

WINDOWS NTx



Historique

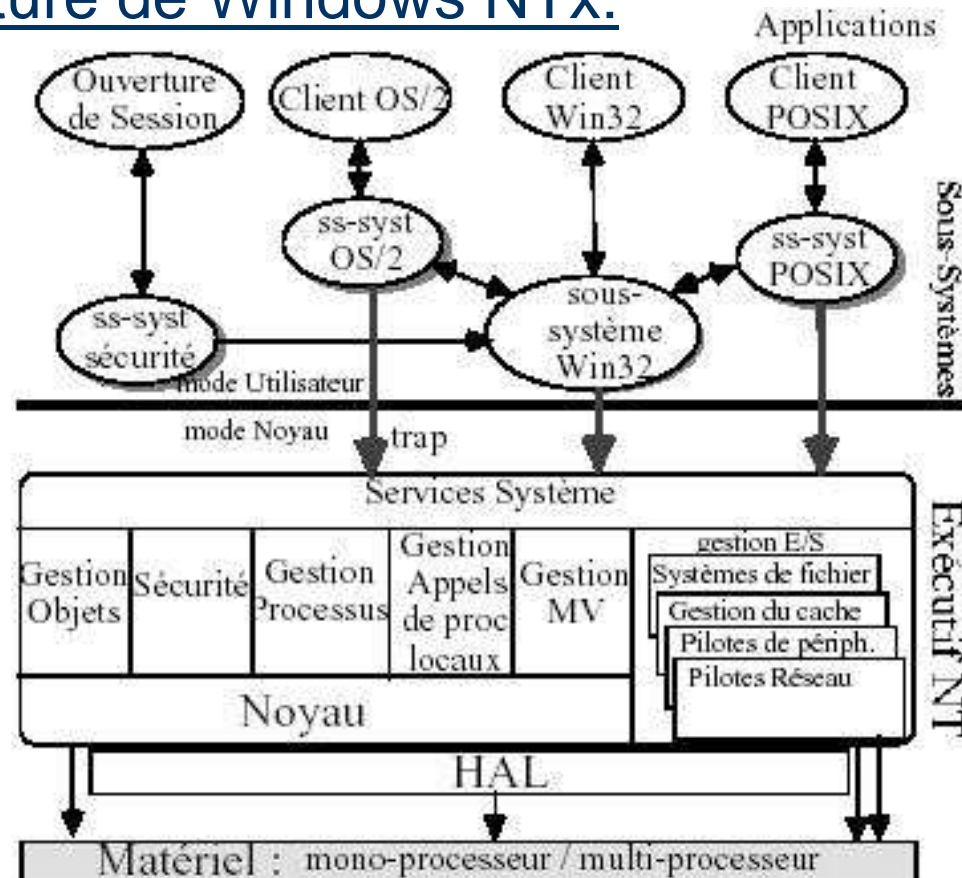
- 1994: Naissance de Windows NT3.5.
- 1996: Naissance de Windows NT4.0.
- 2000: Naissance de Windows NT5 et Windows 2000.
- 2001 à 2003: Naissance de Windows NT5.1, Windows XP et Windows 2003.

Présentation générale

- Windows NTx est un OS préemptif, multi thread, multiprocesseur, et à une architecture 32 bits.
- Il prend en charge les périphérique d'entrée sortie USB (depuis la version NT5).

Présentation générale

- Architecture de Windows NTx:



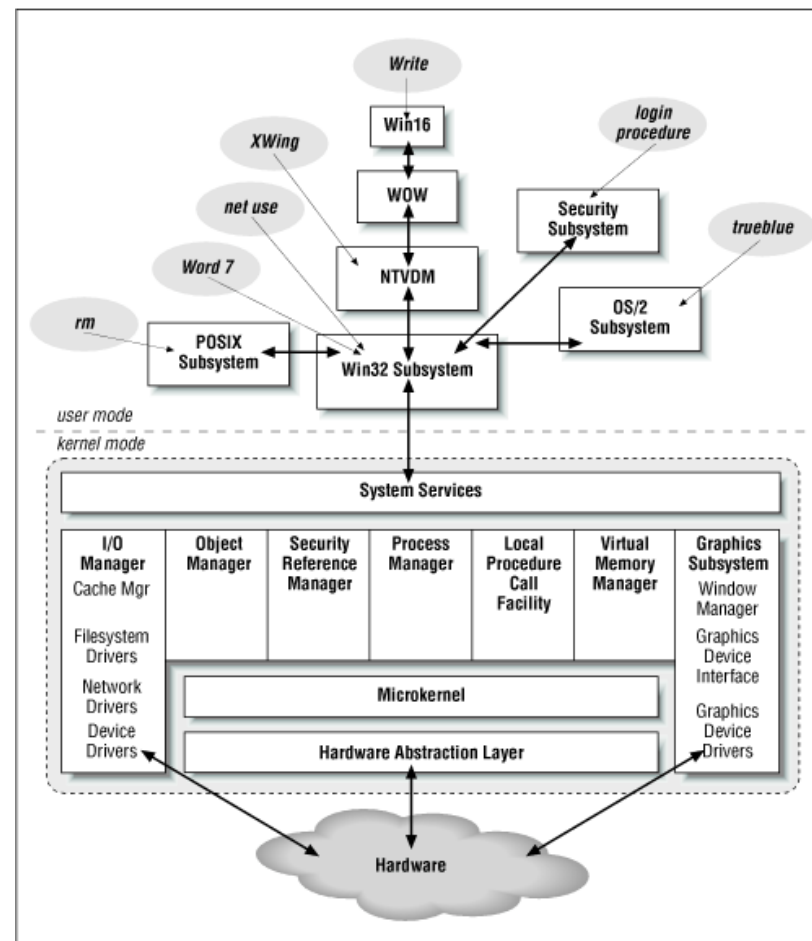
Présentation générale

- Comme vu dans le cours sur Windows 9x on utilise toujours la notion de User Space, de Kermel, d'API, de couche d'abstraction matérielle, Micro Noyau
- Mais maintenant une nouvelle notion viens. Il s'agit des sous-systèmes d'environnement.

Présentation générale

- Les sous systèmes d'environnements:
 - Ils permettent à de nombreuses application de types différents de s'exécuter de manière transparente sur le même environnement de bureau graphique.
 - Par exemple pour MS-DOS, il émule l'environnement du système d'exploitation DOS en créant un machine virtuelle DOS sur laquelle peut tourner toutes les applications DOS.
 - Ils sont protégés les une des autres (processus différents et espaces mémoires séparés.
 - Si le sous-système Win32 plante plu rien ne marche.

Présentation générale



Présentation générale

- Le sous-système d'environnement Win32 gère donc tous les autres sous-système ainsi que toutes les applications, les procédures d'ouverture de session, la sécurité et envoie des informations au micro noyau de Windows NTx à l'aide de ntdll.dll.
 - Pour tous ce qui est de la technologie Windows NTx le Kermel fournit des services de bas niveau. Programme d'applications appelés serveur qui offrent des fonctions complémentaires de l'os.
- La base du système reste stable et les serveurs sont modifiés ou créés.

Présentation générale

- Les sous système d'environnements sont des serveurs en mode utilisateur. Chaque serveur est situé dans un processus séparé dont la mémoire est protégée.
- Les applications utilisateurs sont lancées lorsque les clients demandent des services aux sous-système protégés qui sont des serveurs. Il y a alors une division du système en processus qui dialoguent avec les clients. Ces principes sont identiques en local ou à travers un réseau.

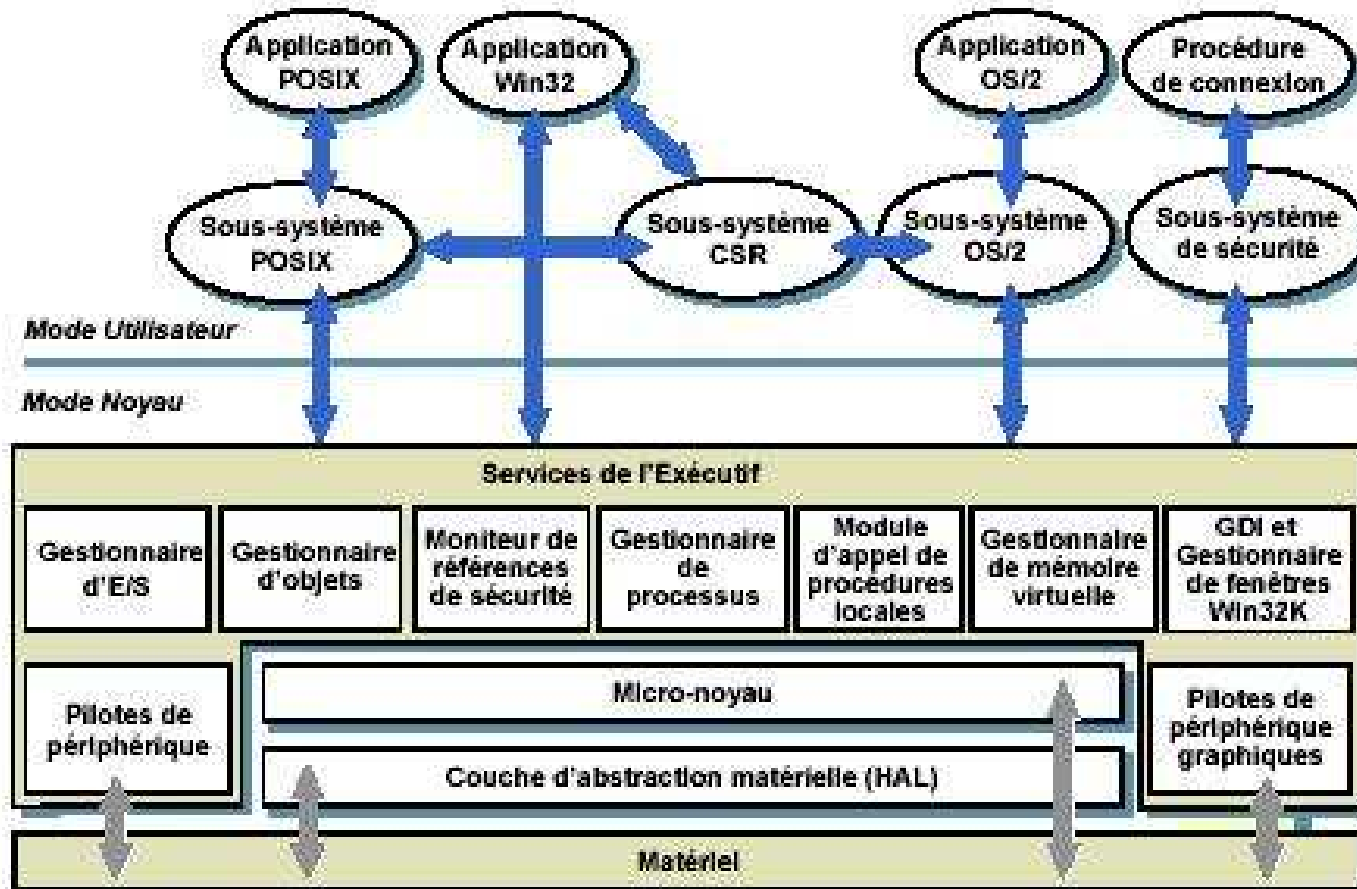
Présentation générale

- Le Mode Noyau est un mode privilégié d'executions de code dans un microprocesseur, dans lequel toute la mémoire est totalement accessible et toutes les instructions du microprocesseur peuvent être employées. Il permet de garantir la stabilité du système si une application plante.
- Le Mode Utilisateur fait en sorte que les applications soient séparés de l'OS (en mode Noyau). Ce qui donne un accès limité aux données et au matériel à travers des API.

