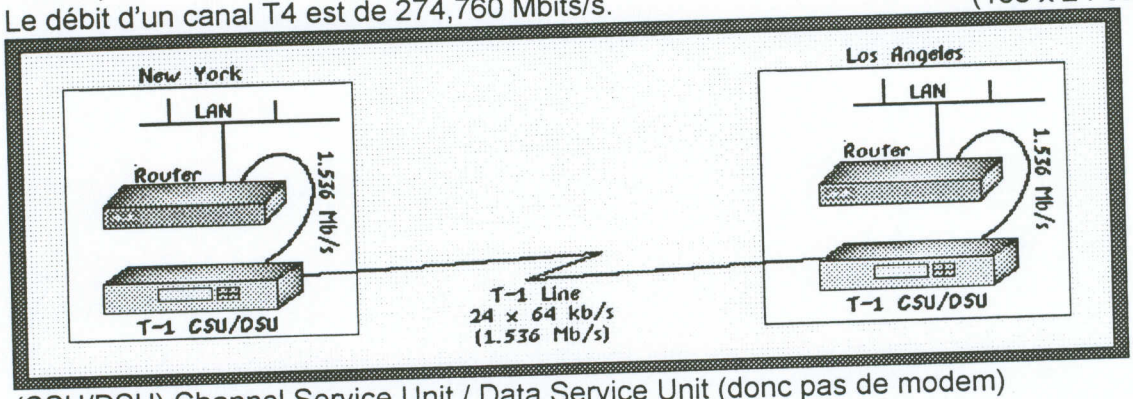
Dans d'autres pays, notamment au Japon et aux **USA**, le PRA est un peu différent :

Le débit d'un canal T1 est de 1.544 Mbits/s compose de 24 canaux: (4 x 24 canaux)

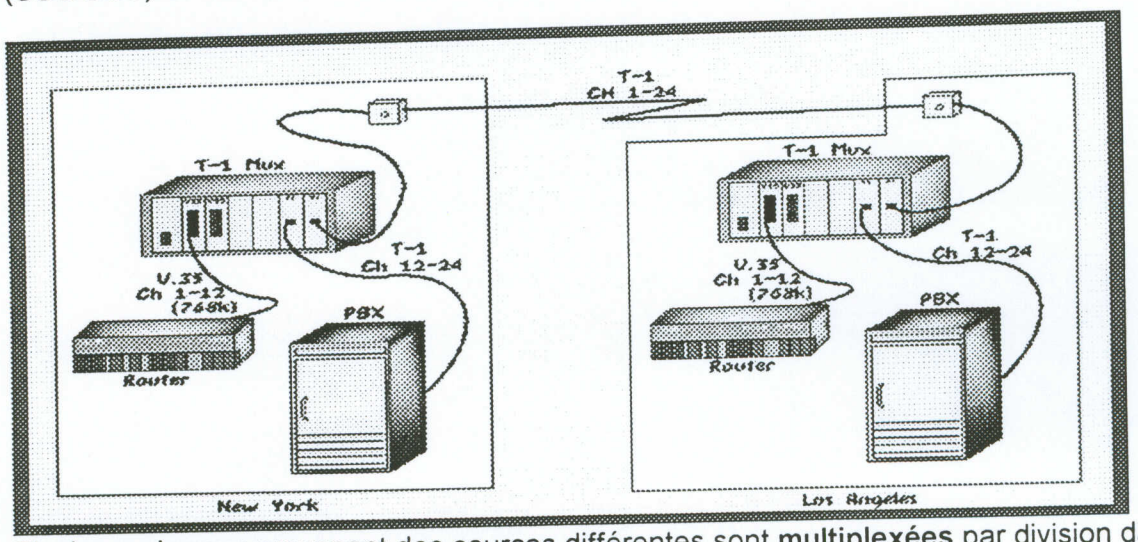
Le débit d'un canal T2 est de 6.312 Mbits/s.

Le débit d'un canal T3 est de 6 à 45 Mbits/s (44.736)(**28** x 24 canaux)

Le débit d'un canal T4 est de 274,760 Mbits/s. (168 x 24 canaux)

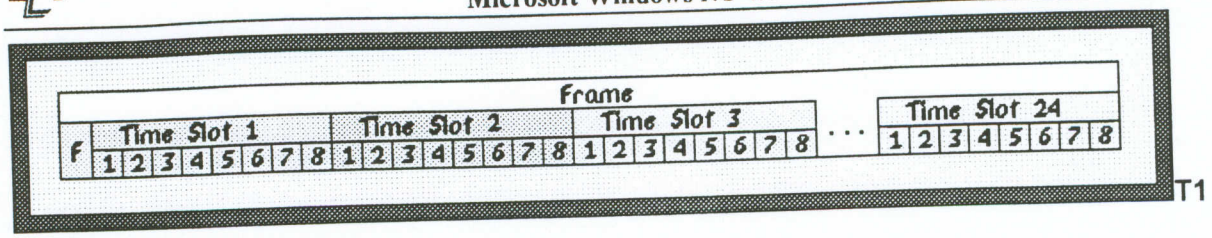


(CSU/DSU) Channel Service Unit / Data Service Unit (donc pas de modem)

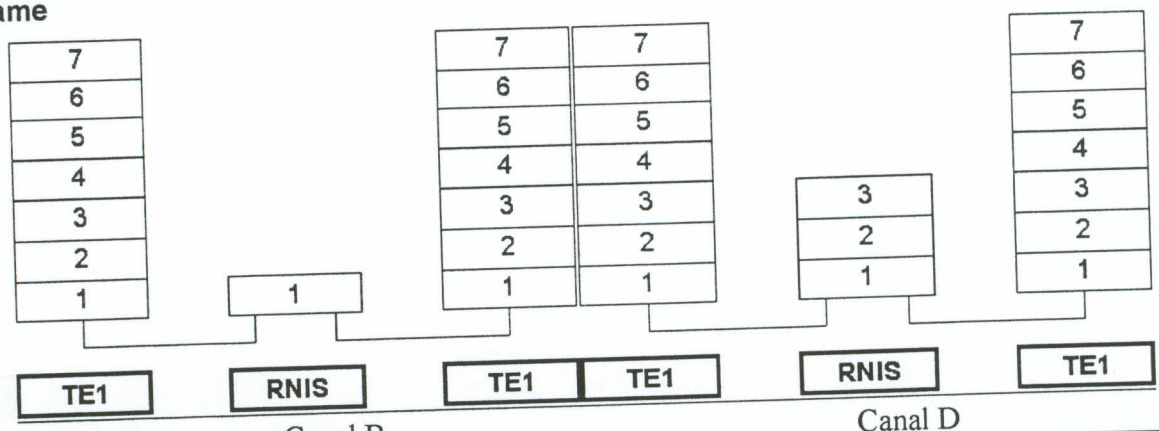


Plusieurs signaux provenant des sources différentes sont **multiplexées** par division dans le temps(*TDM*).

PBX= Private Branch Exchange = ACU (Autocommutateur d'usagers ou central téléphonique)



frame



Le **réseau de transport** du RNIS commute des canaux de 64 kbit/s (commutation de circuit). Il est commandé par le réseau de signalisation afin de fournir un canal B transparent reliant les 2 extrémités	L'usager (TE1) utilise son canal D sécurisé pour établir une communication. Il communique avec le **réseau de signalisation** du RNIS, disponible pour transmettre la taxation, gérer d'autres appels, utiliser la commutation par paquet,...

ISDN est un service commuté et occupe les réseau pendant toute la durée de la communication, c'est ce qu'on appelle une technique plesiochrone (STM : Synchronous Transfert Mode)
Swisscom propose des forfait pour une installation qui comprend le raccordement du terminal NT sur une prise téléphonique ainsi qu'une prise 220V existantes. Dans le cas de l'installation d'une nouvelle prise téléphone, l'installation existante sera raccordée au port analogique.
L'installation d'un Mini S0-Bus permet de raccorder : 5 raccordements ISDN et 2 raccordements analogiques. Les taxes mensuelles sont prévu pour 10 numéros ou 5 numéros. Le raccordement ISDN Light : 3 numéros.

Transmission analogiques : Utilisation de modems dans les communications réseau
-Asynchronous Communications (Async)
Presque tous les fabricants de téléphones, appareils fax ou répondeurs automatiques utilisent une prise RJ11 pour le raccordement téléphonique. Les petites prises RJ11 sont fabriquées de PVC transparent et normalement munies de 4 contacts dorées. Cependant, la ligne téléphonique analogique nécessite que 2 des 4 fils conducteurs. C'est pourquoi certains câbles ne sont confectionnés qu'avec 2 fils conducteurs.
NORME SUISSE : Mondialement, tous les fabricants veillent à ce que la ligne téléphonique est branchée sur les deux fils conducteurs au milieu de la prise. En Suisse, il existe cependant une norme spéciale de Swisscom, selon laquelle la ligne téléphonique est branchée sur les fils conducteurs 1 et 2. Cette norme spéciale est appliquée à tous les téléphones vendus par Swisscom. Un câble spécial existe qui connecte les fils conducteurs 2 et 3 de l'adaptateur a/b avec les raccordements 1 et 2 du téléphone.

Standard	BPS
V.22 bis	2400
V.32	9600
V.32bis	14,400
V.32terbo	19,200
V.FastClass (V.FC)	28,800
V.34	28,800
V.42	57,600

-Synchronous Communication :Porteuses

X 25

X25 est un ensemble de protocoles incorporés à un réseau à commutation de paquets. Le réseau à commutation de paquets est constitué de services de commutation qui, à l'origine, permettaient de relier des terminaux distants à des grands systèmes hôte.
Un réseau à commutation de paquets X25 utilise les commutateurs, les circuits et les routes disponibles pour assurer le routage optimal à un instant donné. Les premiers réseaux X25 transmettaient les données sur des lignes téléphoniques. Etant donné que ce support, peu fiable, générait de nombreuses erreurs, X25 intègre désormais des fonctionnalités de contrôle très complètes. En raison du contrôle d'erreurs et de la retransmission, X25 peut paraître lent.
La suite de protocoles X25 définit l'interface entre un équipement fonctionnant en mode de paquets syncrone et le réseau public.
Un PAD (Paquet Assembler Disassembler) reçois des caractères asynchrones et les assemble en paquets pour les transmettre sur le réseau. TELEPAC est le nom du réseau X25 en Suisse.

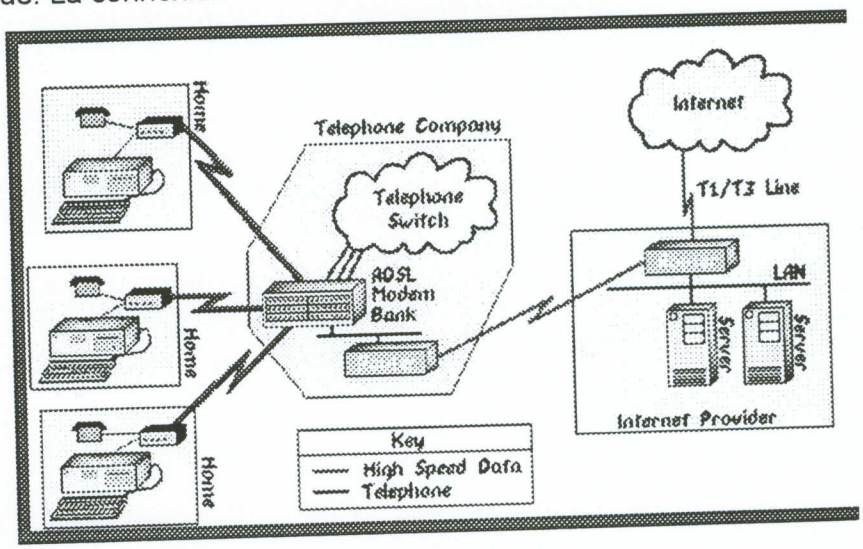
Relais de trame (Frame Relay) :

Le relais de trame (Frame Relays) est une technologie numérique avancée de commutation de paquets performante en terme de vitesse qui utilise des paquets de longueur variable.

Les concepteurs de cette technologie ont éliminé plusieurs fonctions X25 de comptabilisation et de contrôle, car elles étaient devenues inutiles dans un environnement sécurisé et fiable à base de fibre optique.
FRAME RELAY permet d'obtenir une bande passante sur demande.

ADSL (Asymmetric Digital Subscriber Line)

Le principe de l'ADSL repose sur la sous-exploitation du cuivre qui débouchent chez tous les usagers. En envoyant la voix et les données à des fréquences différentes, on parvient à délivrer, sur une seule ligne téléphonique, un accès rapide a INTERNET tout en conservant les services habituels de la ligne (réception et émission d'appels). L'accès à INTERNET ne paralyse pas la ligne téléphonique. La connexion INTERNET est facturée au forfait.



Le rayon d'action de L'ADSL est de 4 à 5 Kilomètres.
L'opérateur téléphonique doit installer dans son central un modem pour chaque abonné.
Les abonnés au téléphone qui résident trop loin des centraux téléphoniques ne bénéficieront pas de l'offre ADSL.
L'ADSL autorise des débits allant jusqu'à 8 Mbits/s en voie descendante et 640 Kbits/s en voie remontante.
SWISSCOM propose un débit de Max 256 Kbits/s pour 399.- SFr. par mois.
Un technicien doit installer un filtre répartiteur chez l'abonné et le modem ADSL (SWISSCOM facture l'installation 3200.- SFr)
Une solution ADSL Light sera proposé et le déplacement du technicien sera inutile. La phase de production des modems ADSL Light doit démarrer en l'an 2000.

ATM (Asynchronous Transfert Mode)

Pourquoi une nouvelle couche 2 (liaison)?

Au cours des années 80 une méthode a été proposé permettant d'intégrer une communication Multimédia avec une bande passante importante. Cette méthode, ATM (Transmission Temporelle Asynchrone) a été normalisée par l'ISO et le CCITT en 1989.

