Systèmes d'exploitation de réseaux locaux d'entreprise (RLE)

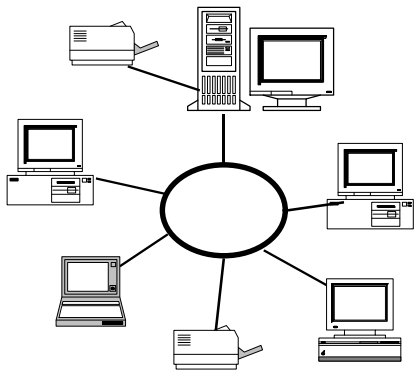
Partage de fichiers et administration des utilisateurs

1- Généralités et définitions
2- Réseaux et serveurs NetWare de Novell
3- Réseaux et serveurs Windows NT de Microsoft
4- NFS (Network File System)
5- Appleshare

version CNAM 1999-2000

1ère partie: Généralités et Définitions

- Un **réseau local d'entreprise** (RLE) est composé :
  - d'un (ou plusieurs) serveur(s) de fichiers et d'impression, auquel est rattaché les ressources partageables (disques durs, cédéroms, imprimantes, modems, etc...)
  - de postes de travail clients
  - l'ensemble est interconnecté par un réseau local (Ethernet, Token-Ring, etc...)



- Un **serveur** est un ordinateur, dédié ou non, et fournissant un ensemble de services comme le partage de fichiers et d'imprimante, la messagerie électronique, etc...

R.CHALON Systèmes d'exploitation de réseaux locaux 2

Systèmes d'exploitation de réseaux

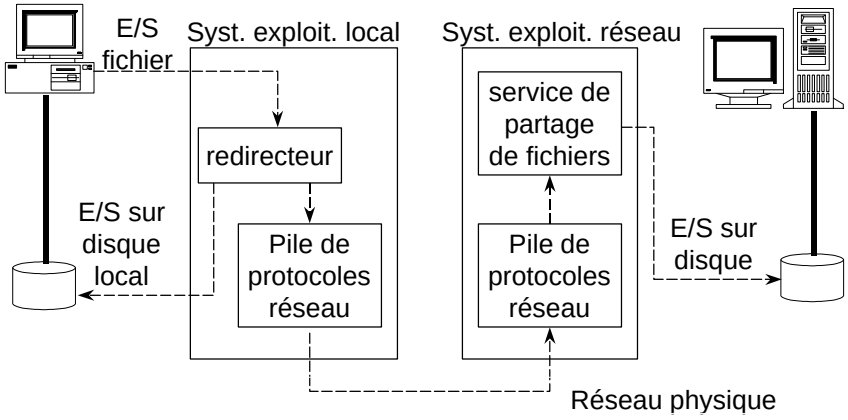
- Un système d'exploitation de réseaux [NOS=Network Operating System] est un système d'exploitation dédié ou spécialement adapté à la constitution de serveurs.
- Exemples:
  - Netware de Novell: serveur dédié
  - Windows NT de Microsoft: serveur «spécialisé»
  - Unix: serveur non dédié et multi-utilisateur
  - AppleShare d'Apple, Vines de Banyan, OS/2 d'IBM, ...
- Il permet le partage de ressources sur un réseau comme :
  - partager des fichiers, des bases de données,
  - partager des applications,
  - partager des imprimantes,
  - supporter des applications clients/serveurs comme la messagerie électronique, des agendas partagés, etc...

Partage de ressources

- Partager des fichiers pour:
  - travailler à plusieurs sur les mêmes documents: par exemple un directeur et sa secrétaire, des ingénieurs dans un groupe de projet
  - utiliser des logiciels communs: permet d 'éviter d'installer les applications sur chaque poste de travail:
    - économie d 'espace disque sur chaque poste,
    - mise à jour facilitée à chaque changement de version des logiciels
    - ATTENTION cependant aux licences d 'utilisation des logiciels
  - etc...
  - ➡ La centralisation des fichiers sur un serveur permet de mieux gérer les sauvegardes des données
- Partager des imprimantes pour:
  - réduire les coûts d 'investissement
  - pouvoir accéder à des équipements spéciaux: imprimantes en couleur, imprimantes grand-format

Connexion des postes clients

- Les systèmes d'exploitation des postes clients sont «étendus» par des services permettant l'accès au(x) serveur(s) du réseau local et donc aux ressources partagées



R.CHALON Systèmes d'exploitation de réseaux locaux 5

Contrôle et droits d'accès

- Un système d'authentification permet de limiter l'accès à un système aux seules personnes autorisées:
  - ➡ processus d'**ouverture de session** [login]
- Une fois authentifiées les personnes n'ont accès qu'aux ressources qui leur sont strictement nécessaires (limitations des **droits d'accès**) afin de:
  - préserver **la sécurité**: la plupart des informations produites et utilisées dans une société doivent rester confidentielles:
    - vis-à-vis des personnes externes,
    - vis-à-vis du personnel de la société
  - préserver **l'intégrité des données**: éviter l'effacement volontaire ou accidentel de données
- ➡ directement lié à la confiance que peuvent avoir les utilisateurs dans les services apportés par le réseau

R.CHALON Systèmes d'exploitation de réseaux locaux 6

2ème partie: Serveurs NetWare de Novell

- NetWare est un système d'exploitation de réseaux [NOS=Network Operating System] fonctionnant sur un serveur dédié de type Intel x86 (486, Pentium, Pentium II)
- Il permet le partage de ressources comme :
  - partager des fichiers, des bases de données,
  - partager des applications,
  - partager des imprimantes,
  - supporter des applications clients/serveurs, etc...
- Il accepte toutes sortes de postes clients :
  - MS-DOS, Windows 3.1, Windows 95, Windows NT,
  - OS/2,
  - MacOS,
  - UNIX,
  - etc...

R.CHALON Systèmes d'exploitation de réseaux locaux 7

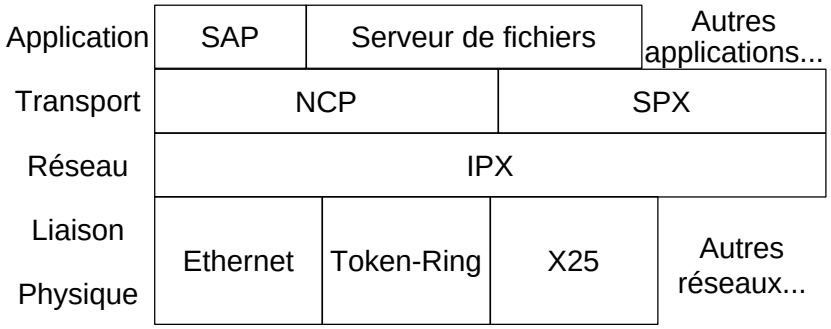
Versions de Netware

- NetWare v 2.2 (obsolète) :
  - version 16 bits conçue pour les 286
  - jusqu'à 100 utilisateurs
- NetWare v 3.x (3.12 et bientôt 3.20) :
  - version 32 bits conçue pour les 386
  - architecture ouverte : les NLM [NetWare Loadable Modules] permettent de rajouter de nouveaux services en cours de fonctionnement
- NetWare v 4.x (4.11) :
  - orientée grands réseaux, jusquà 1000 utilisateurs
  - service d'annuaire NDS [NetWare Diretory Services] basé sur la norme X500 permettant de gérer tous les objets du réseau (utilisateurs, groupes, serveurs, imprimantes, ...)
- ➡ Par la suite, sauf mention contraire, nous étudierons la **version 3.X**