Présentation générale

- Le Micro-Noyau de NT assure les services d'un micro noyau (gestion des ressources de la machine).
- C'est un Noyau simple, léger, flexible et assez stable mais un peu plus lent que les noyaux monolithiques.
- Il gère les entrées sorties, les interruptions, les planifications des threads, la synchronisation,...(conf cours principe fondamentaux de OS).
- Différence entre Win NT3.51 et WinNT4.0/5.0 et 5.1:
→ Déplacement d'une partie du sous système d'environnement Win32 en mode Noyau (gain d'espace mémoire et de temps d'accès).

Présentation générale



Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Le gestionnaire d'entrée/Sortie:**
 - Il gère toutes les E/S de l'OS.
 - Il gère les communications entre différents pilotes (FS, périphériques matériels, périphériques réseaux).
 - Les périphériques communiquent entre eux grâce à des paquets de demande d'E/S.

Présentation générale

- **Les différents gestionnaire de Windows NT:**
→ Le gestionnaire d'entrée/Sortie se décomposent ainsi:

Gestionnaire d'E/S

Gestionnaire de cache

Systèmes de fichiers

Pilote de périphérique

Pilote de réseau

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Le gestionnaire d'entrée/Sortie, le gestionnaire de cache:**
 - Il prend en compte les opérations de cache disque. C'est-à-dire qu'il stocke temporairement les fichiers fréquemment utilisés dans une cache en mémoire.
 - On peut augmenter et diminuer dynamiquement la taille de la cache.
 - Quand un processus ouvre un fichier en cache, le gestionnaire copie simplement les données de cache vers l'espace adressable virtuel du processus.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, les pilotes des FS:
 - C'est le gestionnaire d'E/S qui gère les pilotes de système de fichiers.
 - NT supporte les système de fichiers FAT et NTFS.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, les pilotes de périphériques matériels:
 - Ce sont des programmes qui permettent de gérer les périphériques de l'ordinateur (cartes d'extension, périphériques externes, clavier, souris,...).

Présentation générale

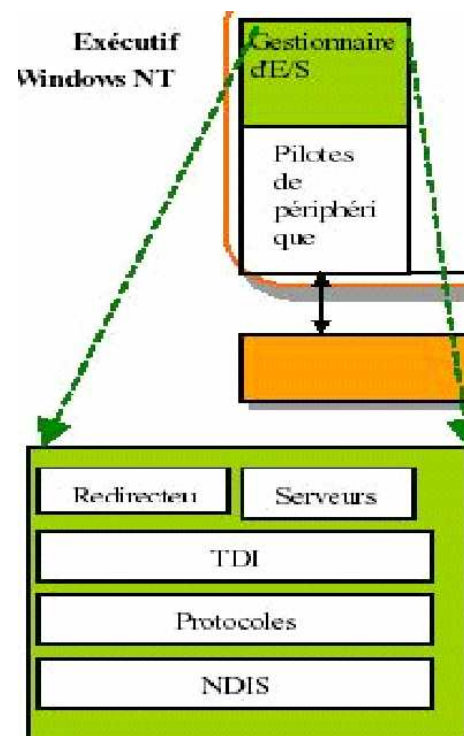
- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, les pilotes de périphériques réseaux:
 - Ils permettent de gérer les périphériques d'un réseau (carte réseau, disque réseau,...).

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - Le gestionnaire d'entrée/Sortie, exemple d'accès à un fichier;
 - Un appel système part d'une appli utilisateur, passe par un sous-système d'environnement puis par Win32 qui...
 - ... redirige la requête vers le Pilote de FS qui...
 - envoi paquet de demande au gestionnaire d'E/S
 - Qui envoie paquet au pilote de périphérique
 - Pilote de périphérique transfère le fichier du disque vers système

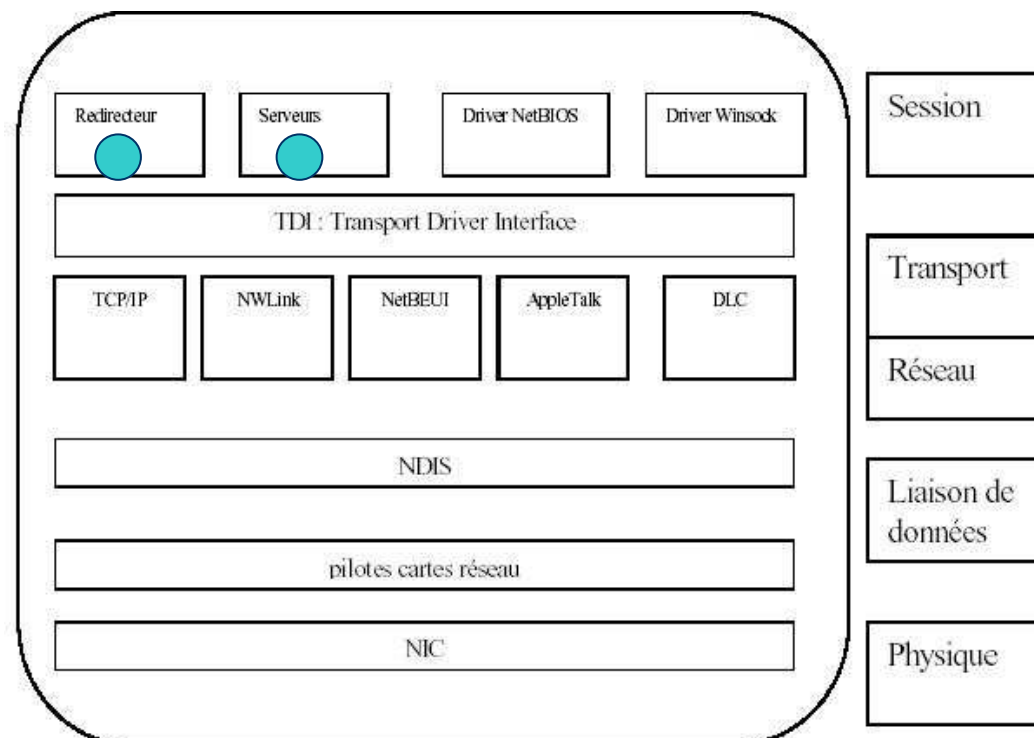
Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:



Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:



Présentation générale

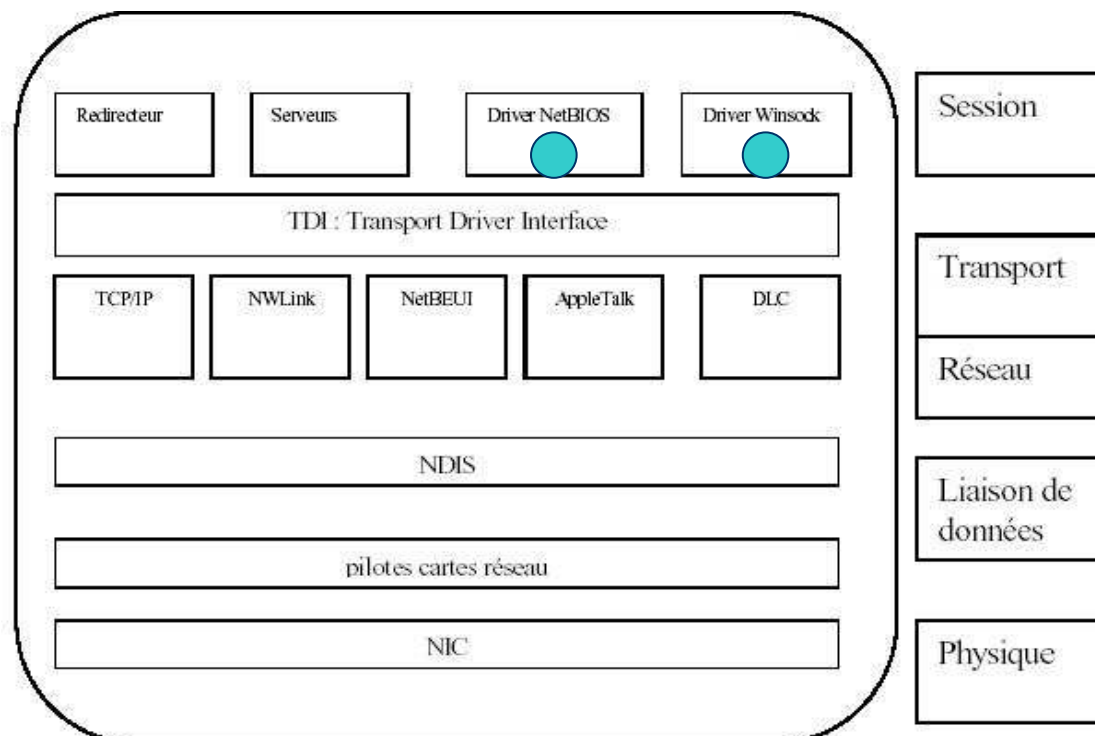
- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **Redirecteur et serveur: Pilote du système de fichier réseau.**
 - Le redirecteur dirige les demandes d'E/S. Il fournit les fonctions nécessaires pour l'accès aux ressources situées sur d'autres machines du réseau en mettant en place le protocole SMB (Server Message Box).

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Le gestionnaire d'entrée/Sortie, gestion du réseau:**
 - **Redirecteur et serveur: Pilote du système de fichier réseau.**
 - Le serveur traite les demandes provenant des redirecteurs des autres machines.
 - Déjà présent avec MS-DOS 3.x. Il permet les connexions vers Win 3.11, LanManager,...

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:



Présentation générale

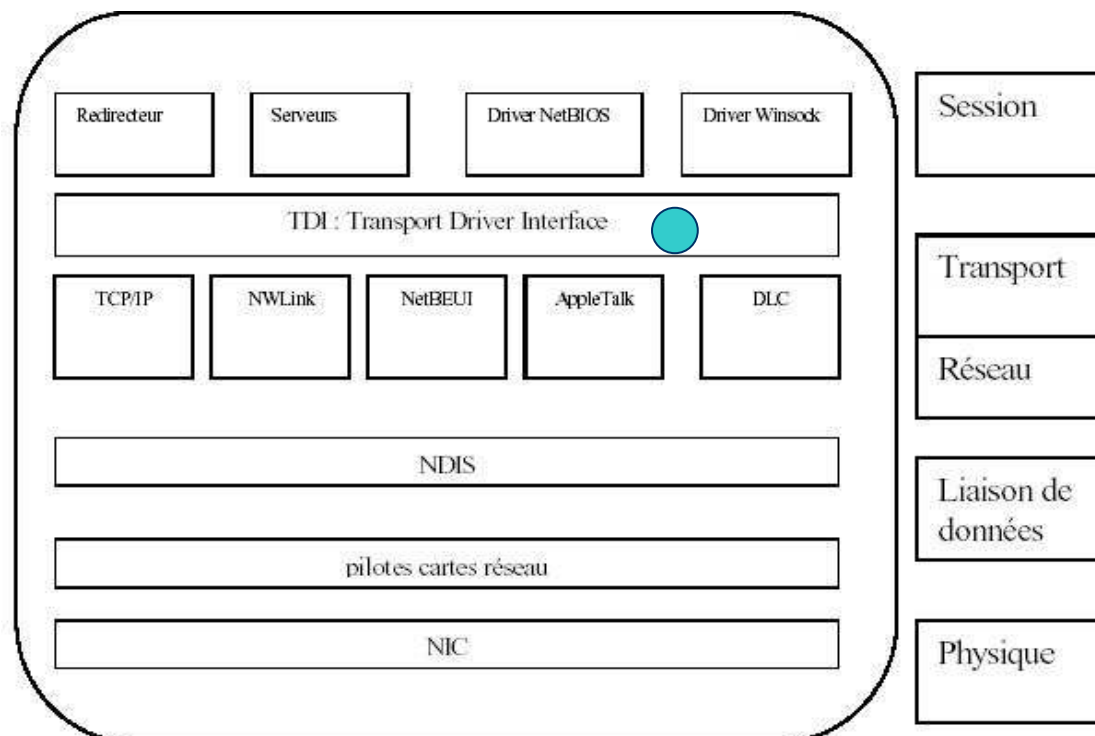
- **Les différents gestionnaire de Windows NT:**
 - **Le gestionnaire d'entrée/Sortie, gestion du réseau:**
 - **API NetBIOS et Winsock (Windows Socket):**
 - Un socket est une extrémité de communication, c'est-à-dire un objet par lequel une application envoie ou reçoit des paquets de données sur un réseau. Un socket a un type et est associé à un processus d'exécution et peut porter un nom.
 - API NetBIOS: NetBeui ou API Winsocks (TCP/IP).

