

Microsoft Windows 2000 :
Notions Fondamentales

Essentiel
de préparation
aux certifications

Par :
NEDJIMI Brahim
THOBOIS Loïc
TUDURY Matthieu



23, rue Château Landon
75010 – PARIS
www.supinfo.com

Table des Matières

Table des Matières.....	2
Module 1 Présentation de Windows 2000 et des concepts des réseaux.....	5
1 Systèmes d'exploitation Windows 2000	5
2 Présentation des réseaux	5
a) Types de réseaux	5
b) Système d'exploitation réseau	6
3 Implémentation de la gestion de réseau dans Windows 2000	6
a) Implémentation en Groupe de travail ou en domaine	6
b) Avantages d'un domaine	6
c) Organisation des domaines	6
d) Fonctionnalités et avantages d'Active Directory.....	7
e) Accès à un réseau Windows 2000	7
Module 2 Administration d'un réseau Windows 2000	8
1 Aide de Windows 2000	8
2 Tâches administratives.....	8
3 Outils d'administration	8
Module 3 Sécurisation d'un réseau Windows 2000.....	9
1 Comptes d'utilisateurs.....	9
a) Comptes d'utilisateurs locaux.....	9
b) Comptes d'utilisateurs de domaine.....	9
c) Groupes.....	9
2 Droits d'utilisateurs	10
a) Droits d'utilisateurs courants	10
b) Droits accordés aux groupes prédéfinis.....	10
3 Autorisations	10
a) Autorisations sur les fichiers NTFS	10
b) Autorisations sur les dossiers NTFS.....	11
c) Autorisations sur les dossiers partagés	11
d) Autorisations sur les imprimantes	11
Module 4 Examen d'un réseau	12
1 Les cartes Réseaux.....	12
2 Les Câbles Réseaux.....	12
a) Les câbles à paires torsadées	12
b) Le câble coaxial.....	12
c) La fibre optique	12
3 Communications sans fil	12
a) Transmission infrarouge	12
b) Transmission radio à bande étroite.....	12
4 Topologies des réseaux	12
a) Topologie en bus	13
b) Topologie en étoile.....	13
c) Topologie en anneau.....	13
d) Topologie maillée.....	13
e) Topologie hybride.....	13
5 Technologies réseaux	13
a) Ethernet.....	13
b) Token Ring.....	13
c) ATM	14

d) FDDI.....	14
e) Relais de trame	14
6 Extension d'un réseau	14
a) Répéteurs et concentrateurs (Hubs)	14
b) Ponts	14
c) Commutateurs (Switches).....	14
d) Routeurs	14
e) Passerelles.....	14
f) Accès Distant	14
g) RTC	15
h) Réseau RNIS	15
i) Réseau X.25	15
j) Technologie ADSL	15
Module 5 Examen des protocoles réseau	16
1 Présentation des protocoles.....	16
a) Modèle de référence OSI	16
b) Types de protocoles.....	16
2 Protocoles et transmissions de données.....	16
a) Protocoles prenant en charge ou non le routage	16
b) Types de transmission de données.....	16
3 Protocoles couramment utilisés	16
a) Protocole TCP/IP	17
b) Protocole IPX/SPX.....	17
c) Protocole NetBEUI.....	17
d) Protocole AppleTalk.....	17
4 Autres Protocoles de communication.....	17
a) Protocole ATM.....	17
b) Protocole IrDA	17
5 Protocoles d'accès distant	17
a) Protocoles d'accès à distance.....	17
b) Protocoles VPN	17
Module 6 Examen du protocole TCP/IP	19
1 Présentation du protocole TCP/IP	19
a) Couches TCP/IP	19
b) Identification des applications	19
2 Suite de protocoles TCP/IP	19
a) Protocole TCP.....	19
b) Protocole UDP.....	19
c) Protocole IP	19
d) Protocole ICMP	20
e) Protocole IGMP	20
f) Protocole ARP.....	20
g) Utilitaires TCP/IP	20
3 Résolution de noms	20
a) Types de noms	21
b) Mappage IP statique	21
c) Mappage IP dynamique	21
d) Résolution des noms dans Windows 2000	21
4 Examen du processus de transfert de données.....	21
a) Terminologie relative aux paquets.....	22
b) Flux de données.....	22
5 Routage de données	22
a) Routage IP	22

Module 7 Examen de l'adressage IP.....	23
1 Adressage IP par classes.....	23
2 Création de sous-réseaux.....	23
3 Planification d'adressage IP.....	24
Principales règles d'adressage	24
4 Affectation d'adresses IP.....	24
a) Adressage IP Statique	24
b) Adressage IP automatique	24
c) Utilisation d'ipconfig.....	24
Module 8 Optimisation de l'allocation d'adresses IP.....	25
1 Routage CIDR.....	25
a) Restrictions imposées par l'adressage IP par classes.....	25
b) Définition du routage CIDR	25
c) Masques de sous-réseau binaire.....	25
d) Notation CIDR	25
e) Calcul d'identificateur de réseau	25
f) Identifications d'hôtes locaux et distants	25
2 Allocations d'adresses IP à l'aide du routage CIDR.....	26
a) Identificateurs d'hôtes disponibles	26
b) Optimisation de l'allocation d'adresses IP	26
Module 9 Examen des services web	27
1 Identification des concepts d'Internet.....	27
a) Internet.....	27
b) Services Internet	27
c) Réseaux Intranets.....	27
d) Dénomination de domaine	27
2 Utilisation des technologies clientes.....	27
a) Client Mails	27
b) Navigateurs.....	28
c) Lecteurs de news	28
d) Client FTP	28
3 URL.....	28
4 Connexion à Internet	28
a) Traducteurs NAT	28
b) Serveurs proxy.....	28
c) Pare-feu (Firewall).....	29
5 Identification des concepts des serveurs Web	29
a) Définition d'un serveur Web	29
b) Services IIS.....	29

Module 1

Présentation de Windows 2000 et des concepts des réseaux

Définition d'un système d'exploitation

Un système d'exploitation (O.S.) est un ensemble de programmes de gestion du système qui permet de gérer les quatre éléments fondamentaux de l'ordinateur :

- Le matériel
- Les logiciels
- La mémoire
- Les données

Définition d'un réseau

Un réseau est une structure permettant à plusieurs entités d'échanger des informations. L'ensemble ordinateurs – serveurs - imprimantes dans une entreprise est un réseau (Internet est un réseau gigantesque rassemblant des centaines de milliers de machines).

1 Systèmes d'exploitation Windows 2000

L'offre Windows 2000 constitue une gamme complète de serveurs et de postes de travail permettant de répondre à tous les besoins d'une structure réseau efficace. Les systèmes d'exploitation Windows 2000 intègrent un certain nombre de fonctions avancées comme :

- Le Multitâche
- La gestion avancée de la mémoire (mémoire protégée, mémoire virtuelle, ...)
- La gestion des machines multiprocesseurs (SMP)
- Le Plug & Play
- La mise en clusters (regroupement de plusieurs ordinateurs pour une même tâche)
- La gestion avancée des fichiers (NTFS)
- La Qualité de service réseau (QoS)
- Les Services Terminal Server (Déportation de l'affichage sur un poste distant)
- Les Services d'installation à distance (Outils de déploiement avancés)

La famille Windows 2000 se compose de 4 versions :

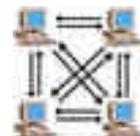
- Windows 2000 Professionnel (Poste de travail)
- Windows 2000 Server (Serveur)
- Windows 2000 Advanced Server (Serveur + Mise en Cluster)
- Windows 2000 Datacenter Server (Data Warehouse)

2 Présentation des réseaux

L'avantage d'un réseau est de pouvoir offrir un accès généralisé aux ressources de l'entreprise. Ainsi un certain nombre de tâches vont pouvoir être déléguées à des machines dédiés (serveurs) sur le réseau (ex : Bases de données, Messagerie, Télécopie, Fichiers, Impression, ...) auxquelles tous les utilisateurs auront accès.

a) Types de réseaux

Egal à égal : Aucune centralisation des ressources, les machines sont autonomes et chaque utilisateurs choisit les ressources qu'il veut mettre à disposition sur le réseau. Ce mode de fonctionnement est aussi appelé Groupe de Travail.



