Guide d'implémentation du plan de mise en réseau Windows

Contenu

Introduction

Le terme « réseau » couvre une large gamme de technologies, qui, combinées, permettent à des ordinateurs de partager des données. Les composants de réseau peuvent être classés dans diverses catégories : applications pour système d'extrémité, systèmes d'exploitation de réseau, et équipements de réseau.

Un système d'exploitation de réseau est logiciel exécuté sur tous les systèmes interconnectés. Les exemples implémentation incluent de Novell NetWare, de Sun NFS (système de fichiers en réseau), AppleShare, et de Microsoft des Windows Networking généralement appelés de système d'exploitation de réseau. Des Windows Networking sont maintenant intensivement déployés avec des millions de Noeuds.

Ce guide de conception explique les concepts de base des Windows Networking et fournit la vue sur la façon dont concevoir des réseaux (des réseaux locaux et des WAN) au meilleur utilisent ce système d'exploitation. Le guide explique également des protocoles, nommer, et des problèmes d'échantillonnage associés avec des Windows Networking.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Quels sont des Windows Networking ?

Les Windows Networking se rapportent au système réseau partagé par le logiciel qui est livré avec tous les systèmes ou serveurs suivants d'exploitation Microsoft :

- Le LAN Manager de Microsoft
- MS-DOS avec le client du LAN Manager
- Windows pour des groupes de travail
- Windows 95, 98, et MOI
- Windows NT et 2000

Le LAN Manager de Microsoft, le client du LAN Manager pour le MS-DOS, et Windows NT 3.1 ne sont pas discutés dans ce document excepté dans un contexte historique.

Domaines contre des groupes de travail

Les Windows Networking ont trois concepts d'un groupe des groupes de travail relatifs d'ordinateurs, des domaines et d'une hiérarchie de domaine. Les groupes de travail peuvent être n'importe quelle collection logique d'ordinateurs ; n'importe quel ordinateur sur le réseau peut joindre un groupe de travail existant ou créer un neuf. Des entités plus formelles, des domaines sont créées et gérées par un processus du contrôleur principal de domaine (PDC) qui fonctionne sur un serveur de Windows NT ou de Windows 2000. Un domaine a la Sécurité et les propriétés administratives qu'un groupe de travail ne fait pas. Chaque domaine doit avoir au moins un NT ou 2000 serveurs, qui est responsable du processus PDC, des informations de compte utilisateur dans le domaine, et de la Sécurité dans le domaine. Les domaines de Windows Networking ne sont pas identiques que des noms de domaine Internet comme utilisés par le Système de noms de domaine (DNS). Une hiérarchie de hiérarchie de domaine ou de Répertoire actif est une collection de domaines organisés en rapports parent-enfant. Cette convention, présentée avec le Windows 2000, rechercher plus facile d'enables par des plusieurs domaines dans une requête simple (notamment). Cette hiérarchie trace étroitement à un espace de noms de DN.

Quel Protocol utilise-il ?

Avant le Windows 2000, les Windows Networking ont utilisé le protocole de Netbios pour le partage de fichier, l'imprimante partageant, la Messagerie, l'authentification, et la résolution de noms. Une installation pure de Windows 2000 exigerait Netbios seulement pour l'Interopérabilité avec des versions antérieures des Windows Networking utilisant l'espace de noms plat de Netbios. Netbios est un protocole de session-couche qui peut fonctionner sur l'un des après des protocoles de transport :

- NetBEUI (Netbios au-dessus de LLC2)
- NWLink (Netbios au-dessus d'Internetwork Packet Exchange [IPX])
- Netbios au-dessus du TCP (NBT)

Bien que Microsoft recommande que les clients utilisent seulement un protocole de transport à la fois pour des performances maximales, cette installation est seulement le par défaut pour le Windows 2000. Vous devriez sélectionner un protocole pour utiliser pour votre tout le réseau, de préférence TCP/IP, et puis arrêtez les autres protocoles parce que le service de nom NetBIOS met à jour des informations sur des noms de l'ordinateur (un espace de nom) séparément pour chaque transport. Les espaces de nom n'interagissent pas les uns avec les autres ; chaque transport fonctionne comme réseau indépendant.

NetBEUI (Netbios au-dessus de LLC2) est le moins extensible des trois protocoles parce qu'il doit pont. NetBEUI est inclus pour prendre en charge seulement des services très vieux (par exemple, de vieilles versions du LAN Manager). NetBEUI n'exige aucune configuration d'adresse du client. Il n'y a aucune limite fixe au nombre de clients Windows peut avoir avec NetBEUI, mais il est commun pour que cette solution rencontre des problèmes de performances car le nombre de clients à un seul groupe de ponts va au-dessus de 50 à 100 utilisateurs. La topologie et la confiance plates dans des émissions ne mesure pas, particulièrement quand le trafic doit traverser un lien WAN.

NWLink est recommandé seulement pour des réseaux exécutant déjà l'IPX qui ne peut pas être mis à jour pour utiliser le TCP/IP. Semblable à NetBEUI, NWLink n'a besoin d'aucune configuration d'adresse du client. NWLink utilise des paquets de type 20 IPX pour permuter l'enregistrement et les informations de navigation. Pour expédier les paquets IPX type-20 à travers des Routeurs de Cisco, vous devez configurer la **propagation IPX type-20** sur chaque interface sur chaque routeur sur votre réseau.

Il est recommandé pour utiliser Netbios au-dessus du TCP (NBT) pour la plupart des réseaux, ou lorsque le réseau inclut un WAN. Puisque NBT utilise le TCP/IP, chaque ordinateur doit être configuré pour utiliser une adresse IP statique, ou pour chercher une adresse IP dynamiquement avec le protocole DHCP (DHCP). Pour la facilité de l'administration réseau, il est fortement recommandé pour utiliser le DHCP ; pour la performance réseau optimale, il est fortement recommandé pour utiliser le serveur WINS a (service de nom de Windows Internet) aussi bien. Un serveur WINS permet à des clients pour obtenir les informations de navigation sans doit des demandes de diffusion chaque fois. Il y a une corrélation directe entre le nombre d'émissions dans un réseau et les performances du réseau ; les émissions sont nécessaires pour qu'un réseau fonctionne, mais les réduire peuvent être essentielles.

Cisco recommande que la plupart des clients utilisent le TCP/IP pour des Windows Networking. La partie de ce guide de conception se concentre sur des conceptions utilisant NBT.

Adressage IP dynamique

Quel est DHCP ?

S'adresser manuellement à des clients TCP/IP est coûteux en temps et sujet aux erreurs. Pour résoudre ce problème, l'Internet Engineering Task Force (IETF) a développé le DHCP, le protocole DHCP. Le DHCP est conçu pour fournir automatiquement à des clients une adresse IP valide et des informations de configuration associées (voyez les options DHCP de section ci-dessous). Chaque plage d'adresses qu'un serveur DHCP gère s'appelle une portée.

Portées de DHCP

Vous devez configurer une plage d'adresses pour chaque IP de sous-réseau où les clients demanderont une adresse DHCP ; chaque plage d'adresses s'appelle une portée de DHCP. Vous pouvez configurer un serveur DHCP pour servir plusieurs portées puisque le serveur DHCP ou les serveurs n'a pas besoin d'être physiquement connecté au même réseau que le client. Si le serveur DHCP est sur un IP de sous-réseau différent du client, alors vous devez utiliser le relais DHCP pour expédier des requêtes DHCP à votre serveur DHCP.

Relais DHCP

Le relais DHCP fonctionne typiquement sur un routeur et le support de relais est disponible sur la version 4.0 et le Windows 2000 Server de serveur de Windows NT. Sur des Routeurs de gamme Cisco 700, vous pouvez activer le relais DHCP avec la commande de **relais DHCP de positionnement**. Vous pouvez activer le relais DHCP sur un routeur Cisco IOS en configurant le **helper-address d'IP** avec l'adresse du serveur DHCP sur chaque interface qui aura des clients DHCP. La commande de **helper-address d'IP** en avant beaucoup l'autre IP des paquets annonce, y compris de DN, de Protocole TFTP (Trivial File Transfer Protocol), et de nom NetBIOS service. Pour expédier seulement des requêtes DHCP, voyez l'exemple de configuration suivant. Le pour en savoir plus, voient « configurer l'émission traitant » la section dans les protocoles réseau guide de configuration, la partie I.