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Le gestionnaire d'entrée/Sortie, gestion du réseau:**
 - **API NetBIOS et Winsock (Windows Socket):**
 - Les API Sockets ont pour rôle de rendre le réseau sous-jacent tout à fait transparent, ce qui vous évite d'avoir des connaissance particulières sur ce réseau et permet à une application de s'exécuter sur n'importe quel réseau prenant en charge les sockets.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:

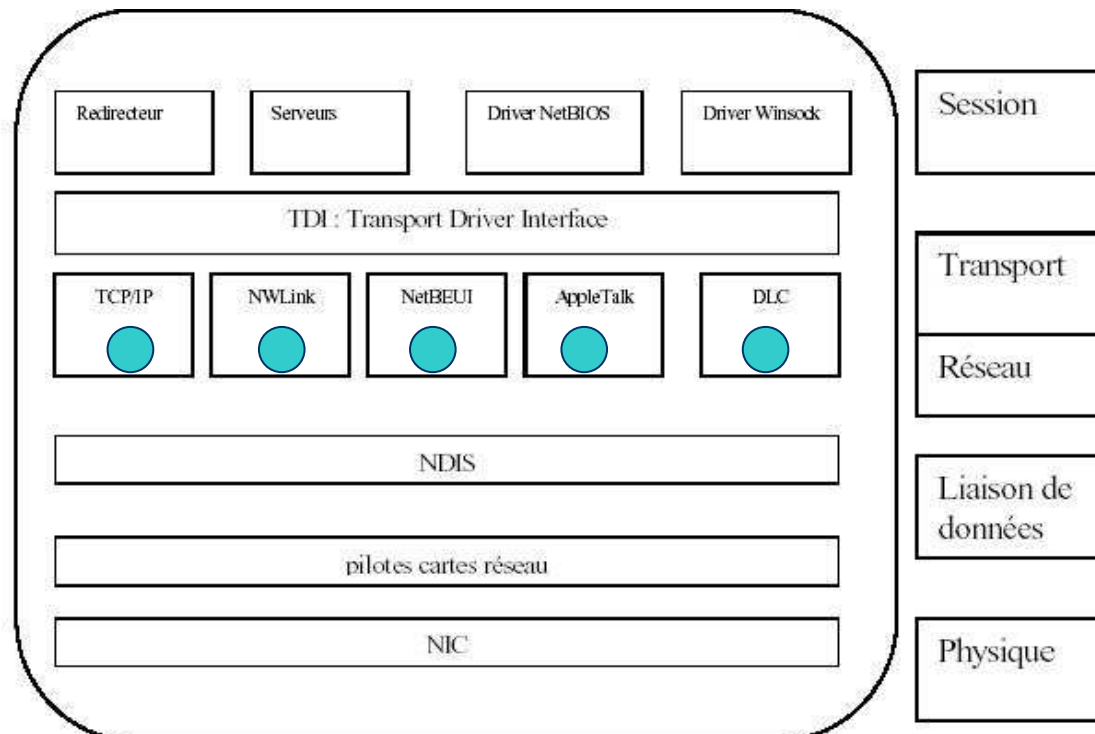


Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **La couche TDI:**
 - Elle isole les couches dites hautes (applications) des protocoles de transports. C'est une interface de programmation. Elle permet aux redirecteurs et serveurs de communiquer avec les couches transports et restant indépendant, sans se soucier du type de protocole réseau utilisé.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:



Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
- Les protocoles réseau:**
 - NetBEUI: NetBIOS extended user interface.
 - C'est le standard des réseaux Microsoft. Ce protocole à été développé pour exécuter des applications NetBIOS sur un réseau Local. Il n'est plus utilisé que pour quelques serveurs d'impression. Il est fortement conseillé de désactiver NetBUI et NetBIOS dans les protocoles réseau pour des raisons de sécurité.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
- Les protocoles réseau:**
 - NWLink (NetWork Link):
 - Couche transport compatible avec les protocoles Novell IPX/SPX. Il permet aux clients NetWare d'accéder aux ressources d'un serveur Windows NT. Il peut supporter les applications NetBIOS et Winsock.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
- Les protocoles réseau:
 - TCP/IP
 - Supporte les sockets UNIX (WinSocks, NetBIOS). On peut dire que TCP/IP est le protocole réseau universel. Il est intégré par quasiment tous les OS actuels.

Présentation générale

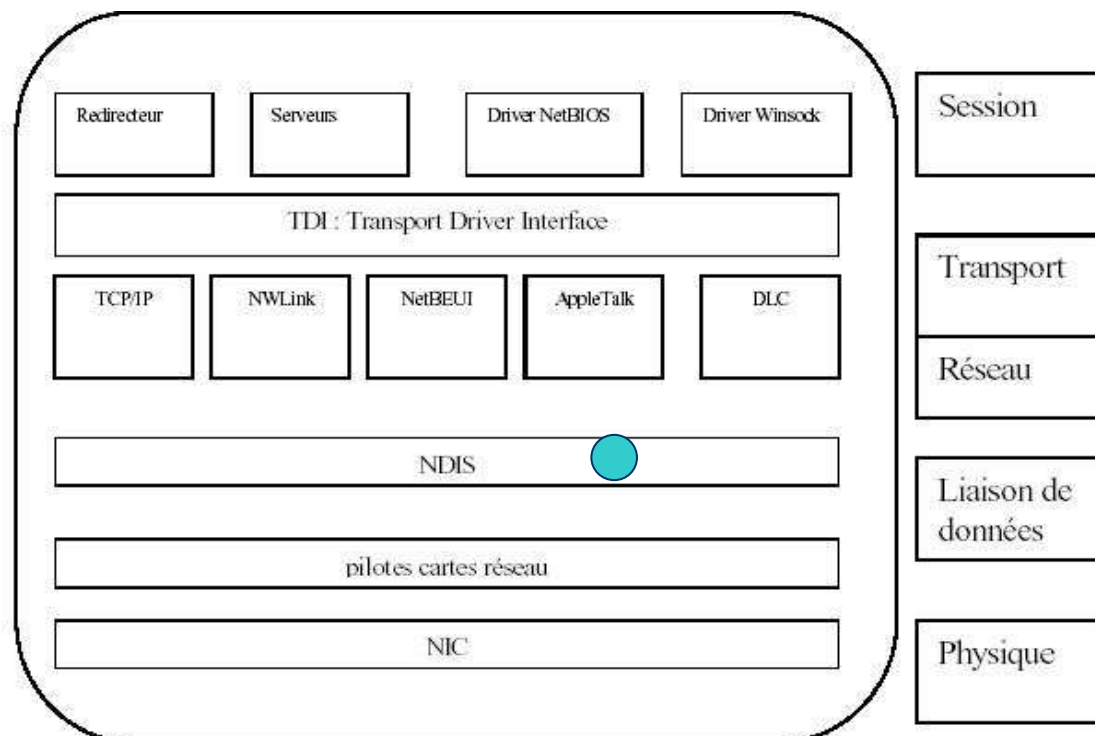
- **Les différents gestionnaire de Windows NT:**
 - **Le gestionnaire d'entrée/Sortie, gestion du réseau:**
 - **Les protocoles réseau:**
 - DLC: Data Link Control.
 - Protocole réseau utilisé pour se connecter aux imprimantes compatibles DLC (ex: anciennes imprimantes HP).

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **Les protocoles réseau:**
 - AppleTalk.
 - A la base utilisé sur les anciennes versions de Mac OS X mais désormais Mac utilise le protocole TCP/IP.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:

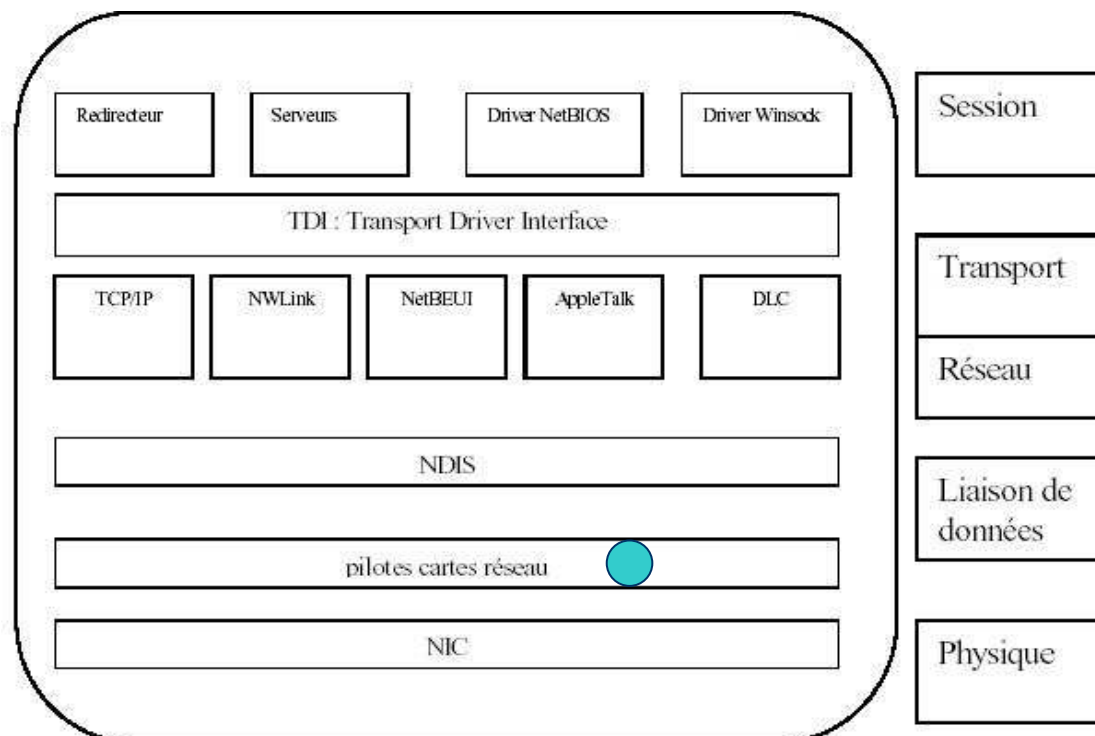


Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **La couche NDIS:**
 - NDIS supporte plusieurs piles de protocoles. Il rend les protocoles indépendants de la carte réseau. Plusieurs protocoles peuvent être liées à la même carte. Il permet aux pilotes de protocoles d'agir de manière identique sans souci du type de protocole utilisé.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:

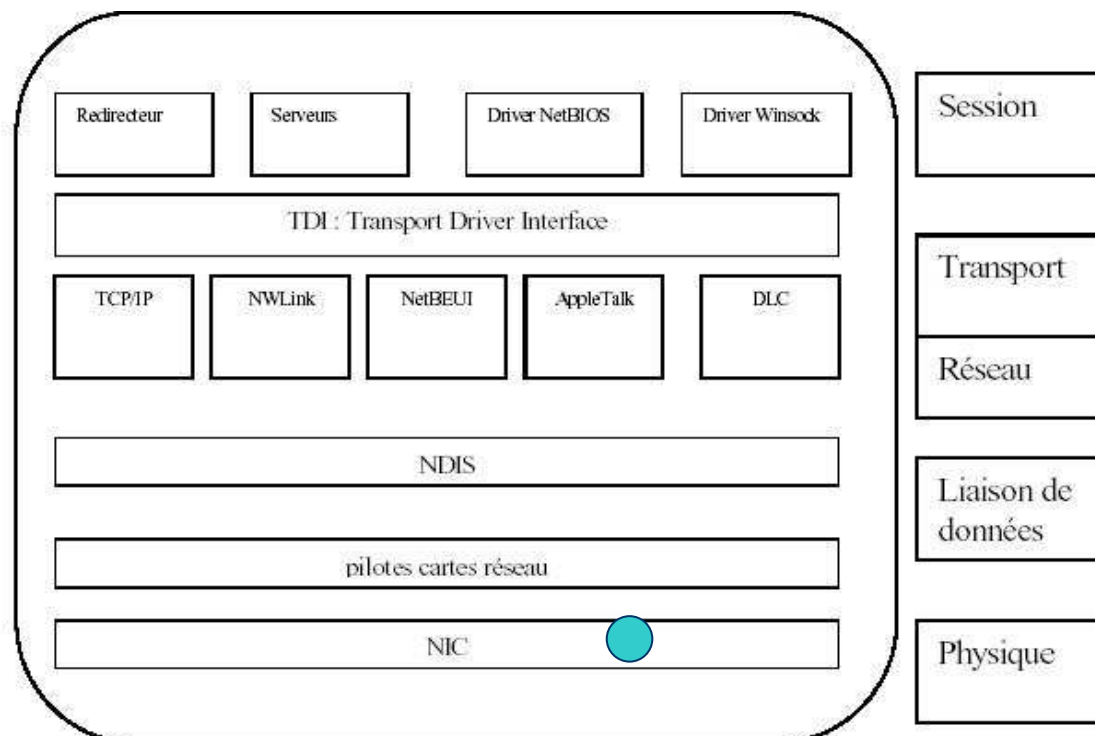


Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Le gestionnaire d'entrée/Sortie, gestion du réseau:**
 - **Les pilotes de cartes réseau:**
 - Ils permettent la communication avec le matériel.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:

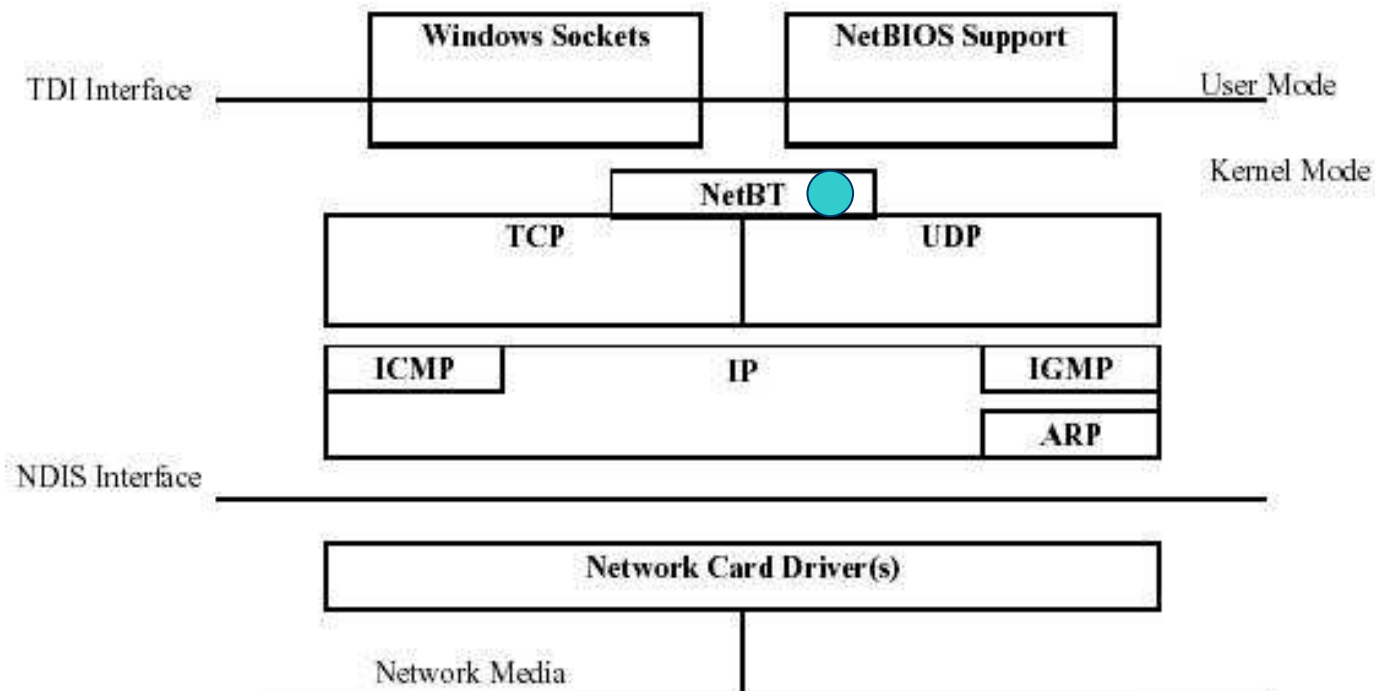


Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **NIC:**
 - C'est l'interface réseau.

Présentation générale

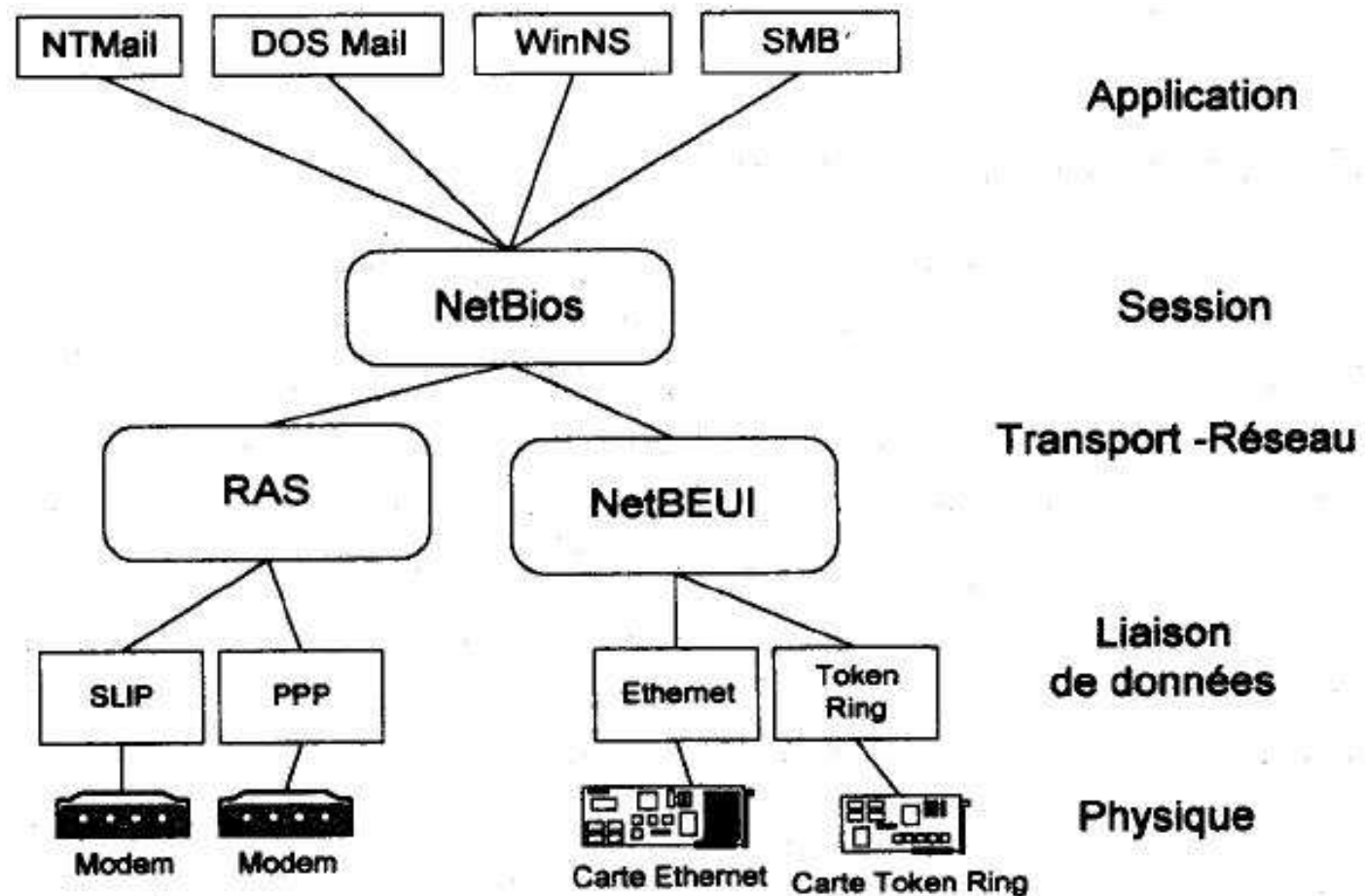
- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:



Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **NetBT: NetBIOS sur TCP/IP:**
 - Rappel sur NetBIOS.

Présentation générale



Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **NetBT: NetBIOS sur TCP/IP:**
 - Il est important de ne pas confondre les termes réseau suivant: « NetBUI », « NetBIOS » et « NetBT ». Mais ils sont tous liés.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **NetBT: NetBIOS sur TCP/IP:**
 - NetBIOS (couche application) Network Basic Input/Output System. C'est l'équivalent à HTTP.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **NetBT: NetBIOS sur TCP/IP:**
 - NetBUI (couche réseau). NetBIOS Extended User Interface. C'est l'équivalent à IP/ARP/ICMP.