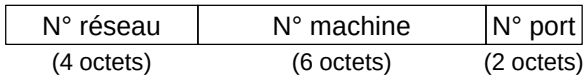
R.CHALON Systèmes d'exploitation de réseaux locaux 8

Pile de protocoles sur NetWare (1/2)

- Modèle de pile de protocoles utilisés par Novell/NetWare :
  - modèle antérieur à celui de l'OSI
  - 5 couches : pas de «session», ni «présentation»



- Adresses:

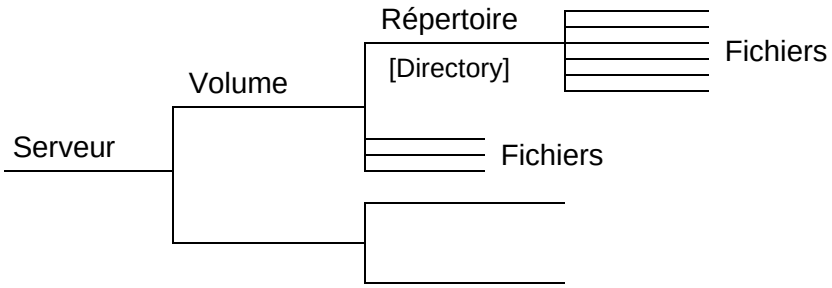


Pile de protocoles sur NetWare (2/2)

- IPX [Internetwork Packet eXchange] : protocole réseau de NetWare utilisant des adresses de 12 octets (Similaire à IP)
- NCP [NetWare Core Protocol] : protocole de transport orienté connexion sur lequel sont bâtis la plupart des services de NetWare (partage de fichiers et d'imprimantes, etc...)
- SPX [Sequenced Packet eXchange]: autre protocole de transport utilisé par certaines applications (par exemple, Lotus Notes)
- SAP [Service Advertising Protocol] : ce protocole permet d'annoncer les services disponibles sur un serveur par la diffusion de messages toutes les minutes (utilisé par les routeurs)
  - ➡ un poste client qui s'initialise diffuse une demande de recherche de serveur le plus proche : soit un serveur, soit un routeur qui connaît les serveurs grâce à SAP, répond

Structure des répertoires NetWare

- Organisation hiérarchique des répertoires et des fichiers



- Notation:

  `SERVEUR/VOLUME:REPERTOIRE/(SOUS-)REPERTOIRE/FICHIER`

R.CHALON Systèmes d'exploitation de réseaux locaux 11

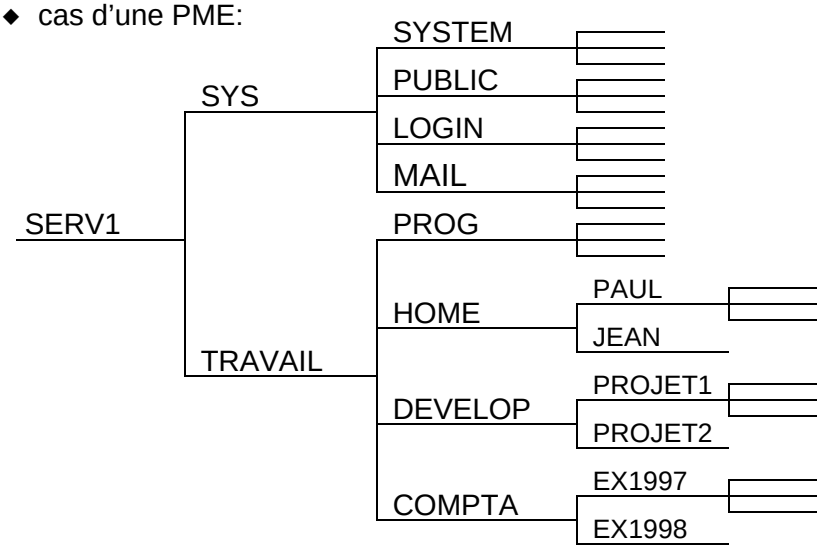
Répertoires du volume SYS

- SYS:SYSTEM
  - contient les fichiers du système d'exploitation et les outils d'administration
- SYS:PUBLIC
  - contient les utilitaires réseaux pour les utilisateurs ordinaires
- SYS:LOGIN
  - contient les programmes nécessaires à l'établissement de la connexion au serveur (visible même aux utilisateurs non-authentifiés)
- SYS:MAIL
  - contient les fichiers pour la messagerie électronique et le fichier de script de connexion [login script] (n 'existe plus dans la v 4.xx)

R.CHALON Systèmes d'exploitation de réseaux locaux 12

Exemple de structure (1/2)

- cas d'une PME:



R.CHALON Systèmes d'exploitation de réseaux locaux 13

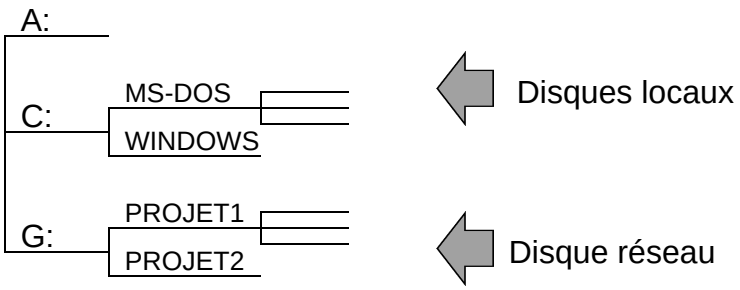
Exemple de structure (2/2)

- TRAVAIL:PROG
  - contient des programmes partagés entre les utilisateurs (traitements de textes, logiciels de dessins, etc...)
- TRAVAIL:HOME
  - contient des répertoires privés: un pour chaque utilisateur ayant un compte sur ce serveur
- TRAVAIL:DEVELOP
  - répertoire de travail de l'équipe de recherche et développement; chaque projet a son propre répertoire
- TRAVAIL:COMPTA
  - répertoire de travail pour le service comptabilité; un sous-répertoire par exercice comptable
- etc...