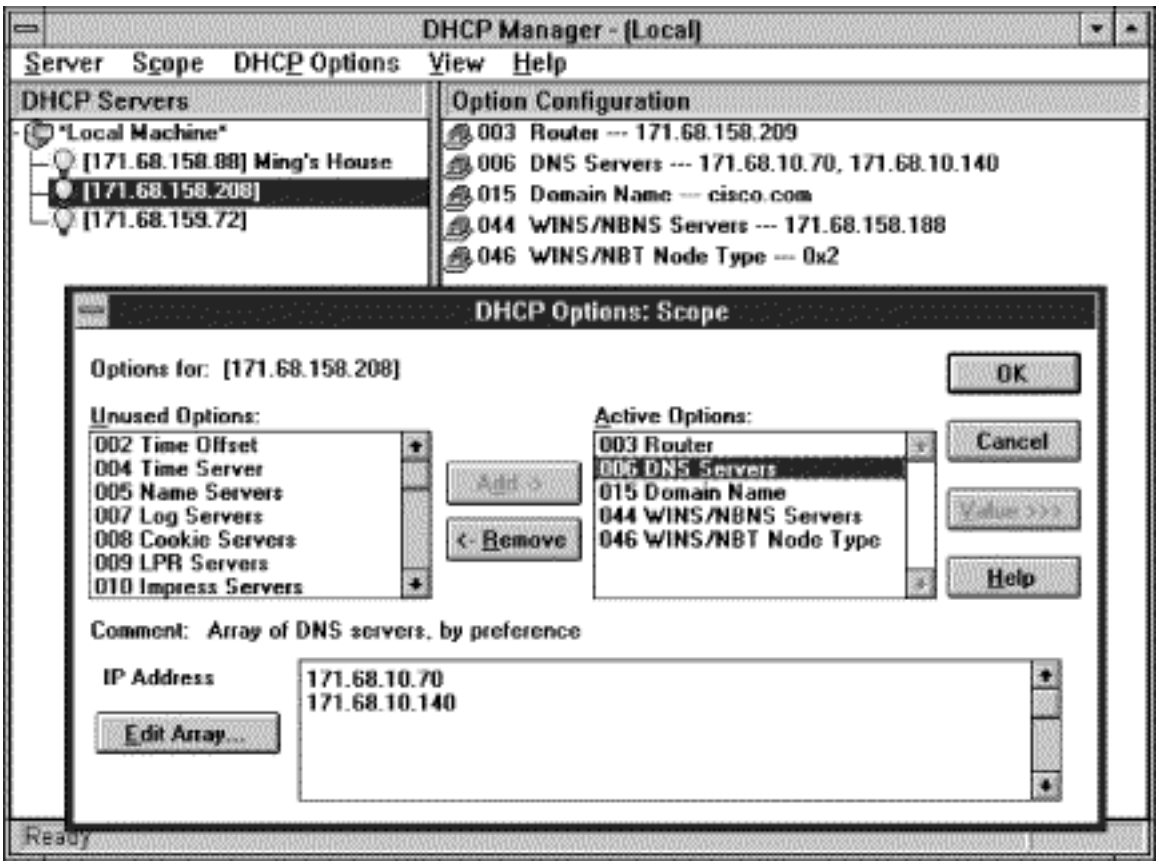
```
no ip forward-protocol udp tftp

no ip forward-protocol udp dns

no ip forward-protocol udp time

no ip forward-protocol udp netbios-ns

no ip forward-protocol udp netbios-dgm

no ip forward-protocol udp tacacs

ip forward-protocol udp bootpc

!

interface ethernet 0

ip helper-address 172.16.12.15

interface ethernet 1

ip helper-address 172.16.12.15
```

Options DHCP

En plus de son adresse IP, un DHCP Client peut obtenir d'autres informations de configuration TCP/IP d'un serveur DHCP, y compris le masque de sous-réseau, la passerelle par défaut, et

l'information DNS. Ces informations, appelées les options DHCP, peuvent être configurées dans le gestionnaire DHCP sur votre Windows NT ou serveur DHCP de Windows 2000.

Figure 1 : Gestionnaire DHCP de Microsoft



Si vos clients utilisent le service de nom de Windows Internet (WINS) pour la résolution de noms (discutée plus tard), vous devriez configurer l'adresse du serveur WINS et du type de noeud de WINS. Une brève liste de types de noeud est incluse dans la section de « résolution de noms ». Le p-noeud de type de noeud (**0x2**) est fortement recommandé.

Serveurs DHCP de Cisco

Cisco a actuellement un DHCP et un serveur DNS intégrés pour Windows NT, le Windows 2000 et l'UNIX ; le serveur a une interface graphique, le soutien de l'adressage secondaire, et beaucoup d'autres fonctionnalités de l'édition Enterprise. Les Routeurs de gamme Cisco 700 (dans la version 4.1 et ultérieures) et les routeurs Cisco IOS (dans la version 11.2(7)F et ultérieures) incluent également un serveur DHCP qui peut assigner des adresses sur des segments de réseau local. Les deux styles de routeur incluent le réseau et la traduction d'adresses niveau du port.

Résolution de noms

La résolution de noms est le processus d'associer un nom commode, tel que FRED ou fred.domain.com, avec une adresse réseau (souvent une adresse IP). Pour les buts actuels, cette discussion s'applique à la manière que les Windows Networking résolvent un seul nom de poste de travail de Netbios (décrit comme *WORKSTATION<00>* dans une section postérieure) à une adresse IP. Ce processus ne devrait pas être confondu avec le processus connexe mais différent du furetage (qui utilise d'autres types de noms NetBIOS). En date de la release du Microsoft Windows 2000, les clients de Windows Networking utilisent jusqu'à cinq méthodes de résolution

de noms :

- Cache de nom NetBIOS
- Émissions d'IP de sous-réseau
- LMHOSTS
- WINS
- DN d'Internet

Cache de nom NetBIOS

Les Windows Networking gardent un petit cache de noms NetBIOS utilisés récemment aux mappages d'adresse IP. Ces entrées sont ajoutées après résolution de noms réussie et puis sont retirées après une certaine période. Des entrées supplémentaires peuvent être préchargées au démarrage du système et à la constante faite en créant une entrée dans le fichier lmhosts avec la balise #PRE (voyez la section LMHOSTS ci-dessous).

Émissions d'IP de sous-réseau

Des émissions d'IP de sous-réseau peuvent être utilisées pour la résolution de noms. Des émissions sont reçues par tous les ordinateurs sur un sous-réseau, ayant besoin de le temps de traitement à chaque ordinateur. Les Windows Networking mettent à jour également un maître de navigation indiqué qui met à jour une liste de toutes les ressources disponibles sur un sous-réseau. Un processus d'élection qui utilise des émissions détermine ce maître de navigation parce que les enregistrements, les élections de navigateur, et les requêtes de noms pourraient tout générer des émissions, utilisation de la méthode de résolution de nom de diffusion n'est pas recommandé.

LMHOSTS

Les Windows Networking peuvent consulter une table statique dans un fichier appelé le LMHOSTS. Pour utiliser cette méthode, le PDC devrait mettre à jour au moins une liste statique de tous les ordinateurs et de leurs adresses IP dans ce domaine et les noms et adresse du PDCs pour tous autres domaines dans le réseau. Tous les clients doivent alors avoir un fichier lmhosts avec l'adresse IP de leur PDC et le chemin au fichier lmhosts principal sur le PDC.

Service de nom de Windows Internet

Des WINS ont été créés pour permettre à des clients sur différents sous-réseaux IP pour résoudre dynamiquement des adresses, s'enregistrer, et parcourir le réseau sans envoyer annonce. Les clients envoient des paquets monodiffusions au serveur WINS à une adresse connue. Pour la compatibilité avec des clients plus âgés de réseau Microsoft, cependant, la résolution de nom de diffusion est encore activée par défaut, même lorsque des WINS sont également configurés.

Pour répéter ce qui a été énoncé ci-dessus, il est fortement recommandé pour que la performance réseau optimale utilise des WINS. De nouveau, il y a une corrélation directe entre le nombre d'émissions dans un réseau et les performances du réseau ; les émissions sont nécessaires pour qu'un réseau fonctionne, mais les réduire peuvent être essentielles.

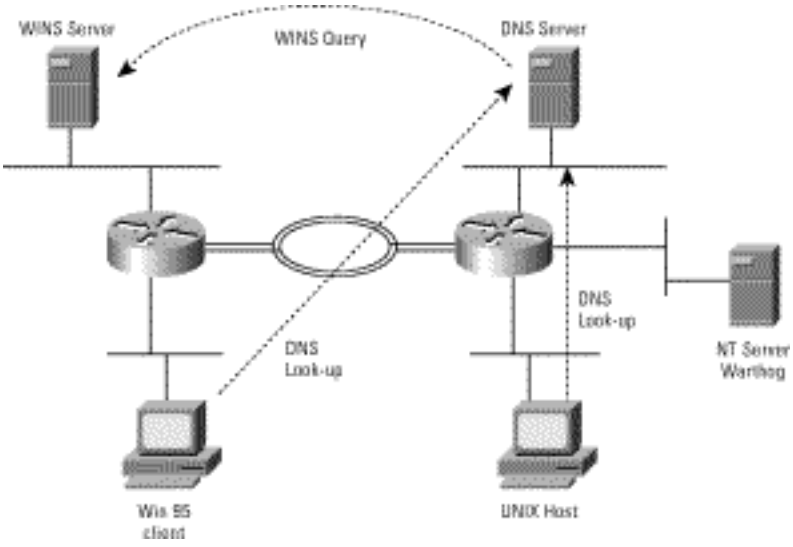
DN d'Internet

N'importe quel serveur DNS peut être configuré statiquement pour répondre à des requêtes pour des ordinateurs avec des adresses IP fixes. Ce scénario est utile si les ordinateurs en réseau ont des adresses IP fixes. Quand les systèmes Windows emploient le DHCP pour obtenir une adresse IP et des WINS pour inscrire un nom NetBIOS, vous pouvez installer un serveur DNS de Windows pour questionner un serveur WINS pour les noms ou les adresses qui n'ont pas été introduits statiquement. Dans des les deux cas, les systèmes de Windows et de non-Windows peuvent résoudre des adresses IP correctement.

Si un administrateur configure chaque serveur de Windows Networking avec une adresse IP statique, il peut être commode de présenter chaque serveur dans le système DNS et d'utiliser des DN pour la résolution de noms. De temps en temps (par exemple, en utilisant une liaison de numérotation à la demande) il est commode d'enregistrer des clients avec des WINS et de faire des requêtes avec des DN. La Microsoft NT 3.51 kits de ressources, serveur et Windows 2000 tous de Windows NT 4.0 incluent un serveur DNS qui peut répondre à des requêtes DNS en questionnant un serveur WINS à l'arrière-plan. Pour plus d'informations sur la façon configurer cette architecture, voir l'annexe R.

Avec le Windows 2000, des serveurs DNS peuvent également être dynamiquement configurés avec l'adresse aux mappages de noms. Les clients DHCP, les serveurs DHCP et les serveurs DNS dynamiques travaillent ensemble pour mettre à jour le nom aux reproductions d'adresses dans le serveur DNS. Le serveur DHCP exécutera cette mise à jour pour non-Windows 2000 clients DHCP.