Client-serveur : Un certain nombre de machines sont désignées comme serveurs et centralisent les ressources communes du réseau.



b) Système d'exploitation réseau

Afin de pouvoir exister, un réseau doit être composé de machines fonctionnant avec des systèmes d'exploitation réseau. Ainsi les applications peuvent appeler les fonctionnalités nécessaires pour pouvoir communiquer sur le réseau.

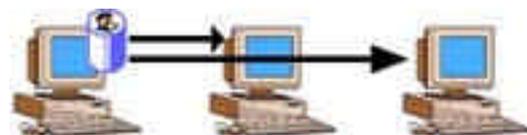
3 Implémentation de la gestion de réseau dans Windows 2000

a) Implémentation en Groupe de travail ou en domaine

Groupe de travail : Les informations de Comptes d'utilisateurs sont stockées localement sur les machines hébergeant les ressources réseau. Si une modification doit être apportée à un compte, celle-ci devra être répercutée manuellement sur toutes les machines où le compte existe.



Domaine : Les informations de comptes sont centralisées sur un serveur, dans l'annuaire des objets du réseau. Si une modification doit être apportée à un compte, elle doit être effectuée uniquement sur le serveur qui la diffusera à l'ensemble du domaine.



b) Avantages d'un domaine

L'administration des Comptes d'utilisateurs du domaine étant centralisée en un point unique, il est possible d'organiser ces derniers de façon à obtenir une représentation structurée de l'entreprise et donc de mieux maîtriser la sécurité sur le réseau.

L'organisation hiérarchique des objets de l'annuaire permet une délégation facilitée des pouvoirs administratifs sur une partie des objets du réseau.

Les recherches d'objets dans le domaine (utilisateurs, ressources telles les imprimantes ou les partages de fichiers, ...) s'appliquent sur l'ensemble du réseau de l'entreprise, les rendants plus efficaces.

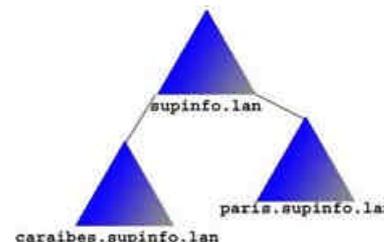
c) Organisation des domaines

Chaque **domaine** est géré par un ou plusieurs **contrôleurs de domaine**. Un contrôleur de domaine doit être un serveur utilisant Windows 2000 Server au minimum et doit être configuré avec Active Directory.

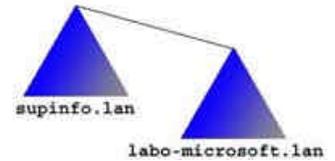


Afin de mieux administrer les réseaux étendus, il est possible de réunir plusieurs domaines ensemble. On appelle alors ces ensembles Arborences ou Forêts.

Une **arborescence** est un ensemble de domaines partageant un nom commun (ex : supinfo.lan est le domaine parent du domaine paris.supinfo.lan et du domaine caraïbes.supinfo.lan).



Une **forêt** est un ensemble de domaines n'ayant pas de nom en commun mais une configuration commune (ex : supinfo.lan et labo-microsoft.lan).



d) Fonctionnalités et avantages d'Active Directory

Active Directory est le service d'annuaire de Windows 2000, toutes les informations concernant les objets et ressources du réseau y sont stockées.

Il permet une gestion efficace, centralisée mais diffusée de la structure du réseau, même dans le cas d'une base contenant des millions d'objets.

Grâce aux stratégies systèmes d'Active Directory, il est possible de réduire le TCO (Coût de revient de fonctionnement d'un ordinateur) en limitant les modifications possibles de l'utilisateur sur le système ou en installant de façon centralisée des applications sur l'ensemble (ou partie) des machines du réseau.

e) Accès à un réseau Windows 2000

Sur une machine membre d'un domaine, Windows 2000 requiert à chaque démarrage une authentification. Cette authentification s'effectue par le biais d'un nom de compte (Identifiant unique dans la base des comptes du domaine) et d'un mot de passe (correspondant au compte) associés au domaine sur lequel se trouve le compte.

Module 2

Administration d'un réseau Windows 2000

1 Aide de Windows 2000

Dans le menu Démarrer, cliquez sur Aide (ou faites  - F1).

L'aide de Windows 2000 peut être parcourue de plusieurs façons différentes :

- Le sommaire : Affichage par catégories de l'intégralité de l'aide (Niveau débutant).
- L'index : Recherche par mots clés déjà référencés dans l'aide (Niveau avancé).
- La recherche : Recherche des rubriques contenant un mot ou un ensemble de mots spécifiques (Niveau confirmé).
- Les Favoris : Liste constituée par l'utilisateur au fur et à mesure de ses recherches dans l'aide.

2 Tâches administratives

L'administrateur d'un réseau a un certain nombre de tâches à réaliser de façon régulière :

- La gestion des Comptes d'utilisateurs et des groupes d'utilisateurs.
- La maintenance des ressources matérielles (imprimantes, télécopie, ...).
- Le contrôle de la sécurité du réseau.
- La vérification du bon fonctionnement du réseau.
- La maintenance des serveurs.
- La gestion des sauvegardes et des restaurations de données.
- La maintenance des applications serveurs (messagerie, bases de données, ...).
- Le contrôle de l'intégrité des disques.

 Il est possible pour certaines tâche de planifier leur déroulement à l'aide de l'utilitaire Tâches planifiées (Démarrer\Programmes\Accessoires\Outils Système\).

3 Outils d'administration

Afin de réaliser les tâches administratives qui lui sont assignées, l'administrateur du réseau dispose d'un certain nombre d'utilitaires :

Panneau de configuration	Permet d'accéder à la plupart des outils d'administration de Windows 2000
Propriétés système	Permet de modifier les propriétés générales du système (identifiant système)
Informations système	Donne un compte rendu de la configuration logicielle actuelle.
Observateur d'événements	Journal répertoriant tous les événements importants du système.
Gestionnaire des tâches Windows	Liste les applications actuellement en mémoire. Donne l'état des ressources du processeur et de la mémoire.
Performances	Permet de surveiller les performances système de l'ordinateur local ou d'un ordinateur distant.
Imprimantes	Permet de gérer la configuration des périphériques d'impression.
Dossiers partagés	Donne toutes les informations sur les partages en cours.
Gestion des disques	Permet de formater, de défragmenter et de nettoyer les disques.
Gestion des sauvegardes	L'utilitaire de sauvegarde et de restauration permet la programmation des sauvegardes.
Gestion de la sécurité	Permet de fixer le niveau de sécurité sur la machine et de définir les comptes pouvant avoir accès au domaine ou à la machine.
Outils réseau	Gère les connexion réseau locales et distantes. Surveille l'activité du réseau.
Autres outils	Configuration du serveur (Accès simplifié aux différentes fonctions administratives).
Console MMC	Outils de création de consoles d'administration.

Module 3

Sécurisation d'un réseau Windows 2000

1 Comptes d'utilisateurs

Les Comptes d'utilisateurs permettent aux utilisateurs d'accéder aux ressources réseau. Ils sont associés à un mot de passe et fonctionnent dans un environnement défini (machine local ou domaine).