Les contraintes de l'intégration

En ce qui concerne les données informatiques, il faut envoyer un maximum d'informations en un temps très court, cela est traditionnellement réalisé en augmentant la taille des paquets en fonction de la masse d'informations à transporter.
En effet, plus le paquet est grand, plus le temps, généralement fixe, nécessaire à la détermination du chemin à parcourir dans le réseau devient négligeable par rapport au temps de transfert du paquet. Il en résulte de cette technique un temps de transmission optimisé mais variable (fonction de la taille du paquet).
En revanche les données représentant la voix ou la vidéo nécessitent un temps de transmission constant et une bande passante garantie.
Ces deux types de contraintes sont incompatibles car sur un réseau classique avec des paquets de taille variable, un paquet transportant de la voix ou de la vidéo placé derrière un grand paquet transportant des données informatiques, ne pourra se voir garantir un délai d'acheminement et l'information (voix, vidéo) sera déformée et tronquée;
Il faut donc trouver une méthode qui combine les avantages de la commutation de circuits (temps de transfert constant et bande passante garantie) avec les avantages de la commutation de paquets (souplesse et prise en compte optimisée d'un trafic intermittent).

Principe d'ATM

ATM intervient au niveau de la couche 2 du modèle OSI (liaison);
Cette technique consiste à transporter de tout petits paquets de 53 octets appelés cellules.
Ces cellules comportent en fait 48 octets de données plus 5 données d'en-tête.
Ces cellules sont de longueur constante.
Les cellules passent par des noeuds de commutation rapide et les temps de transport des cellules d'un bout à l'autre du réseau sera pratiquement constant.
Comme dans la commutation de paquets X25 **on définit des circuits virtuels dans lesquels l'acheminement des cellules sera effectué de façon logique par les commutateurs** en lisant l'en-tête. Vu de l'utilisateur ces circuits apparaîtront comme des circuits commutés.
Cette technique se rapproche donc du mode de communication synchrone ce qui est satisfaisant pour la communication de la voix et de la vidéo.
Les cellules ATM sont remplies à l'émission par l'information arrivant de façon asynchrone depuis les applications. Les cellules ne sont envoyées qu'a la demande des applications on alloue dynamiquement, selon la bande passante disponible, les différents débits nécessaires.
Le temps de commutation est très bref par rapport au temps de propagation.
Exemple : pour une vitesse de 1Gbit/s il faut 424 microsecondes pour émettre une cellule de 53 octets (424 bits). Les noeuds de commutation permettent de commuter cette cellule en 10 microsecondes. Sur un réseau de fibre optique il faut environ 1 ms pour propager cette cellule sur 250 km ce qui est bien supérieur au temps de commutation.
Un noeud de commutation est un simple PABX qui en entrée analyse l'information pour savoir vers quelle sortie l'orienter.
Les cellules ATM sont reçues dans leur ordre d'émission. Il peut y avoir des erreurs de transmission car le CRC ne protège que l'en-tête et pas les informations. Il faut donc une correction au niveau des couches supérieures. Les procédures de contrôle de flux ne sont pas encore totalement définies (décembre 1994).

La couche physique : ATM appartenant à la couche 2 du modèle de référence OSI il est donc indépendant du support de transmission mais est pleinement efficace sur les réseaux de fibres optiques. Au niveau de la couche physique, il est nécessaire d'utiliser un protocole qui décrit précisément comment les cellules vont être émises sur le médium. Plusieurs solutions sont envisageables. La plus couramment utilisée se nomme SONET (Synchronous Optical Network) ou son équivalent en Europe SDH (Synchronous Digital Hierarchy) .

Le principe consiste à faire transiter en permanence toutes les 125 microsecondes une trame (un bloc de paquets parfaitement défini et de longueur constante) entre deux noeuds de commutation. Schématiquement, ceci correspond à un train qui circule en permanence entre deux gares, une cellule ATM peut monter dans ce train à n'importe quel moment et à n'importe quel endroit de ce train.
SONET est une recommandation du CCITT et a déjà été adoptée par la téléphonie américaine pour la gestion de ses réseaux et adaptée pour recevoir ATM.
SONET exploite aussi les différentes vitesses pour le support optique :
OC-1(Optical Carrier) 45 Mbits/s
OC-3 135 Mbits/s (3 x 45)
OC-12 540 Mbits/s (12 x 45)
Ces vitesses ne sont limitées que par la technique des interfaces, on envisage déjà les vitesse OC-24 36 ou 48, soit 1,24, 1,86 et 2,5 Gbits/s.
La génération existante aujourd'hui est dite plésiochrone. La vitesse de base est de 2 Mbits/s suivie par des vitesses multiples de celle-ci soit 34 et 140 Mbits/s. C'est l'offre actuelle (1993) de France Télécom et des autres PTT européennes.
Les nouveaux matériels de transmission qui arrivent depuis peu (1993) aux USA sont basés sur la technique SONET ou SDH avec des débits de 155 Mbits/s puis 620 Mbits/s...

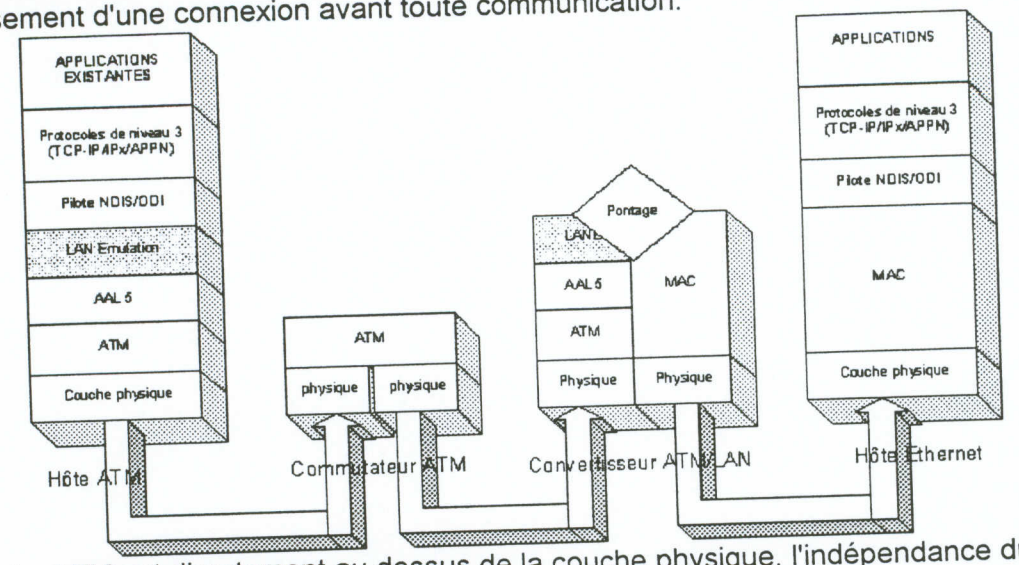
Perspectives

L'introduction de produits SDH correspondent aux besoins du réseau de communication interurbain des grands commutateurs régionaux. Le réseau de distribution ne sera pas sous cette technique avant longtemps.
On prévoit d'installer une prise ATM dans les foyers vers 2010, mais cette technique intéresse surtout les opérateurs du câble pour le multimédia.
Cette technique s'applique aux interconnexions d'ordinateurs et également aux besoins vidéo. Cette dernière catégorie apparaît comme l'une de plus prometteuses car elle est déjà très demandée pour la visioconférence.
Actuellement Alcatel dispose déjà de "chips" ATM à **620 Mbits/s**.
Le RNIS se trouvant au niveau 3 profite naturellement des améliorations en vitesse qu'apportera ATM.

Déploiement d'ATM, ATM et les réseaux locaux existants.

Bien q'ATM permette la connexion directe de stations de travail et de serveurs cela nécessite le changement des cartes d'interface et peut-être de la topologie du réseau. Pour préserver l'investissement fait dans les réseaux locaux (70 millions de noeuds Ethernet installés dans le monde) le forum ATM a défini un protocole d'émulation de réseaux locaux (LAN Emulation - LANE) dont " Le principal objectif consiste à permettre aux applications existantes d'accéder à un réseau ATM via les piles de protocoles APPN, NetBIOS, IPx, etc ..., comme si elles s'exécutaient sur un réseau local traditionnel ".
Il existe des différences fondamentales entre les réseaux locaux ATM et les réseaux locaux à support partagé (Ethernet, Token Ring, FDDI, ...) :
ATM est "orienté connexion " alors que les réseaux locaux classiques sont " sans connexion " ;
Les réseaux locaux classiques utilisent la diffusion générale (broadcast) alors qu'ATM ne permet que des connexions point à point ou point à multipoint.

Afin de protéger les investissements des utilisateurs au niveau des applications et des logiciels réseau, et pour rendre le support ATM utilisable par les protocoles existants, ATM va devoir se comporter comme un réseau local classique grâce à LANE.
Du point de vue conceptuel LANE offre une couche de traduction entre les couches hautes s'appuyant sur un service sans connexion et la couche basse ATM qui nécessite l'établissement d'une connexion avant toute communication.



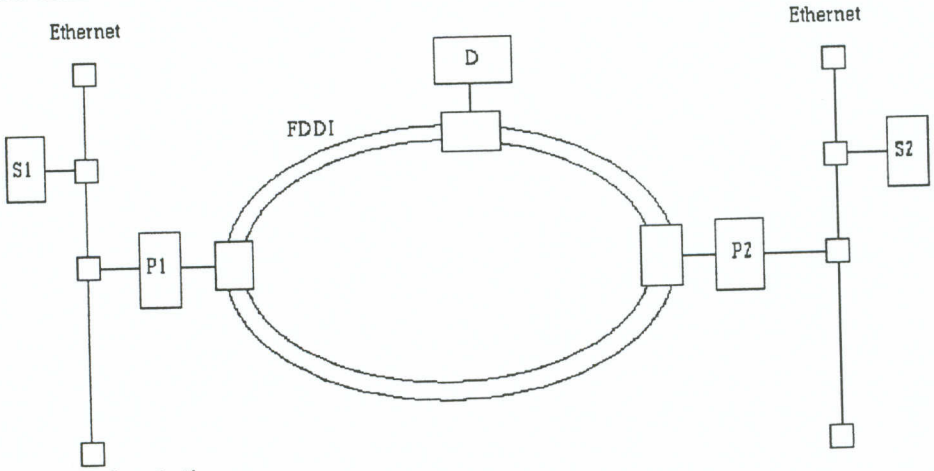
La couche ATM est directement au dessus de la couche physique, l'indépendance du support est un principe fondamental d'ATM. La couche ATM gère les en-têtes des cellules ATM qui sont de longueur fixe. Elle reçoit, des couches supérieures, les informations à mettre dans les cellules, elle ajoute l'en-tête et passe les cellules résultantes (53 octets) à la couche physique. En réception elle reçoit les cellules de la couche physique, extrait l'en-tête, et passe les 48 bits restants aux couches supérieures. La couche ATM n'a pas connaissance du type de trafic qu'elle transporte, cependant elle doit distinguer les qualités de service grâce aux informations acquises pendant la phase de connexion.
La couche d'adaptation ATM (ATM Adaptation Layer - AAL) découpe les données en " morceaux " de 48 bits afin de pouvoir les " charger " dans les cellules (cette opération s'appelle la segmentation). Lorsque les cellules ATM atteignent leur destination, on reconstruit les données pour les couches supérieures, ce processus s'appelle ré assemblage.
Comme ATM doit pouvoir transmettre différents type de trafic, il existe, au niveau de la couche adaptation, plusieurs protocoles, chacun travaillant simultanément. C'est l'AAL de type 5 qui est utilisée pour l'émulation de réseau local, LANE est donc au dessus de AAL5.
Dans un convertisseur LAN/ATM LANE résout les problèmes pour tous les protocoles (routables ou non routables) en traduisant les adresses LAN et les adresses ATM au niveau de la couche MAC. LANE est totalement indépendant des protocoles des couches supérieures, des services et des applications. LANE est entièrement transparent pour les réseaux ATM et pour les hôtes Ethernet ou Token Ring. LANE masque complètement l'établissement de la connexion et les fonctions de prise de contact (handshaking) nécessaires aux commutateurs ATM.
LANE traduit les communications entre noeuds ayant une adresse MAC (réseaux locaux classiques) en communications sur des circuits virtuels ATM. Le réseau ATM apparaît alors comme un réseau sans connexion (pour les couches supérieures).
Grâce aux modifications apportées a NDIS5 de Windows 2000, il sera possible de communiquer de façon directe et orienté connexion par l'ATM. L'architecture QoS (Quality of Service) peut alors être utilise. Etant donné qu'ATM est orienté connexion et utilise des commutations, chaque client a accès à toute la bande passante. Il est possible d'utiliser IP par le bias d'ATM et d'obtenir une communication ATM directe. Ce point est particulièrement important pour les applications multimédia, qui impliquent le transfert de grandes quantités de données.

FDDI (Fiber Distributed Data Interface)

Norme ANSI : X3T9.5 (Le comité X3T9 définit les interfaces d'entrées/sorties Exemple : X3T9.2 = SCSI).
Le début des études date de 1982, les premiers produits commerciaux sont apparus en 1990.
Généralités, caractéristiques : La topologie est constituée d'un double anneau redondant en fibre optique, la lumière se propage en sens inverse dans chaque anneau.
La méthode d'accès est semblable à Token Ring (802.5) Débit 100 Mbps
La fibre Multimode :Diamètres : 62,5/125 um, Fenêtre : 1300 nm, Emission par LED (Light Emitting Diodes)
Réception par photo détecteurs PIN (P-Insulated N-Channels), Vitesse 100 Mbits/s
Taille du jeton 11 octets soit 448 m de fibre occupés
Taille minimale du paquet : 28 octets soit 448 m de fibre occupés
Taille maximale du paquet : 4500 octets soit 7200 m de fibre occupés
Retard induit par une station : 15 octets soit 1,32us

Topologie (2 anneaux redondantes)

L'anneau peut avoir une circonférence de 100 km, on peut avoir jusqu'à 2 km entre les stations, au delà de 2 km le signal est trop dispersé (les stations jouent le rôle de répéteur), la distance entre les stations sera étendue à 60 km avec les fibres monomodes.