Figure 2 : Les systèmes chacun des deux de Windows et de non-Windows envoient des consultations de DN pour Warthog Désignée serveuse windows nt. Le serveur DNS n'a pas une entrée pour la phacochère, ainsi elle questionne le serveur WINS et renvoie l'adresse IP.



Ordre de recherche des noms

Les composants de Windows Networking envoie des requêtes de résolution de noms dans une commande différente, selon le type de noeud de Netbios. Si le système est Windows NT 4.0 et le nom est plus long que 15 caractères, alors Windows NT envoie seulement une requête DNS. D'autres composants réseau et services peuvent également utiliser une commande différente selon l'API appelé pour exécuter la résolution de noms. Par exemple, une application de sockets appelle le gethostbyname() utilisera des DN pour la résolution de noms d'abord. Autrement la recherche de noms est effectuée dans l'ordre suivant :

- Vérifiez le cache de nom NetBIOS.

- Envoyez une requête d'émission ou un nom de requête de WINS, selon le type de noeud en cours de Netbios.
- Vérifiez le fichier lmhosts.
- Vérifiez le fichier HOSTS (si la « résolution utilisant des DN » est vérifiée).
- Envoyez une requête DNS d'Internet (si la résolution utilisant des DN est vérifiée).

Tableau 1 : Des noms NetBIOS sont recherchés différemment ont basé sur le type de noeud de Netbios

Type de noeud de Netbios	Ordre de recherche des noms
b-noeud (**0x1**)	Émission seulement
p-noeud (**0x2**)	WINS seulement
m-noeud (**0x4**)	Émission, puis WINS
h-noeud (**0x8**)	Les WINS, ont alors annoncé

Le RÉSEAU LOCAL de Microsoft entretient le navigateur

Des Windows Networking ont été initialement conçus pour fonctionner sur un segment de LAN unique ou un réseau traversier (d'appartement). À ce moment-là, seulement le protocole netbeui a été pris en charge.

Microsoft a développé le navigateur de services de RÉSEAU LOCAL pour permettre à l'utilisateur de parcourir une liste de tous les ordinateurs disponibles sur le réseau. Chaque client de Windows Networking a inscrit son nom NetBIOS périodiquement en envoyant des émissions.

Chaque ordinateur a dû également envoyer des émissions pour élire un maître de navigation pour le réseau. Le maître de navigation (et plusieurs maître de navigation de sauvegarde) ont mis à jour la liste d'ordinateurs et de leurs adresses. Quand un utilisateur a parcouru le réseau, le client a envoyé une demande de diffusion et un des maître de navigation a répondu.

Par la suite Microsoft a ajouté le soutien de Netbios au-dessus d'IPX et de NetBIOS sur TCP/IP, mais les Windows Networking supposaient toujours que tous les clients et serveurs étaient sur le même réseau logique ou l'IP de sous-réseau IPX------ils envoyaient toujours des émissions pour enregistrer et trouver des ordinateurs sur le réseau.

Cette architecture, bien que simple pour implémenter, généré une énorme charge sur le réseau et sur la CPU de chaque client sur le réseau. En raison de ces problèmes d'évolutivité, Microsoft a commencé à offrir d'autres méthodes de furetage et de résolution de noms------manières pour que les clients tracent un nom à l'adresse IP d'autres ordinateurs sur le réseau. Par la suite Microsoft a également fourni une manière de parcourir et de résoudre des noms sans émissions.

Le reste de cette section explique comment le furetage fonctionne dans divers environnements. La section précédente expliquée comment différents noms NetBIOS sont résolus. Ces deux activités sont semblables mais distinctes. Les utilisateurs parcourent le réseau en ouvrant le voisinage réseau, utilisant la commande nette de vue, ou se connecter dans un domaine Windows NT au startup. La résolution de noms est le processus de résoudre des noms précédemment connus, ou fondez en parcourant. Veuillez noter que cette discussion est indépendante des navigateurs Web.

Noms NetBIOS

Les noms NetBIOS sont 15-character, les noms majuscules qui ont un identifiant spécial ajouté au 16ème octet. Aussi bien, les noms NetBIOS peuvent s'appliquer à une adresse IP simple (seule), ou à plus d'une (groupe). Quelques types de nom peuvent être noms de seuls ou de groupe. Une partie du plus commun de ces derniers caractères est répertoriée comme suit (toutes les valeurs sont dans l'hexadécimal) :

Tableau 2 : Un Tableau partiel des noms NetBIOS spéciaux et de leurs descriptions

Noms spéciaux inscrits	Description
Noms d'utilisateur	
<USERNAME><00>	Utilisé pour inscrire le nom de l'utilisateur actuellement ouvert une session dans la base de données de WINS, de sorte que les utilisateurs puissent recevoir le **net envoient des** commandes envoyées à leurs noms d'utilisateur.
Noms de l'ordinateur	
<COMPUTER><00>	Utilisé par des postes de travail de réseau Microsoft pour recevoir des demandes de mailslot de deuxième classe. Tous les postes de travail doivent ajouter ce nom afin de recevoir des demandes de mailslot. C'est le nom de l'ordinateur inscrit aux services de poste de travail par un client de WINS.
<COMPUTER><03>	Utilisé comme nom de l'ordinateur qui est inscrit au service de messagerie sur un ordinateur qui est un client de WINS.
<COMPUTER><20>	Utilisé comme nom qui est inscrit au service de serveur de pair sur un ordinateur de Windows 95 (ou au service de serveur sur un ordinateur de Windows NT) qui est un client de WINS.
<COMPUTER><Be>	Utilisé comme nom unique qui est inscrit quand l'agent de supervision du réseau est commencé sur l'ordinateur.
<COMPUTER><Bf>	Utilisé comme nom de groupe qui est inscrit quand l'agent de supervision du réseau est commencé sur l'ordinateur. Si ce nom n'est pas 15 caractères de longueur, il est complété avec (+) des symboles plus.
<COMPUTER><1f>	Utilisé comme nom unique qui est inscrit à d'échange de données dynamique de réseau (DDE) quand le service de NetDDE est commencé sur

	l'ordinateur.
Noms de groupe	
<01><02>MSBROWSE<02><01>	Utilisé par des serveurs du navigateur principal pour annoncer périodiquement leur domaine sur un sous-réseau local. Cette annonce contient le nom de domaine et le nom du serveur du navigateur principal pour le domaine. En outre, les serveurs du navigateur principal reçoivent ces annonces de domaine à ce nom et les mettent à jour dans leur interne parcourent la liste avec le nom de l'ordinateur de l'annonceur.
<DOMAIN><00>	Utilisé par des serveurs et station de travail aux annonces de serveur de processus pour prendre en charge le LAN Manager de Microsoft. Les serveurs exécutant le Windows 95, le Windows NT, serveur windows nt, et Windows pour des groupes de travail n'annoncent pas ce nom à moins que l'option de LMAnnounce soit activée dans les propriétés de serveur.
<DOMAIN><1b>	Utilisé pour identifier le nom de navigateur principal du domaine, qui est un nom unique que seulement le contrôleur principal de domaine (PDC) peut ajouter. Le PDC traite des demandes de GetBrowserServerList sur ce nom. Les WINS supposent que l'ordinateur qui enregistre un nom de domaine avec le caractère <1b> est le PDC.
<DOMAIN><1c>	Utilisé pour le nom de groupe d'Internet, que les contrôleurs de domaine inscrivent. Le nom de groupe Internet est une liste dynamique de jusqu'à 25 ordinateurs qui ont inscrit le nom. C'est le nom utilisé pour trouver un ordinateur de Windows NT pour l'authentification d'intercommunication.
<DOMAIN><1d>	Utilisé pour identifier un navigateur principal (pas un navigateur principal du domaine). Le navigateur principal ajoute ce nom comme seul nom NetBIOS quand il commence. Les postes de travail annoncent que leur présence à ce nom de sorte que les navigateurs principaux puissent construire le leur parcouriez la liste.

	Pour des groupes de travail, ce nom a la forme <WORKGROUP><1d>.
<DOMAIN><1e>	Utilisé pour tout le groupe de travail ou annonces de la taille du domaine par des serveurs de navigateur dans un groupe de travail de réseau Windows ou un domaine serveur windows nt. Ce nom est ajouté par tous les serveurs de navigateur et serveurs potentiels dans le groupe de travail ou le domaine. Tous les paquets d'élection de navigateur sont envoyés à ce nom. Pour des groupes de travail, ce nom a la forme <WORKGROUP><1e>.

Le processus de démarrage

Sur le startup, n'importe quel système en réseau envoie une gamme de paquets pour découvrir des adresses réseau, pour s'enregistrer, pour s'authentifier, et pour découvrir des services. Les systèmes de Windows Networking qui se connectent dans un domaine Windows NT doivent entrer en contact avec un contrôleur de domaine pour authentifier. Ce processus utilise la résolution de noms et le furetage.

D'abord le système de démarrage doit enregistrer un nom de l'ordinateur (*WORKSTATION<00>*). Si le paramètre de LMAnnounce est allumé (pour la compatibilité avec des serveurs du LAN Manager), alors le système enregistre également *DOMAIN<00>*. Ensuite le système localise un contrôleur de domaine pour le domaine de procédure de connexion près d'essayer pour résoudre *DOMAIN<1C>*. Avant le Windows 2000, ceci a fonctionné seulement avec l'émission, LMHOSTS, ou GAGNE des méthodes de résolution de noms. Avec le Windows 2000, des DN est essayés d'abord. Ensuite, le système ouvre une session au contrôleur de domaine utilisant les messages basés sur Netbios de mailslot, qui sont envoyés sur le port 138 de Protocole UDP (User Datagram Protocol). En conclusion, après que la procédure de connexion soit réussie, le système enregistre l'utilisateur que qui a ouvert une session (*USERNAME<03>*) ainsi le service de messagerie peut trouver cet utilisateur.