Un utilisateur disposant d'un compte de domaine pourra s'authentifier sur toutes les machines du domaine (sauf restriction explicite de l'administrateur).

Un utilisateur disposant d'un compte local ne pourra s'authentifier que sur la machine où est déclaré le compte.

a) Comptes d'utilisateurs locaux

Il existe deux types de Comptes d'utilisateurs locaux :

Les Comptes d'utilisateurs personnalisés. Ils sont créés par l'administrateur de la machine. A l'ouverture de la session, un profil personnalisé est créé localement pour le compte.

Les Comptes d'utilisateurs prédéfinis. Il en existe deux, Administrateur et Invité. Ils sont créés par défaut lors de l'installation de Windows 2000. Administrateur nous permet d'administrer la machine lorsqu'elle n'est pas encore sur membre d'un domaine. Invité nous permet un accès restreint à la machine sans avoir à créer de compte personnalisé.

✍ Pour des raisons de sécurité, le compte Invité est désactivé par défaut.

Les comptes locaux sont gérés dans le snap-in MMC Utilisateur et groupes locaux de la console Gestion de l'ordinateur (Clic droit sur Poste de travail, puis Gérer).

✍ Ce Snap-in est désactivé sur les contrôleurs de domaine qui ne peuvent pas avoir de comptes locaux.

b) Comptes d'utilisateurs de domaine

Il existe deux types de comptes d'utilisateurs de domaine :

Les comptes de domaine personnalisés : Ils sont créés par l'administrateur sur l'un des contrôleur de domaine. A l'ouverture de session, un profil est créé localement ou sur un serveur, si l'administrateur a configuré des profils itinérants. Dans ce cas, quel que soit le poste Windows 2000 que l'utilisateur emploiera, il retrouvera son environnement de travail.

Les Comptes d'utilisateurs de domaine prédéfinis : Il en existe deux, Administrateur et Invité. Ils sont créés à l'installation de l'Active Directory. Administrateur permet de gérer tout le domaine ainsi que les domaines enfants. Ce compte peut être renommé mais pas supprimé. Invité est désactivé par défaut et permet d'accéder à tout le réseau dans les mêmes conditions qu'un utilisateur de base.

✍ Les comptes de domaine sont gérés par la console MMC Utilisateurs et ordinateurs Active Directory. Il apparaît sur les contrôleurs de domaine lors de l'installation d'Active Directory mais peut être installé sur n'importe quel système sous Windows 2000 pour de l'administration à distance grâce au kit d'administration à distance (adminpak.msi).

c) Groupes

Un groupe permet de lier ensemble un certain nombre d'utilisateurs (Un groupe n'est pas un conteneur). Il permet d'accorder des autorisations aux utilisateurs qu'il représente.

Il y a deux types de groupes :

Groupes sur un ordinateur local : ils permettent d'accorder des permissions uniquement au niveau de la machine. Dans le cas d'une machine non-relié à un domaine, il est possible d'inclure uniquement seul des comptes locaux peuvent être inclus dans les groupes.

Groupes sur un contrôleur de domaine : ils sont utilisables sur l'ensemble des machines du domaine et permettent d'avoir une gestion centralisée de la hiérarchie des groupes. Ils peuvent contenir des utilisateurs du domaine et même d'autres domaines.

2 Droits d'utilisateurs

Un droit définit la possibilité ou non d'un utilisateur à réaliser une action. Les droits sont applicables aux utilisateurs et aux groupes.

a) Droits d'utilisateurs courants

Les actions de base que peut réaliser un utilisateur nouvellement créé sont :

- Ouvrir une session localement
- Modifier l'heure du système
- Arrêter le système
- Accéder à cet ordinateur depuis un réseau

b) Droits accordés aux groupes prédéfinis

Windows 2000 inclus, lors de son installation, un certain nombre de groupes avec des droits prédéfinis :

Groupe	Droits	Contrôleur de domaine	Ordinateur local
Administrateurs	Tous les droits lui sont automatiquement affectés.	Oui	Oui
Utilisateurs	Dispose uniquement des droits qui lui ont été spécifiquement affectés.	Oui	Oui
Utilisateurs avec pouvoir	Peut réaliser les tâches administratives de base mais n'a pas le contrôle total du système.	Non	Oui
Opérateurs de sauvegarde	Possède des droits uniquement sur les fichiers et sur les tâches administratives de sauvegarde et de restauration.	Oui	Oui

3 Autorisations

Les autorisations permettent de définir les possibilités d'accès aux fichiers, aux imprimantes et aux partages des utilisateurs. Pour assurer la sécurité d'accès aux fichiers, il est nécessaire d'utiliser le système de fichiers NTFS.

☞ Pour convertir un volume en NTFS il suffit d'utiliser la commande : **CONVERT x: /FS:NTFS** (où x désigne la lettre du lecteur à convertir).

☞ Il est possible de vérifier les autorisations d'un objet à l'aide de l'onglet Sécurité des propriétés de l'objet (clic droit sur l'objet, puis **Propriétés**).

a) Autorisations sur les fichiers NTFS

Lecture	Lire les fichiers
Ecriture	Ecraser les fichiers
Lecture et exécution	Lire les fichiers et exécuter les applications
Modifier	Lire, modifier et supprimer les fichiers
Contrôle total	Lire, modifier, supprimer et modifier les autorisations des fichiers

b) Autorisations sur les dossiers NTFS

Lecture	Voir les fichiers et sous-dossiers du dossier
Ecriture	Créer des fichiers et sous-dossiers dans le dossier
Afficher le contenu du dossier	Afficher le nom des fichiers et des sous-dossiers du dossier
Lecture et exécution	Parcourir les dossiers, lire les fichiers et exécuter les applications
Modifier	Lire, modifier et supprimer les dossiers
Contrôle total	Lire, modifier, supprimer et modifier les autorisations des dossiers

c) Autorisations sur les dossiers partagés

Lecture	Voir les fichiers et sous-dossiers du partage
Modifier	Lire, modifier et supprimer les dossiers et les fichiers dans le partage
Contrôle total	Lire, modifier, supprimer et modifier les autorisations du contenu du partage

d) Autorisations sur les imprimantes

Imprimer	Imprimer et annuler vos propres impressions
Gestion des documents	Suspendre, reprendre, redémarrer et abandonner les impressions de tous les documents.
Gestion d'imprimantes	Suspendre, reprendre, redémarrer, abandonner les impressions de tous les documents, partager une imprimante et modifier les autorisations.

Module 4 Examen d'un réseau

1 Les cartes Réseaux

Selon l'étendue géographique d'un réseau, plusieurs dénominations lui sont données :

- Les réseaux locaux (LAN, Local Area Network)
- Les réseaux métropolitains (MAN, Metropolitan Area Network)
- Les réseaux étendus (WAN, Wide Area Network)

Les cartes réseaux sont l'interface entre l'ordinateur et le réseau. Les données qui traversent les câbles réseaux sont organisées en paquets. Ces paquets se décomposent généralement en une en-tête, des données et un bloc de fin. Chaque carte réseau possède une adresse MAC unique au monde, définie en général par le constructeur.

2 Les Câbles Réseaux

Les trois principales catégories de câbles réseaux sont :

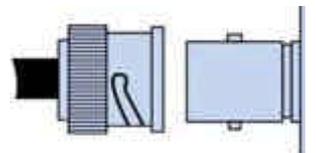
a) Les câbles à paires torsadées

Se composent de huit brins de cuivre isolés, torsadés par paires. Il en existe deux types : les câbles UTP et STP, les câbles STP sont blindés. Ils peuvent transporter les signaux sur environ 100m. Cette catégorie de câble est la plus répandue. Les connecteurs utilisés pour ces câbles sont nommés RJ45.



b) Le câble coaxial

Il utilise uniquement un fil pour transporter les données il est protégé par un blindage de métal tressé. Il existe deux types de câbles coaxiaux : le câble ThinNet (10Base2, 185m max) et le câble ThickNet (10Base5, 500m max). Ce type de câble est particulièrement adapté pour des transmissions longues distances. Ils utilisent des connecteurs de type BNC.



c) La fibre optique

Adaptée aux transmissions rapides et fiables, ce type de câble est très peu sensible aux interférences. Il est toutefois bien plus fragile que les autres types de câbles.