R.CHALON Systèmes d'exploitation de réseaux locaux 14

Accéder à un répertoire

- Depuis une machine cliente sous MS-DOS (ou Windows): la commande MAP fait correspondre une lettre disponible d'un lecteur à un répertoire du serveur :
  - exemple: `MAP ROOT G:=TRAVAIL:DEVELOP`
- Depuis la machine cliente, on «voit» le serveur de fichiers comme un (ou plusieurs) disque(s) supplémentaire(s) :



R.CHALON Systèmes d'exploitation de réseaux locaux 15

Utilisateur

- Un utilisateur est toute personne déclarée sur le serveur et autorisée à se connecter (**login**) pour utiliser les ressources auxquelles elle a droit:
  - chaque utilisateur a un nom unique (max 47 caractères)
- Deux utilisateurs par défaut :
  - SUPERVISOR : compte de l'administrateur du système ; il a tous les droits
  - GUEST : compte invité ; il n'a que des droits minimaux (par défaut, aucuns droits)
- L'administrateur peut créer autant de compte qu'il y a d'utilisateurs potentiels ; cependant, seul un nombre limité peut se connecter **simultanément** à un serveur (en fonction de la licence achetée, de 5 à 1000 utilisateurs)
- Exemple :
  - JEAN et PAUL sont 2 utilisateurs déclarés sur SERV1

R.CHALON Systèmes d'exploitation de réseaux locaux 16

Groupes d'utilisateurs

- Pour simplifier la gestion des utilisateurs et de leurs droits d 'accès, l'administrateur peut créer des groupes d'utilisateurs
- Un groupe créé par défaut : EVERYONE
  - ➡ tout nouvel utilisateur est automatiquement membre de ce groupe (mais il peut en être retiré si nécessaire)
- Tout utilisateur peut être membre d'un nombre quelconque de groupes :
  - tout droit appliqué à un groupe l'est automatiquement à tous les utilisateurs de ce groupe (**héritage** des droits)
  - si un utilisateur appartient à plusieurs groupes, les droits **se cumulent**
- Exemples :
  - JEAN est membre du groupe PROJ1 (et EVERYONE)
  - PAUL est membre du groupe COMPTABILITE (et EVERYONE)

Sécurité

- 4 niveaux de sécurité :
  - sécurité à la connexion (login)
  - droits d'accès aux répertoires et aux fichiers
  - attributs de fichiers
  - sécurité d'accès à la console du serveur de fichier
- Contrôler :
  - qui accède au serveur à travers le réseau
  - à quelles ressources (répertoires et fichiers) un utilisateur peut accéder
  - ce qu'un utilisateur peut faire avec ces ressources (lire, créer, modifier, effacer, ...)
  - qui peut travailler sur la console du serveur

Ouverture de session [login] (1/2)

- Pour ouvrir une session [login] sur un serveur, tout utilisateur doit s'authentifier en fournissant :
  - son nom d'utilisateur
  - son mot de passe
- il est possible de forcer :
  - une longueur minimale des mots de passe
  - un changement périodique des mots de passe
  - le changement ou non du mot de passe par l'utilisateur, etc...
- Il est possible de restreindre l'accès pour un utilisateur :
  - à se connecter depuis certaines machines du réseau
  - à certaines heures
  - de bloquer le compte automatiquement après une date donnée
  - de bloquer le compte après plusieurs échecs de connexion
  - etc...

R.CHALON Systèmes d'exploitation de réseaux locaux 19

Ouverture de session [login] (2/2)

- A chaque ouverture de session, le système exécute une séquence de commande : le script de login
  - le script de login du système, le même pour tous les utilisateurs,
  - puis le script de l'utilisateur (qui peut être absent)
- Le rôle principal du script de login est d'établir un environnement de travail pour l'utilisateur :
  - connecter son répertoire privé [home directory] à un lecteur de sa machine
  - connecter un ou plusieurs répertoires du réseau en fonction de ses besoins pour son travail (accès à des programmes ou des données partagées)
  - connecter une ou plusieurs imprimante
  - envoyer des messages d'information, etc...
- Les scripts de login ont une structure proche (mais **non identique**) aux fichiers de commande MS-DOS [Batch file]

R.CHALON Systèmes d'exploitation de réseaux locaux 20

Droits d'accès [trustees]

- Les droits d'accès («trustees») permettent d'accorder:
  - à des utilisateurs ou à des groupes,
  - certains droits d'accès (lecture, écriture, effacement, etc...),
  - sur un répertoire ou un fichier
- les droits possibles sont :
  - S supervision [supervisory]
  - R lecture [read]
  - W écriture [write]
  - C création [create]
  - E effacement [erase]
  - M modification [modify]
  - F parcourir les fichiers [file scan]
  - A contrôle d'accès [access control]

R.CHALON Systèmes d'exploitation de réseaux locaux 21

Tableau des droits d'accès

	Pour un répertoire	Pour un fichier
S	■ tous les droits d'accès sur le répertoire et les fichiers et leur attributs et les masques d'héritage des droits	
R	■ ouvrir et lire le contenu de fichiers ■ exécuter des programmes	
W	■ ouvrir et modifier le contenu de fichiers	
C	■ créer des fichiers ou des sous-rép	■ récupérer le fichier après effac^{ent}
E	■ effacer les fichiers, les sous-rép et les fichiers des sous-rép	■ effacer le fichier
M	■ modifier les attributs du répertoire ou des fichiers, de renommer ATTENTION: N 'autorise pas la modification du contenu des fichiers !	
F	■ voir les fichiers du répertoire	■ voir le nom du fichier
A	■ modifier les droits d'accès du répertoire ou des fichiers ■ modifier le masque d'héritage des droits	

R.CHALON Systèmes d'exploitation de réseaux locaux 22

Droits effectifs

- Les droits effectifs d'un utilisateur sur un répertoire ou un fichier dépendent :
  - des droits d'accès qui lui ont été attribués,
  - des droits d'accès attribués aux groupes auxquels il appartient,
  - des droits d'accès qui sont annulés par le masque d'héritage des droits (I.R.M. = [Inherited Rights Mask])
- Calcul des droits effectifs :
  - les droits de l'utilisateur et des groupes sur un répertoire ou un fichier **se cumulent**
  - si un droit d'accès est directement attribué sur le répertoire (utilisateur et/ou groupe), l'héritage et **l'IRM sont ignorés** pour cet utilisateur/ce groupe
  - sinon, les droits sont hérités du répertoire parent et le masque d'héritage (IRM) **annule éventuellement certains droits**

Exemples de calcul de droits effectifs (1/2)

- Exemple 1 : droits d'accès directs (pour l'utilisateur JEAN)

DEVELOP	
Effectif=	[ ]

PROJET1	
I.R.M.	[S]
(groupe) PROJ1	[R F]
(utilis.) JEAN	[WCEM]
Effectif=	[RWCEMF]

- Exemple 2 : droits d'accès hérités (pour l'utilisateur PAUL)

COMPTA	
I.R.M.	[SRWCEMFA]
PAUL	[RWCEMF]
Effectif=	[RWCEMF]

EX1998	
I.R.M.	[SRWCEMFA]
Effectif=	[RWCEMF]

Exemples de calcul de droits effectifs (2/2)

- Exemple 3 : droits d'accès hérités avec masque d'héritage

COMPTA	
I.R.M.	[SRWCEMFA]
PAUL	[RWCEMF]
Effectif=	[RWCEMF]

EX1997	
I.R.M.	[SR F]
Effectif=	[R F]

- Exemple 4 : droits d'accès «supervision»