Trouver un ordinateur

Quand demandes d'utilisateur une ressource sur un ordinateur de nom (par exemple : **\ net d'utilisation \ Fred \ someshare**, ou découvertes FRED), les tentatives de système local de résoudre le nom de l'ordinateur. Cette requête est pour un seul nom NetBIOS du type <00>, ou les DN ou l'entrée de fichier HOSTS.

Visionnement du voisinage réseau

Quand un utilisateur ouvre le voisinage réseau pour demander une liste de domaines, le système tentera d'obtenir une liste de navigateurs de sauvegarde, la radiodiffusion au nom du navigateur principal, ou en se connectant directement au navigateur principal du domaine (ou chacun des deux). Une fois une liste de navigateurs de sauvegarde est récupérée, le système choisira un navigateur de sauvegarde, se connecte à ce système et récupère la liste de domaines. Des demandes ultérieures pour des serveurs dans un domaine sont expédiées au même navigateur de sauvegarde.

Sous-réseau parcourant

Pendant les années 1980, la plupart des réseaux étaient « plats, » ou ont eu seulement quelques sous-réseaux. NetBEUI et NWLink utilisent ce modèle, et des émissions IP peuvent pont ou aidées à travers un nombre restreint de sous-réseaux. La discussion suivante assume le cas d'un réseau linéaire.

Chaque sous-réseau a un navigateur principal de sous-réseau par domaine ou le groupe de travail et peut avoir quelques navigateurs de sauvegarde de sous-réseau (également par domaine ou groupe de travail). Après démarrage, les navigateurs de sauvegarde et les nonbrowsers envoient des annonces par radio à intervalles croissants de 1, 2, 4, et 8 minutes ; ils par la suite annonces par radio seulement toutes les 12 minutes. Les navigateurs principaux de sous-réseau écoutent ces annonces pour établir une liste de furetage.

Les navigateurs principaux et les navigateurs de sauvegarde de sous-réseau sont responsables de la réponse parcourent des requêtes à partir d'autres ordinateurs. Les navigateurs principaux peuvent répondre à ces demandes directement de la liste de furetage. Les navigateurs de sauvegarde gardent également une liste de furetage, qu'ils demandent au navigateur principal de sous-réseau toutes les 15 minutes.

Émission parcourant à travers des sous-réseaux

En réalité, la plupart des réseaux ont aujourd'hui plusieurs sous-réseaux. De domaines les sous-réseaux d'envergure souvent et les sous-réseaux contiennent parfois des systèmes dans plus d'un domaine. Le logiciel navigateur sur quelques systèmes peut communiquer avec un navigateur principal du domaine (habituellement le PDC) pour permuter parcourent des listes de beaucoup de sous-réseaux, mais il doit connaître l'adresse de monodiffusion du navigateur principal du domaine. Un navigateur principal de sous-réseau peut obtenir l'adresse de monodiffusion du PDC à partir d'un fichier lmhosts (pour une description détaillée, voyez la section de résolution de noms) ou des WINS (voir la section suivante).

LMHOSTS est un fichier texte que le logiciel navigateur peut lire pour trouver l'adresse de monodiffusion d'un PDC. Un échantillon suit. Est d'abord l'adresse IP d'unicast du PDC, ensuite le nom NetBIOS du PDC (**ENG_PDC**), une balise qui enregistre cette ligne dans le cache de nom NetBIOS, (**#PRE**) et en conclusion, une balise qui marque ce système comme contrôleur de domaine pour le domaine ANGLAIS (**#DOM**).

```
10.1.3.4 ENG_PDC #PRE #DOM:eng
```

Quand un navigateur principal de sous-réseau connaît l'adresse de monodiffusion du navigateur principal du domaine, l'échange de navigateurs parcourent des listes toutes les 15 minutes (utilisant des paquets d'unicast sur IP). Puisqu'un navigateur principal est consulté, les clients peuvent parcourir seulement les domaines qui ont un système sur le sous-réseau local (un navigateur principal de sous-réseau). Dans la pratique, ce scénario fonctionne assez bien pour trouver un serveur de procédure de connexion au startup, mais ne permet pas à des utilisateurs pour parcourir utilisant le voisinage réseau.

L'information importante : En raison d'une bogue dans quelques versions de Windows pour les groupes de travail 3.11 et le Windows 95, ces systèmes ne peuvent pas fonctionner comme navigateur principal ou navigateur de sauvegarde de sous-réseau. La bogue empêche le navigateur de sous-réseau de contacter le navigateur principal du domaine. Cette bogue a été réparée dans le Windows 95 OSR (lancement du service OEM) 2. en conséquence, parcourant sur le sous-réseau échoue s'il y a Win31 ou maître ou navigateurs de sauvegarde de Win95 sur le

sous-réseau.

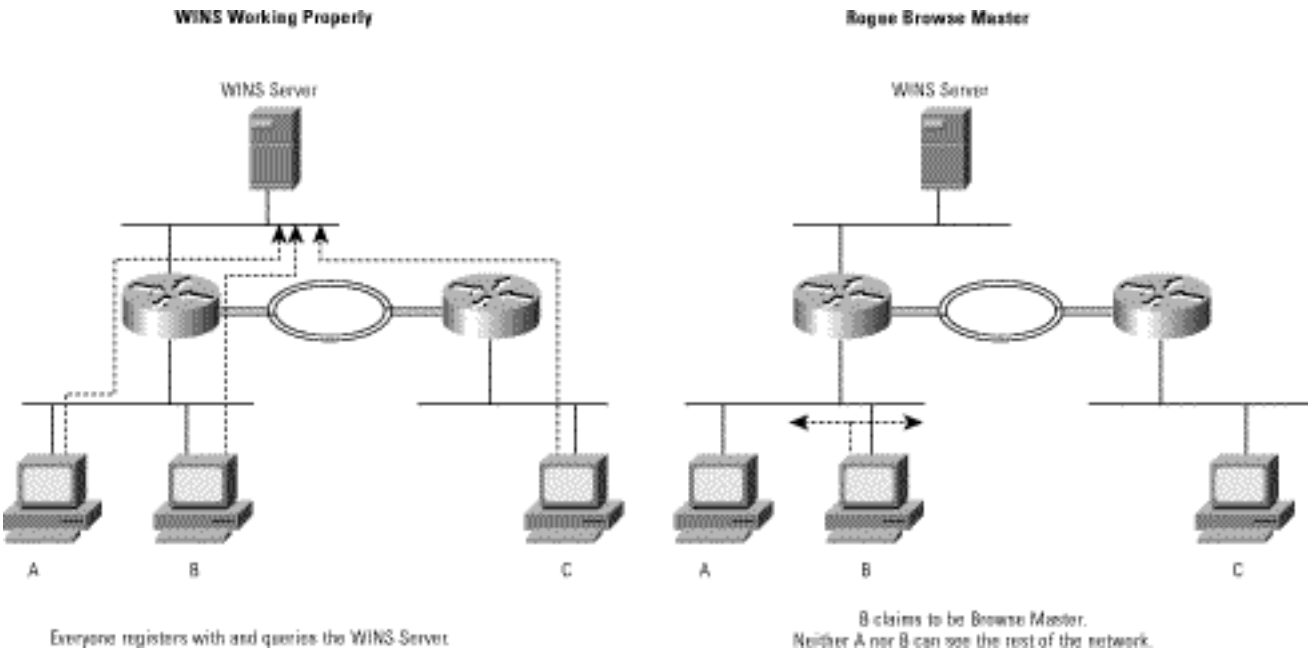
Furetage de tout domaine avec des WINS

Dans une organisation avec plusieurs domaines, il n'est pas raisonnable à l'architecte qu'un réseau a basé sur les restrictions a tracé les grandes lignes dans la section précédente. Quand les WINS s'exécutent, le navigateur de sous-réseau peut être un client de WINS et peut obtenir l'adresse IP d'unicast du navigateur principal du domaine (le PDC) pour n'importe quel domaine. Cependant, des émissions sont encore envoyées fréquemment et à plusieurs reprises par défaut (voyez que la table décrivant le noeud de WINS saisit la section suivante) sur l'occasion qu'il peut y avoir des clients de quelques non-WINS sur le sous-réseau. La meilleure solution dans la plupart des réseaux est d'arrêter l'émission parcourant.

Arrêter des émissions

Le défi important en arrêtant des émissions évite les maître de navigation escrocs, qui entraînent le ravage sur un sous-réseau parce qu'ils perturbent le processus de furetage.

Figure 3 : Maître de navigation escroc



Vous pouvez désactiver la résolution de nom de diffusion en plaçant le BrowseMaster plaçant avez désactivé. Dans Windows pour les groupes de travail 3.11, des émissions sont arrêtées en ajoutant une commande au fichier SYSTEM.INI. (Voir l'annexe B pour des détails.) Dans Windows 95/98, la configuration de BrowseMaster dans le fichier avancé et la copie partageant Properties doivent être placées handicapée. Dans Windows NT, il n'est pas nécessaire d'arrêter le furetage dans la plupart des cas, bien qu'il puisse être desirable. Dans Windows NT, placez le **Hkey_local_machine \ système \ CurrentControlSet \ services ** clé de registre de **navigateur \ paramètres \ MaintainServerList** non aux administrateurs peut contrôler des émissions envoyées par des clients DHCP en sélectionnant le type de noeud approprié de WINS (p-noeud : **0x2**). Une liste complète de types de noeud de WINS suit.

Tableau 3 : Liste de types de noeud de WINS

Type de noeud de WINS	Ordre de recherche des noms
b-noeud (**0x1**)	Émission seulement

p-noeud (**0x2**)	WINS seulement
m-noeud (**0x4**)	Émission, puis WINS
h-noeud (**0x8**)	Les WINS, ont alors annoncé

Évolution aux réseaux plus vastes

Domaines de confiance

En prévoyant un réseau Windows, considération de quel modèle de domaine utiliser est important. Les paragraphes suivants discutent les avantages et les inconvénients de plusieurs modèles de domaine. Si vous avez plusieurs domaines, vous voulez probablement aux données d'échange avec d'autres domaines dans votre réseau. Les relations de confiance sont une manière de gagner ou accès de concession à un domaine sans devoir gérer chaque utilisateur individuellement. Chaque relations permettent la confiance dans une direction seulement. Le pour en savoir plus, voient le *kit de ressources de serveur de Windows NT 4.0*, le volume 2, le chapitre 4.