3 Communications sans fil

Il existe deux types de transmission sans fil :

a) Transmission infrarouge

Aucun obstacle ne doit être présent entre l'émetteur et le récepteur. Les signaux sont limités en distance car très sensibles aux interférences.

b) Transmission radio à bande étroite

L'émetteur et le récepteur peuvent être séparés par des obstacles (excepté des objets métalliques).

4 Topologies des réseaux

a) Topologie en bus

Dans la topologie en bus, tous les ordinateurs sont reliés au même câble. Chaque extrémité est reliée à une terminaison. En cas de rupture du câble en un point, toutes les communications sont interrompues. A chaque extrémité du câble il est nécessaire d'avoir un bouchon terminateur. Plus le nombre d'ordinateurs sur le segment est élevé, plus l'efficacité du réseau diminue.



b) Topologie en étoile

Dans une topologie en étoile, tous les ordinateurs sont reliés à l'aide d'un câble à un concentrateur. Si l'un des câbles se rompt seul l'ordinateur relié à ce câble en est affecté, toutefois, si le concentrateur tombe en panne, l'ensemble des ordinateurs ne peut plus communiquer.



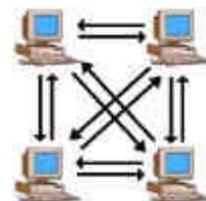
c) Topologie en anneau

Dans une topologie en anneau, les ordinateurs sont reliés à un seul câble en anneau. Les signaux transitent dans une seule direction. Chaque ordinateur joue le rôle de répéteur, régénérant le signal, ce qui en préserve la puissance. Dans cette topologie, les ordinateurs "parlent" à tour de rôle. Un jeton circulant sur le réseau donne le droit d'émettre des données. Lorsqu'un ordinateur reçoit le jeton et qu'il souhaite "parler", il stocke le jeton, puis envoie sa trame de données, attend de recevoir la confirmation de réception envoyée par l'ordinateur destinataire, puis enfin, passe le jeton. Cette topologie est la plus efficace dans des réseaux où le trafic est élevé.



d) Topologie maillée

Dans une topologie maillée, chaque ordinateur est connecté à chacun des autres par un câble séparé. Son principal avantage, est sa capacité de tolérance de panne. En effet, lorsqu'un câble se rompt, il existe de nombreux autres itinéraires routés. Cette topologie est toutefois très coûteuse.



e) Topologie hybride

Dans une topologie hybride, plusieurs topologies sont combinées. La topologie étoile/bus et étoile/anneau sont les plus répandues.

5 Technologies réseaux

Chaque technologie réseau utilise sa propre méthode d'accès. Une méthode d'accès est la manière de placer et de retirer des informations du réseau. On parle aussi de média réseau.

a) Ethernet

Ethernet est une technologie réseau très répandue. Elle fait appel au protocole CSMA/CD (Carrier Sens Multiple Access with Collision Detection) entre les clients, et peut être utilisé avec différentes topologies. Pour émettre, un ordinateur regarde si le réseau est libre, et se met à émettre. Lorsque plusieurs ordinateurs tentent d'émettre en même temps, il se produit une collision. Cette dernière est détectée, obligeant les protagonistes à attendre un délai aléatoire avant d'essayer de ré-émettre la trame. Les vitesses de transfert sur un réseau Ethernet sont 10Mb/s (10BaseT), 100Mb/s (100BaseT) ou 1Gb/s (1000BaseT).

b) Token Ring

Les réseaux Token Ring sont implémentés dans une topologie en anneau. Toutefois, la topologie physique est en étoile et c'est dans le concentrateur que se font les liaisons d'un ordinateur à l'autre. La méthode d'accès pour cette technologie est l'utilisation du Jeton qui n'autorise que son détenteur à utiliser le réseau. Aucune collision n'est alors possible. Les vitesses de transferts sur un réseau Token Ring sont de 4Mb/s ou de 16Mb/s.

c) ATM

ATM (Asynchronous Transfer Mode) est un réseau à commutation de paquets de taille fixe. Des commutateurs ATM doivent être placés à chaque extrémité de la ligne ATM. Un réseau ATM utilise la méthode d'accès Point à Point. La vitesse de transfert d'une ligne ATM varie de 155Mb/s à 622Mb/s.

d) FDDI

Les réseaux FDDI (Fiber Distributed Data Interface) ressemblent aux réseaux Token Ring à Jeton. Ils sont constitués de deux anneaux appelés Anneau principal et anneau secondaire. Elle utilise une méthode d'accès par Jeton, toutefois, cette méthode est plus efficace que le Token Ring traditionnel car plusieurs trames peuvent circuler sur l'anneau simultanément. La vitesse de transfert d'un réseau FDDI est comprise entre 155Mb/s et 622Mb/s.

e) Relais de trame

Un réseau à relais de trame est constitué de plusieurs entités de routage reliées les unes aux autres par des liaisons. Une trame peut être divisée et prendre différents chemins. Elle sera réassemblée à l'arrivée. La méthode d'accès à un réseau à relais de trame est le Point à Point. La vitesse dépend des supports matériels.

6 Extension d'un réseau

a) Répéteurs et concentrateurs (Hubs)

Un répéteur redistribue les paquets reçus. Cela permet d'étendre la distance entre deux périphériques réseaux. Le concentrateur est tout simplement un répéteur à plusieurs ports.

b) Ponts

Un pont analyse les paquets qui lui parviennent. Si un paquet arrivé sur le port A est destiné à un ordinateur connecté à son autre extrémité, alors, il le fait transiter. L'analyse se fait sur l'adresse MAC du destinataire.

c) Commutateurs (Switches)

Un commutateur est constitué de ponts qui relient chaque ports à tous les autres. Un paquet qui entre sur un port ressort sur le port où le destinataire est connecté.

d) Routeurs

Les routeurs sont des commutateurs évolués. Ils analysent les paquets à des couches supérieures (Couche réseau : IP, IPX...). Ils permettent de sélectionner le meilleur itinéraire lorsqu'il y en a plusieurs. Ils permettent de passer d'un segment de réseau à un autre dans le cas de réseaux segmentés.

e) Passerelles

Les passerelles permettent à des architectures réseaux différentes de communiquer entre elles. Par exemple, elles permettent de transférer un paquet d'un réseau Ethernet vers un réseau Token Ring.

f) Accès Distant

L'accès distant permet de se connecter à un réseau à l'aide de différents périphériques, le plus courant étant le modem. Le Réseau privé virtuel (VPN) est un accès à distance utilisant une technique de cryptage pour garantir la confidentialité des données.

g) RTC

Le RTC (Réseau Téléphonique Commuté) permet à l'aide de modems analogiques d'utiliser les lignes téléphoniques comme moyen de transport des données. Les lignes téléphoniques n'étant pas prévu pour cela, les transmissions sont limitées à 56kbps et sont très sensibles aux bruits.

h) Réseau RNIS

Le réseau RNIS (Réseau Numérique à Intégration de Services) permet de transférer des données numériques sur une ligne téléphonique. Les canaux RNIS ont un débit de 64kb/s.

i) Réseau X.25

Le réseau X.25 utilise la transmission de paquets par commutations. X.25 utilise des équipements de communications de données pour créer un réseau mondial complexe de nœuds qui se transmettent les paquets de données pour les remettre à l'adresse indiquée.

j) Technologie ADSL

La technologie ADSL (Asymmetric Digital Subscriber Line) permet de transmettre des volumes de données très important sur des lignes téléphoniques classique. Comme l'indique le nom, les débits de données sont asymétriques, donc plus importants en réception qu'en envoi.