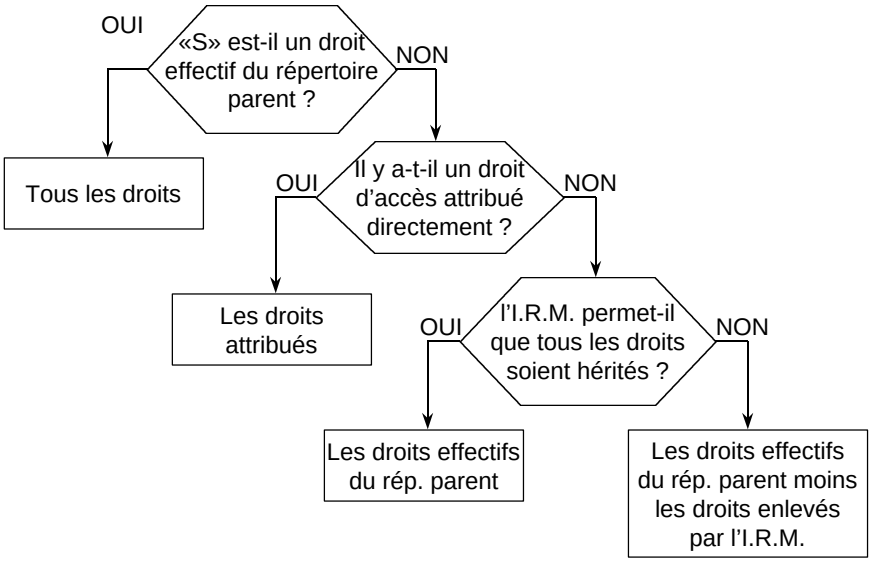
Le droit «S» est toujours hérité !

COMPTA	
I.R.M.	[SRWCEMFA]
JEAN	[S]
Effectif=	[SRWCEMFA]

EX1997	
I.R.M.	[SRWCEMFA]
JEAN	[R F]
Effectif=	[SRWCEMFA]

R.CHALON Systèmes d'exploitation de réseaux locaux 25

Résumé sur le calcul des droits effectifs



R.CHALON Systèmes d'exploitation de réseaux locaux 26

Exemples de combinaisons de droits

- Tous les droits sur une partie de l'arborescence :
  - `[S ]` ou `[SRWCEMFA]`
- Interdire tout accès, y compris ne pas voir le rép. ou le fichier :
  - `[ ]`
- Déposer des fichiers dans un répertoire, sans pouvoir les modifier ultérieurement (style «boîte aux lettres») :
  - `[ C ]`
- Voir les fichiers et les ouvrir en lecture seule :
  - `[ R F ]`
- Ouvrir, modifier les fichiers, les effacer, les renommer :
  - `[ RWCEMF ]`
- En plus, modifier des droits d'accès des utilisateurs (y compris soi-même) :
  - `[ RWCEMFA]`

R.CHALON Systèmes d'exploitation de réseaux locaux 27

Attributs de fichier et de répertoire

- Les attributs des fichiers et des répertoires permettent de **limiter** les actions sur ces fichiers **malgré les droits effectifs** que peuvent avoir les utilisateurs (y compris l'administrateur)
- Les principaux attributs sont :
  - A à archiver [archive needed]
  - C copie interdite [copy inhibit]
  - D effacement interdit [delete inhibit]
  - X en exécution seulement [execute only]
  - H caché [hidden]
  - P peut être purgé [purgeable]
  - Ro/Rw lecture seule/lecture-écriture [read only/read write]
  - R changement de nom interdit [rename inhibit]
  - S partageable [shareable]
  - Sy système
  - T transactionnel

R.CHALON Systèmes d'exploitation de réseaux locaux 28

Tableau des attributs (1/2)

	rép.	fich.	description
A		✓	■ marque les fichiers modifiés depuis la dernière sauvegarde ■ assigné automatiquement
C		✓	■ empêche la copie (pour utilisateur MacIntosh seul[en]t) ■ masque les droits R et F ■ droit M nécessaire pour ôter cet attribut
D	✓	✓	■ empêche l'effacement du fichier ou du répertoire ■ masque le droit E ■ droit M nécessaire pour ôter cet attribut
X		✓	■ empêche la copie du fichier ■ assigné pour .COM et .EXE seul. ■ ne peut être ôté
H	✓	✓	■ empêche de voir le fichier ou le rép. avec DIR
P	✓	✓	■ purge le fichier dès qu'il est effacé ■ le fichier ne peut plus être récupéré par SALVAGE

R.CHALON Systèmes d'exploitation de réseaux locaux 29

Tableau des attributs (2/2)

	rép.	fich.	description
Ro/ Rw		✓	■ les nouveaux fichiers sont par défaut Rw et peuvent être modifiés jusqu'à ce que l'attribut Ro soit positionné ■ mettre Ro, positionne automatiquement attributs D et R ■ droit M nécessaire pour enlever l'attribut Ro
R	✓	✓	■ empêche le changement du nom du fichier ou du répertoire ■ droit M nécessaire pour ôter cet attribut
S		✓	■ permet l'accès à un fichier par plusieurs utilisateurs simultanément
Sy	✓	✓	■ assigné aux répertoires et fichiers du système ■ empêche de voir le fichier ou le rép. avec DIR
T		✓	■ active le système de suivi transactionnel (T.T.S.) ■ permet de synchroniser l'ensemble des modifications sur un fichier (utile pour les bases de données)

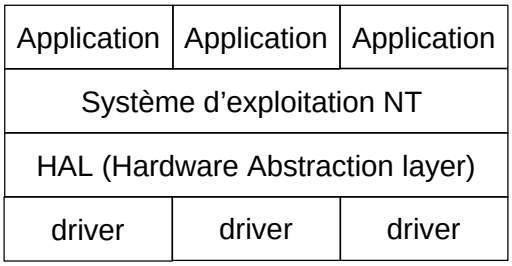
R.CHALON Systèmes d'exploitation de réseaux locaux 30

3ème partie: Windows NT

- Windows NT est un système d'exploitation de réseaux (NOS) fonctionnant sur un serveur non-dédié:
  - Intel x86,
  - DEC Alpha Systems,
  - MIPS R4x00
  - IBM PowerPC
- Il permet le partage de ressources comme :
  - partager des fichiers, des bases de données,
  - partager des applications,
  - partager des imprimantes,
  - supporter des applications clients/serveurs, etc...
- Il accepte toutes sortes de postes clients :
  - MS-DOS, Windows 3.1, Windows 95, Windows NT,
  - OS/2,
  - MacOS,
  - UNIX, etc...

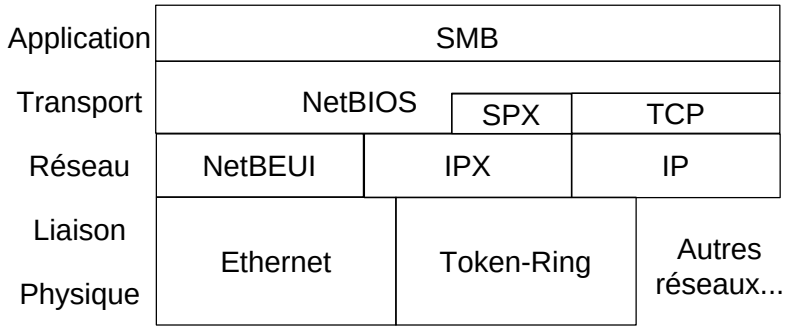
Structure de Windows NT

- Basé sur un noyau multitâche préemptif (contrairement à Novell)
- Possibilité de multi-processus symétrique [SMP=Symmetrical Multiprocessing]
- Indépendance de la plate-forme grâce à la couche d'abstraction matérielle [HAL=Hardware Abstraction Layer]
- Compatibilité avec MS-DOS grâce aux machines virtuelles [VDM=Virtual Dos Machine]