Domaine simple

Ce modèle de domaine est le plus simple------le réseau a seulement un domaine. Cette installation fonctionne pour de petites ou moyennes installations sans WAN.

Global Trust

Conçue pour des sociétés sans administratif central ou EST l'organisation, il est le plus facile comprendre le modèle global de confiance et le plus difficile à gérer. Chaque domaine fait confiance à chaque autre domaine.

Domaine principal

Dans ce modèle, un domaine principal est de confiance par tous autres domaines, mais le domaine principal ne fait confiance à personne. Cette option est salutaire quand les services ou les divisions veulent le contrôle administratif au-dessus de leurs propres services, mais veut toujours authentifier centralement.

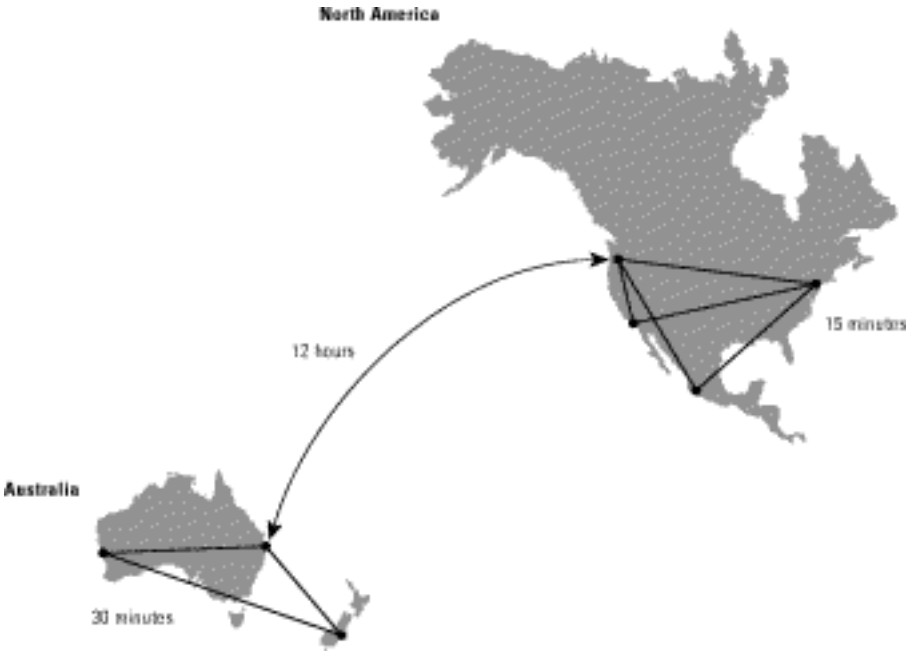
Plusieurs domaines principaux

Ce modèle est conçu pour être une plus grande version du modèle de domaine principal. Plusieurs domaines principaux toute la confiance, et chacun des domaines principaux est consécutivement faits confiance par chaque domaine départemental.

Répliquer des WINS

Pour la Redondance ou il est desirable d'optimiser le trafic BLÊME, parfois ayant plusieurs serveurs WINS. Les serveurs de Windows NT et de Windows 2000 peuvent répliquer ou resynchroniser des bases de données de WINS dans l'un ou l'autre ou les deux directions. Dans la figure 4, une grande société multinationale a plusieurs serveurs WINS distribués, ainsi GAGNE des requêtes ne doivent pas voyager à travers des continents.

Figure 4 : Exemple d'une configuration au niveau de l'entreprise pour la réplication de WINS



Accès par modem

Windows NT et Windows 2000 été livré avec le Remote Access Server de Microsoft (RAS), qui utilise le Protocole point à point (PPP). Les clients peuvent vouloir utiliser des serveurs d'accès Cisco au lieu du NT RASs pour leurs groupes d'accès distant en raison de la densité et de la représentation meilleures d'accès distant disponibles sur des serveurs d'accès Cisco.

Windows prend en charge le TCP/IP, l'IPX, et le NetBEUI (protocole de contrôle IP [IPCP], protocole de contrôle IPX [IPXCP], et protocoles de contrôle de Control Protocol de vues de Netbios [NBFCP] pour le PPP). NetBEUI cadran-dans le support a été ajouté au logiciel de Cisco IOS dans la version 11.1. Pour NetBEUI connectez-vous, utilisez la commande de **netbios nbf** (suivant les indications de l'exemple suivant) sur chaque interface asynchrone ou sur une interface asynchrone du groupe sur le serveur d'accès.

Ethernets 0 d'interface

netbios nbf

group-async 0 d'interface

group-range 1 16

netbios nbf

Pour configurer l'IPX connectez-vous, utilisez la commande d'**ipx ppp-client** (suivant les indications de l'exemple suivant) sur chaque interface asynchrone ou sur une interface asynchrone du groupe sur le serveur d'accès. Cette commande exige de vous de configurer une adresse de réseau IPX sur une interface de bouclage. Les clients entrant n'ont pas besoin d'entendre des messages de Protocol de publicité de service (SAP), ainsi ces messages devraient être arrêtés avec la commande du SAP-**intervalle 0 IPX**.

```
Interface loopback 0
```

```
ipx network <network number> interface group-async 0 group-range 1 16 ipx ppp-client loopback 0
ipx sap-interval 0
```

Afin d'assigner des adresses IP aux clients entrant, les serveurs d'accès Cisco peuvent utiliser un groupe d'adresses locales ou agir en tant que proxy pour un serveur DHCP. Le serveur d'accès demande une adresse du serveur DHCP et les utilisations qui adressent pendant la négociation PPP. Le client peut également négocier l'adresse de son serveur WINS.

```
ip dhcp-server n.n.n.n async-bootp nbns-server m.m.m.m async-bootp dns-serverp.p.p.p ip address-
pool dhcp-proxy-client ! interface group-async 0 group-range 1 16 peer default ip address dhcp
```

Routage à établissement de connexion à la demande

Le Routage à établissement de connexion à la demande (DDR) fournit des connexions réseau à travers le réseau téléphonique public commuté (PSTN). Traditionnellement, les connexions WAN ont été des liaisons louées dédiées. Le DDR fournit les connexions réseau à faible volume et périodiques, permettant des services sur demande et des coûts du réseau décroissants. Integrated Services Digital Network (le RNIS) est une technologie avec commutation à circuit. Comme le réseau téléphonique de téléphone analogique, des connexions RNIS sont établies seulement quand il y a un besoin de communiquer.

Les Routeurs de Cisco emploient le DDR pour déterminer quand un rapport doit être établi à un autre site. Des paquets sont classifiés en tant qu'intéressant ou inintéressant, basé sur des Listes d'accès de Protocol-particularité et des listes d'appels. Les paquets inintéressants peuvent voyager à travers un lien actif DDR, mais ils n'évoquent pas le lien, ni ils gardent le lien.

Windows pour des groupes de travail et Windows 95/98 client avec lesquels les fichiers partagés ou les imprimantes s'enregistrent eux-mêmes GAGNE toutes les douze ou quinze minutes en envoyant un paquet monodiffusion au serveur WINS (sur le port de service de nom NetBIOS de port UDP 137---the).

Les systèmes de Windows NT peuvent également envoyer un grand choix d'autres paquets périodiques, qui peuvent entraîner des coûts BLÊMES élevés. Ces paquets périodiques incluent la synchronisation de navigateur, la réplication de WINS, la réplication, l'imprimante parcourant, et le DHCP SAM (base de données de compte utilisateur). Beaucoup de ces services ont des clés de registre qui peuvent être accordées pour apporter à la connexion de Connexion à la demande moins fréquemment. Le pour en savoir plus, voient la *base de connaissances de Microsoft*, article : Q134985. Les importantes entrées dans le registre incluent :

Hkey_local_machine \ système \ CurrentControlSet \ services \ navigateur \ paramètres \ MasterPeriodicity

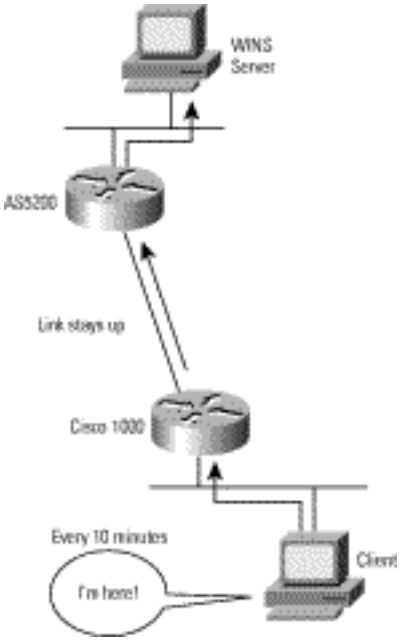
Hkey_local_machine \ système \ CurrentControlSet \ services \ navigateur \ paramètres \ BackupPeriodicity

Hkey_local_machine \ système \ CurrentControlSet \ services \ Replicator \ intervalle

Hkey_local_machine \ système \ CurrentControlSet \ services \ Netlogon \ PulseMaximum

Hkey_local_machine \ système \ CurrentControlSet \ services \ contrôle \ copie \ DisableServerThread