Module 5

Examen des protocoles réseau

Un protocole réseau est un langage que vont utiliser toutes les machines d'un réseau pour communiquer entre elles.

1 Présentation des protocoles

Un protocole se présente sous la forme d'un logiciel dans le système d'exploitation. Ils sont parfois composés d'une multitude de protocoles afin de pouvoir acheminer l'information (ex : TCP/IP avec IP, TCP, UDP, ICMP, ...).

a) Modèle de référence OSI

Le modèle OSI est une norme définie par l'ISO (International Organisation for Standardization) qui permet l'interconnexion réseau des systèmes hétérogènes. Il est composé des 7 couches suivantes:

Application	Assure l'interface avec les applications.
Présentation	Définit le formatage des données (représentation, compression, cryptage, ...).
Session	Définit les canaux de communication sur les machines du réseau.
Transport	Chargée du transport des données et de la gestion des erreurs.
Réseau	Permet de gérer les adresses et le routage des données.
Liaison Données	Définit l'interface avec la carte réseau.
Physique	Codage des données en signaux numériques.

b) Types de protocoles

Un protocole peut s'intégrer à plusieurs niveaux dans le modèle OSI :

- Protocoles d'application : Echange de données entre application (ex : FTP, IMAP, ...)
- Protocoles de transport : Assure la fiabilité des données transportées (ex : TCP, ...)
- Protocoles réseau : Détermine le chemin d'accès à la destination (ex : IP, ...)

2 Protocoles et transmissions de données

a) Protocoles prenant en charge ou non le routage

La routabilité est la faculté d'un protocole à pouvoir transporter des données à travers différents segments d'un même réseau.

Tout les protocoles ne gèrent pas le routage. TCP/IP et IPX/SPX le gèrent tandis que NetBEUI et DLC ne le gèrent pas.

✍ Pour pouvoir communiquer avec un autre segment de réseau, il est nécessaire d'intégrer un routeur au réseau afin qu'il achemine les paquets sur l'autre segment.

b) Types de transmission de données

Il existe trois types de transmissions des données sur un réseau :

- Monodiffusion : Les données sont transmises à un poste précis.
- Diffusion : Les données sont envoyées à l'ensemble du réseau sans distinction.
- Multidiffusion : Les données sont transmises une seule fois, aux différents ordinateurs qui en font la demande.

3 Protocoles couramment utilisés

a) Protocole TCP/IP

Le protocole TCP/IP est une suite de protocoles développée par l'armée américaine qui prend en charge le routage. TCP/IP étant le protocole de base d'Internet, il est présent sur la majorité des systèmes d'exploitation du commerce. TCP/IP est le protocole de base de Windows 2000.

b) Protocole IPX/SPX

Protocole propriétaire de Novell, il prend en charge le routage. Il peut être utilisé avec Windows 2000 grâce à l'implémentation NWLink IPX/SPX/NetBIOS.

c) Protocole NetBEUI

Le protocole NetBEUI est l'un des premiers protocoles disponibles pour ordinateurs personnels. Il ne prend pas en charge le routage et n'est utilisé que dans le cas de petites structures intégrant divers systèmes d'exploitation souvent anciens. Il peut être utilisé sous Windows 2000 grâce au protocole NetBIOS Frame (NBF).

d) Protocole AppleTalk

Protocole propriétaire d'Apple, il prend en charge le routage. Il peut être intégré à Windows 2000 Server afin de pouvoir communiquer avec les environnements Macintosh.

4 Autres Protocoles de communication

a) Protocole ATM

Protocole Grande Vitesse Asynchrone qui permet de faciliter le transfert de données de type multimédia. Il permet de faire passer simultanément plusieurs types de données tout en maximisant la bande passante.

b) Protocole IrDA

Le Protocole IrDA permet une communication sans fil entre 2 périphériques infrarouges. Il est intégré en standard à Windows 2000.

5 Protocoles d'accès distant

a) Protocoles d'accès à distance

Protocole SLIP : Protocole de connexion distante par modem. Il transmet les mots de passe en texte clair et ne supporte que TCP/IP. Windows 2000 supporte le protocole SLIP en client mais ne peut pas servir de serveur.

Protocole PPP : Protocole de connexion distante par modem. Il permet de crypter les mots de passe et de transporter différents protocoles. Windows 2000 supporte intégralement ce protocole.

b) Protocoles VPN

Permet de transiter par Internet pour se connecter à un serveur. Les connexions se font de façon sécurisée, même sur la zone Internet.

Protocole PPTP : Sécurise les transferts par un encapsulage des données. Il supporte une multitude de protocoles réseau.

Protocole L2TP : Protocole de tunneling. Il utilise le protocole IPSec pour crypter les données. Il supporte une multitude de protocoles réseau.

Protocole IPSec : Garantit la sécurité des transmissions de données sur le réseau en ajoutant une couche de cryptage au cours des communications TCP/IP. Requiert des ressources processeur supplémentaires (excepté dans le cas d'une implémentation matérielle dans la carte réseau) au niveau du client et du serveur.

Module 6

Examen du protocole TCP/IP

1 Présentation du protocole TCP/IP

Le protocole TCP/IP désigne une suite de protocoles. Ce protocole permet d'établir des communications entre différents périphériques réseau.

a) Couches TCP/IP

Le protocole TCP/IP utilise un modèle réseau sur quatre couches dérivé de celui de l'OSI. Les quatre couches sont les suivantes :

Couche TCP/IP	Couche OSI	Protocoles
Application	Application Présentation Session	HTTP, FTP, ...
Transport	Transport	TCP et UDP
Internet	Réseau	IP, ICMP, IGMP et ARP
Interface réseau	Liaison Physique	Ethernet, Token Ring, ATM, ...

b) Identification des applications

Afin de pouvoir utiliser différentes applications simultanément, TCP/IP emploie une méthode basée sur des numéros de ports pour les identifier.

- **Adresse IP** : Numéro unique sur le réseau, l'adresse IP permet d'identifier la source et la destination des données.
- **Port TCP/UDP** : Identifie l'application en cours d'exécution. Il est associé au protocole TCP ou UDP et à un numéro compris 0 et 65535 (ex : HTTP – TCP 80).
- **Socket** : Combinaison d'une adresse IP, du numéro de port et du type de protocole TCP ou UDP

2 Suite de protocoles TCP/IP

a) Protocole TCP

Le protocole TCP assure au niveau de la couche transport un service orienté connexion entre deux périphériques réseau. Dans ce type de connexion il n'est pas possible d'avoir plus de deux intervenants (ex : transfert de fichiers).

Le protocole TCP organise l'envoi des données par paquets, il affecte un numéro à chaque paquet et réorganise les paquets à l'arrivée. Il garantit la bonne remise des paquets et procède automatiquement au renvoi des paquets perdus.

b) Protocole UDP

Le protocole UDP assure au niveau de la couche transport un service de remise de paquets sans connexion. Il permet l'envoi simultané d'informations à plusieurs machines sans augmenter la bande passante occupée (ex : streaming vidéo).

☞ Le protocole UDP n'assure pas la remise des paquets ni le bon ordre d'arrivée de ceux-ci.

c) Protocole IP

Le protocole IP détermine, au niveau de la couche Internet, le chemin que vont prendre les paquets. Il n'assure aucune sécurité des paquets transmis.