Pile de protocoles sur Windows NT (1/2)

- Modèle de pile de protocoles utilisé par Windows NT :
  - modèle antérieur à celui de l'OSI
  - 5 couches : pas de «session», ni «présentation»



R.CHALON Systèmes d'exploitation de réseaux locaux 33

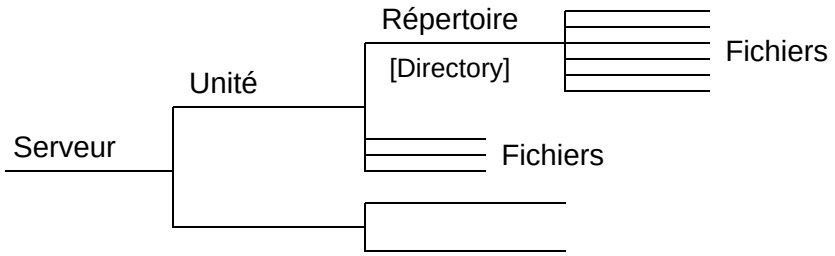
Pile de protocoles sur Windows NT (2/2)

- NetBEUI [NetBIOS Extended User Interface]: protocole réseau simple, **non-routable,** et ne supportant que NetBIOS
- NetBIOS [Network Basic Input/Ouput System]: protocole de transport. Permet e particulier d'annoncer les services disponibles sur un serveur NT. Il sert à établir des sessions entre un serveur et un client.
- SMB [Server Message Block]: protocole général de partage de fichiers et d'imprimantes. Il gère la segmentation des messages qui sont délivrés entre le serveur et le client par les couches inférieures:
  - NetBEUI,
  - NetBIOS sur SPX/IPX,
  - TCP/IP

R.CHALON Systèmes d'exploitation de réseaux locaux 34

Structures des répertoires Windows NT

- Organisation hiérarchique des répertoires et des fichiers

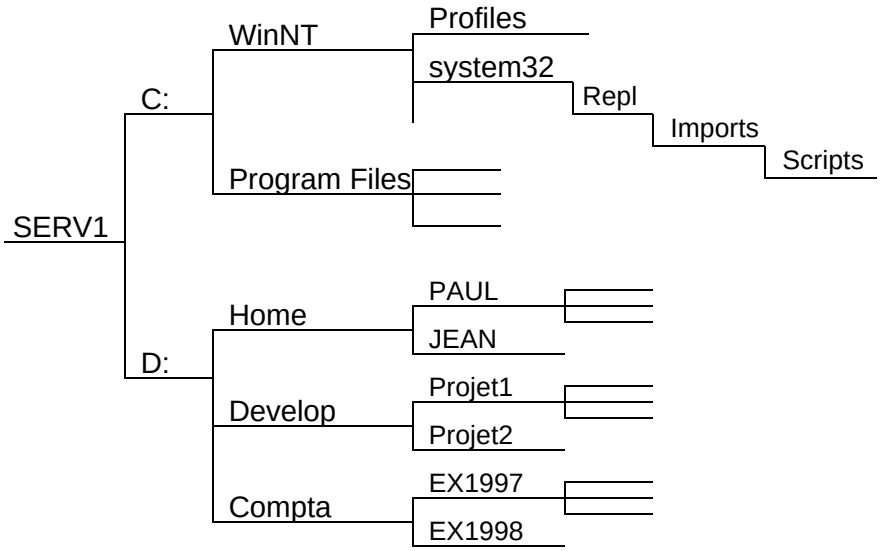


- Possibilité de partager tout répertoire de l'arborescence sous un nom de partage quelconque
- Notation:

  `\\SERVEUR\NOM_PARTAGE\REPERTOIRE\(SOUS-)REPERTOIRE\FICHIER`

R.CHALON Systèmes d'exploitation de réseaux locaux 35

Exemple de structure (1/2)



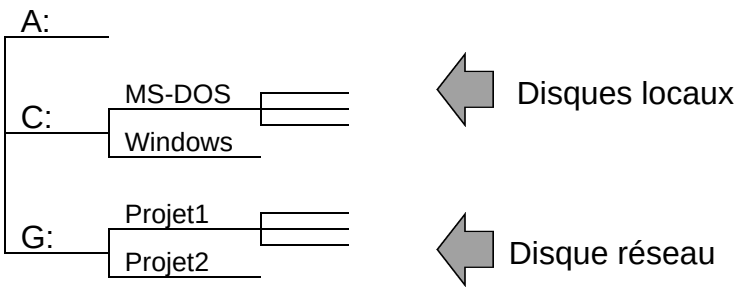
R.CHALON Systèmes d'exploitation de réseaux locaux 36

Exemple de structure (2/2)

- Partages: rendre des répertoires partageables sur le réseau
  - exemple: `NET SHARE D:\Develop \\SERV1\Projets`
- Partages du système:
  - `C:\Winnt\Profiles` sous le nom `\\SERV1\Profiles$`
    - contient les « profils » des utilisateurs
  - `C:\Winnt\System32\Repl\Imports\Scripts` sous le nom `\\SERV1\NETLOGON`
    - contient les scripts de connexion
- Partages pour le travail:
  - `D:\Home` sous le nom `\\SERV1\Users`
    - contient les répertoires privés des utilisateurs
  - `C:\Program Files` sous le nom `\\SERV1\Logiciels`
  - `D:\Develop` sous le nom `\\SERV1\Projets`
  - `D:\Compta\EX1998` sous le nom `\\SERV1\Comptabilité`
  - etc...

Accéder à un répertoire

- Depuis une machine cliente on fait correspondre une lettre disponible d'un lecteur à un **partage** du serveur :
  - exemple: `NET USE G: \\SERV1\Projets`
- Depuis la machine cliente, on «voit» le serveur de fichier comme un (ou plusieurs) disque(s) supplémentaire(s) :



Domaines Windows NT

- Par défaut, chaque serveur ou station de travail NT contient sa propre base d'utilisateur et de groupes
- Pour simplifier la gestion, les serveurs et les stations clientes peuvent être regroupés dans un **domaine**
- Un **contrôleur de domaine** gère l'ensemble des utilisateurs et des groupes de ce domaine (il peut exister plusieurs contrôleurs pour des raisons de redondances)
- utilisateur ou groupe **global**:
  - il peut être référencé par tout serveur ou client du domaine pour gérer la sécurité des accès à ses ressources
- utilisateur ou groupe **local**:
  - il ne peut être référencé que sur le serveur sur lequel il est déclaré

R.CHALON Systèmes d'exploitation de réseaux locaux 39

Utilisateurs et groupes

- Utilisateurs prédéfinis:
  - Administrateur [Administrator]:
  - Invité [Guest]
- Groupes prédéfinis (dans un domaine)
  - Admins du domaine [Domain Admins] (Global)
  - Administrateurs [Administrators] (Local)
  - Utilisa. du domaine [Domain Users] (Global)
  - Utiisateurs [Users] (Local)
  - Invités du domaine [Domain Guests] (Global)
  - Invités [Guests] (Local)
  - Opérateurs de compte [Account Operators] (Local)
  - Opérateurs d'impression [Print Operators] (Local)
  - Opérateurs de serveur [Server Operators] (Local)
  - Duplicateurs [Replicators] (Local)
  - Tout le monde [Everyone]: pseudo-groupe global qui contient tous les utilisateurs du réseau (authentifiés ou non)

R.CHALON Systèmes d'exploitation de réseaux locaux 40

Niveaux de sécurité Windows NT

- niveaux de sécurité :
  - la sécurité à la connexion (**logon**)
  - les «**droits**»
  - les **permissions** d'accès aux partages, répertoires et fichiers
  - attributs de fichiers
- Contrôler :
  - qui accède au serveur à travers le réseau
  - quels droits spécifiques un utilisateur peut avoir comme:
    - se connecter localement,
    - s'approprier des fichiers, etc...
  - à quels ressources partagées, répertoires et fichiers un utilisateur peut accéder
  - ce qu'un utilisateur peut faire avec ces fichiers (lire, créer, modifier, effacer, ...)