Présentation générale

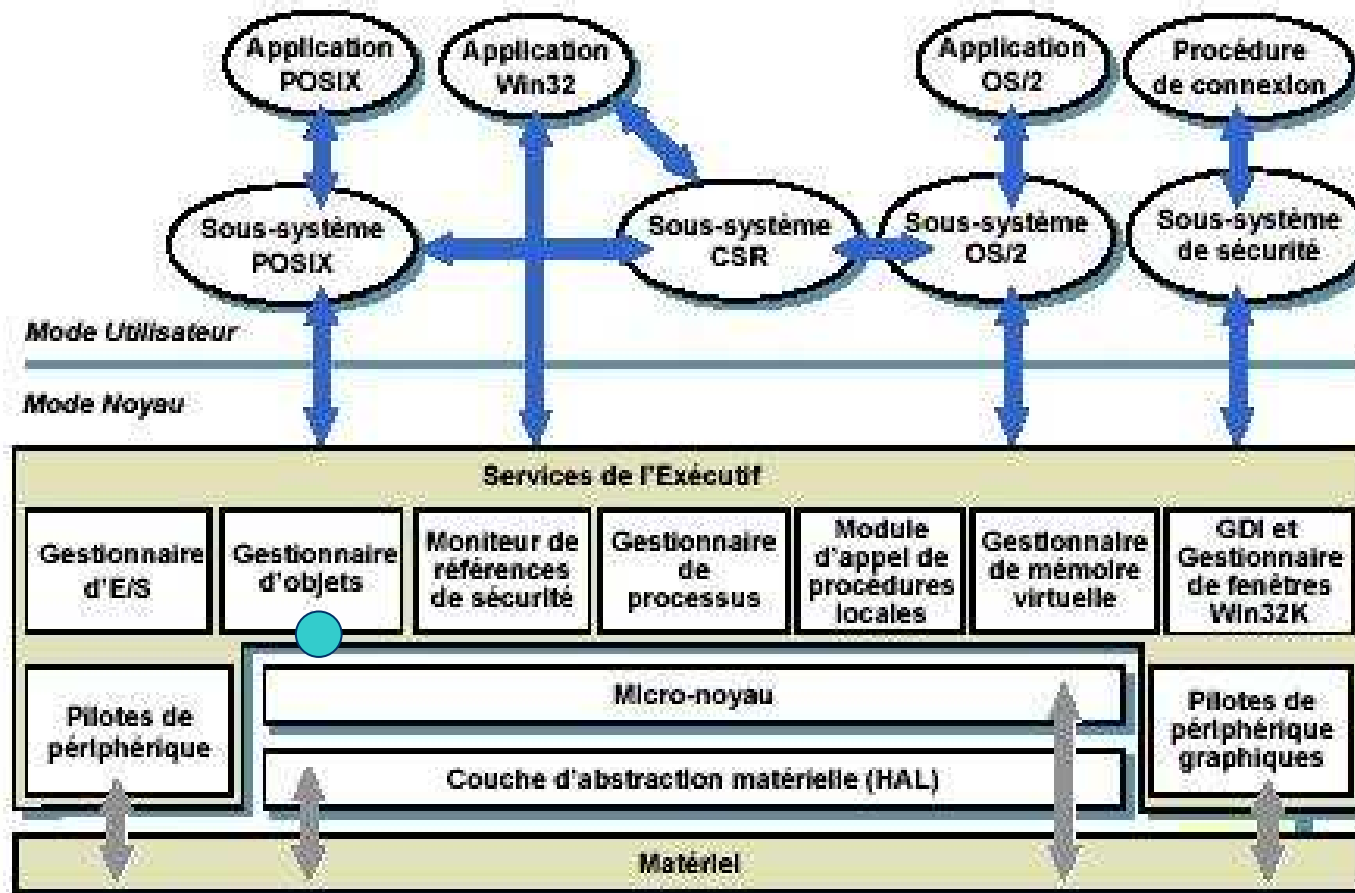
- Les différents gestionnaire de Windows NT:
 - Le gestionnaire d'entrée/Sortie, gestion du réseau:
 - **NetBT: NetBIOS sur TCP/IP:**
 - NetBT (couche transport). NetBIOS over TCP/IP. C'est l'équivalent à UDP/TCP. C'est une couche intermédiaire qui effectue les correspondance Noms NetBIOS (adresse IP). Il autorise les applications écrites avec l'API NetBIOS, à s'exécuter au dessus des couches TCP/IP (exemple: commande Net).

Présentation générale

Les applications NetBIOS (partage de fichiers par exemple) utilisent l'API NetBIOS (via NetBios.dll) puis NetBT.

Application	Applications NetBIOS (voisinage réseau, explorer,...) Interface NetBIOS (netbios.dll)	
Transport		NetBIOS sur TCP/IP (NetBT)
Réseau	NetBEUI	TCP/IP
Matériel	NDIS	

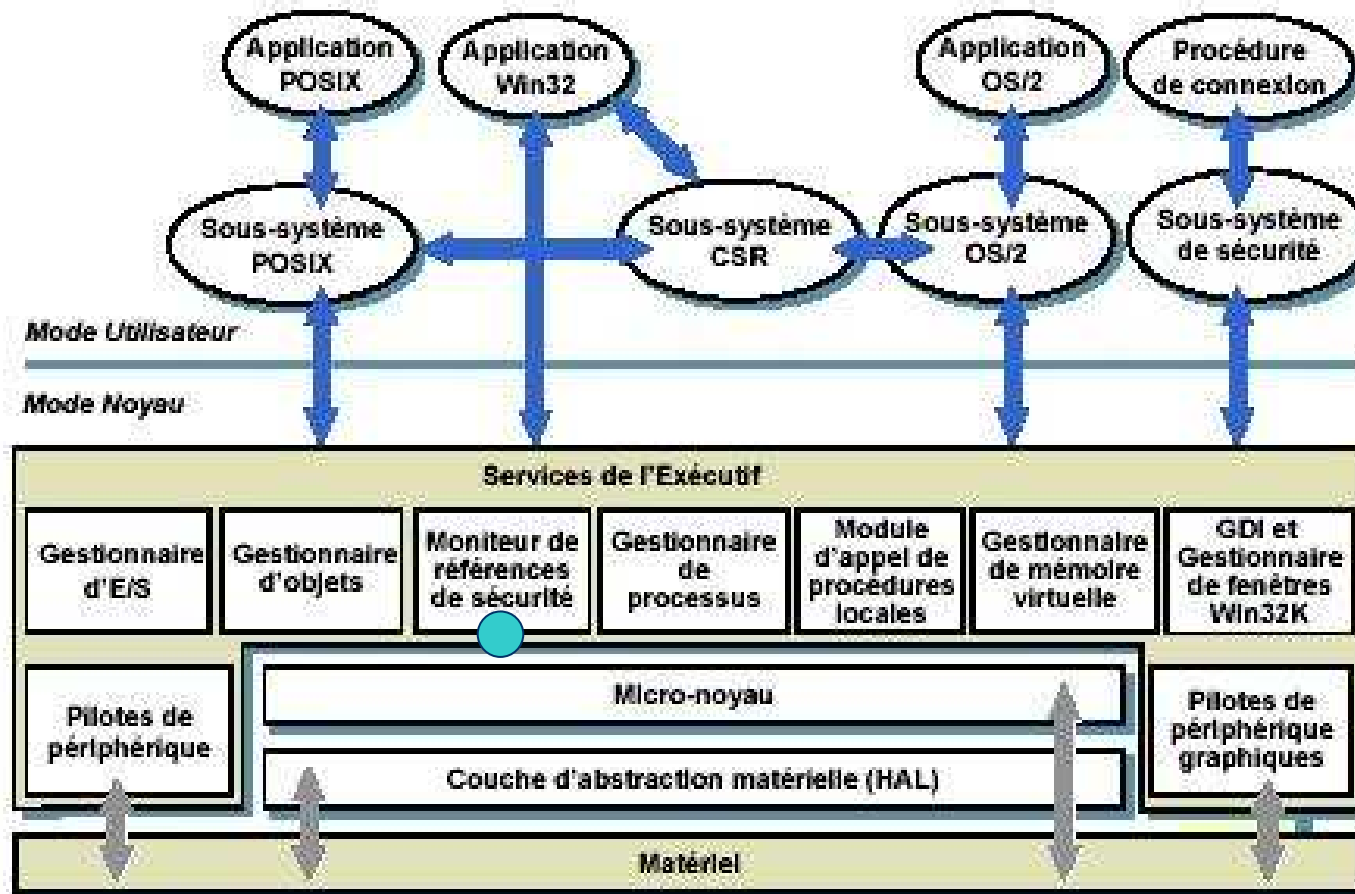
Présentation générale



Présentation générale

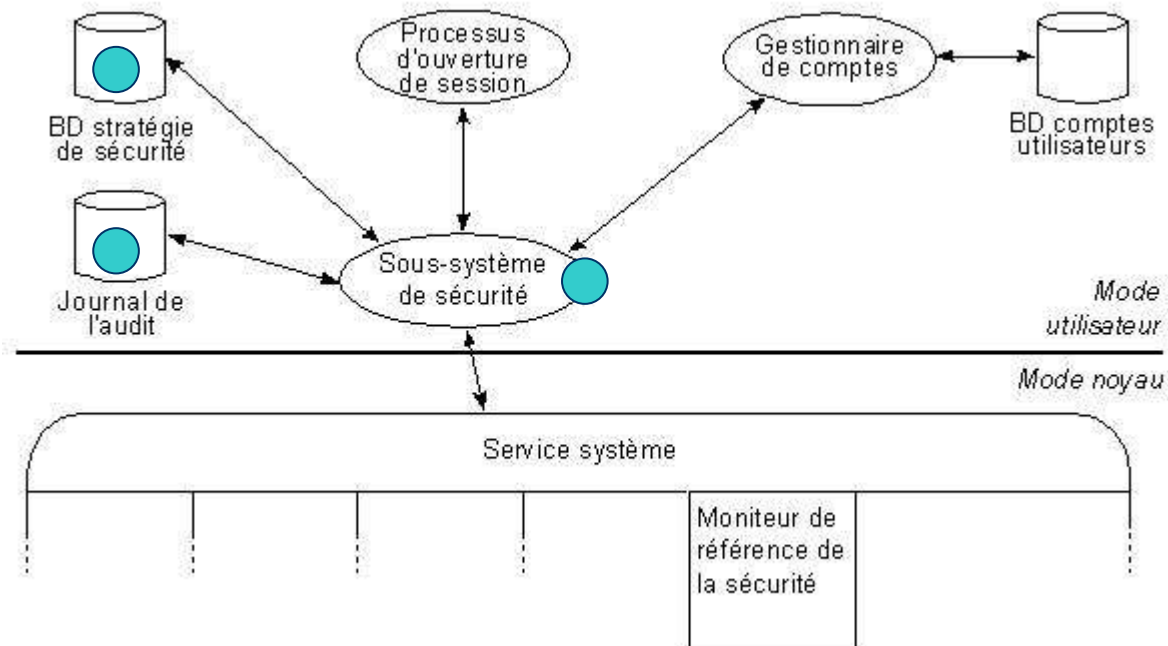
- Les différents gestionnaire de Windows NT:
 - Les gestionnaires d'objets.
 - Permet aux sous-systèmes d'accéder aux ressources sous forme d'objets.
 - Ils gèrent de façon centralisée les processus, les threads, les fichiers, les ports.
 - Les accès aux objets sont régis par des listes d'autorisation (ACL: Access Control List).