✍ Le protocole IP fournit la gestion du routage des paquets TCP/IP et en détermine le TTL (Time to Live) afin qu'un paquet perdu ne reste pas indéfiniment sur le réseau.

d) Protocole ICMP

Le protocole ICMP assure au niveau de la couche Internet les fonctions de dépannage de TCP/IP. Il permet de déterminer les erreurs possibles sur un réseau. L'utilitaire ping travaille avec ICMP.

e) Protocole IGMP

Le protocole IGMP gère la liste des destinataires pour la multidiffusion sur IP. Il est souvent associé au protocole UDP car la multidiffusion permet l'acheminement vers plusieurs ordinateurs clients ce qui implique, pour des raisons de performance, une impossibilité d'assurer la remise des paquets.

f) Protocole ARP

Le protocole ARP permet la résolution d'adresses IP en adresses MAC. La résolution ARP ne peut intervenir qu'une fois le paquet arrivé sur le segment de destination. Le protocole RARP permet de réaliser la résolution inverse (MAC → IP)

g) Utilitaires TCP/IP

La suite de protocoles TCP/IP fournit des utilitaires de base permettant à un ordinateur exécutant TCP/IP (Windows 2000, Unix, Mac OS X,...) de tester ou d'utiliser le réseau.

Ces utilitaires sont divisés en trois catégories :

- Utilitaires de diagnostic

- ?? Arp : Cet utilitaire affiche et modifie le cache ARP.
- ?? Hostname : Affiche le nom d'hôte de votre ordinateur.
- ?? Ipconfig : Affiche et met à jour la configuration TCP/IP.
- ?? Nbtstat : Affiche le cache NetBIOS.
- ?? Netstat : Affiche les sessions TCP/IP en cours.
- ?? Ping : Permet la vérification des connexions IP par le biais du protocole ICMP.
- ?? Tracert : Affiche l'itinéraire des paquets pour atteindre leur destination.

- Utilitaires de connexion

- ?? Ftp : Utilitaire de transfert de fichiers basé sur TCP.
- ?? Telnet : Utilitaire de configuration à distance en mode console.
- ?? Tftp : Utilitaire de transfert de fichiers basé sur UDP.

- Logiciels serveur

- ?? Service d'impression TCP/IP : Permet aux clients TCP/IP d'utiliser une imprimante connectée à Windows 2000.
- ?? Service Internet (IIS) : Logiciels serveurs Web, News, Mail, FTP.

3 Résolution de noms

Le protocole TCP/IP identifie les ordinateurs source et de destination grâce à leur adresse IP. Pour des raisons de maintenance et de gestion il est important de faire correspondre ces numéros (ex : 192.168.1.1) à des noms intelligibles.

a) Types de noms

Il existe deux types de noms conviviaux :

- **Les noms d'hôtes** : Basés sur le système DNS, les noms d'hôtes se présentent sous diverses formes (ex : saga ou saga.supinfo.com). La longueur d'un nom d'hôte ne peut dépasser les 255 caractères.
- **Les noms NetBIOS** : Un nom NetBIOS peut représenter un ordinateur ou un groupe d'ordinateurs. La longueur maximale d'un nom NetBIOS est de 15 caractères. Windows 2000 ne nécessite pas de noms NetBIOS mais assure une compatibilité pour les versions antérieures à Windows 2000.

b) Mappage IP statique

Il est possible de mapper statiquement les noms intelligibles avec leur adresse IP. Ceci grâce à deux fichiers :

- **Fichier Hosts** : Permet des mappages IP / nom d'hôte
- **Fichier Lmhosts** : Permet des mappages IP / nom NetBIOS

c) Mappage IP dynamique

Il est possible de centraliser, à la manière des comptes utilisateurs, la gestion de la résolution des noms en adresses IP. Pour ceci il existe les deux serveurs suivants :

- **Serveur DNS** : Permet la résolution des noms d'hôte en adresse IP. Ce sont les serveurs DNS qui font la résolution des noms sur Internet (ex : www.labo-microsoft.com).
- **Serveur WINS** : Permet la résolution des noms NetBIOS en adresse IP.

d) Résolution des noms dans Windows 2000

Windows 2000 suit une procédure pour pouvoir résoudre efficacement les noms NetBIOS. Cette procédure peut être modifiée dans la configuration de l'ordinateur. Les procédures suivantes sont celles de base.

- Processus de résolution de noms d'hôte
 - ?? L'ordinateur vérifie si le nom indiqué correspond à son nom d'hôte local.
 - ?? L'ordinateur recherche dans son fichier Hosts.
 - ?? L'ordinateur envoie une requête au serveur DNS.
 - ?? L'ordinateur recherche dans son cache ARP (Windows 2000 traite les noms NetBIOS comme des noms d'hôtes).
 - ?? L'ordinateur envoie une requête au serveur WINS.
 - ?? L'ordinateur envoie une diffusion générale sur le réseau.
 - ?? L'ordinateur recherche dans son fichier Lmhosts.
- Processus de résolution de noms NetBIOS
 - ?? L'ordinateur recherche dans son cache NetBIOS (Windows 2000 traite les noms NetBIOS comme des noms d'hôtes).
 - ?? L'ordinateur envoie une requête au serveur WINS.
 - ?? L'ordinateur envoie une diffusion générale sur le réseau.
 - ?? L'ordinateur recherche dans son fichier Lmhosts.
 - ?? L'ordinateur recherche dans son fichier Hosts.
 - ?? L'ordinateur envoie une requête au serveur DNS.

4 Examen du processus de transfert de données

Afin d'améliorer l'efficacité des transferts sur un réseau, il est important de transmettre de petit paquets. En effet, si l'on envoie des paquets de taille trop importante, le réseau peut se bloquer et tout incident lors du transfert du paquet obligera à le renvoyer dans son intégralité.

a) Terminologie relative aux paquets

Lors de l'envoi d'un paquet sur le réseau, les données passent par différents états. Chacun de ces états possède une terminologie particulière.

Terminologies	Couches et protocoles	Contenu
Segment	TCP - Transports	Contient l'en-tête TCP ainsi que les données.
Message	UDP - Transports	Contient l'en-tête UDP ainsi que les données.
Datagramme	IP - Internet	Contient l'en-tête IP ainsi que le message ou le segment.
Trame	Interface réseau	Contient l'en-tête de l'interface réseau ainsi que le datagramme.

Une trame comprend trois composants :

- **En-tête** : L'en-tête contient un signal d'alerte (permettant d'indiquer que le paquet est en cours de transmission), l'adresse source et l'adresse de destination.
- **Données** : Données réelles envoyées par l'application. La taille varie selon les limites du réseau entre 0,5 Ko et 4 Ko avec une taille moyenne de 1,5 Ko.
- **Délimiteur de fin de trame** : Sur la plupart des protocoles, le délimiteur de fin de trame contient un CRC (Contrôle d'intégrité du paquet).

b) Flux de données

Pour chaque couche réseau traversée, le protocole correspondant intègre une entête au paquet. Et ceci pour les quatre couches :

- **Couche Application** : l'application organise les données dans un format propre à l'application.
- **Couche Transport** : Selon le protocole appelé, l'entête est différente. Dans le cas de TCP, un numéro de séquence est affecté à chaque segment à transmettre, les informations d'accusé de réception sont ajoutés, les numéros de port TCP de la source et de la destination sont ajoutés. Dans le cas de l'UDP, les numéros de port UDP de la source et de la destination sont ajoutés.
- **Couche Internet** : le protocole IP ajoute les informations d'adresse IP source, d'adresse IP de destination, le protocole de transport, la valeur du total contrôle, la valeur TTL et l'adresse MAC.
- **Couche Interface réseau** : Ajoute une séquence d'identification de début de trame et le code CRC.