R.CHALON Systèmes d'exploitation de réseaux locaux 41

Ouverture de session [login] (1/2)

- Deux types de login:
  - S'il n'existe pas de domaine:
    - login local à un serveur ou une station,
    - login à distance à un (ou plusieurs) serveur(s),
  - S'il existe un domaine:
    - login local à un serveur ou une station,
    - login au domaine (permet d'accéder à toutes ressources autorisées tant au niveau local que sur les serveurs du domaine)
- Les possibilités de restrictions sont similaires à celles de NetWare:
  - longueur minimale des mots de passe, changement périodique, etc...
  - restriction d'accès: à se connecter depuis certaines machines du réseau, à certaines heures, de bloquer le compte automatiquement après une date donnée, etc...

R.CHALON Systèmes d'exploitation de réseaux locaux 42

Ouverture de session [login] (2/2)

- A chaque ouverture de session, on peut demander l'exécution d'un script de login; tout fichier de commande convient:
  - soit sur la machine locale,
  - soit dans le partage \\SERVER\NETLOGON
- Le rôle principal du script de login est d'établir un environnement de travail pour l'utilisateur :
  - connecter son répertoire privé [home directory] à un lecteur de sa machine
  - connecter un ou plusieurs répertoires du réseau en fonction de ses besoins pour son travail (accès à des programmes ou des données partagées)
  - envoyer des messages d'information, etc...
- Les scripts de login sont des fichiers de commande MS-DOS [Batch file]

Droits Windows NT

- A chaque utilisateur (ou groupe) peut être associé un ensemble de droits spécifiques
- **ATTENTION**: Aucun rapport avec les droits d'accès de NetWare
- Droits les plus courants:
  - Accéder à cet ordinateur depuis le réseau,
  - Ajouter des stations de travail à un domaine,
  - Sauvegarder les fichiers et les répertoires,
  - Changer l'heure du système,
  - Forcer l'arrêt du système à distance,
  - Charger et décharger des pilotes de périphériques,
  - ouvrir une session localement,
  - gérer les fichiers d'audit et de sécurité,
  - S'approprier des fichiers ou d'autres objets,
  - etc...
- En général, ces droits sont donnés à des administrateurs

Permissions

- Les permissions permettent d'accorder:
  - à des utilisateurs ou à des groupes (locaux ou globaux),
  - certaines permissions (lecture, écriture, effacement, etc...),
  - sur une ressource (partage, répertoire, fichier, imprimante, ...)
- Les permissions s'appliquent:
  - aux partages de ressources sur un réseau,
  - aux répertoires et fichiers sur un système de fichiers NTFS
- Les permissions ressemblent aux droits d 'accès de Netware mais il existe de nombreuses différences

R.CHALON Systèmes d'exploitation de réseaux locaux 45

Permissions pour un partage

- Les permissions possibles pour un **partage** de répertoire**:**
  - Contrôle total
  - Pas d'accès
  - Lecture
  - Modification
- Les permissions ne s'appliquent qu'aux utilisateurs accédant au répertoire partagé à travers le réseau, elles ne s'appliquent pas aux utilisateurs locaux
- Si plus d'une permission s'applique à un utilisateur (appartenance à plusieurs groupes) elles s'additionnent sauf pour «Pas d'accès» qui annule toutes les autres permissions
- Par défaut, un nouveau partage est créé avec «Contrôle total» pour «Tout le Monde», ce qui signifie qu'il n'y a **aucune restriction** !

R.CHALON Systèmes d'exploitation de réseaux locaux 46

Permissions NTFS (1/2)

- NTFS [NT File System] est le système de fichier «natif» de Windows NT, qui, contrairement à FAT, permet de définir des permissions d'accès aux répertoires et fichiers
- Les permissions possibles sont (combinaisons de permissions «spéciales» sur les répertoires et les fichiers)
  - Pas d'accès ( ) ( )
  - Lister (RX) ( )
  - Lire (RX) (RX)
  - Ajouter (WX) ( )
  - Ajouter et Lire (RWX) (RX)
  - Modifier (RWXD) (RWXD)
  - Contrôle Total (RWXDPO) (RWXDPO)
  - Accès spécial au répertoire
  - Accès spécial au fichier

R.CHALON Systèmes d'exploitation de réseaux locaux 47

Permissions NTFS (2/2)

- Les permissions NTFS s'appliquent **après** les permissions de partage de ressources
- Si plus d'une permission s'applique à un utilisateur (appartenance à plusieurs groupes) elles s'additionnent sauf pour «Pas d'accès» qui annule toutes les autres permissions
- Si aucune permission n'est accordé à un utilisateur ou à un groupe auquel il appartient alors il n'a aucun accès au répertoire ou au fichier
- Il n'y pas d'héritage hiérarchique des droits comme dans NetWare sauf à la création d'un fichier ou d'un répertoire où les permissions du répertoire père sont recopiées
- Le **propriétaire** d'un répertoire ou d'un fichier a tous les droits (les permissions sont ignorées). Similaire au droit d'accès «**S**» de Netware

R.CHALON Systèmes d'exploitation de réseaux locaux 48

Tableau des permissions spéciales

	Pour un répertoire	Pour un fichier
R read	■ lire le nom des fichiers et des sous-répertoires	■ ouvrir et lire le contenu des fichiers
W write	■ créer des fichiers et des sous-répertoires	■ mettre à jour le fichier
X execute	■ mettre à jour les sous-répertoires	■ exécuter le programme
D delete	■ effacer le répertoire courant	■ effacer le fichier
P change permissions	■ Changer les permissions du répertoire courant	■ Changer les permissions du fichier
O take ownership	■ S'approprier le répertoire courant	■ S'approprier le fichier

R.CHALON Systèmes d'exploitation de réseaux locaux 49

Attributs de fichiers NTFS

- Les attributs des fichiers et des répertoires permettent de **limiter** les actions sur ces fichiers **malgré les droits effectifs** que peuvent avoir les utilisateurs
- Les principaux attributs sont :
  - Lecture seule
  - Fichier caché
  - Fichier système
  - Archive
  - Compressé