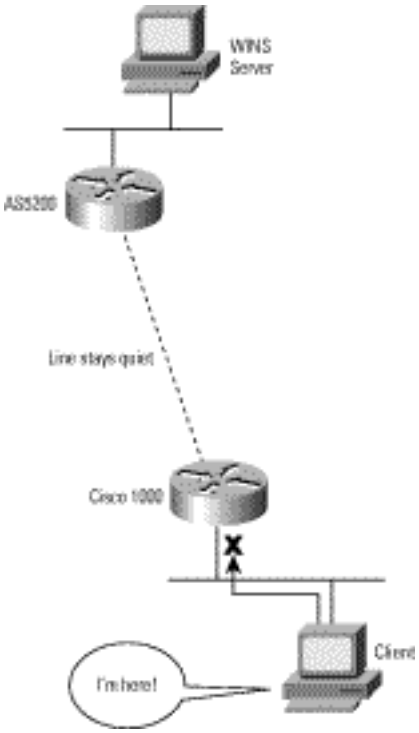
Figure 5 : Liaison de numérotation à la demande tout le temps



L'envoi d'un paquet au serveur WINS évoque normalement la liaison de numérotation à la demande. Si, cependant, ce port est classifié comme inintéressant au logiciel de Cisco IOS, alors le routeur ni n'évoque ni maintient le lien.

```
Interface bri 0

dialer-group 1 ! dialer-list 1 protocol ip list 101 access-list 101 deny udp any any eq netbios-
ns access-list 101 permit ip any any
```

Figure 6 : Le port UDP 137 est inintéressant, lien est vers le bas



Les filtres pour la gamme Cisco 700 sont disponibles dans la version 4.1(2). Un filtre d'exemple pour rendre le trafic SAM de Windows NT inintéressant suit :

```
SET netbsp OFFSET 2 FROM TCPHDR PATTERN 00 8b

SET netbnsp OFFSET 2 FROM UDPHDR PATTERN 00 89
```

```
SET netbdgp OFFSET 2 FROM UDPHDR PATTERN 00 8a

SET refresh OFFSET 10 FROM UDPHDR PATTERN 40 00

SET netbsm OFFSET 20 FROM TCPHDR PATTERN 00

SET smb OFFSET 24 FROM TCPHDR PATTERN ff 53 4d 42

SET tcppat2 OFFSET 13 FROM TCPHDR PATTERN 02

SET netbsr OFFSET 20 FROM TCPHDR PATTERN 81

SET keepali OFFSET 20 FROM TCPHDR PATTERN 85

SET tcpres OFFSET 13 FROM TCPHDR PATTERN 04
```

SET IP FILTER OUT netbnsp refresh IGNORE SET IP FILTER OUT netbdgp IGNORE SET IP FILTER OUT netbsp netbsm smb IGNORE SET IP FILTER OUT netbsp tcppat2 IGNORE SET IP FILTER OUT netbsp tcpres IGNORE SET IP FILTER OUT netbsp netbsr IGNORE SET IP FILTER OUT netbsp keepali IGNORE

Accès par RNIS

Cette section couvre les cartes RNIS et les adaptateurs de terminal (TAS). Pour des informations sur utiliser des Windows Networking avec des Routeurs RNIS, voyez la section précédente sur le routage de Connexion à la demande.

Adtran

Puisqu'Adtran et Cisco ont fonctionné étroitement pendant le test d'Interopérabilité, Adtran est un bon candidat à considérer pour le TAS externe. PPP à liaisons multiples de support TAS d'Adtran (député britannique), protocole d'authentification CHAP (Challenge Handshake Authentication Protocol), Password Authentication Protocol (PAP), interfaces synchrones ou de série asynchrone, et la configuration automatique d'identifiant de service profile (AutoSPID).

Motorola BitSURFR

La manière la plus simple de faire un BitSURFR connecté à un PC pour interopérer à un routeur de Cisco est d'activer la conversion d'asynchrone/synchrone avec la commande **AT%A2=95** (le pour en savoir plus, voient la page 7-1 du manuel de BitSURFR). Si vous utilisez un BitSURFR pro et voulez utiliser les deux canaux B, vous devez utiliser l'authentification PAP. Le BitSURFR pro ne peut pas correctement répondre au défi de CHAP envoyé en évoquant le deuxième canal B. Pour placer un appel utilisant deux canaux B, vous devez introduire le numéro de téléphone deux fois. Par exemple, si le numéro de téléphone est 555-1212, vous écririez ATD555-1212&555-1212. Le tableau suivant présente les commandes d'entrer pour plusieurs types de connexions :

Tableau 4 : Commandes de configuration utiles pour Motorola BitSURFR

Type de connexion	Commande
Connectez en utilisant le PPP	%A2=95
Utilisez les deux canaux B (la député britannique)	@B0=2
Authentification PAP d'utilisation	@M2=P
Vitesse du matériel d'arrêt de données (DTE) (port COM PC)	&M

Appels de l'endroit 64-kbps	%A4=0
Appels de l'endroit 56-kbps	%A4=1
Communications voix d'endroit	%A98

Logiciel client

CiscoRemote Lite

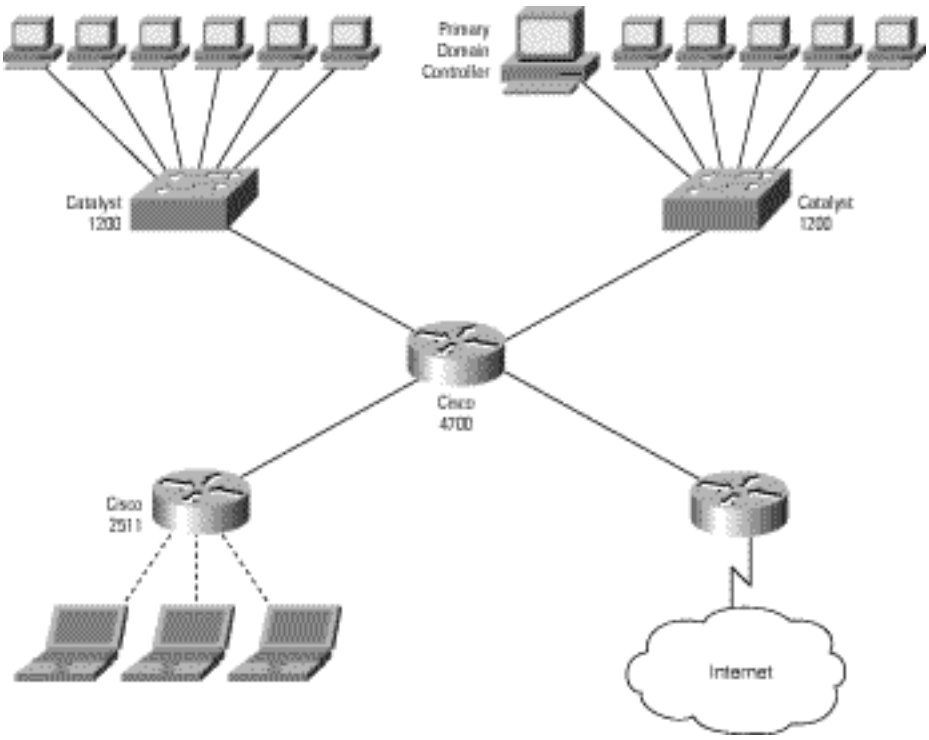
CiscoRemote Lite est une demande libre de pile TCP/IP et de numéroteur de Windows 3.1 et Windows pour des groupes de travail. PPP de supports de CiscoRemote et protocoles de Serial Line Internet Protocol (SLIP).

Exemples

Exemple 1

L'exemple 1 affiche un petit, réseau de simple-domaine utilisant NWLink (Netbios au-dessus d'IPX). La figure 7 affiche un graphique de l'installation.

Figure 7 : Petit, réseau de Simple-domaine utilisant NWLink



Configuration de routeur de Cisco 4700

```
hostname 4700 ipx routing ! interface ethernet 0 ipx network 50 ipx type-20-propagation
interface ethernet 1 ipx network 60 ipx type-20-propagation interface ethernet 2 ipx network 7B
ipx type-20-propagation interface ethernet 3 ipx network 95 ipx type-20-propagation
```

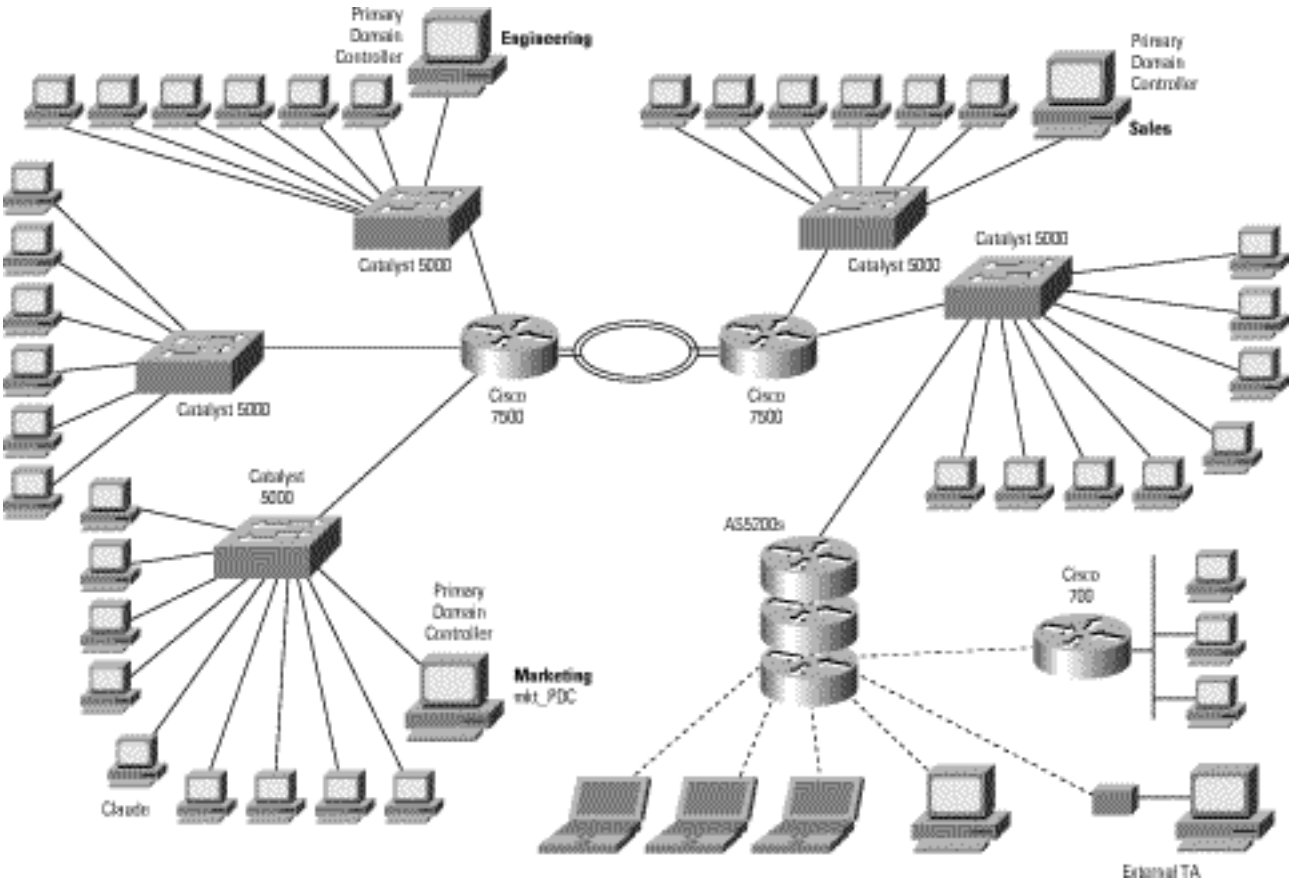
Configuration de Serveur d'accès Cisco 2511

```
hostname 2511 ipx routing ! interface ethernet 0 ipx network 98 interface loopback 0 ipx network
163 interface group-async 0 group-member 1 16 ipx ppp-client loopback 0 ipx sap-interval 0
encapsulation ppp async mode dedicated ! line 1 16 modem inout speed 115200 flowcontrol hardware
```