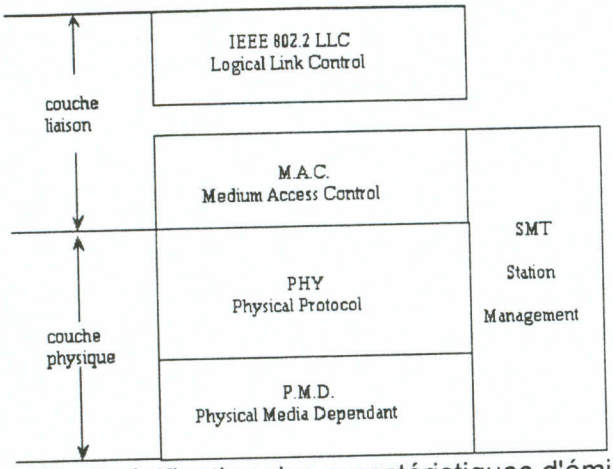
La norme définit 3 types de stations :
- DAS (Dual Attachment Stations) - classe A
Elles sont connectées à l'anneau actif et à l'anneau de secours.
- SAS (Single Attachment Stations) - classe B
Elles sont uniquement connectées à l'anneau actif (primaire)
- Concentrateurs - classe C
Les stations DAS permettent la redondance en validant leur connexion à l'anneau de secours en cas de coupure de l'anneau principal.
On peut avoir jusqu'à 255 concentrateurs en cascade

La méthode d'accès

Différences avec Token Ring :
- Le jeton est libéré après l'émission de la trame alors que pour token ring il n'est libéré qu'après son retour à la station émettrice.
- Le jeton n'est pas attribué par une station maîtresse mais négocié par l'ensemble des stations: avant d'émettre les stations calculent et transmettent le temps de capture du jeton

(temps nécessaire au remplissage du jeton) _ la station qui a le droit d'émettre est celle qui a le temps de capture le plus court.

FDDI et le modèle OSI



PMD :Spécification des caractéristiques d'émission telles que le taux d'erreur soit inférieur à 10^{-9}.
- Définition d'un relais optique (Bypass) permettant de relier directement en aval ou en amont une station défectueuse ou hors tension.
PHY : - Encodage et décodage des données

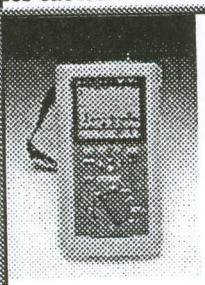
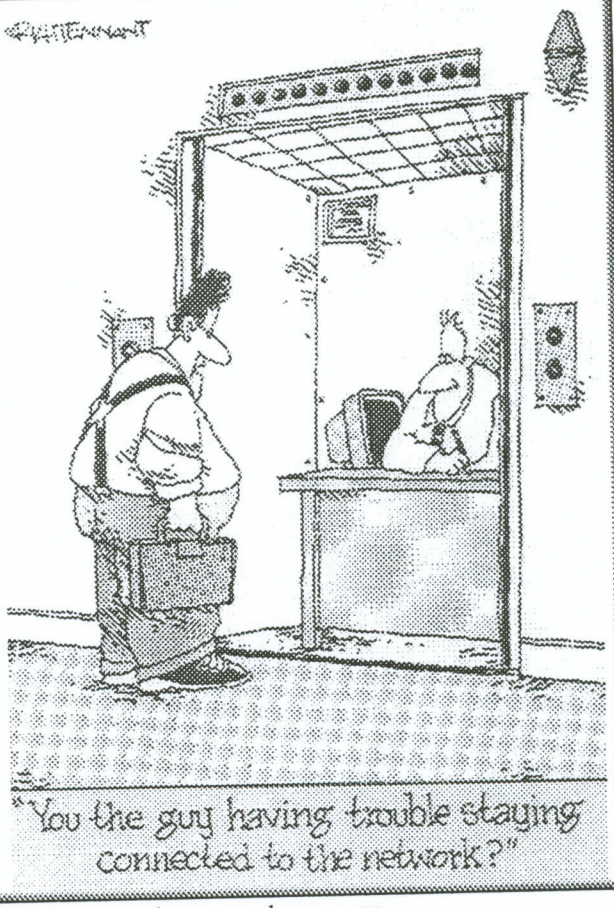
Beaconing : Dans un réseau FDDI tous les ordinateurs sont chargés de surveiller le passage du jeton. Pour isoler les défaillances graves dans l'anneau, FDDI emploie un système nommé beaconing (balisage). Avec ce système, l'ordinateur qui détecte une défaillance envoie un signal appelé beacon (balise) jusqu'à ce qu'il détecte un beacon provenant de son voisin situé en amont. Ce processus se poursuit jusqu'à ce que le seul ordinateur à émettre un beacon soit celui qui se trouve immédiatement en aval de la défaillance. Lorsque l'ordinateur qui émet un beacon reçoit finalement son propre beacon, il part du principe que le problème a été résolu. Il régénère alors un jeton et le réseau se remet à fonctionner normalement.

FDDI peut aussi être mis en œuvre avec des câbles en cuivre. On parle alors de CDDI (Copper Distributed Data Interface) Avec cette variante les distances de transmission sont beaucoup plus courtes.

Dépannage du réseau

TECHNICAL SUPPORT

Méthodologie de dépannage.
Outils spéciaux tels que le contrôleur de câble et les analyseurs de protocole

Outils (Tool)	Fonction
Digital Volt Meters (DVM)	Principalement utilisé pour diagnostiquer des court circuits, coupures ou autres problèmes avec les câbles.
Réflectomètres temporels Time-Domain Reflectometer (TDRs) Optical TDR	 Envoient sur le câble des impulsions semblables à celles d'un SONAR afin de rechercher une coupure, un court-circuit ou une imperfection dans le câble. 
Oscilloscope	Utilisé conjointement avec des réflectomètres temporels permet de mesurer Plis dans les câbles, court circuits ou coupures.
Contrôleurs de câbles sophistiques	Fonctionne au-delà de la couche Physique du modèle OSI, au niveau des couches 2,3 et même 4. Ils affichent des informations sur l'état du câble physique ainsi que sur : le nombre de trame, l'excès de collisions, les dernières collisions, le nombre de trames altérées, les erreurs d'encombrement, le beaconing (balisage)
Moniteur reséau	Examines parquet types, errors and traffic to and from each computer on a network.
Analyseur de protocoles	Les analyseurs de protocole, également appelés analyseurs de réseau, effectuent un certain nombre de tâches d'analyse de trafic en temps réel. De plus, ils peuvent capturer les paquets, les décoder et les réexpédier. Il est un outil de prédilection en matière de surveillance interactive du réseau.

Historique d'Internet

Internet est le "Père de tous les réseaux" et signifie "International Network". Il s'agit d'un important réseau informatique qui se compose de nombreux petits réseaux locaux. À l'origine, on appelait encore Internet **Arpanet**. ARPA (Advanced Research Project Agency) est la branche du département américain de la Défense qui avait été chargée de l'organisation du réseau informatique "résistant à la destruction". Dans les années 60, sur fond de crise de Cuba et de menace d'une guerre nucléaire, les stratèges américains se demandaient ce qu'il adviendrait si des installations de communications comme les lignes téléphoniques, les stations de radio et de télévision étaient détruites par des attaques.
Le Pentagone a établi une structure de communication qui promettait de fonctionner de façon fiable, même en cas de dommages importants. En 1964, le développeur de logiciels Baran a présenté un modèle de réseau d'informations basé sur ordinateur, qui ne possédait aucune gestion centralisée, aucun point central défini ni aucune autorité de gestion. Les villes des USA devaient elles aussi être mises en réseau sur un système confus. Ce concept représentait un chaos organisé - et pourtant les militaires acceptèrent cette idée.

Routage

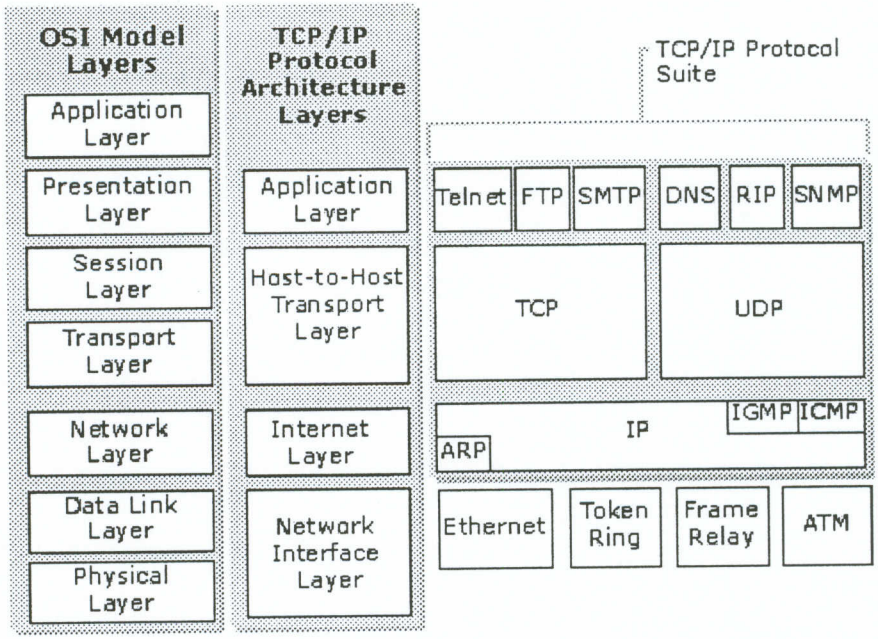
Les informations électroniques envoyées sont divisées en petites parties (paquets) par le réseau de Baran. Chaque paquet est placé dans une enveloppe numérique comportant l'expéditeur et l'adresse. A la réception les paquets sont alors "dépaquetés" et reconstitués. En cas d'absence de certains paquets, l'ordinateur cible envoie un message à l'ordinateur source qui renvoie le paquet. En théorie, chaque paquet de données peut être envoyé via une autre ligne informatique. L'ordre d'arrivée des paquets n'est pas prédéfini. Si une ligne est défectueuse, les paquets d'informations trouvent tout simplement un nouveau chemin d'acheminement.

Les premiers expérimentations de la DARPA

En 1970, les universités de UCLA (Los Angeles), UCLB (Santa Barbara), UTAH (Salt Lake City) et SRI international (Stanford-SanFrancisco) ont mis en réseau leurs ordinateurs selon le principe de Baran : ainsi naquit Internet. En 1972, une démonstration reliait cinquante nœuds et vingt hôtes.
Le terme nœud est un nom générique pour tout périphérique connecté à un réseau. Ce périphérique peut etre un périphérique de routage ou un ordinateur (ordinateur personnel, station de travail, mini-ordinateur ou mainframe)
Un autre terme, hôte est aussi très largement employé dans le monde des réseaux. Historiquement, ce terme se rapporte à un ordinateur puissant sur lequel sont connectés plusieurs terminaux. Aujourd'hui, ce terme est utilisé pour toute machine qui offre un service à des utilisateurs.
1984 le nombre de hosts atteint 1000
1984 Microsoft en est à la version MSDOS 3.1 qui ajoute un support pour les réseaux.
Après 1984, les réseaux militaires formèrent un réseau unique indépendant des autres réseaux.
Grâce au concept de Baran, le nombre d'ordinateurs connectés à Internet s'élève de nos jours à environ 4,5 millions, ceci n'ayant entraîné aucun problème de gestion important. On put bientôt déjà distinguer les avantages de ce réseau en constante expansion :
L'invention du courrier électronique (E-mail).
Des données et programmes peuvent être chargés via des liaisons de données sur un ordinateur personnel à partir d'un autre ordinateur du réseau. File Transfer Protocol (FTP).
Il est possible d'exécuter une application sur un système distant (TELNET).
Ce n'est qu'en 1993 qu'a été "introduit" le WWW (World Wide Web). C'est grâce à ce dernier que l'utilisation d'Internet a connu une telle extension car il a depuis lors été possible d'émettre, via Internet, des textes, des images, du son et même des films.

La suite des protocoles TCP/IP : Vue d'ensemble

La suite des protocoles Microsoft TCP/IP est constitué de *core protocol elements* et *services*, séparé par des interfaces.
La Transport Driver Interface (TDI) et the Network Device Interface (NDIS) sont publiques et leurs spécifications sont disponible chez Microsoft.
Il y a aussi un certain numéro de higher level interfaces disponibles pour application user-mode.
Les plus utilisés sont Windows Sockets et NetBIOS.



IP Le protocole IP fournit un transfert non sécurisé de transmission des paquets en mode datagramme. Ce protocole assure la fonction de la couche 3 du modèle OSI.
La couche transport (couche 4 selon la représentation OSI) comprend - dans le monde UNIX - trois protocoles essentiellement : UDP, TCP et VMTP. UDP et TCP sont les plus utilisés. Le protocole TCP est plus complexe que le protocole UDP mais il offre un transport sécurisé des données ainsi qu'un certain nombre de contrôle comme nous allons le voir.

TCP (Transport Control Protocol)

Le protocole TCP peut fonctionner sur d'autres couches 3 que la couche IP (contrairement au protocole UDP). TCP offre une couche simple et harmonieuse pour interfacer une application et la couche IP. L'interface entre les applications et la couche TCP (que l'on nomme en anglais *"The Internet Stream Delivery Service"*) présente cinq caractéristiques essentielles :

Fonctionnement par flux (*"stream orientation"*)

Deux applications échangeant de gros volumes de données s'échangent en fait des flux de bits. TCP est le service protocolaire permettant une transmission sécurisée de ces flux.

Connexion par circuit virtuel

Quatre étapes ponctuent le fonctionnement d'une connexion par TCP :
Avant le transfert des données, émetteur et récepteur échangent des données nécessaires à leur couche protocolaire. Une fois les vérifications faites, la couche transport informe l'application qu'elle peut utiliser la connexion qui vient d'être établie. La couche applicative voit donc la connexion comme un tuyau bi-directionnel dans lequel les données seront véhiculées. Durant le transfert, les couches transport poursuivent leur dialogue indépendamment des dialogues des couches applicatives. Ce dialogue a pour but de vérifier que les données arrivent vers la bonne destination, sans détérioration et sans engorgement du réseau, rétablir la connexion si celle-ci est "*tombée*" durant le transfert.

Transfert bufferisé

L'application émet et reçoit les données au rythme et suivant les volumes qu'elle souhaite. La couche transport découpe de manière transparente ces buffers pour les passer à la couche IP. Ce découpage entraîne la création de paquets. TCP optimise ce découpage afin de garantir le meilleur débit possible.

Flux non structuré

La couche TCP n'impose pas une structure particulière aux données véhiculées : il considère les données applicatives comme des boîtes noires. Cette technique donne une certaine souplesse d'utilisation.

Connexion bi-directionnelle (ou mode "*full duplex*")

Les transferts peuvent s'effectuer simultanément dans les deux sens. Il n'y a pas de contrainte spécifique.