Présentation générale



Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les moniteurs de références de sécurité:

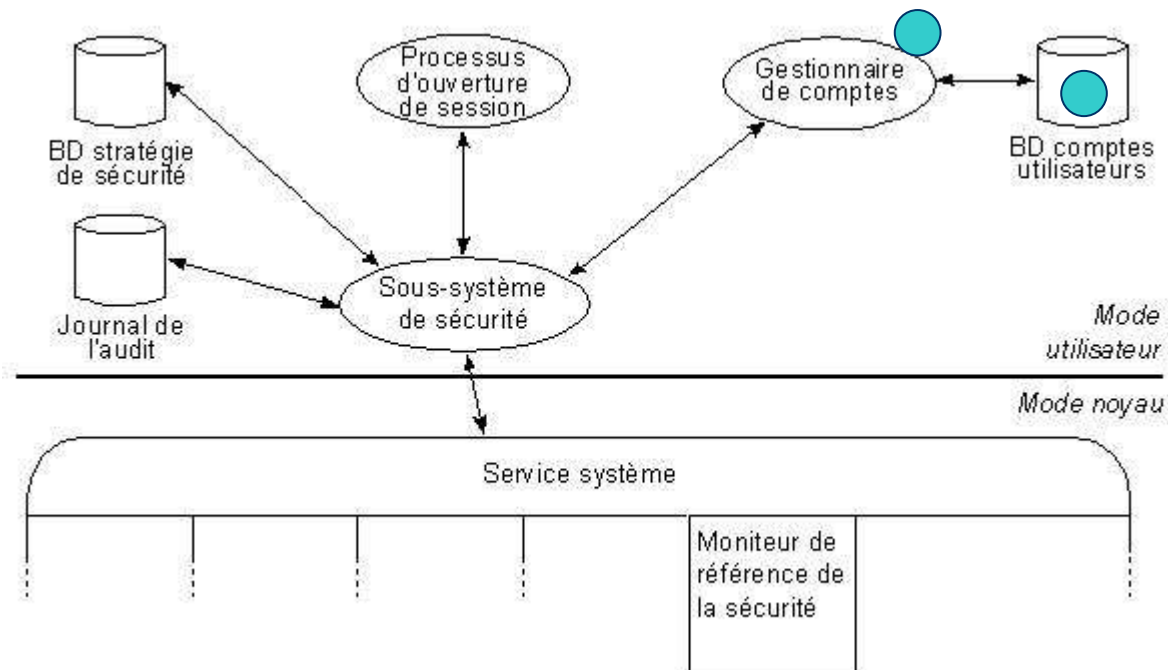


Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les moniteurs de références de sécurité:
 - Sous-système de sécurité ou LSA (Local Security Authority).
 - Composant principal des modules relatifs à la sécurité. Son rôle est triple.
 - Gère et applique la stratégie de sécurité locale.
 - Gère et applique la stratégie d'audit.
 - Service interactif de validation des utilisateurs.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les moniteurs de références de sécurité:

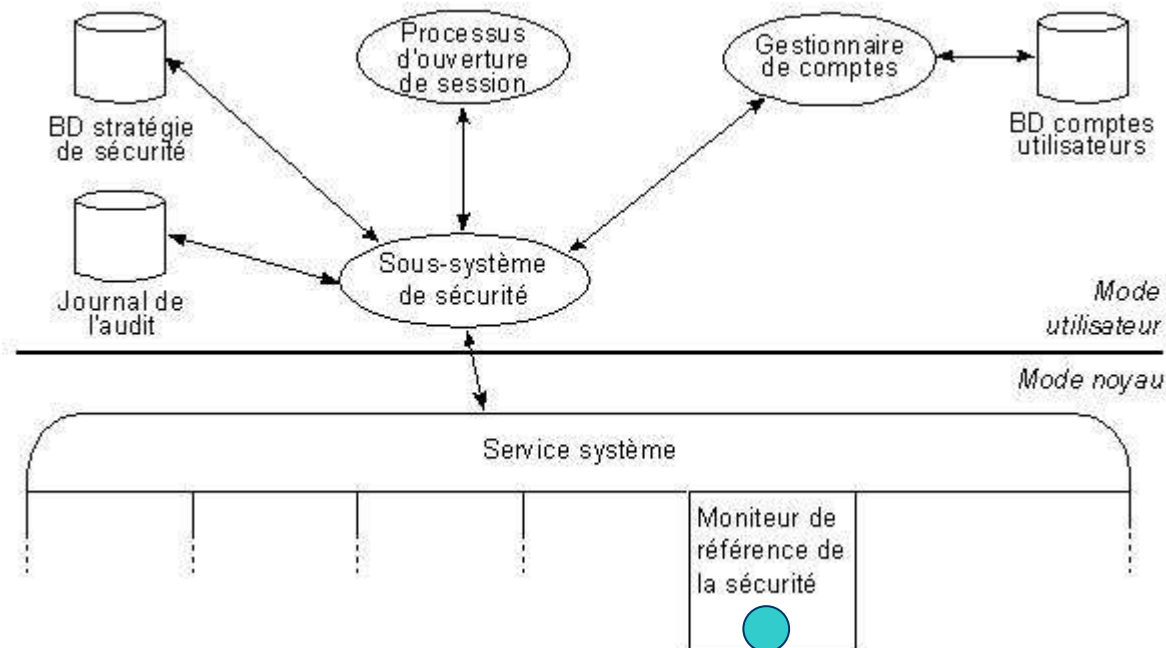


Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Les moniteurs de références de sécurité:**
 - Le gestionnaire de comptes SAM (Security Account Manager).
 - Gère la base de données des comptes utilisateurs, qui reprend l'ensemble des groupes et utilisateurs du système.
 - Offre au sous-système de sécurité un service d'authentification d'un utilisateur.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les moniteurs de références de sécurité:



Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les moniteurs de références de sécurité:
 - Le moniteur de référence de la sécurité est le seul module de sécurité qui s'exécute en mode noyau.
 - Il vérifie que les processus utilisateurs ont le droit d'accéder aux objets auxquels ils tentent d'accéder.
 - Généré les messages d'audit utilisés par les sous-système de sécurité.

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Les moniteurs de références de sécurité:**
 - Lors d'une ouverture de session l'utilisateur se logue en entrant son nom et son mot de passe.
 - Le processus d'ouverture de session se crée et envoie les informations reçues au gestionnaire des comptes de sécurité (BD SAM). Qui les compare avec les comptes utilisateurs enregistrés dans la base de données SAM.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les moniteurs de références de sécurité:
 - Lorsque l'accès est autorisé, l'autorité de sécurité locale (LSA) crée un jeton d'accès de sécurité pour cet utilisateur durant le processus d'ouverture de session.
 - Jeton d'accès est passé au sous-système Win32.
 - Win32 génère un nouveau processus associé au jeton d'accès.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les moniteurs de références de sécurité:
 - Tout au long de la connexion de l'utilisateur le moniteur de référence de sécurité (SRM) renforce la validation d'accès aux objets (fichiers, reps) en testant les comptes utilisateurs par rapport aux permissions qui leur sont accordées.

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Les moniteurs de références de sécurité:**
 - **La sécurité de NT est basée sur 4 possibilités offertes aux utilisateurs:**
 - Les aptitudes:
Les utilisateurs les obtiennent lorsqu'ils sont attribués à des groupes prédéfinis.

Présentation générale

- **Les différents gestionnaire de Windows NT:**

→ **Les moniteurs de références de sécurité:**

- **La sécurité de NT est basée sur 4 possibilités offertes aux utilisateurs:**

- Les droits:

Ils s'appliquent au système dans sa totalité.

Exemple: Un opérateur de sauvegarde a le droit de sauvegarder tous les fichiers sur le réseau même s'il n'est pas autorisé à lire. Cette possibilité est donnée à l'opérateur en assignant le droit de sauvegarder des fichiers et les répertoires.

Présentation générale

- Les différents gestionnaire de Windows NT:

→ Les moniteurs de références de sécurité:

- **La sécurité de NT est basée sur 4 possibilités offertes aux utilisateurs:**

- Les Permissions:

Elles s'appliquent à des objets spécifiques tels que les fichiers, les répertoires et les imprimantes.

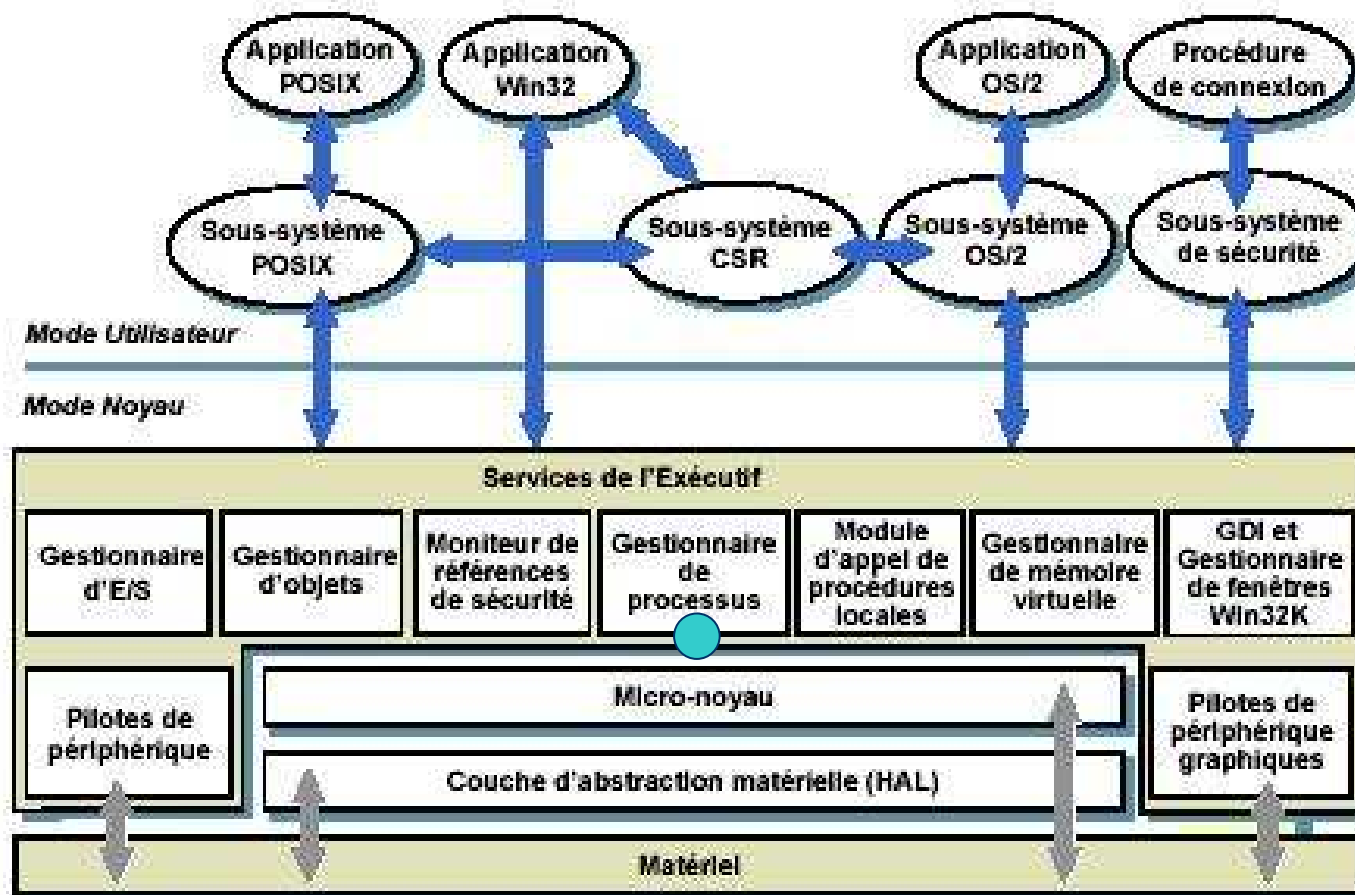
Exemple: On donne à un utilisateur la permission de lire un fichier, d'accéder à un répertoire,...

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Les moniteurs de références de sécurité:**
 - **La sécurité de NT est basée sur 4 possibilités offertes aux utilisateurs:**
 - Les Partages:

On partage un ensemble de fichiers et répertoires sur les réseaux en leur attribuant des permissions pour leur sécurité.