Exemple 2

2show d'exemple un réseau moyen utilisant NBT (Netbios au-dessus de TCP) et résolution de noms statique (LMHOSTS). La figure 8 affiche un graphique de l'installation.

Figure 8 : Réseau moyen utilisant NBT et LMHOSTS



Configuration du fichier LMHOSTS sur Claude (un client dans le domaine de vente)

1.2.1.8	mkt_PDC	#PRE
1.2.7.3	mkt_BDC	#PRE
REMPLAÇANT #BEGIN		
\ #INCLUDE \ \ de mkt_pdc \ public \ lmhosts #INCLUDE \ mkt_bdc \ public \ lmhosts		
REMPLAÇANT #END		

Configuration du fichier LMHOSTS sur le mkt_PDC (Primary Domain Controller pour le domaine de vente)

1.1.1.3	eng_PDC	#PRE #DOM : anglais
1.1.4.5	sales_PDC	#PRE #DOM : ventes
1.2.1.4	somnolent	-

1.2.1.5	sneezy	-
1.2.6.2	Martin	-
1.2.6.78	Theresa	-
1.2.6.89	Claude	-

Configuration de routeur de Cisco 7500

```
hostname 7500 ip forward-protocol udp bootpc ! interface ethernet 0 ip address 1.5.6.1
255.255.255.0 ip helper-addressn.n.n.n ... interface ethernet 23 ip address 1.5.56.1
255.255.255.0 ip helper-addressn.n.n.n
```

Configuration d'un AS5200 dans un groupe de pile

```
hostname as5200-1

!

controller t1 0

framing esf linecode b8zs pri-group controller t1 1 framing esf linecode b8zs pri-group ! sgbp
group as5200s sgbp member as5200-2 sgbp member as5200-3 username as5200s password stackpassword
! ip dhcp-servern.n.n.n ip wins-serverm.m.m.m ip address-pool dhcp-proxy-client ! interface
ethernet 0 ip address 192.168.2.1 255.255.255.0 ! interface group-async 0 group-member 1 48 peer
default ip address dhcp ! interface serial 0:23 dialer rotary-group 1 isdn incoming-voice modem
interface serial 1:23 dialer rotary-group 1 isdn incoming-voice modem interface dialer 1 ip
unnumbered ethernet 0 encapsulation ppp ppp multilink ppp authentication chap ppp use-tacacs
dialer-group 1 ! dialer-list 1 protocol ip permit ! line 1 48 modem inout modem autoconfigure
type microcom-hdms speed 115200 flowcontrol hardware
```

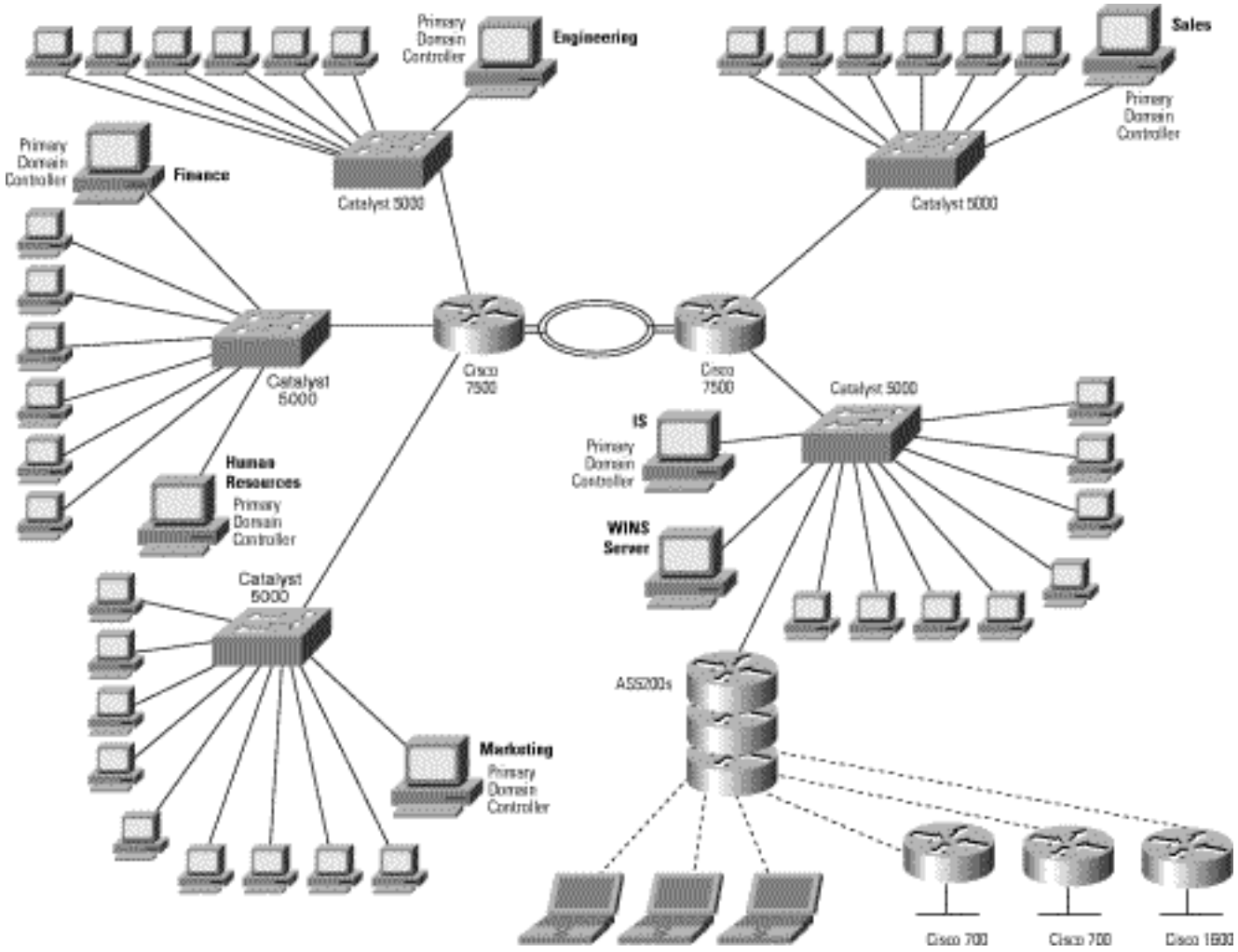
Configuration de routeur de Cisco 700

```
set system 700

cd LAN

set ip address 1.4.3.1 set ip netmask 255.255.255.248 set ip routing on set ip rip update
periodic CD set user as5200s set encapsulation ppp set ip framing none set ip routing on set
number 5551212 set ip route destination 0.0.0.0/0 gateway 0.0.0.0 CD set active as5200s set
bridging off
```

Exemple 3

L'exemple 3 affiche un réseau moyen utilisant NBT (Netbios au-dessus de TCP) et un serveur WINS simple. La figure 9 affiche un graphique de l'installation.