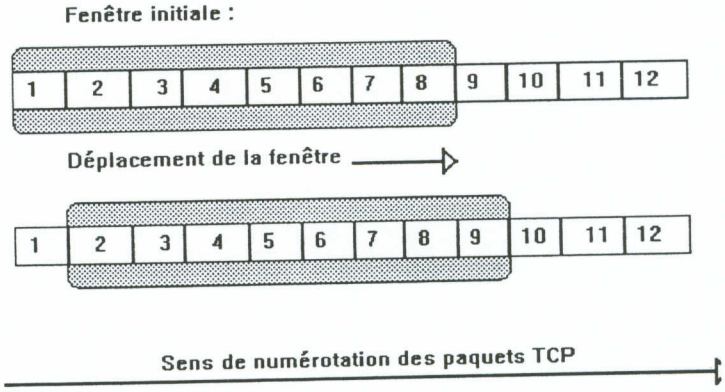
Transport sécurisé par TCP

TCP se base sur des ACKnowledges "positifs" avec retransmission possible des paquets invalidés. Cette solution implique la possibilité de transmettre des messages de quittance. L'émetteur conserve un enregistrement des paquets émis et attend un ACKnowledge pour émettre le paquet suivant :

Fonctionnement de TCP

Taille de fenêtre variable et contrôle de flux

Le protocole TCP autorise la modification de la taille de la fenêtre d'acquittement des paquets. TCP utilise une technique de fenêtre glissante dont la taille pourrait être quelconque. Ce déplacement de fenêtre a été autorisé grâce à l'émission d'un paquet ACK.



Structure des paquets TCP

Dans le langage UNIX, les paquets TCP sont appelés des segments. Il existe plusieurs types de segments: des segments de données, d'acquittement , d'établissement de connexion, de changement de taille de fenêtre et des segments de fermeture de connexion.

Time-out et retransmission

Chaque fois qu'un segment TCP est envoyé, un timer est armé par l'émetteur et TCP attend un acquittement. Si le timer passe à zéro alors que cet acquittement n'est pas reçu, TCP considère AUTOMATIQUEMENT que le segment a été perdu ; il le retransmet donc. Comme les segments TCP passent par des gateways (passerelles) et des machines dont les performances sont variées, TCP doit adapter les timers suivant la topologie du réseau physique par lequel les données circulent. Pour ce faire, il utilise un algorithme adaptatif.

Gestion de l'engorgement

Si un engorgement se produit sur un point du réseau, les délais de transmission augmentent. Les routeurs ou les machines hôtes qui sont engorgées émettent des messages **ICMP Source Quench** pour avertir les machines émettrices que des segments vont être perdus.

L' Adressage IP :

On appelle hôte tout appareil rattaché au réseau et utilisant TCP/IP. Pour recevoir et livrer des paquets convenablement entre les différents hôtes, TCP/IP se fie à trois informations, que fournit l'utilisateur : l'adresse IP, le masque de sous-réseau et la passerelle par défaut.

L'administrateur du réseau fournit ces trois informations pour configurer TCP/IP sur un ordinateur. Sur les réseaux dotés de serveurs DHCP, les utilisateurs de Windows NT peuvent bénéficier de la configuration de système automatique, qui les dispense de configurer manuellement les paramètres TCP/IP. Cette section fournit des détails sur les adresses IP, les masques de sous-réseau et les passerelles IP.

Sur un réseau TCP/IP, chaque interface hôte (ou nœud) est identifiée par une adresse IP unique. Cette adresse sert à localiser un hôte sur un réseau ; elle spécifie également des informations de routage sur un réseau étendu. Chaque adresse IP est une valeur 32 bits unique sur un réseau TCP/IP, habituellement exprimée en notation décimale avec points. Cette notation représente chaque octet (8 bits) d'une adresse IP par sa valeur décimale, en utilisant des points comme séparateurs. Une adresse IP présente l'aspect suivant :
102.54.94.97
Important : Comme les adresses IP identifient des nœuds sur un réseau interconnecté, il faut affecter à chaque hôte du réseau étendu une adresse IP unique, valide pour son réseau particulier.

ID réseau et ID hôte :
Bien que représentée par une seule valeur, une adresse IP contient deux informations : l'ID réseau et l'ID hôte (ou ID système) de votre ordinateur.

- **ID réseau** identifie un groupe d'ordinateurs et d'autres appareils qui se trouvent sur le même réseau logique et sont séparés ou interconnectés par des routeurs. Dans les inter-réseaux (réseaux formés par un ensemble de réseaux locaux interconnectés), chaque sous-réseau possède un ID réseau unique.
- **ID hôte** identifie votre ordinateur à l'intérieur d'un ID réseau déterminé. (On appelle hôte tout appareil rattaché au réseau et utilisant TCP/IP).

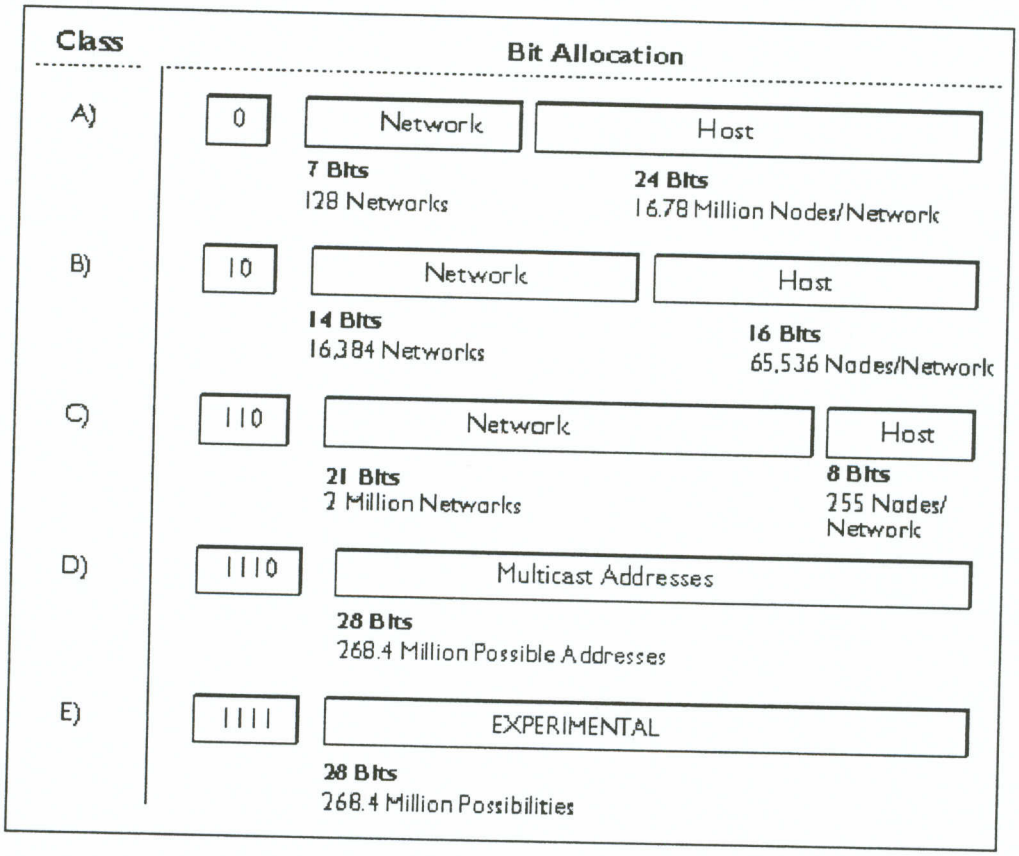
Les réseaux connectés au réseau Internet public doivent soumettre une demande d'attribution d'ID réseau officiel auprès de l'InterNIC, l'organisme qui assure l'unicité des ID réseau IP. Il est possible de contacter l'InterNIC par courrier électronique. Les demandes d'inscription Internet peuvent être envoyées à hostmaster@internic.net.
Une fois l'ID réseau obtenue, l'administrateur du réseau local doit attribuer des ID hôte unique à tous les ordinateurs du réseau. Bien que les réseaux privés non connectés à l'Internet puissent choisir leur propre identificateur réseau, il est toujours recommandé de se faire attribuer un ID réseau valide par l'InterNIC, dans la mesure où cet identificateur officiel permettra à l'avenir de se connecter à l'Internet sans avoir à redéfinir toutes les adresses.

La communauté Internet a défini des classes d'adressage pour prendre en compte la diversité des tailles des réseaux. Chaque classe de réseau se déduit facilement de la valeur du premier octet (8 bits) de son adresse IP. Le tableau suivant résume la relation entre le premier octet d'une adresse donnée et ses champs ID réseau et ID hôte. Il précise également le nombre total d'ID réseau et d'ID hôte pour chaque classe d'adresse qui participe au système d'adressage Internet. Dans ce tableau, les quatre champs de 8 bits d'une adresse IP sont représentés par w.x.y.z.

Classes d'adressage

Classe		ID réseau	ID hôte	Réseaux	PC
A	1-126	w	x.y.z	126	16 777 214
B	128-191	w.x	y.z	16 384	65 534
C	192-223	w.x.y	z	2 097 151	254

L'adresse 127 est réservée aux tests par bouclage et aux communications interprocessus sur l'ordinateur local ; elle ne peut donc être utilisée comme adresse de réseau. Les adresses 224 et suivantes étant réservées pour des protocoles spéciaux (IGMP multidestinataire et autres), elles ne peuvent pas s'utiliser comme adresses d'hôte.



Un hôte réseau utilise les ID réseau et hôte pour déterminer les paquets qu'il doit recevoir ou ignorer, ainsi que l'étendue des transmissions qu'il produit (seuls les nœuds possédant le même ID réseau acceptent mutuellement leurs diffusions de niveau IP). Comme l'adresse IP de l'expéditeur est incluse dans tous les paquets IP sortants, elle permet au système informatique récepteur de déduire l'ID réseau et l'ID hôte de l'émetteur à partir du champ de l'adresse IP. Ceci s'accomplit au moyen de masques de sous-réseau, comme l'explique la section suivante.

Les masques de sous-réseau

Les masques de sous-réseau sont des valeurs 32 bits qui permettent au destinataire de paquets IP de distinguer la partie ID réseau de la partie ID hôte dans l'adresse IP. De même que les adresses IP, les masques de sous-réseau sont souvent exprimés en notation décimale avec points. Un masque de sous-réseau s'obtient en mettant à 1 les bits qui font partie de l'ID réseau et à 0 les bits qui font partie de l'ID hôte. La valeur 32 bits ainsi obtenue est convertie en son équivalent dans la notation décimale avec points, comme le montre le tableau suivant :

Masques de sous-réseau par défaut pour les classes d'adresse IP standard

Classe d'adresse	Bits du masque de sous-réseau	Masque de sous- réseau
Classe A	11111111 00000000 00000000 00000000	255.0.0.0
Classe B	11111111 11111111 00000000 00000000	255.255.0.0
Classe C	11111111 11111111 11111111 00000000	255.255.255.0

Le résultat permet à TCP/IP de déterminer les ID hôte et réseau de l'ordinateur local. A titre d'exemple, si l'adresse IP est 102.54.94.97 et le masque de sous-réseau 255.255.0.0, l'ID réseau est 102.54 et l'ID hôte 94.97.

Bien que la configuration d'un hôte avec un masque de sous-réseau puisse paraître redondante à l'examen des tableaux précédents (puisqu'il est facile de déterminer la classe d'un hôte), les masques de sous-réseau s'emploient également pour continuer à segmenter un ID réseau attribué entre plusieurs réseaux locaux.

Supposons par exemple qu'un réseau reçoive l'adresse réseau de classe B 144.100. Il s'agit de l'une des 16384 adresses de classe B capables de desservir chacune plus de 65 000 nœuds. Cependant, le réseau d'entreprise mondial auquel est attribué cet ID réseau se compose de 12 réseaux locaux internationaux regroupant chacun de 75 à 100 nœuds. Au lieu de soumettre des demandes d'attribution d'ID réseau pour 11 réseaux de plus, il vaut mieux employer des sous-réseaux pour exploiter plus efficacement l'ID réseau déjà obtenue (144.100). Le troisième octet de l'adresse IP peut s'employer comme ID de sous-réseau, afin de définir le masque de sous-réseau 255.255.255.0. Cette technique permet de fragmenter l'adresse de classe B en 254 sous-réseaux (de 144.100.1 à 144.100.254), pouvant compter chacun 254 nœuds. (Il ne faut pas attribuer les ID hôte 0 et 255 à un ordinateur : ils sont utilisés comme adresses de diffusion, généralement reconnues par tous les ordinateurs). Il est possible d'attribuer 12 de ces adresses réseau possibles aux réseaux locaux internationaux de notre exemple. Ainsi, à l'intérieur de chaque réseau local, chaque ordinateur reçoit un ID hôte unique, et tous les ordinateurs ont le masque de sous-réseau 255.255.255.0.

L'exemple précédent illustre une structure de sous-réseau simple (et commune) pour des adresses de classe B. Parfois, il est nécessaire de pousser la segmentation de l'adresse IP jusqu'au niveau du bit, en n'utilisant que quelques bits pour spécifier un ID de sous-réseau (notamment quand des sous-réseaux contiennent plus de 256 nœuds). Votre administrateur de réseau local est en mesure de vous renseigner sur la politique de sous-réseaux et le masque de sous-réseau définis pour votre réseau. Pour tous les systèmes du réseau local, le masque de sous-réseau doit être le même pour cet ID réseau.

Important :Tous les ordinateurs composant un réseau logique doivent employer le même masque de sous-réseau et le même ID réseau. Si tel n'est pas le cas, des problèmes d'adressage et de routage risquent de se poser.

L'adresse IP est composée de deux parties, une partie réseau (network) et une partie noeud (host) :

Classe A	**001.x.y.z**	**126.x.y.z**	**Subnetmask = 255.0.0.0**
Classe B	**128.0.y.z**	**191.255.y.z**	**Subnetmask = 255.255.0.0**
Classe C	**192.0.0.z**	**223.255.255.z**	**Subnetmask = 255.255.255.0**

Voici un aperçu quantitatif des possibilités offertes :

Classe A : 126 réseaux	et	16 777 214 millions de hosts.
Classe B : 16 384 réseaux	et	65 534 hosts
Classe C : 2 097 152 réseaux	et	254 hosts.

A partir de 224, les adresses sont réservées pour des protocoles spéciaux (protocole multidestinataire Internet Group Management Protocol et autres) et ne peuvent pas être utilisées comme des adresses d'hôtes. Le 'subnetmask' (masque de sous-réseau) est un masque qui permet de déterminer par une adition (ET logique) avec l'adresse IP, quelle portion de cette adresse correspond à l'adresse réseau. Il est possible de définir des sous-réseaux à l'intérieur d'une classe d'adresse en utilisant une partie de la zone 'nœud' pour identifier ce sous-réseau. Dans ce cas, le subnetmask devra prendre en compte cette information.