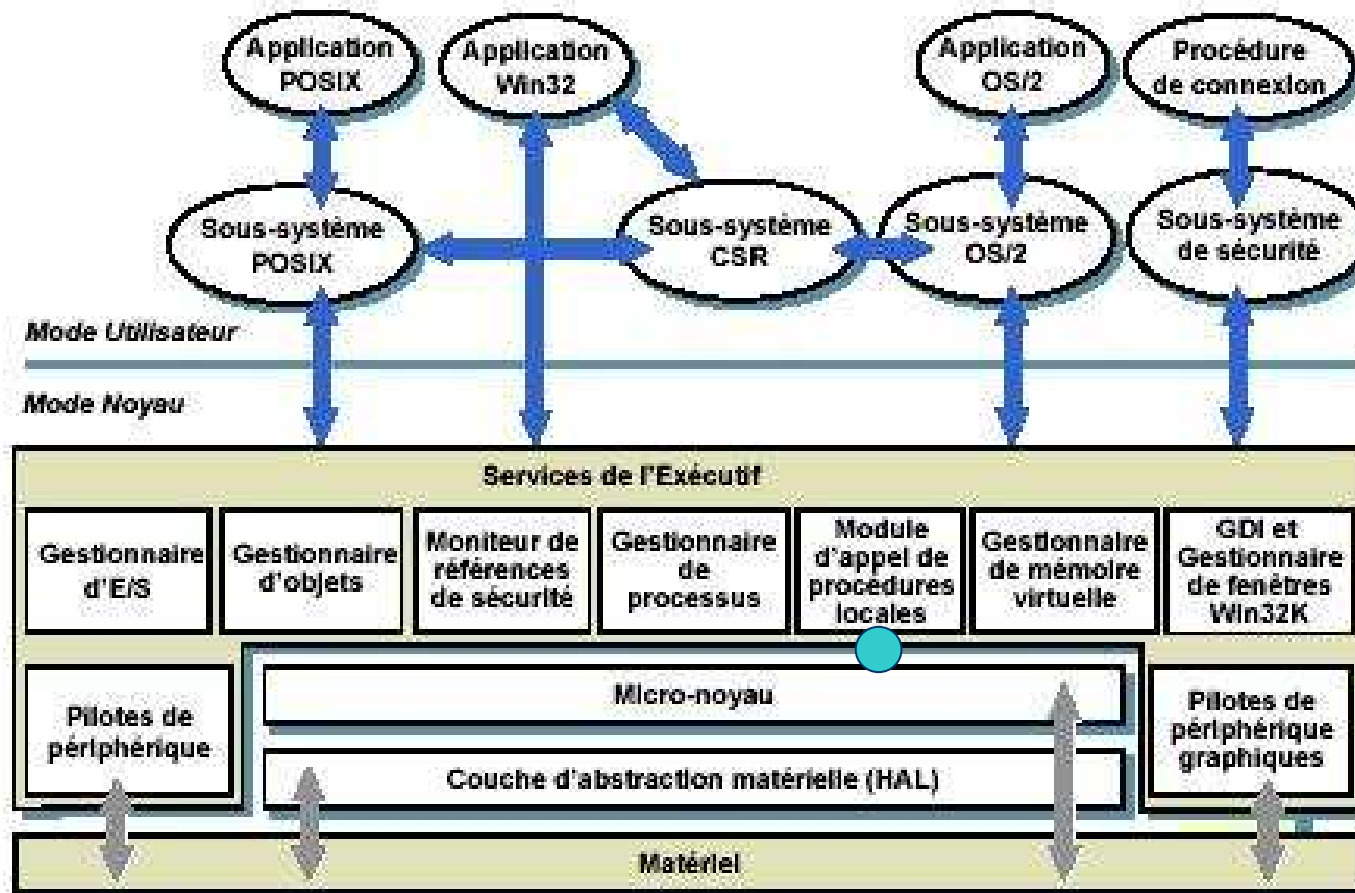
Présentation générale



Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le Gestionnaire de processus:
 - Le gestionnaire de processus est chargé de gérer la création et la suppression de processus.
 - Les processus sont définis par un ensemble de threads + un espace d'adressage (Conf cours notions fondamentales des OS).
 - A chaque processus est associé un jeton d'accès qui lui permet d'accéder aux objets protégés de Windows NT.

Présentation générale



Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Le Gestionnaire d'appels de Procédures Locales:**
 - Il permet la communication entre les applications et les sous systèmes d'environnement via msg.
 - Le processus de communication est caché aux applications grâce à des relais (entités non exécutables utilisés par les appels). Ces relais sont disponibles sous forme de bibliothèques de liaison dynamique.

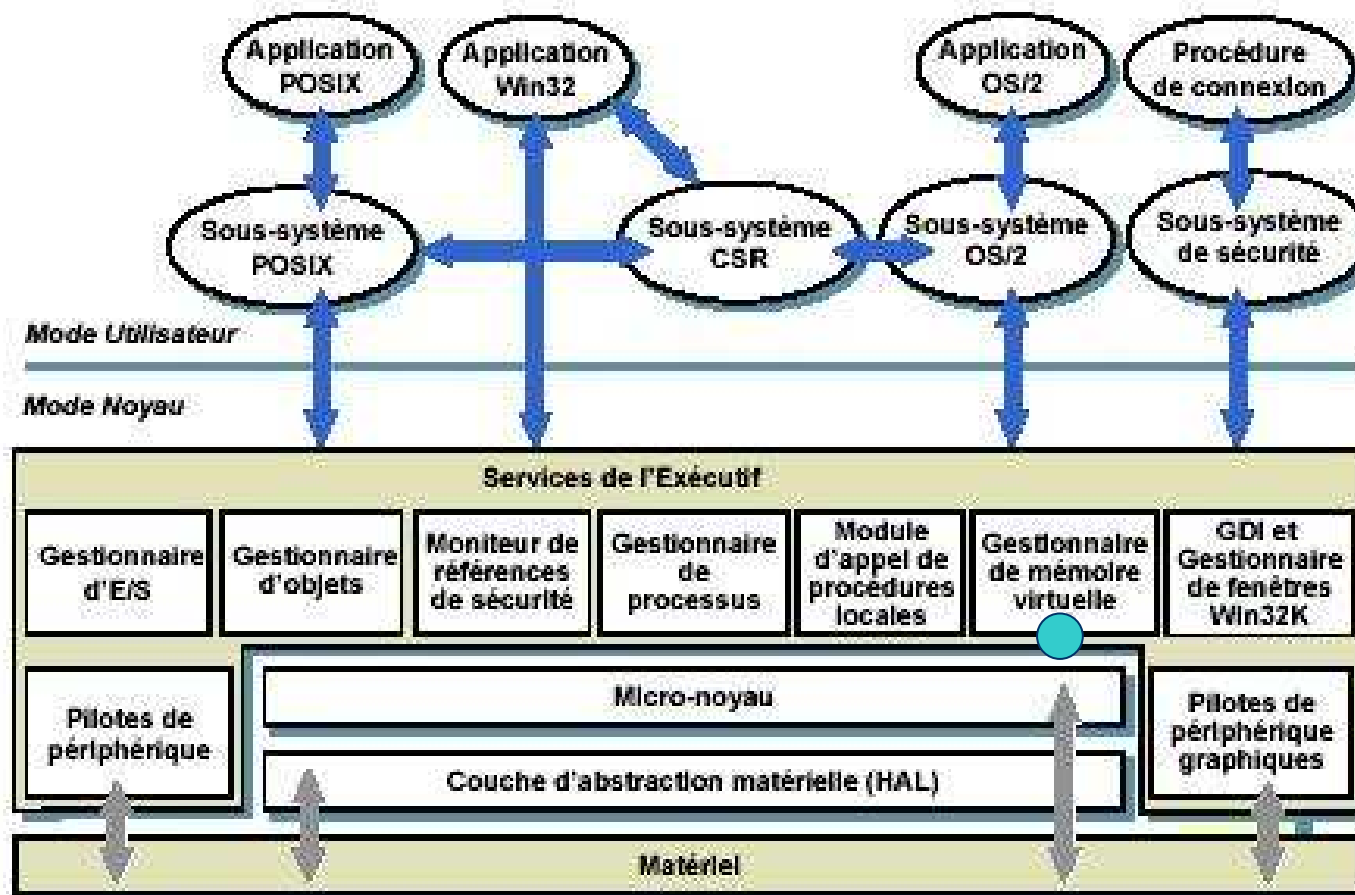
Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le Gestionnaire d'appels de Procédures Locales:
 - Fonctionnement:
 - Une application effectue un appel API vers un sous-système d'environnement.
 - Le relais dans le processus client (application) récupère les paramètres pour cet appel et construit un message contenant toutes les données nécessaires.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le Gestionnaire d'appels de Procédures Locales:
 - Fonctionnement:
 - LPC transmet le message du relais au processus serveur (sous-système) qui implémente l'appel.
 - Le sous-système exécute la fonction associée et envoie le résultat dans un message au relais.
 - Le relais analyse alors le message du serveur et retourne le résultat à l'application.

Présentation générale



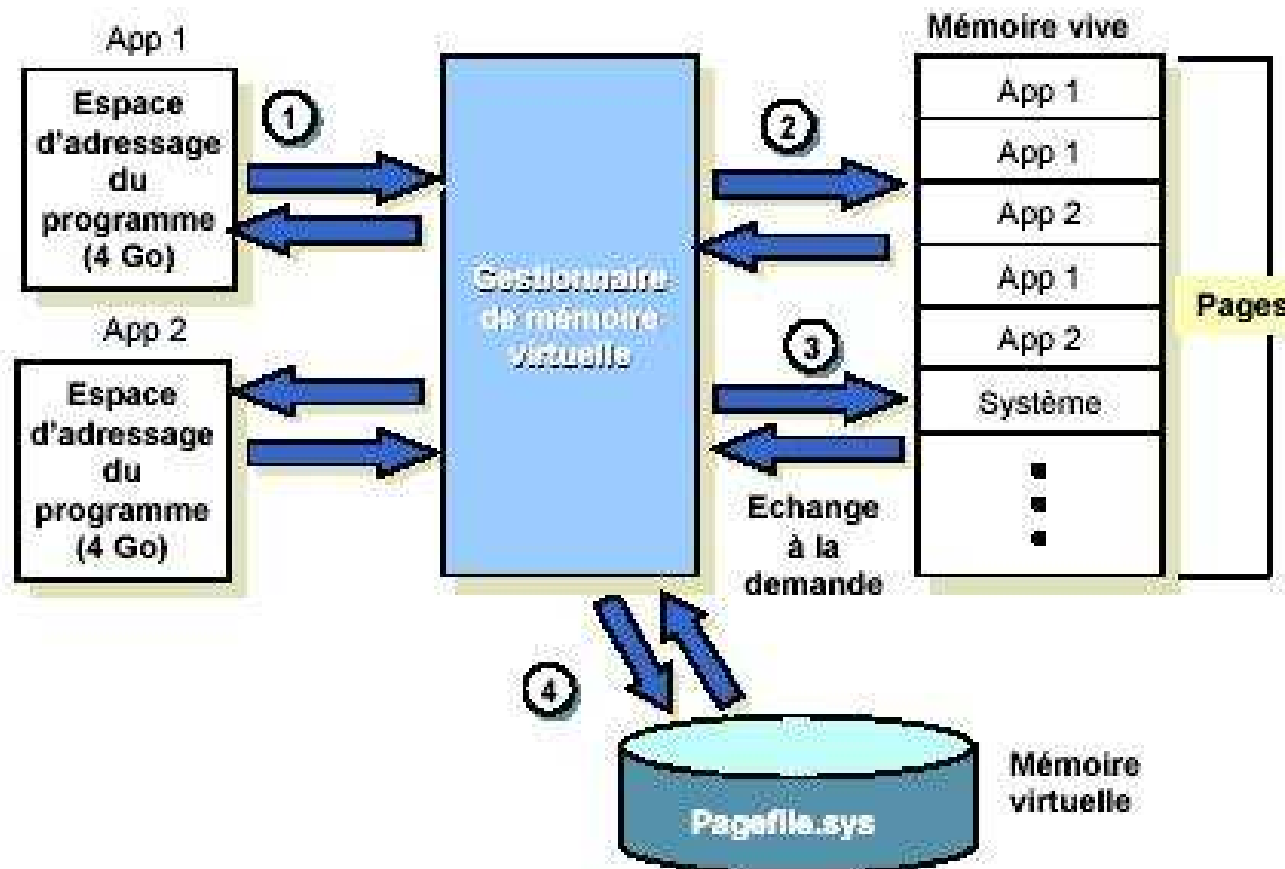
Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le Gestionnaire de mémoire virtuelle:
 - Architecture mémoire de Windows NT est basée sur un système de mémoire virtuelle paginée.
 - La notion de mémoire virtuelle permet au système d'exploitation d'allouer réellement plus de mémoire que l'ordinateur n'en dispose physiquement.