5 Routage de données

a) Routage IP

Les réseaux de grandes tailles sont divisés en segments de taille plus petite. Afin d'interconnecter ces segments, on utilise couramment des ordinateurs munis de deux interfaces réseaux pour faire office, de routeurs transmettant les paquets d'un segment à l'autre. Grâce à une table de routage, le routeur transmet les paquets vers les segments optimaux afin que le paquet arrive dans les meilleurs délais.

Module 7

Examen de l'adressage IP

1 Adressage IP par classes

Pour pouvoir communiquer sur un réseau, chaque ordinateur doit avoir une adresse IP unique. Dans l'adressage IP par classes, trois classes d'adresses sont utilisées pour affecter des adresses IP aux ordinateurs. Le choix de la classe d'adresse IP se fait en fonction de la taille et du type de réseau.

Une adresse IP se présente sous la forme de quatre champs numériques Champ1.Champ2.Champ3.Champ4 (ex : 195.217.13.121), chaque champ représentant un octet pouvant donc prendre une valeur allant de 0 à 255.

Une adresse IP se décompose aussi en deux parties, l'identificateur réseau et l'identificateur d'hôte. Tous les ordinateurs ayant le même identificateur de réseau peuvent se voir et discuter directement.

Le tableau ci-dessous permet de voir la correspondance entre ces différentes décompositions de l'adresse IP en fonction de la classe.

Classe	Champ 1	Champ 2	Champ 3	Champ 4	Maximum de réseau	Maximum d'hôtes
Classe A	Identificateur Réseau	Identificateur d'hôte			126	16777214
Classe B	Identificateur Réseau		Identificateur d'hôte		16382	65534
Classe C	Identificateur Réseau			Identificateur d'hôte	2097150	254

Classe D et E :

Elles ne sont pas affectées aux hôtes. Les adresses de classe D sont utilisées pour la multidiffusion, tandis que les adresses de classe E sont réservées à une utilisation ultérieure.

Classification des classes par rapport au premier champ d'une adresse IP :

Classe	Champ 1	Champ 2	Champ 3	Champ 4
A	1 à 126	XXX	XXX	XXX
B	128 à 191	XXX	XXX	XXX
C	192 à 223	XXX	XXX	XXX

☞ Les adresses IP commençant par 127 sont réservées à des procédures de tests (127.0.0.1=localhost).

2 Création de sous-réseaux

Pour des raisons d'efficacité, on divise les réseaux en sous-réseaux. Cela permet de limiter le nombre de paquets non destinés aux machines locales. Lorsque trop de machines sont sur un même sous-réseau, le trafic augmente, entraînant un nombre grandissant de collisions ce qui a pour conséquence de diminuer l'efficacité du réseau. En divisant en sous-réseau, et en séparant physiquement ces sous-réseaux par des routeurs, on réduit le trafic et on augmente l'efficacité du réseau.

Pour créer des sous-réseaux, on utilise le masque de sous-réseau. C'est ce masque qui permet aux ordinateurs de savoir si le destinataire se trouve dans le même sous-réseau et si ce n'est pas le cas, d'envoyer le paquet au routeur.

Un masque de sous-réseau est comme une adresse IP composé de quatre champs numériques pouvant prendre une valeur de 0 à 255. Les masques de sous-réseaux par défaut sont : pour la classe A : 255.0.0.0, pour la classe B : 255.255.0.0, et pour la classe C : 255.255.255.0, on pourra remarquer que tous les bits des champs identificateurs de réseaux sont à 1 (cf adresse IP).

Pour savoir si un ordinateur est dans notre sous-réseau, rien de plus simple, il suffit de comparer les identificateurs de sous-réseau, s'ils sont équivalents, ils sont dans le même sous-réseau.

Ex :
192.168.200.16 (MS : 255.255.192.0) et 192.168.224.165 (MS : 255.255.192.0)

192								168								200								16							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0
255								255								192								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

192								168								224								165							
1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	0	0	0	0	0	1	0	1	0	0	1	0	1
255								255								192								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

Ce qui donne comme réseau 192.168.192.0 pour les deux adresses IP. Donc elles se trouvent dans le même sous-réseau.

3 Planification d'adressage IP

Principales règles d'adressage

- ?? Le premier segment de l'adresse IP ne peut être égal à 127, cet identificateur est réservé à des fins de tests.
- ?? L'adresse IP ne peut contenir que des 255, car cette IP est réservé à la diffusion.
- ?? L'adresse IP de l'hôte ne peut contenir que des 0, cette adresse servant à désigner un identificateur de réseau. L'adresse IP doit être unique.

Dans la classe A, vous pouvez faire évoluer vos identificateurs réseaux de 1 à 126 (premier champ numérique). Dans la classe B, de 128.0 à 191.255 et dans la classe C de 192.0.0 à 223.255.255. Pour avoir l'identificateur complet, il faut rajouter des 0 à la fin pour remplir les quatre champs.

4 Affectation d'adresses IP

a) Adressage IP Statique

Cela consiste à appliquer machine par machine une IP.

Pour le faire, sous Windows 2000, il faut afficher la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)** Pour y accéder, Faites Démarrer->Paramètres->Connexion réseau et accès distant. Affichez les propriétés de **Connexion au réseau local**. Affichez les propriétés du **Protocole Internet (TCP/IP)**. Sélectionnez l'option Utiliser l'adresse IP Suivante, pour pouvoir définir l'adresse IP et le masque de sous-réseau de votre machine.

b) Adressage IP automatique

Par défaut, Windows 2000 est configuré pour obtenir une adresse IP automatiquement auprès d'un serveur DHCP. Un serveur DHCP contient des plages d'IP, et lorsqu'un ordinateur lui demande une IP, il lui transmet une adresse IP qui n'est pas utilisée sur le réseau. DHCP est très utile dans des grandes entreprises, où le fait de mettre une IP statique à chaque machine serait fastidieux, et prendrait beaucoup de temps.

c) Utilisation d'ipconfig

Sous Windows 2000, un utilitaire en ligne de commande vous permet d'afficher la configuration IP de votre ordinateur. Tapez ipconfig en ligne de commande pour avoir les informations de votre configuration IP. Utilisez le commutateur /all pour afficher des informations complémentaires.

Module 8

Optimisation de l'allocation d'adresses IP

1 Routage CIDR

a) Restrictions imposées par l'adressage IP par classes

L'attribution de plages IP pose actuellement problème, la constante croissance de la demande, et le nombre d'adresses IP limitées, nous montrent les limites de l'adressage par classe. Car une entreprise possédant 2000 ordinateurs se voit assigner une plage d'adresse de 65534 ordinateurs.

b) Définition du routage CIDR

Le routage CIDR (Classless Inter-Domain Routing) utilise la notation binaire (vous pouvez utiliser la calculatrice de Windows pour convertir entre décimal et binaire). Il divise l'adresse IP en 32 valeurs donc sur ce principe, une entreprise contenant 2000 ordinateurs se verra attribuer 2048 adresses IP. Le routage CIDR ne définit pas un masque de sous-réseau en fonction de la classe, mais, au contraire, chaque hôte a son propre masque de sous-réseau.

c) Masques de sous-réseau binaire

Les masques de sous-réseau binaire sont constitués d'une série de 1 contigus suivi d'une série de 0 contigus.