Questions :Parmi les PC suivants lequel ou lesquelles a besoin d'un routeur pour communiquer avec 10.10.210.210 si le *subnet mask est 255.255.240.0*

- 10.10.200.32
- 10.10.244.64
- 10.10.222.129

128	64	32	16	8	4	2	1
1	*1*	*1*	*1*	*1*	*1*	*1*	*1*
0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0

128	64	32	16	8	4	2	1
1	*1*	*1*	*1*	*1*	*1*	*1*	*1*
0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0
0	0	0	0	1	0	1	0

128	64	32	16	8	4	2	1
1	*1*	*1*	*1*	*0*	*0*	*0*	*0*
1	1	0	1	0	0	1	0
1	1	0	0	1	0	0	0
1	1	1	1	0	1	0	0
1	1	0	1	1	1	1	0

128	64	32	16	8	4	2	1
0	*0*	*0*	*0*	*0*	*0*	*0*	*0*
1	1	0	1	0	0	1	0
0	0	1	0	0	0	0	0
0	1	0	0	0	0	0	0
1	0	0	0	0	0	0	1

Lesquels des PC sont sur le même réseau que 164.45.130.9 si *le subnet mask est 255.255.224.0*

- 130.45.130.1
- 164.45.130.1
- 164.45.126.23
- 164.45.148.23

128	64	32	16	8	4	2	1
1	*1*	*1*	*1*	*1*	*1*	*1*	*1*

128	64	32	16	8	4	2	1
1	*1*	*1*	*1*	*1*	*1*	*1*	*1*

128	64	32	16	8	4	2	1
1	*1*	*1*	*0*	*0*	*0*	*0*	*0*

128	64	32	16	8	4	2	1
0	*0*	*0*	*0*	*0*	*0*	*0*	*0*

Subnetting a Class A Network ID

Number of	Subnet Mask	Nombre maximum de	Number of hosts per
0	255.0.0.0 or /8	0	16,777,214
1	invalid		
2	255.192.0.0 or	2	4,194,302
3	255.224.0.0 or	6	2,097,150
4	255.240.0.0 or	14	1,048,574
5	255.248.0.0 or	30	524,286
6	255.252.0.0 or	62	262,142
7	255.254.0.0 or	126	131,070
8	255.255.0.0 or	254	65,534
9	255.255.128.0 or	510	32,766
10	255.255.192.0 or	1,022	16,382
11	255.255.224.0 or	2,046	8,190
12	255.255.240.0 or	4,094	4,094
13	255.255.248.0 or	8,190	2,046
14	255.255.252.0 or	16,382	1,022
15	255.255.254.0 or	32,766	510
16	255.255.255.0 or	65,534	254
17	255.255.255.128	131,070	126
18	255.255.255.192	262,142	62
19	255.255.255.224	524,286	30
20	255.255.255.240	1,048,574	14
21	255.255.255.248	2,097,150	6
22	255.255.255.252	4,194,302	2

Subnetting a class B network ID

Number of	Subnet Mask	Nombre maximum de	Number of hosts per
0	255.255.0.0 or	0	65,534
1	invalid		
2	255.255.192.0 or	2	16,382
3	255.255.224.0 or	6	8,190
4	255.255.240.0 or	14	4,094
5	255.255.248.0 or	30	2,046
6	255.255.252.0 or	62	1,022
7	255.255.254.0 or	126	510
8	255.255.255.0 or	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1,022	62
11	255.255.255.224	2,046	30
12	255.255.255.240	4,094	14
13	255.255.255.248	8,190	6
14	255.255.255.252	16,382	2

Subnetting a class C network ID

Number of	Subnet Mask	Numéro maximum de	Number of hosts per
0	255.255.255.0 or	0	254
1	invalid		
2	255.255.255.192	2	62 (64 à 191)
3	255.255.255.224	6	30 (32 à 223)
4	255.255.255.240	14	14 (16 à 239)
5	255.255.255.248	30	6 (8 à 247)
6	255.255.255.252	62	2 (4 à 251)
7	invalid		
8	invalid		

Définition de la plage d'ID de réseau pour deux sous-réseaux

Dans cet exercice, vous allez définir une plage d'ID de réseau pour un inter réseau comprenant deux sous-réseaux, en utilisant deux bits issus d'un masque de sous-réseau de classe B.

1. Enumérez toutes les combinaisons possibles pour le masque de sous-réseau suivant, puis convertissez-les au format décimal pour déterminer la valeur de début de chaque sous-réseau.

255 255 192 0
11111111 11111111 11000000=00000000
Invalide 00000000=0
Sous-réseau 1 0100000=64 à 127
Sous-réseau 2 10000000=128 à 191
Invalide 11000000=192 (masque de sous-réseau)

2. Enumérez la plage d'ID d'hôte de chaque sous-réseau.

Sous-réseau	Valeur de début	Valeur de fin
Sous-réseau 1	w.x.64.1	w.x.127.254
Sous-réseau 2	w.x.128.1	w.x.191.254

Définition de la plage d'ID de 14 sous-réseaux

Dans cet exercice, vous allez définir une plage d'ID de réseau pour un inter réseau comprenant 14 sous-réseaux, en utilisant quatre bits issus d'un masque de sous-réseau de classe B.

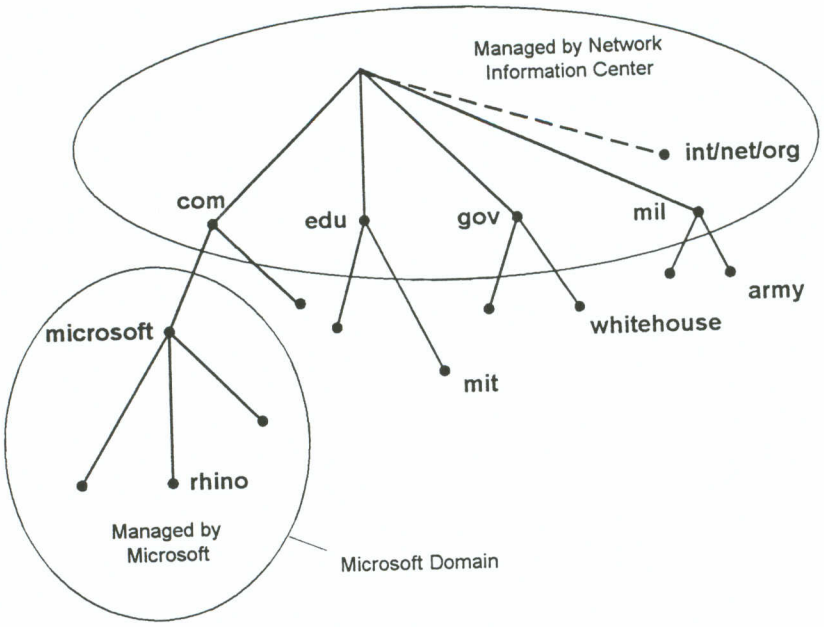
1. Enumérez toutes les combinaisons possibles pour le masque de sous-réseau suivant, puis convertissez-les au format décimal pour déterminer la valeur de début de chaque sous-réseau.

255	255	240	0	
11111111	11111111	11110000	=00000000	
Invalide		00000000	=	0
Sous-réseau 1		00010000	=	16
Sous-réseau 2		00100000	=	32
Sous-réseau 3		00110000	=	48
Sous-réseau 4		01000000	=	64
Sous-réseau 5		01010000	=	80
Sous-réseau 6		01100000-	=	96
Sous-réseau 7		01110000=	=	112
Sous-réseau 8		10000000	=	128
Sous-réseau 9		10010000	=	144
Sous-réseau 10		10100000	=	160
Sous-réseau 11		10110000	=	176
Sous-réseau 12		11000000	=	192
Sous-réseau 13		11001000	=	208
Sous-réseau 14		11100000	=	224
Invalide		11110000	=	240 (masque de sous-réseau)

2 Enumérez la plage d'ID d'hôtes de chaque sous réseau.

Sous-réseau	Valeur de début	Valeur de fin
Sous-réseau 1	w.x.16.1	w.x.31.254
Sous-réseau 2	w.x.32.1	w.x.47.254
Sous-réseau 3	w.x.48.1	w.x.63.254
Sous-réseau 4	w.x.64.1	w.x.79.254
Sous-réseau 5	w.x.80.1	w.x.95.254
Sous-réseau 6	w.x.96.1	w.x.111.254
Sous-réseau 7	w.x.112.1	w.x.127.254
Sous-réseau 8	w.x.128.1	w.x.143.254
Sous-réseau 9	w.x.144.1	w.x.159.254
Sous-réseau 10	w.x.160.1	w.x.175.254
Sous-réseau 11	w.x.176.1	w.x.191.254
Sous-réseau 12	w.x.192.1	w.x.207.254
Sous-réseau 13	w.x.208.1	w.x.223.254
Sous-réseau 14	w.x.224.1	w.x.239.254

Service de NOM de Domaines DNS



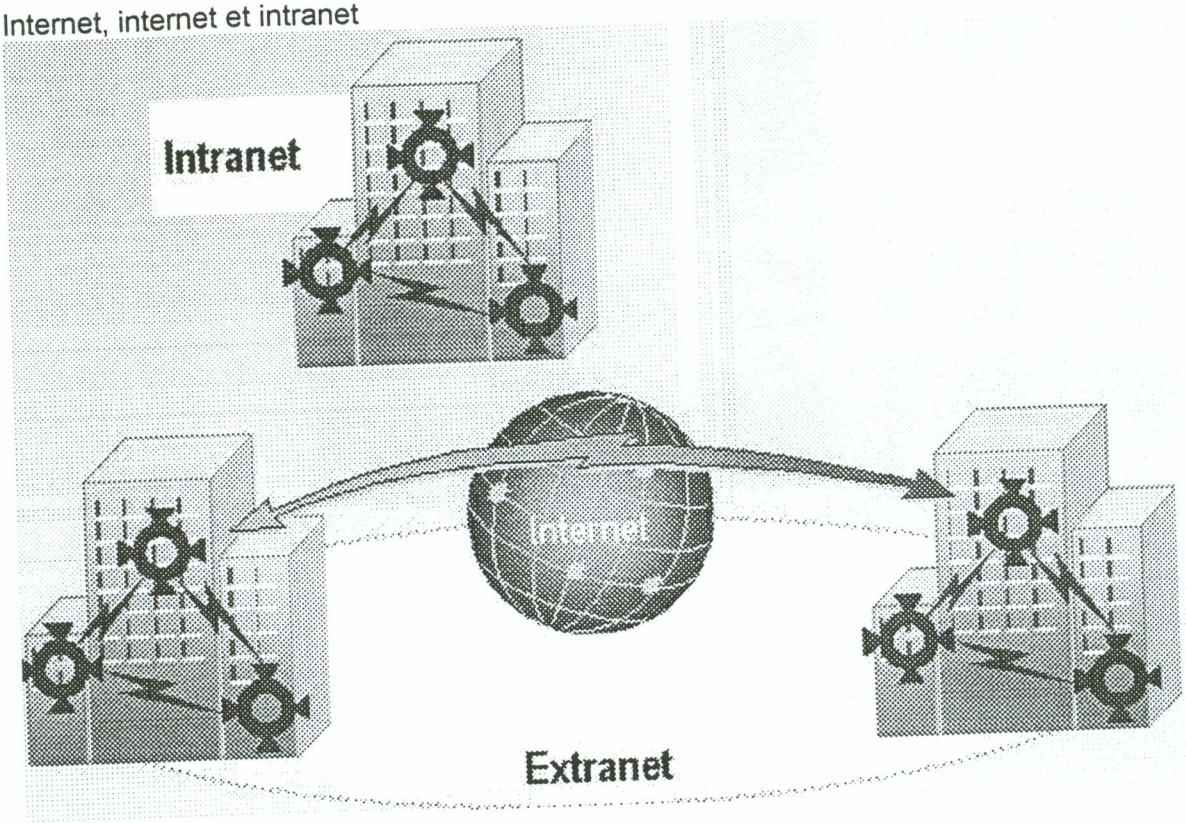
Chaque ordinateur doit disposer d'une adresse IP unique . L'attribution des noms des ordinateurs est prise en compte par des serveurs de noms .Ces machines contiennent une simple base de données qui fait concorder les adresses des ordinateurs et leurs noms . Cette solution est mise en œuvre sur le réseau basé sur le protocole TCP/IP . Le serveur qui permet d'établir la correspondance entre le nom (compréhensible par un humain) et le numéro IP (compréhensible par les ordinateurs) s'appelle le DNS (Domain Name Server) . Pour que deux ordinateurs puissent établir une liaison il leur faut une méthode d'identification !
Le nom des serveurs est généralement suivi d'un code pays composé de deux lettres. Ce code est appelé "Top Level Domain" (TLD).
Par exemple dans le cas de World-Net : "world-net.sct.fr", ".fr" nous informe que ce serveur fait partie du domaine français.
Une version officielle et complète de tous les codes pays est disponible par FTP Anonyme sur le site : <ftp.wisc.edu> dans le répertoire "connectivity table".