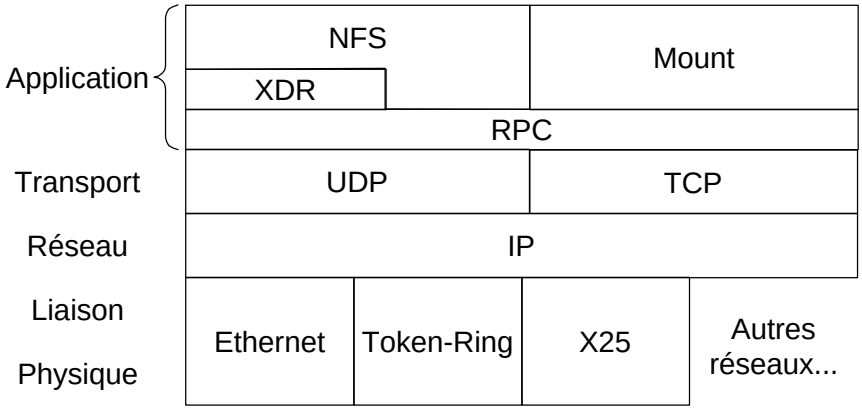
R.CHALON Systèmes d'exploitation de réseaux locaux 50

4ème partie: NFS - Network File System

- NFS [Network File System] permet le partage de fichiers entre ordinateurs fonctionnant sous UNIX.
- Créé par Sun MicroSystems mais aujourd'hui utilisé par tout constructeur
- Utilisable aussi sur d 'autres plates-formes (PC sous MS-DOS ou Windows, OS/2, etc…) avec certaines restrictions dues :
  - à une définition différente des utilisateurs et des groupes
  - à des formats de fichiers différents
- Partage « symétrique » : toute machine peut exporter ses répertoires (agir comme serveur) et importer des répertoires d 'autres machines (agir comme client) simultanément

Pile de protocoles NFS (1/2)

- Modèle basé sur TCP/IP
- Fonctionne principalement sur UDP mais aussi sur TCP

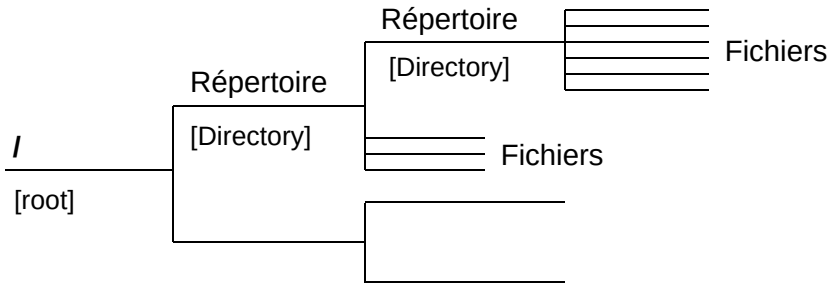


Pile de protocoles NFS (2/2)

- NFS [Network File System]: protocole principal de partage de fichier
- Mount: protocole permettant d ’établir et de supprimer les partages de répertoires entre un client et un serveur
- XDR [eXternal Data Representation]: langage de représentation commune de données sur un réseau (assure la conversion des données)
- RPC [Remote procedure Call]: protocole permettant l ’exécution à distance de procédures sur un serveur
- Ces protocoles ont été établis initialement par Sun Microsystems mais aujourd’hui « normalisés »:
  - XDR=RFC 1014 (1989)
  - RPC=RFC 1057 (1989)
  - NFS=RFC 1094 (1989) et NFS3=RFC 1813 (1995)

Structure des répertoires UNIX (Rappel)

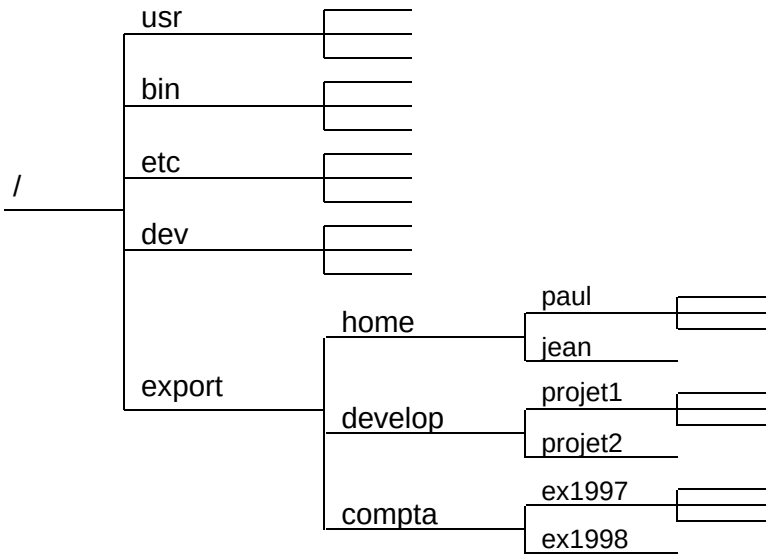
- Structure arborescente



- Notation:

  `/REPERTOIRE/(SOUS-)REPERTOIRE/FICHIER`

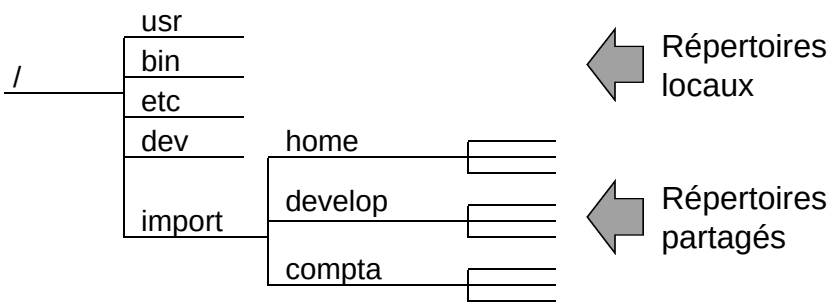
Exemple de structure (1/2)



R.CHALON Systèmes d'exploitation de réseaux locaux 55

Partager et monter un répertoire

- Partages: rendre des répertoires partageables sur le réseau depuis un serveur:
  - exemple: `share -F nfs /export`
- Monter un répertoire sur une machine cliente:
  - exemple: `mount -F nfs server:/export /import`
  - Le répertoire `/import` doit exister sur le poste client (et son contenu sera masqué tant que le répertoire sera monté)



R.CHALON Systèmes d'exploitation de réseaux locaux 56

Utilisateurs et groupes sous UNIX

- Les utilisateurs sont définis par :
  - nom d ’utilisateur
  - mot de passe (codé)
  - n° d ’utilisateur (uid)
  - n° de groupe (gid)
  - nom en clair
  - chemin du répertoire privé [home directory]
  - chemin du programme de commande [shell]
  - utilisateur toujours défini **root** (uid 0), l ’administrateur du système
  - ➡ définitions stockées dans le fichier `/etc/passwd`
- Les groupes sont définis par :
  - nom de groupe
  - n° du groupe (gid)
  - liste des membres du groupe
  - ➡ définitions stockées dans le fichier `/etc/group`