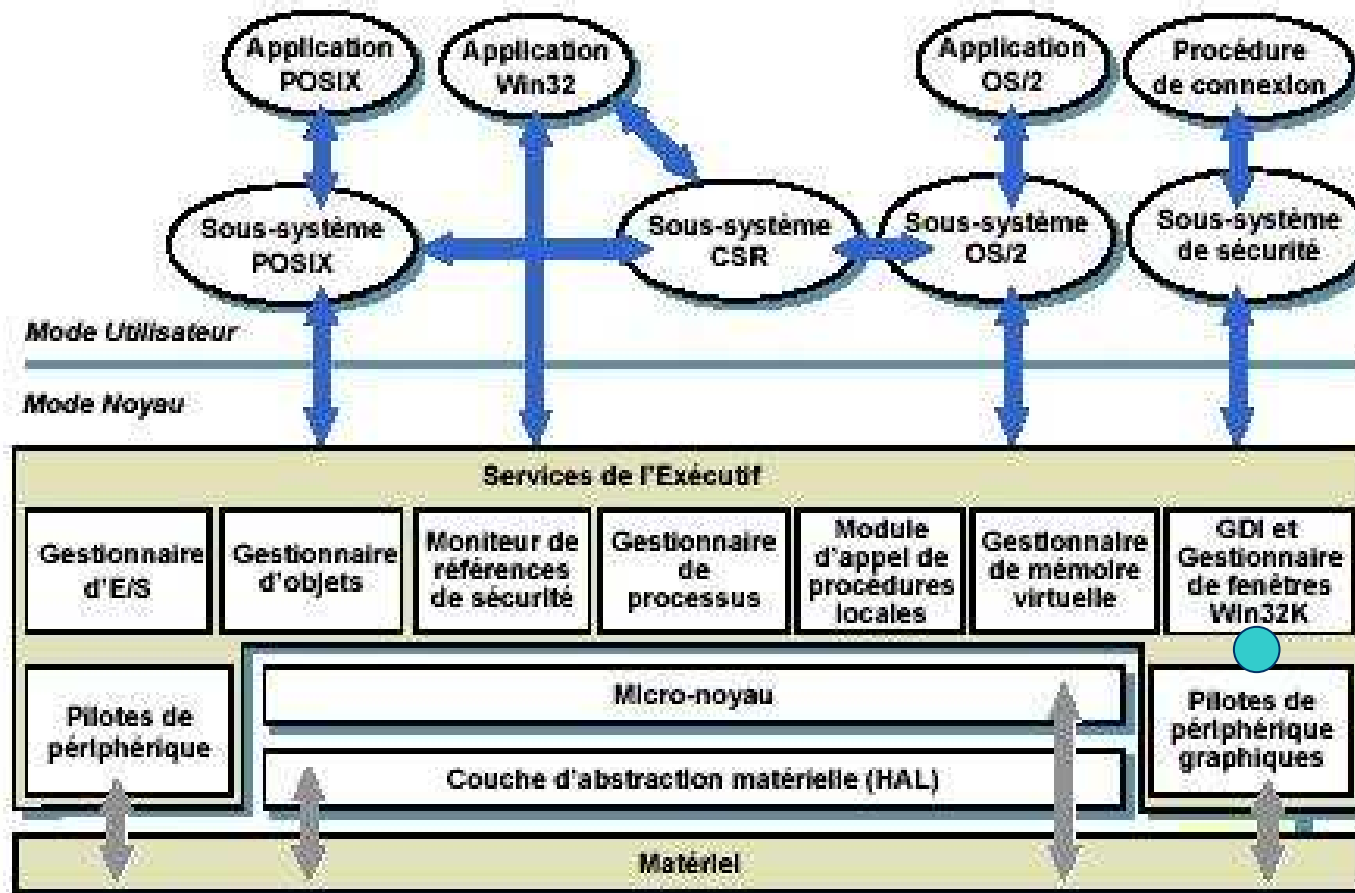
Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le Gestionnaire de mémoire virtuelle:
 - A chaque processus, le gestionnaire alloue un espace adressable virtuel. Cet espace est divisé en blocs de taille identique appelés pages.
 - Lorsqu'un processus à besoin de ces données, le gestionnaire de mémoire virtuelle traduit les adresses virtuelles dans l'espace adressable du processus en pages physique dans la mémoire de l'ordinateur.

Présentation générale



Présentation générale



Présentation générale

- Les différents gestionnaire de Windows NT:
 - Le Gestionnaire de fenêtre Win32 + GDI:
 - Gestionnaire de fenêtres Win32 sous Windows NTx correspond au User space de Win9x.
 - L'User gère les saisies au clavier, et la souris, les périphériques d'entrés et produit les sorties dans l'interface utilisateur.
 - Le GDI est le système graphique qui gère ce qui s'affiche à l'écran. Il fournit aussi la prise en charge des graphique pour les imprimantes.

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Les fichiers « Noyau » de Windows NTx:**
 - NtosKrnI.exe: Correspond au Kermel dans le sens de Windows c'est-à-dire l'ordonnancement, les interruptions et les SMP.
 - Ntkrnlmp.exe, ntkrnlpa.exe, ntkrnpamp.exe
 - Hal.dll: c'est la virtualisation du matériel.
 - Win32K.sys: fait partie du sous-système Win32 et est exécuté en mode Kermel.
 - Ntdll.dll: permet la normalisation des interfaces logicielles, interface user/Kermel mode.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les fichiers « Noyau » de Windows NTx:
 - Kernel32.dll, advapi32.dll, user32.dll et gdi32.dll sont les principales dll du sous-système Win32.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les séquences de Boot de Windows NT:
 - **1er étape:** Le post
 - **2ème étape:** Sélection de l'OS (Ntldr (NT Loader)).
Il fait passer le processeur du mode réel au mode mémoire linéaire 32 bits. Il démarre les pilotes de systèmes de fichiers approprié (FAT et NTFS) pour lire sur les disques durs. Ensuite il lit Boot.ini et affiche les sélections et charge l'OS sélectionné.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les séquences de Boot de Windows NT:
 - Si NT est sélectionné, Ntldr charge Ntdetect.com (sinon Bootsect.dos). Ntldr charge Ntoskrln.exe, Hal.dll et la ruche « system ».
 - Ntdetect.com détecte les périphériques matériels insatllés.
 - NTLDR à été lancé lorsque vous voyez à l'écran « Démarrage de Windows » suivi d'un barre de progression.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les séquences de Boot de Windows NT:
 - Après la détection de Ntdetect.com, NTDLR va charger ntoskrnl et lui fournir les informations collectées.

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - Les séquences de Boot de Windows NT:
 - 3ème étape: Chargement du noyau (le Kermel)
 - Chargement de ntoskrnl.exe et du fichier hall.dll.
 - NTLDR va lire la ruche SYSTEM du registre et sélectionnera la configuration matérielle. Sélection d'un profil matériel à ce niveau. NTLDR va aussi charger tous les pilotes de périphériques qui possèdent une valeur de démarrage (dans le Registre : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services) de 0x0

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les séquences de Boot de Windows NT:
 - 4ème étape: initialisation du noyau
 - NTLDR va créer une ruche HARDWARE dans le registre en utilisant les informations collectées précédemment par ntdetect.com. Ntoskrnl.exe va ensuite initialiser les pilotes de périphériques chargés précédemment, puis va scruter le registre pour les pilotes de périphériques qui ont une valeur de chargement de 0x1.

Présentation générale

- **Les différents gestionnaire de Windows NT:**
 - **Les séquences de Boot de Windows NT:**
 - **5ème étape:** Chargement des services
 - Chargement du processus Session Manager (smss.exe)
 - Smss.exe lance les programmes présents dans l'entrée BootExecute du registre ainsi que les sous-systèmes requis : Win32 par exemple !!

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les séquences de Boot de Windows NT:
 - Le sous-système Win32 va ensuite charger Winlogon.exe qui va lancer la LSA : Local Security Administration (Lsass.exe)
 - La fenêtre Winlogon sera alors visible. Le contrôleur de services (screg.exe) va ensuite scruter le registre à la recherche de services qui ont une valeur de démarrage de 0x2 et va les charger.

Présentation générale

- Les différents gestionnaire de Windows NT:
 - Les séquences de Boot de Windows NT:
 - 6ème étape: Ouverture de Session
 - Un démarrage n'est considéré comme ayant réussi tant que l'utilisateur n'a pas ouvert une session.
 - Traitement du répertoire « Démarrage » du profil utilisateur ou du profil All Users.

Présentation générale

- **Administration et Astuces sous Windows NTx:**

- **Les outils d'administration de Windows NT:**

- APR: Mappage d'adresse IP / Adresse MAC.
- AT: Planification d'exécution de commandes.
- CACLS: Gestion des ACL.
- COMPACT: Compression de FS NTFS.
- IPCONFIG: Gestion paramètres réseaux.
- NBSTAT, NETSTAT: on la déjà vu ça.
- NTBACKUP: Sauvegarde sur bandes
- NTHQ: Vérification Hardware.

Présentation générale

- RDISK: Création d'une disquette de réparation.
- REGEDT32: Editeur de la base de registre.
- SYSDIFF: Permet l'installation d'applications sans surveillance.
- WINDIFF: Permet de comparer des fichiers et des répertoires.
- CHKDSK: Vérification des disques.
- CONVERT: Convertir un volume en NTFS.
- FIND: Recherche de texte dans un fichiers.
- PATH: Ajoute un chemin d'exécutables

Présentation générale

- BACKUP/Restore: Sauvegarde et restauration de fichiers et répertoires en ligne de commandes.
- TREE: Arborescence d'un répertoire ou d'un volume.

→ Toutes les commandes commençant par NET:

http://perso.club-internet.fr/spinard/sys_nt_net.html

Présentation générale

- **Administration et Astuces sous Windows NTx:**

- **Les outils d'administration de Windows 2000:**

- Mêmes outils que sous NT mais en plus:
- certmgr.msc: Certificats.
- ciadv.msc: Service d'indexation
- devmgmt.msc: Gestionnaire de périphériques.
- dfrg.msc: Défragmenteur de disque.
- diskmgmt.msc: Gestionnaire des disques.
- dnsmgmt.msc: Gestionnaire de DNS.
- eventvwr.msc: Observateur d'événements.

Présentation générale

- faxserv.msc: Gestion des services de télécopie.
- fsmgmt.msc: Dossier partagés.
- gpedit.msc: stratégie de groupe (fait pleins de choses).
- ias.msc: Service d'authentification Internet.
- lusrmgr.msc: Utilisateurs et groupes locaux.
- ntmsmgr.msc: Stockage amovible.
- ntmsoprq.msc: Demande de l'opérateur de sauvegarde amovible.
- perform.msc: Analyseur de performance.
- secpol.msc: Paramètre de sécurité locale.

Présentation générale

- services.msc: Services.
- wmimgmt.msc: Infrastructure de gestion Windows (WMI).
- comexp.msc: service de composant.
- iis.msc: Service Internet.
- msinfo32.msc: Information système.
- Fpmmc.msc: Extension Serveur Frontpage2000.

→ Résumé des commandes:

www.baudelet.net/win05.htm

Sources

- www.baudelet.net
- www.commentcamarche.net
- www.supinfo.com