Voici quelques codes pays :

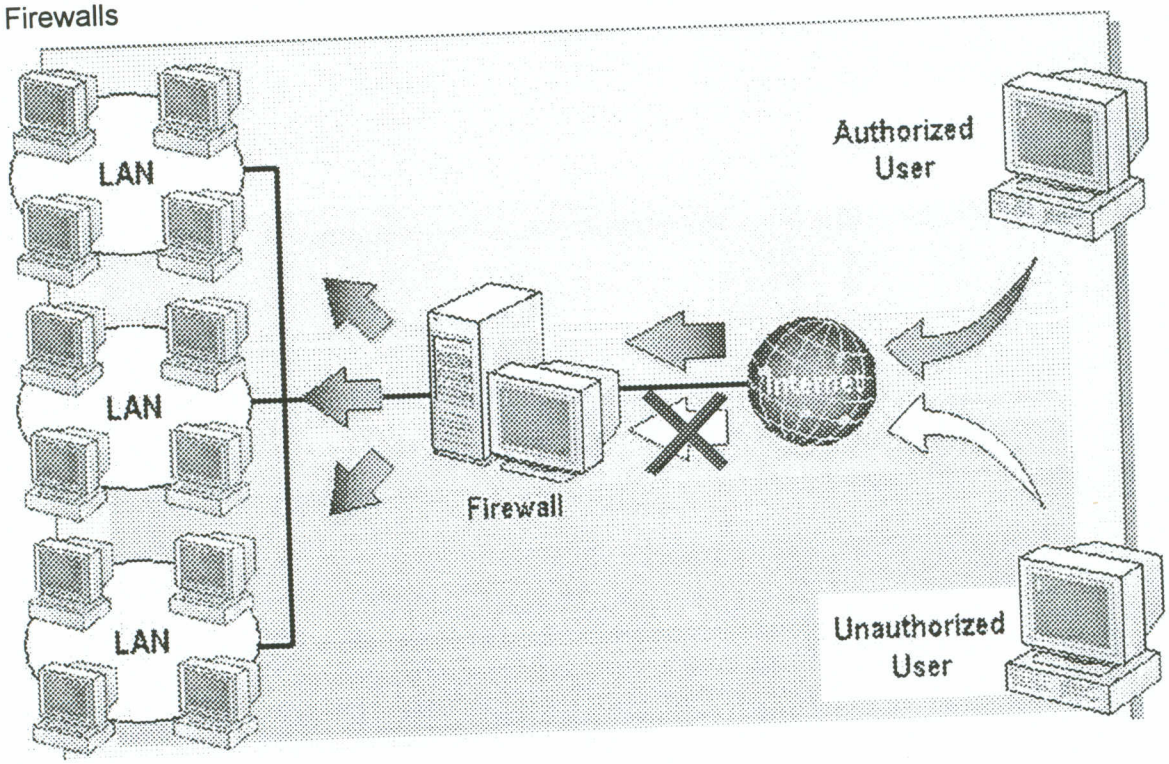
AT	Autriche	ES	Espagne	NL	Pays-Bas
AU	Australie	FR	France	NO	Norvège
CH	Suisse	IT	Italie	UK	Gr-Bretagne
DE	Allemagne	LU	Luxembourg	US	Etats-Unis

Il existe aussi des TLD composés de 3 lettres n'indiquant pas le pays d'origine, mais la fonction de l'organisation. Ces serveurs sont généralement situés au Etats-Unis.
INT Organisme International, COM Entreprise commerciale, EDU Education, GOV Institution gouvernementale, MIL Site militaire, NET Prestataire de Service Internet, ORG Autre ...
Si dans le cas de l'abonné au téléphone il est possible de consulter un annuaire général, il n'en va pas de même sur Internet. Le réseau a une croissance telle qu'il est impossible de faire un annuaire général

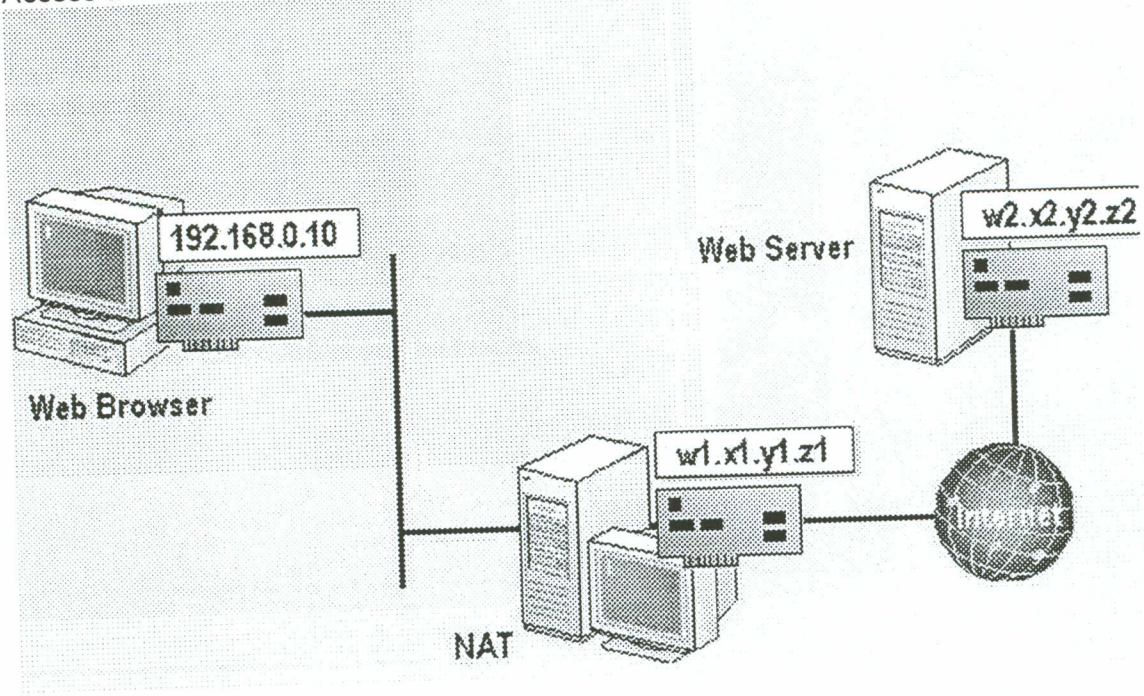
Internet, internet et intranet



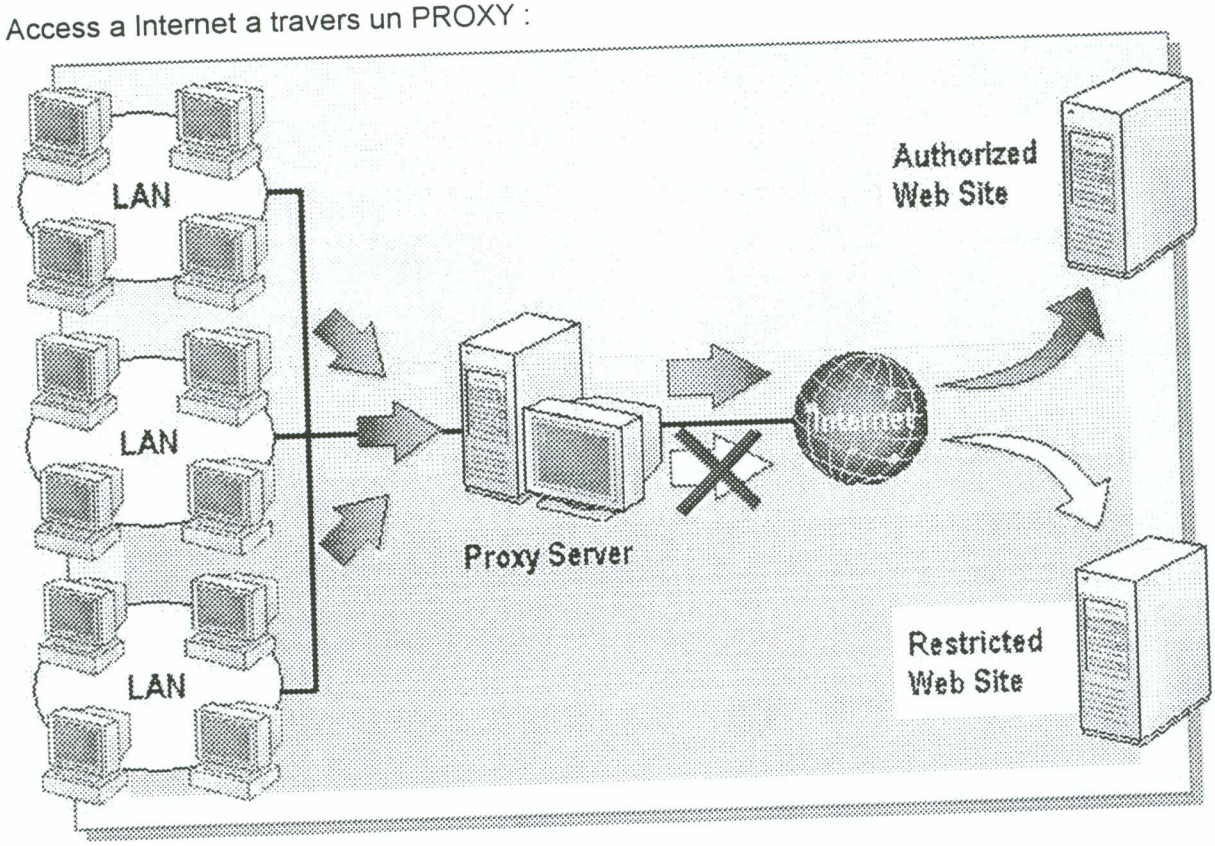
Firewalls



Access a Internet a l'aide du protocole de routage NAT



Access a Internet a travers un PROXY :



128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
								-	192	224	240	248	252	254	255	-	192	224	240	248	252	254	255	-	192	224	240	248	252		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Classe A :1-126(N.H.H.H)				Classe B :128-191(N.N.H.H)				Classe C :192-223(N.N.N.H)				128	64	32	16	8	4	2	1
0	**0000 0000**	40	0010 1000	80	0101 0000	120	0111 1000	160	1010 0000	200	1100 1000	**240**	**1111 0000**	244	1111 0100	**248**	**1111 1000**	**252**	**1111 1100**
1	0000 0001	41	0010 1001	81	0101 0001	121	0111 1001	161	1010 0001	201	1100 1001	241	1111 0001	245	1111 0101	249	1111 1001	253	1111 1101
2	0000 0010	42	0010 1010	82	0101 0010	122	0111 1010	162	1010 0010	202	1100 1010	242	1111 0010	246	1111 0110	250	1111 1010	**254**	**1111 1110**
3	0000 0011	43	0010 1011	83	0101 0011	123	0111 1011	163	1010 0011	203	1100 1011	243	1111 0011	247	1111 0111	251	1111 1011	**255**	**1111 1111**
4	0000 0100	44	0010 1100	84	0101 0100	124	0111 1100	164	1010 0100	204	1100 1100		**Nombre des réseaux : Classe C :2'097'152 (B :16'384, A :126)**						
5	0000 0101	45	0010 1101	85	0101 0101	125	0111 1101	165	1010 0101	205	1100 1101		**Nombre des HOSTS : Classe C :254 hosts (B : 65'534, A : 16'777'214)**						
6	0000 0110	46	0010 1110	86	0101 0110	126	0111 1110	166	1010 0110	206	1100 1110	1	128	La première=Adresse du SubNet et La dernière= Adresse de Diffusion					
7	0000 0111	47	0010 1111	87	0101 0111	127	0111 1111 **B**	167	1010 0111	207	1100 1111	**2**	**192**	**1100 0000 2 subnets, Classe C :62 hosts (B : 16'382, A :4'194'302)**					
8	0000 1000	48	0011 0000	88	0101 1000	**128**	**1000 0000**	168	1010 1000	208	1101 0000			64-127, 128-191					
9	0000 1001	49	0011 0001	89	0101 1001	129	1000 0001	169	1010 1001	209	1101 0001	**3**	**224**	**1110 0000 6 subnets, Classe C : 30 hosts (B : 8'190, A :2'097'150)**					
10	0000 1010	50	0011 0010	90	0101 1010	130	1000 0010	170	1010 1010	210	1101 0010			32-63, 64-95, 96-127, 128-159, 160-191, 192-223					
11	0000 1011	51	0011 0011	91	0101 1011	131	1000 0011	171	1010 1011	211	1101 0011	**4**	**240**	**1111 0000 14 subnets, Classe C : 14 hosts (B : 4'094, A : 1'048'574)**					
12	0000 1100	52	0011 0100	92	0101 1100	132	1000 0100	172	1010 1100	212	1101 0100			16-31, 32-47, 48-63, 64-79, 80-95, 96-111, 112-127, 128-143,					
13	0000 1101	53	0011 0101	93	0101 1101	133	1000 0101	173	1010 1101	213	1101 0101			144-159, 160-175, 176-191, 192-207, 208-223, 224-239					
14	0000 1110	54	0011 0110	94	0101 1110	134	1000 0110	174	1010 1110	214	1101 0110	**5**	**248**	**1111 1000 30 subnets, Classe C : 6 hosts (B : 2'046, A : 524'286)**					
15	0000 1111	55	0011 0111	95	0101 1111	135	1000 0111	175	1010 1111	215	1101 0111			8-15, 16-23, 24-31, 32-39, 40-47, 48-55, 56-63, 64-71, 72-79,					
16	0001 0000	56	0011 1000	96	0110 0000	136	1000 1000	176	1011 0000	216	1101 1000			80-87, 88-95, 96-103, 104-111, 112-119, 120-127, 128-135,					
17	0001 0001	57	0011 1001	97	0110 0001	137	1000 1001	177	1011 0001	217	1101 1001			136-143, 144-151, 152-159, 160-167, 168-175, 176-183, 184-191,					
18	0001 0010	58	0011 1010	98	0110 0010	138	1000 1010	178	1011 0010	218	1101 1010			192-199, 200-207, 208-215, 216-223, 224-231, 232-239, 240-247					
19	0001 0011	59	0011 1011	99	0110 0011	139	1000 1011	179	1011 0011	219	1101 1011	**6**	**252**	**1111 1100 62 subnets, Classe C : 2 hosts (B : 1'022, A : 262'142)**					
20	0001 0100	60	0011 1100	100	0110 0100	140	1000 1100	180	1011 0100	220	1101 1100			4-7, 8-11, 12-15, 16-19, 20-23, 24-27, 28-31, 32-35, 36-39, 40-43, 44-47,					
21	0001 0101	61	0011 1101	101	0110 0101	141	1000 1101	181	1011 0101	221	1101 1101			48-51, 52-55, 56-59, 60-63, 64-67, 68-71, 72-75, 76-79, 80-83, 84-87,					
22	0001 0110	62	0011 1110	102	0110 0110	142	1000 1110	182	1011 0110	222	1101 1110			88-91, 92-95, 96-99, 100-103, 104-107, 108-111, 112-115, 116-119,					
23	0001 0111	63	0011 1111	103	0110 0111	143	1000 1111	183	1011 0111	223	1101 1111			120-123, 124-127, 128-131, 132-135, 136-139, 140-143, 144-147,					
24	0001 1000	64	0100 0000	104	0110 1000	144	1001 0000	184	1011 1000	**224**	**1110 0000**			148-151, 152-155, 156-159, 160-163, 164-167, 168-171, 172-175,					
25	0001 1001	65	0100 0001	105	0110 1001	145	1001 0001	185	1011 1001	225	1110 0001			176-179, 180-183, 184-187, 188-191, 192-195, 196-199, 200-204,					
26	0001 1010	66	0100 0010	106	0110 1010	146	1001 0010	186	1011 1010	226	1110 0010			204-207, 208-211, 212-215, 216-219, 220-223, 224-227, 228-231,					
27	0001 1011	67	0100 0011	107	0110 1011	147	1001 0011	187	1011 1011	227	1110 0011			232-235, 236-239, 240-243, 244-247, 248-251					
28	0001 1100	68	0100 0100	108	0110 1100	148	1001 0100	188	1011 1100	228	1110 0100	**7**	**254**	**1111 1110--126 subnets ----------(B : 510, A : 131'070)**					
29	0001 1101	69	0100 0101	109	0110 1101	149	1001 0101	189	1011 1101	229	1110 0101	**8**	**255**	**1111 1111-254 subnets---------- ----------(B : 254, A : 65'534)**					
30	0001 1110	70	0100 0110	110	0110 1110	150	1001 0110	190	1011 1110	230	1110 0110	**9**	**255.128**	---------510 subnets--------- ----------	(B : 126,	A : 32'768)			
31	0001 1111	71	0100 0111	111	0110 1111	151	1001 0111	191	1011 1111	231	1110 0111	**10**	**255.192**	-----1'022 subnets-------- ----------	(B : 62,	A : 16'382)			
32	0010 0000	72	0100 1000	112	0111 0000	152	1001 1000	**192**	**1100 0000**	232	1110 1000	**11**	**255.224**	----2'046 subnets------- ----------	(B : 30,	A : 8'190)			
33	0010 0001	73	0100 1001	113	0111 0001	153	1001 1001	193	1100 0001	233	1110 1001	**12**	**255.240**	-----4'094 subnets------ ----------	(B : 14,	A : 4'094)			
34	0010 0010	74	0100 1010	114	0111 0010	154	1001 1010	194	1100 0010	234	1110 1010	**13**	**255.248**	------8'190 subnets----- ----------	(B : 6,	A : 2'046)			
35	0010 0011	75	0100 1011	115	0111 0011	155	1001 1011	195	1100 0011	235	1110 1011	**14**	**255.252**	----16'382 subnets--- ----------	(B : 2,	A : 1'022)			
36	0010 0100	76	0100 1100	116	0111 0100	156	1001 1100	196	1100 0100	236	1110 1100	**15**	**255.254**	-----32'768 subnets- ----------		(A : 510)			
37	0010 0101	77	0100 1101	117	0111 0101	157	1001 1101	197	1100 0101	237	1110 1101	**16**	**255.255**	-----65'534 subnets- ----------		(A : 254)			
38	0010 0110	78	0100 1110	118	0111 0110	158	1001 1110	198	1100 0110	238	1110 1110	**17**	**255.255.128**	131'070 subnets				(A : 126)	
39	0010 0111	79	0100 1111	119	0111 0111	159	1001 1111	199	1100 0111	239	1110 1111	**18**	**255.255.192**	262'142 subnets				(A :62)	