R.CHALON Systèmes d'exploitation de réseaux locaux 57

Fichiers UNIX

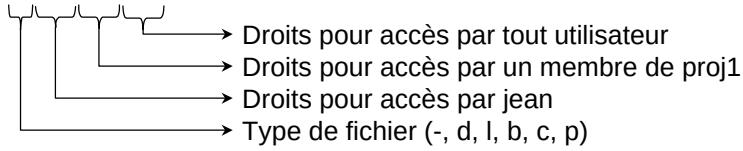
- A chaque fichier ou répertoire est associé un i-node qui contient un certain nombre d ’attributs:
  - propriétaire de ce fichier (uid)
  - groupe propriétaire de ce fichier (gid)
  - type de fichier:
    - - = fichier ordinaire
    - d = répertoire
    - l = lien symbolique sur un fichier
    - b,c, p = fichiers spéciaux
  - taille en octets
  - date de dernière modification, de dernier accès, …
  - droits d ’accès au fichier :
    - par l ’utilisateur propriétaire
    - par un membre du groupe propriétaire
    - par les autres utilisateurs

R.CHALON Systèmes d'exploitation de réseaux locaux 58

Droits d ’accès (1/2)

- Les droits d ’accès principaux sont:
  - r [read] : accès en lecture
  - w [write] : accès en écriture
  - x [execute] : accès en exécution (ou parcours pour un répertoire)
  - s [setuid ou setgid] : accès spécial en exécution
- Ces droits peuvent être attribués à 3 catégories d ’utilisateurs :
  - u [user] : le propriétaire du fichier
  - g [group] : le groupe propriétaire du fichier
  - o [other] : tous les autres utilisateurs
- Notation avec la commande « **ls -l** » :

```
-rw-rw-r--  1  jean   proj1   1362  Jan 23 14:18  memo.txt
```



Droits d ’accès (2/2)

- Droits spéciaux « setuid » et « setgid » :
  - pour un programme, le droit « s » permet que ce programme s ’exécute sous le nom de l ’utilisateur (pour setuid) ou du groupe (pour setgid) quelle que soit l ’utilisateur qui a lancé le programme
  - exemple:
    `-rwsr-xr-x  1  jean   proj1  25456  Mar 12 15:34  calcul`
    si paul lance « calcul », le programme fonctionnera avec :
    - les droits de l ’utilisateur jean (au lieu de paul)
    - et les droits du groupe comptabilite (groupe de paul)
- A la création d ’un fichier (ou d ’un répertoire) :
  - le uid du créateur est affecté au fichier
  - le gid du créateur est affecté au fichier sauf si « setgid » est positionné sur le répertoire auquel cas c ’est le gid du répertoire qui est utilisé
  - les droits **`rwxrwxrwx`** sont affectés sauf si le « umask » masque certains droits. Classiquement on autorise **`rw-r-----`**

Droits d ’accès et NFS

- Dans un répertoire monté par NFS, un utilisateur accède aux fichiers (et aux répertoires) avec l ’uid et le gid de la machine cliente
  - ➡ cela implique d ’avoir des déclarations d ’utilisateurs et de groupes cohérentes entre les 2 machines et, en pratique, à avoir les mêmes fichiers `/etc/passwd` et `/etc/group`
- L ’accès avec l ’uid 0 (root) à un répertoire monté par NFS n ’est pas possible sauf autorisation explicite au moment de la déclaration du partage.
- Pour éviter toute boucle, les accès à des répertoires monté par NFS n ’est pas récursif : par exemple :
  - A partage `/usr` et B le monte dans `/import/exportA`
  - B partage `/import` et C le monte dans `/imp/exportB`
  - ➡ C **ne verra pas** dans `/imp/exportB/exportA` le contenu de `/usr` de A

Options NFS

- Options pour les partages :
  - limiter un partage en lecture seule
  - limiter le partage à un groupe de machine en lecture/écriture ou en lecture seule (les autres machines n ’auront pas d ’accès)
  - autoriser un groupe de machine à ce que root puisse accéder au partage
  - interdire les setuid et setgid
- Options pour le montage de répertoire :
  - limiter le montage à un accès en lecture seule
  - ne pas autoriser la fonction setuid sur un partage
  - activer une authentification sécurisée des postes clients (DES, kerberos, etc…)

AFS - Andrew File System

- Améliorations par rapport à NFS
- Basé également sur les RPC et XDR
- Basé sur un espace virtuel de fichiers à l 'échelle mondiale offrant une vue unique : `/afs/ec-lyon.fr/...`
- Gère des volumes logiques qui peuvent être montés au gré des besoins par des clients AFS
- Gère un cache sur le disque de la machine cliente ce qui améliore les performances mais complexifie la gestion de la cohérence avec les autres utilisateurs
- Gère ses propres listes de contrôle d 'accès pour les partages de répertoires avec héritage des contrôles d 'accès :
  - ➡ inutile d 'avoir les mêmes utilisateurs déclarés sur les clients et les serveurs
  - ➡ gestion plus facile de plate-formes non UNIX (MS-Dos, MacOS, …)

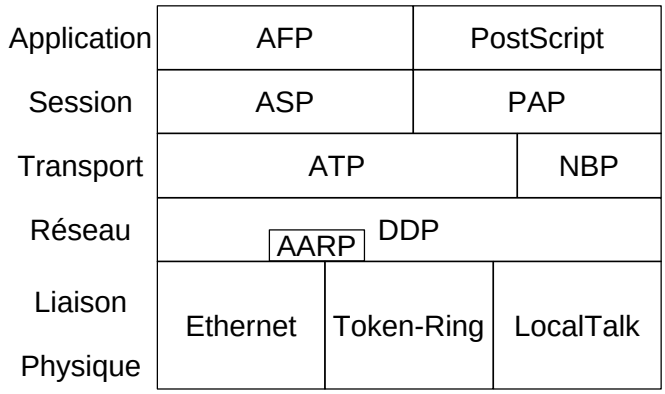
5ème partie: Appleshare

- Serveur de partage de fichiers et d'imprimantes dans l'environnement **Apple MacIntosh**
- Caractéristiques:
  - Utilise une pile de protocoles spécifiques: AppleTalk
  - Fonctionnement "Plug-and-Play":
    - ➡ attribution automatiques des adresses des ordinateurs dans le réseau
  - Adresses de la forme:

N° réseau	N° machine
(2 octets)	(1 octet)

  - Gestion de "zones": regroupements logiques de machines différents des réseaux physiques
    - une zone peut couvrir plusieurs réseaux
    - un réseau peut contenir plusieurs zones
    - ➡ comparable aux "domaines NT" ou au "DNS TCP/IP"

Pile de protocoles AppleTalk (1/2)



R.CHALON Systèmes d'exploitation de réseaux locaux 65

Pile de protocoles AppleTalk (2/2)

- AFP [AppleTalk Filing Protocol]: protocole de partage de fichiers entre un client MacIntosh et un serveur AppleShare
- ASP [AppleTalk Session Protocol]: couche session
- ATP [AppleTalk Transaction Protocol]: couche transport
- PAP [Printer Access Protocol]: protocole d'accès aux imprimantes et aux files d'impression sur le réseau AppleTalk
- NBP [Name Binding Protocol]: permet de connaître les services disponibles sur un réseau AppleTalk
- DDP [Datagram Delivery Protocol]: protocole réseau non-fiable de remise de paquet
- AARP [AppleTalk Address Resolution Protocol]: protocole établissant la corespondance entre les adresses AppleTalk et les adresses physiques Ethernet ou Token-Ring (adresses MAC)

R.CHALON Systèmes d'exploitation de réseaux locaux 66