Ex :

255								255								255								196							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0

255								255								255								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	

d) Notation CIDR

La notation CIDR contient l'IP de l'hôte ou du réseau suivi du masque sous une forme raccourcie. Par exemple, 192.168.0.1/24 représente l'IP d'une machine qui a comme masque de sous-réseau 255.255.255.0 soit 11111111 11111111 11111111 00000000. Le nombre après le « / » est le nombre de 1 dans la notation binaire du masque de sous-réseau.

e) Calcul d'identificateur de réseau

Prenons l'adresse IP CIDR suivante : 10.217.123.7/20

Transformons l'adresse IP sous forme Binaire :

10								217								123								7							
0	0	0	0	1	0	1	0	1	1	0	1	1	0	0	1	0	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1

Nous n'allons garder que les 20 premiers chiffres et remplacer les chiffres restants par des 0. Cela revient à appliquer un ET logique entre chaque bit du masque de sous-réseau et de l'adresse IP.

10								217								112								0							
0	0	0	0	1	0	1	0	1	1	0	1	1	0	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0

Ce qui nous donne comme identificateur de réseau : 10.217.112.0/20

f) Identifications d'hôtes locaux et distants

Pour savoir si un ordinateur fait partie du même réseau (ou sous-réseau), on extrait les identificateurs réseau de chacun des ordinateurs et on les compare. S'ils sont égaux, ils appartiennent au même réseau.

2 Allocations d'adresses IP à l'aide du routage CIDR

a) Identificateurs d'hôtes disponibles

Le masque de sous-réseau en notation CIDR (que l'on notera 'n') nous permet de trouver facilement le nombre d'hôte possible dans le sous-réseau. En effectuant l'opération : $2^{(32-n)} - 2$ nous trouvons le nombre d'hôtes possible dans le sous-réseau.

Nb : lorsque nous connaissons le nombre de machines et que nous souhaitons trouver le masque de sous-réseau le plus adapté, il suffit d'utiliser l'opération inverse soit : $32 - ((\ln(\text{nbmachines} + 2) / \ln(2)))$ et d'arrondir à l'entier inférieur.

b) Optimisation de l'allocation d'adresses IP

Pour une entreprise qui possède 800 ordinateurs, le routage CIDR permet à l'entreprise de n'utiliser que 1022 adresses IP (/22) contre les 65534 en classe B.

Rien n'empêche cette entreprise de sous segmenter son réseau interne pour le rendre plus efficace.

Module 9

Examen des services web

1 Identification des concepts d'Internet

a) Internet

Internet est le réseau des réseaux, il réunit un très grand nombre d'entreprises, d'organismes et de particuliers. Construits autour de TCP/IP, les ordinateurs connectés à Internet utilisent une architecture de type client-serveur et doivent posséder une adresse IP publique.

Au vu de l'évolution grandissante du nombre d'ordinateurs connecté à Internet, le nombre d'adresses IP demandé est devenu supérieur à celui du nombre d'adresses IP publique pouvant être affectées. Pour résoudre ce problème, l'IANA (Internet Assigned Numbers Authority) a réservé des plages d'adresses IP dites privées. Les adresses privées sont bloquées par les routeurs de l'infrastructure Internet.

b) Services Internet

Un certain nombres de services sont disponibles sur Internet :

- Messagerie électronique : Le service le plus utilisé sur Internet. Permet d'envoyer des messages aux utilisateurs connecté à Internet.
- Services Web : Ensemble des pages HTML, Flash ou autres...
- Chat : Discussions en temps réel entre plusieurs personnes (IRC, ...).
- News : Ensemble de contributions correspondant à un thème précis.
- FTP : Publication de fichiers avec possibilité de téléchargement.
- Telnet : Ouverture d'une session à distance en mode invite de commande.

c) Réseaux Intranets

Un Intranet consiste en un déploiement interne à une entreprise des technologies d'Internet.

Si les ressources sont accessible sur Internet, on parle alors d'extranet.

d) Dénomination de domaine

Afin de rationaliser les millions d'adresses IP que constitue Internet, la technologie DNS a été choisie afin de faire correspondre les adresses IP en nom intelligibles (ex : www.microsoft.com = 207.46.197.113).

Un certain nombre de domaines principaux ont été définis pour normaliser les noms :

com	Entreprises commerciales
edu	Enseignement
gov	Administrations
int	Associations internationales
mil	Organisations militaires américaines
net	Centres de maintenance du réseau
org	Autres organisations
xx	Code pays (ex : fr - France, be – Belgique, ...)

2 Utilisation des technologies clientes

a) Client Mails

Afin de pouvoir exploiter avec efficacité et simplicité des protocoles de messagerie comme POP3, IMAP4 ou SMTP, il existe des clients mails rendant l'exploitation de la messagerie beaucoup plus efficace.

Windows 2000 inclut Outlook Express, mais il est possible d'installer des clients plus évolués, comme Outlook XP, Lotus Notes, Eudora, ...

b) Navigateurs

Pour avoir un aperçu graphique des langages HTML, XML, DHTML, Flash, ... Windows 2000 intègre le navigateur Internet Explorer 5, il est possible d'installer d'autre navigateur comme Opéra, Netscape, Tout ces langages transitent via les protocoles HTTP, HTTPS,

La recherche sur Internet passe par des moteurs de recherche (ex : www.google.com, www.yahoo.fr, www.voila.fr, ...).

c) Lecteurs de news

Afin de pouvoir lire les news, Outlook prend en charge aussi les protocoles de news comme NNTP (Network News Transfert Protocol).

d) Client FTP

Pour pouvoir télécharger aisément les fichiers d'Internet, Internet Explorer supporte le protocole FTP. Mais il peut être utile d'employer des client spécialisé comme CuteFTP, FlashFXP, WSftp, ...

3 URL

Une URL est le chemin complet d'accès à une page d'un serveur (ex : <http://supinfo-2.supinfo.com/fr/partenaires/Informations/PartenariatMicrosoft.htm>).

Il est composé du protocole suivi du nom du domaine ainsi que du chemin pour accéder au fichier.

En cas de chemin incomplet (ex : <http://www.mtv.com/onair/jackass/>) le fichier index.html ou default.html sera implicitement sélectionné par le serveur.

4 Connexion à Internet

Lorsqu'un organisme n'a pas assez d'adresses publiques pour pouvoir connecter l'ensemble de son parc informatique à Internet. Il est obligé de passer par un système de routage pour contourner le problème. Dans ce cas, il est important d'empêcher tout individu externe à l'entreprise de pénétrer via Internet dans le réseau de l'entreprise.

Pour cela il existe un certain nombre de composants qui permettent d'assurer ces fonctions :

a) Traducteurs NAT

Le Traducteurs NAT (Network Address Translator) masque les adresses privées de l'entreprise par une adresse publique. Il nécessite une machine possédant 2 interfaces réseau, l'une connectée à Internet et l'autre au réseau interne de l'entreprise.

Windows 2000 intègre cette fonction afin de pouvoir connecter un petit nombre de postes à Internet.

b) Serveurs proxy

Le serveur proxy travaille à un niveau supérieur du traducteur NAT, en effet il est mandataire des requêtes de ses clients. Il reçoit une demande d'accès à Internet, puis effectue la requête en son nom, puis renvoi le document à son client. Il est ainsi possible de restreindre l'accès à certains sites, ou de mettre en cache certaines pages fréquemment demandées afin de réduire la bande passante.

c) Pare-feu (Firewall)

Il permet de restreindre les communications entre le réseau interne d'une entreprise et Internet. Il est alors possible de bloquer certains ports en entrée ou en sortie (donc de bloquer les applications correspondantes).

5 Identification des concepts des serveurs Web

a) Définition d'un serveur Web

Un serveur Web est une machine qui va recevoir des requêtes (URL) de type HTTP ou HTTPS pour lesquelles elle va renvoyer les documents au format HTML correspondants.

b) Services IIS

Windows 2000 intègre IIS, qui comprend un certain nombre de fonctionnalités utiles dont les services d'indexation, le support de SSL ou les services Windows Media.