Informations détaillées sur les produits et documentation sur les prestations Microsoft:

Microsoft Info-Service	Tél : 0800 55 59 00
Case postale 8021 Zurich	Fax : 01-311 72 27

Informations sur l'enregistrement:

Microsoft Info-Service	Fax 01-831 15 15
Enregistrement des utilisateurs	(enregistrements uniquement!)
Informations sur la formation	Tél : 0848 858 868
Service technique :	Tél : 022 738 96 88

Echange de disquettes et de CDROM défectueux, achat Service Packs:

Microsoft Direct Services CP	Tél : 0848 830 835 (Edinburg)
Email swiss@msdirectservices.com	Fax :0848 830 836
TechnetSubscription Center Irlande	Tél : 0800 55 73 82 (en français)
	Fax 00353 1 703 87 40
Contrat Priority Comprehensive	Tél :0848 802 330
Microsoft AG Alte Wintenthurerstrasse 14a	Tél. 01-839 61 11
8304 Wallisellen	Fax 01-831 08 69
Service clientèle:	Tél. 0848 858 868
AnswerPoint	Tél. 0848 80 23 30
Informations MCP	**Tél: 0800 55 03 19**

Internet: http://www.microsoft.com/switzerland

Online tool pour MCP : http ://wclp.sourceoneworldwide.com/mcp

Microsoft Certified Professional

Microsoft Certified Professional Systems Engineer

****

****

CERTIFICATION MCP et MCPSE

Enregistrement pour tests de certification MCP et MCPSE :
tél. gratuit de VUE:0800 83 75 50 ou directement auprès de ISEIG qui en partenariat avec VUE vous propose de passer les 7 tests suivants :

70-215 Windows 2000 Server
70-210 Windows 2000 Professional
70-216 Implémentation et administration d'une infrastructure réseaux Windows 2000
70-217 Implémentation et administration d'une infrastructure Services d'annuaires Windows 2000

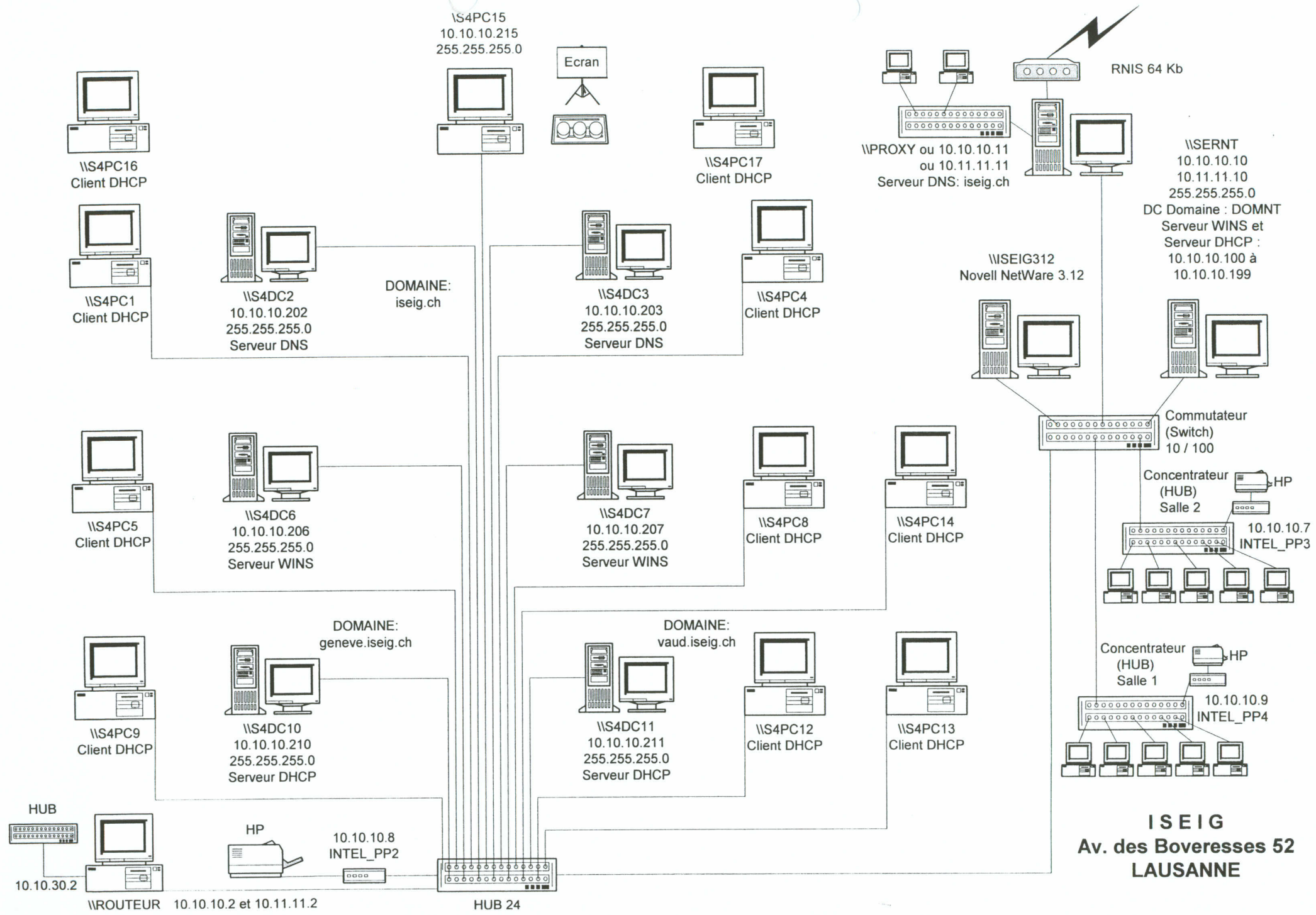
+ 1 autre test parmi les suivantes :
70-219 Planifier une infrastructure des services d'annuaires
70-220 Planifier la sécurité Windows 2000
70-221 Planifier une infrastructure réseau Windows 2000

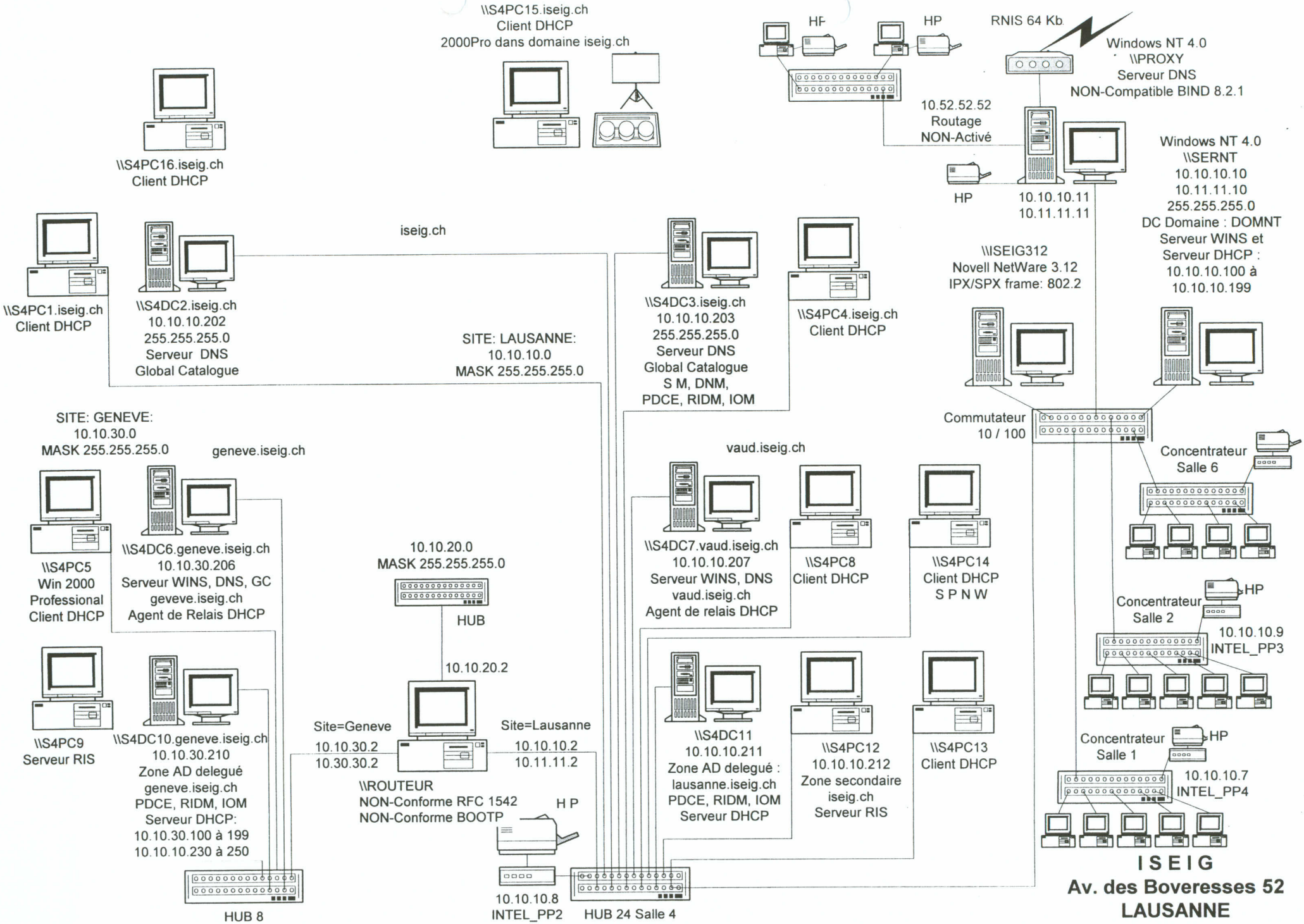
+ 2 tests parmi les suivantes :
70-219 Planifier une infrastructure des services d'annuaires
70-220 Planifier la sécurité Windows 2000
70-221 Planifier une infrastructure réseau Windows 2000
70-222 Planifier la Migration de NT4 à Windows 2000
Exchange, IIS, Proxy, SMS, SQL

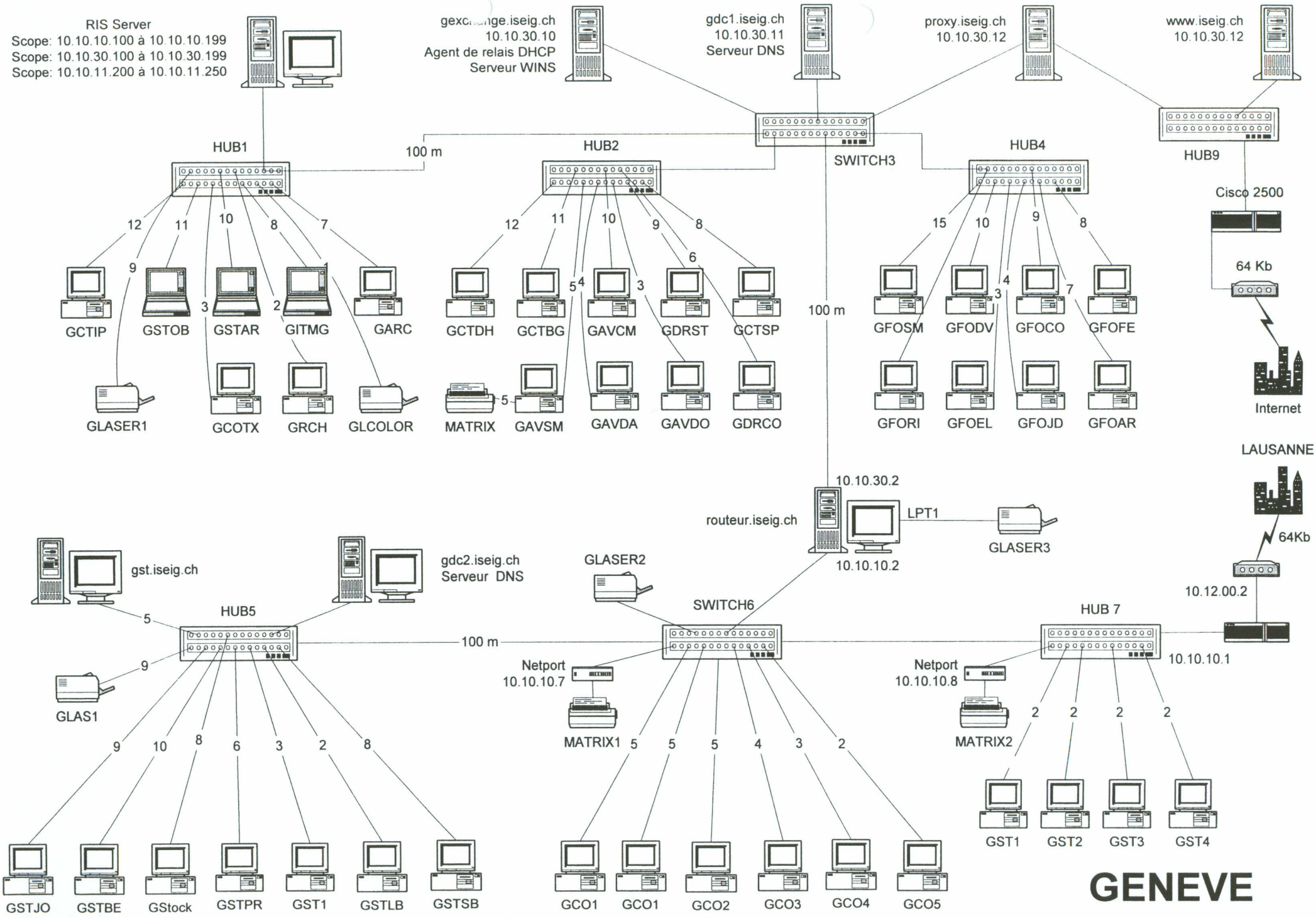
Microsoft Regional Education Service Center Tél : 0800 55 03 19

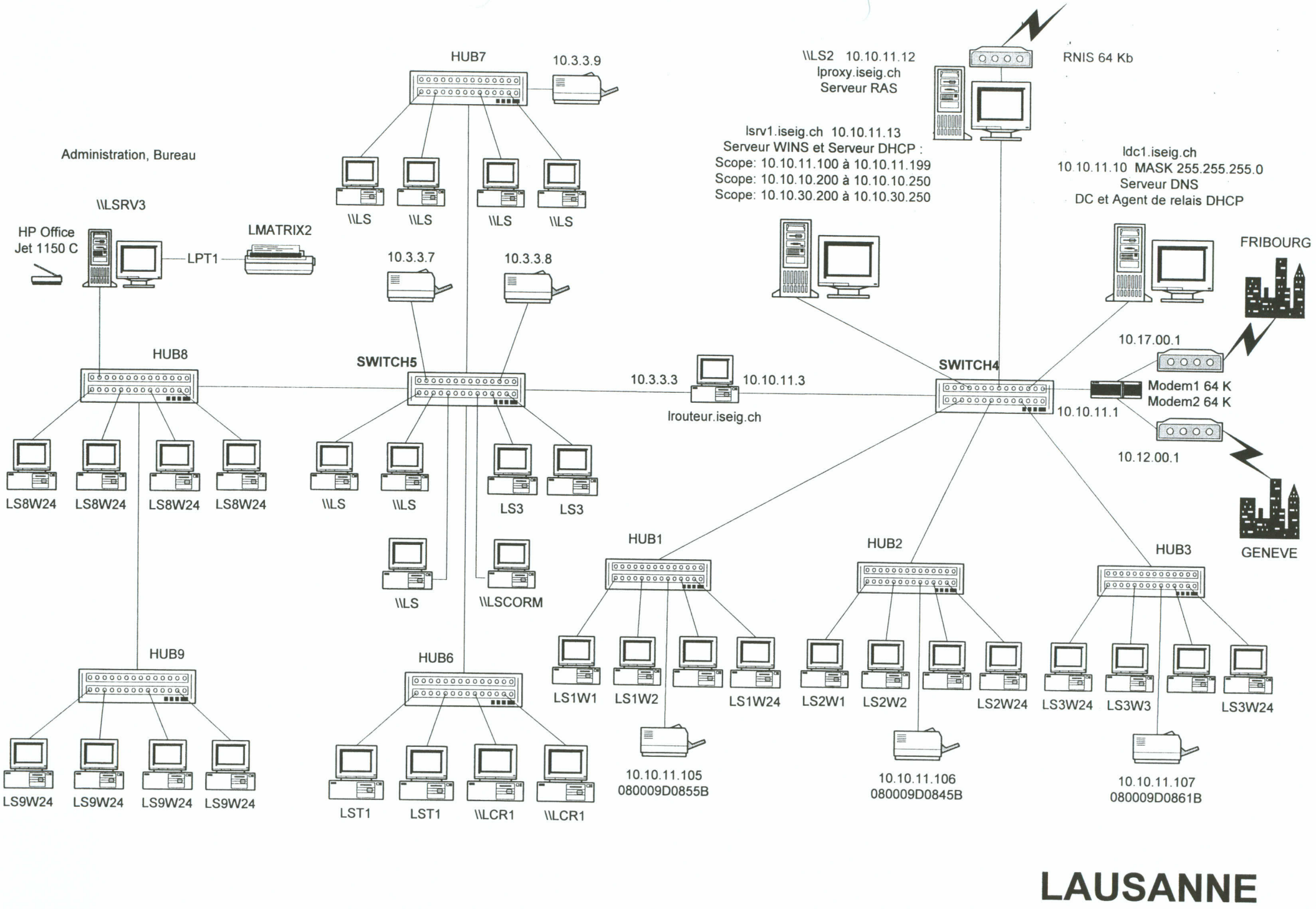
Nombre de certifications (mai 2000)

MCP : 505 624	MCSD : 26 478	MCDBA : 5 164
MCSE : 266 841	MCT : 26 091	MCP Site Building :


\S4PC15
10.10.10.215
255.255.255.0
Ecran
RNIS 64 Kb
\\S4PC16
Client DHCP
\\S4PC17
Client DHCP
\\PROXY ou 10.10.10.11
ou 10.11.11.11
Serveur DNS: iseig.ch
\\SERNT
10.10.10.10
10.11.11.10
255.255.255.0
DC Domaine : DOMNT
Serveur WINS et
Serveur DHCP :
10.10.10.100 à
10.10.10.199
\\S4PC1
Client DHCP
\\S4DC2
10.10.10.202
255.255.255.0
Serveur DNS
DOMAINE:
iseig.ch
\\S4DC3
10.10.10.203
255.255.255.0
Serveur DNS
\\S4PC4
Client DHCP
\\ISEIG312
Novell NetWare 3.12
Commutateur
(Switch)
10 / 100
\\S4PC5
Client DHCP
\\S4DC6
10.10.10.206
255.255.255.0
Serveur WINS
\\S4DC7
10.10.10.207
255.255.255.0
Serveur WINS
\\S4PC8
Client DHCP
\\S4PC14
Client DHCP
Concentrateur
(HUB)
Salle 2
HP
10.10.10.7
INTEL_PP3
DOMAINE:
geneve.iseig.ch
DOMAINE:
vaud.iseig.ch
\\S4PC9
Client DHCP
\\S4DC10
10.10.10.210
255.255.255.0
Serveur DHCP
\\S4DC11
10.10.10.211
255.255.255.0
Serveur DHCP
\\S4PC12
Client DHCP
\\S4PC13
Client DHCP
Concentrateur
(HUB)
Salle 1
HP
10.10.10.9
INTEL_PP4
HUB
HP
10.10.10.8
INTEL_PP2
10.10.30.2
\\ROUTEUR
10.10.10.2 et 10.11.11.2
HUB 24
I S E I G
Av. des Boveresses 52
LAUSANNE


\\S4PC15.iseig.ch
Client DHCP
2000Pro dans domaine iseig.ch
HP
HP
RNIS 64 Kb
Windows NT 4.0
\\PROXY
Serveur DNS
NON-Compatible BIND 8.2.1
10.52.52.52
Routage
NON-Activé
\\S4PC16.iseig.ch
Client DHCP
HP
10.10.10.11
10.11.11.11
Windows NT 4.0
\\SERNT
10.10.10.10
10.11.11.10
255.255.255.0
DC Domaine : DOMNT
Serveur WINS et
Serveur DHCP :
10.10.10.100 à
10.10.10.199
iseig.ch
\\S4PC1.iseig.ch
Client DHCP
\\S4DC2.iseig.ch
10.10.10.202
255.255.255.0
Serveur DNS
Global Catalogue
\\S4DC3.iseig.ch
10.10.10.203
255.255.255.0
Serveur DNS
Global Catalogue
S M, DNM,
PDCE, RIDM, IOM
\\S4PC4.iseig.ch
Client DHCP
\\SEIG312
Novell NetWare 3.12
IPX/SPX frame: 802.2
SITE: LAUSANNE:
10.10.10.0
MASK 255.255.255.0
Commutateur
10 / 100
SITE: GENEVE:
10.10.30.0
MASK 255.255.255.0
geneve.iseig.ch
vaud.iseig.ch
Concentrateur
Salle 6
\\S4PC5
Win 2000
Professional
Client DHCP
\\S4DC6.geneve.iseig.ch
10.10.30.206
Serveur WINS, DNS, GC
geveve.iseig.ch
Agent de Relais DHCP
\\S4DC7.vaud.iseig.ch
10.10.10.207
Serveur WINS, DNS
vaud.iseig.ch
Agent de relais DHCP
\\S4PC8
Client DHCP
\\S4PC14
Client DHCP
S P N W
10.10.20.0
MASK 255.255.255.0
HUB
Concentrateur
Salle 2
HP
10.10.10.9
INTEL_PP3
10.10.20.2
\\S4PC9
Serveur RIS
\\S4DC10.geneve.iseig.ch
10.10.30.210
Zone AD delegué
geneve.iseig.ch
PDCE, RIDM, IOM
Serveur DHCP:
10.10.30.100 à 199
10.10.10.230 à 250
Site=Geneve
10.10.30.2
10.30.30.2
Site=Lausanne
10.10.10.2
10.11.11.2
\\ROUTEUR
NON-Conforme RFC 1542
NON-Conforme BOOTP
\\S4DC11
10.10.10.211
Zone AD delegué :
lausanne.iseig.ch
PDCE, RIDM, IOM
Serveur DHCP
\\S4PC12
10.10.10.212
Zone secondaire
iseig.ch
Serveur RIS
\\S4PC13
Client DHCP
Concentrateur
Salle 1
HP
10.10.10.7
INTEL_PP4
H P
10.10.10.8
INTEL_PP2
HUB 8
HUB 24 Salle 4
I S E I G
Av. des Boveresses 52
LAUSANNE


RIS Server
Scope: 10.10.10.100 à 10.10.10.199
Scope: 10.10.30.100 à 10.10.30.199
Scope: 10.10.11.200 à 10.10.11.250
gexchange.iseig.ch
10.10.30.10
Agent de relais DHCP
Serveur WINS
gdc1.iseig.ch
10.10.30.11
Serveur DNS
proxy.iseig.ch
10.10.30.12
www.iseig.ch
10.10.30.12
HUB1
100 m
HUB2
SWITCH3
HUB4
HUB9
Cisco 2500
64 Kb
Internet
GCTIP
GSTOB
GSTAR
GITMG
GARC
GLASER1
GCOTX
GRCH
GLCOLOR
GCTDH
GCTBG
GAVCM
GDRST
GCTSP
MATRIX
GAVSM
GAVDA
GAVDO
GDRCO
GFOSM
GFODV
GFOCO
GFOFE
GFORI
GFOEL
GFOJD
GFOAR
LAUSANNE
10.10.30.2
routeur.iseig.ch
LPT1
GLASER3
10.10.10.2
64Kb
10.12.00.2
gst.iseig.ch
gdc2.iseig.ch
Serveur DNS
GLASER2
HUB5
SWITCH6
HUB 7
10.10.10.1
Netport
10.10.10.7
Netport
10.10.10.8
GLAS1
MATRIX1
MATRIX2
GSTJO
GSTBE
GStock
GSTPR
GST1
GSTLB
GSTSB
GCO1
GCO1
GCO2
GCO3
GCO4
GCO5
GST1
GST2
GST3
GST4
GENEVE


HUB7
10.3.3.9
\\LS2 10.10.11.12
lproxy.iseig.ch
Serveur RAS
RNIS 64 Kb
lsrv1.iseig.ch 10.10.11.13
Serveur WINS et Serveur DHCP :
Scope: 10.10.11.100 à 10.10.11.199
Scope: 10.10.10.200 à 10.10.10.250
Scope: 10.10.30.200 à 10.10.30.250
ldc1.iseig.ch
10.10.11.10 MASK 255.255.255.0
Serveur DNS
DC et Agent de relais DHCP
Administration, Bureau
\\LSRV3
HP Office
Jet 1150 C
LPT1
LMATRIX2
\\LS
\\LS
\\LS
\\LS
10.3.3.7
10.3.3.8
FRIBOURG
10.17.00.1
Modem1 64 K
Modem2 64 K
10.10.11.1
10.12.00.1
GENEVE
HUB8
SWITCH5
10.3.3.3
10.10.11.3
lrouteur.iseig.ch
SWITCH4
LS8W24
LS8W24
LS8W24
LS8W24
\\LS
\\LS
LS3
LS3
\\LS
\\LSCORM
HUB1
HUB2
HUB3
HUB9
HUB6
LS1W1
LS1W2
LS1W24
LS2W1
LS2W2
LS2W24
LS3W24
LS3W3
LS3W24
10.10.11.105
080009D0855B
10.10.11.106
080009D0845B
10.10.11.107
080009D0861B
LS9W24
LS9W24
LS9W24
LS9W24
LST1
LST1
\\LCR1
\\LCR1
LAUSANNE