Figure 9 : Réseau moyen utilisant NBT (Netbios au-dessus de TCP) et un serveur WINS simple



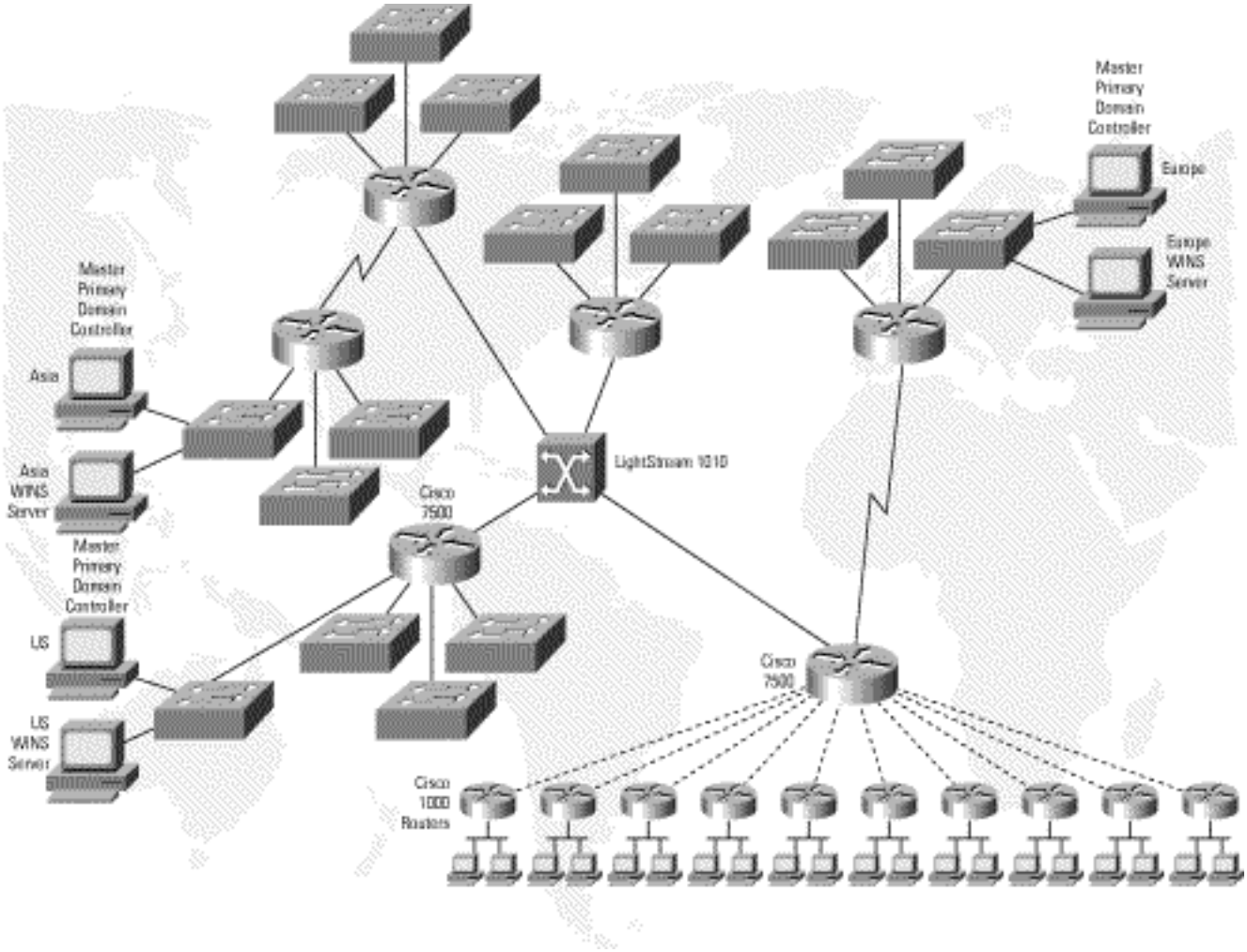
Configuration de Cisco 1600

```
hostname 1600 username as5200s password secret ! interface ethernet 0 ip address 1.4.3.1
255.255.255.248 interface bri 0 ip unnumbered ethernet 0 encapsulation ppp ppp multilink dialer
string 5551212 dialer-group 1 ! dialer-list 1 protocol ip list 101 access-list 101 deny udp any
any eq netbios-ns access-list 101 permit ip any any
```

Exemple 4

La figure 10 affiche un grand réseau utilisant NBT (Netbios au-dessus de TCP) avec des plusieurs domaines principaux et des serveurs WINS répliqués.

Figure 10 : Grand réseau utilisant NBT avec des plusieurs domaines principaux et des serveurs WINS répliqués



Annexe A : Arrêter la résolution de nom de diffusion

En utilisant Windows pour les groupes de travail 3.11

En utilisant Windows pour les groupes de travail 3.11, un nouveau fichier de navigateur, **VREDIR.386**, qui est inclus avec Windows NT 3.5, doit être utilisé pour permettre le furetage à fonctionner correctement. Windows 95/98 inclut déjà ce navigateur modifié. Le fichier VREDIR.386 est typiquement localisé dans le répertoire de **C:\WINDOWS\SYSTEM**.

Windows pour des clients de groupes de travail devrait apporter la modification suivante au SYSTEM.INI classer :

; SYSTEM.INI

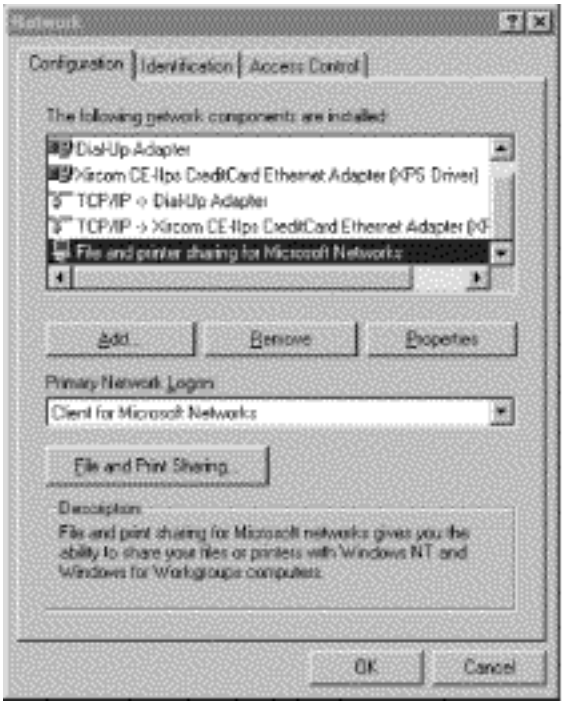
;

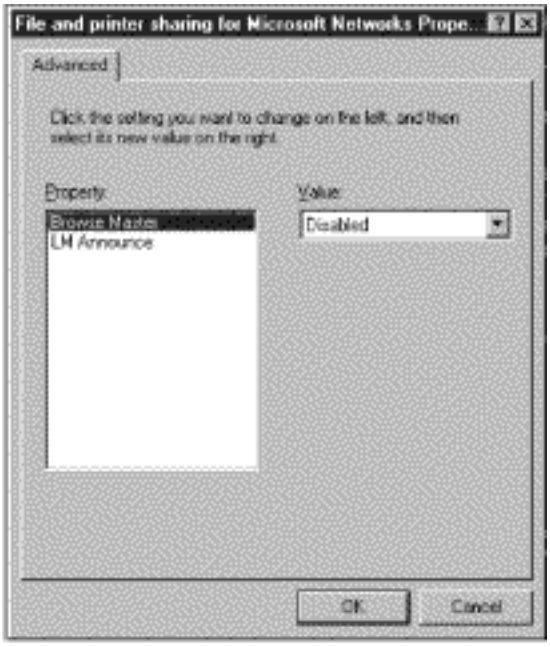
[Réseau]

MaintainServerList=No

Windows 95/98

Figure 11 : Arrêter le maître de navigation dans Windows 95/98





Windows NT 3.51

Windows NT 3.51 serveurs et station de travail qui sont configurés pour la résolution de noms de WINS n'envoient pas des émissions à moins que d'autres ordinateurs sur la demande réseau une élection de navigateur. Aucune action n'est requise.

Entrées dans le registre de Windows NT

Ces entrées dans le **hkey_local_machine \ système \ currentcontrolset \ services ** zone de **navigateur \ paramètres du** registre devraient être placées comme suit : **MaintainServerList** devrait être placé à l'oui, et **IsDomainMaster** devrait être placé à faux. Ce sont les valeurs par défaut.

La configuration de **MasterPeriodicity** (en quelques secondes) spécifie combien de fois le sous-réseau parcourent des serveurs questionnent le maître de domaine pour obtenir une liste de furetage. Quand le sous-réseau parcourent des serveurs et le maître de domaine sont séparés par un lien à vitesse réduite ou de charge-par-paquet, vous pouvez placer ceci à une heure ou à plus.

Trouver les maître de navigation escrocs

Windows 3.1 et Windows 95/98 poste de travail ne peuvent pas fonctionner comme maître de navigation dans un réseau de Windows NT parce qu'elles ne traitent pas le serveur NT et l'information de domaines. Malheureusement, par défaut, Windows 95/98 tentative de devenir un maître de navigation. Un seul poste de travail prétendant inexactement être le maître de navigation gêne rechercher chaque ordinateur sur ce tout le sous-réseau. La priorité pour aller bien à un maître de navigation est PDC, BDC, serveur NT, poste de travail NT, puis Windows 95/98, qui devrait empêcher ceci de se produire.

Le kit de ressources de serveur de Windows NT 4.0 contient un utilitaire appelé le **BROWSTAT**. Le moyen le plus simple de trouver un diffuseur escroc sur un sous-réseau est d'exécuter BROWSTAT sur un ordinateur de Windows NT sur le sous-réseau affecté.

Annexe B : Configurer la résolution de DN des noms de WINS

Le serveur et le Windows 2000 chacun des deux de Windows NT 4.0 incluent un serveur DNS qui peut répondre à des requêtes DNS en questionnant un serveur WINS à l'arrière-plan. Le serveur DNS de Windows 2000 prend en charge également des mises à jour dynamique par RFC 2136. Le serveur WINS et le serveur DNS n'ont pas besoin d'être sur le même ordinateur de Windows Nt/2000. Toutes les requêtes DNS à un sous-domaine (dans cet exemple, wins.cisco.com) devraient être déléguées au serveur DNS/WINS. Configurer un serveur DNS de Windows Nt/2000 à l'aide d'un fichier de démarrage n'est pas nécessaire ou recommandé de Microsoft. Le gestionnaire de DN fournit une interface riche pour le service.

Le fichier de démarrage de DN

; DÉMARRAGE	-	-
cache	.	CACHE
primaire	domain.com	domain.dom
primaire	8.17.1.in-addr.arpa	1-17-8.rev

Le fichier de DN pour domain.com

; domain.dom				
@	DANS	SOA	ns.domain.com.	rohan.domain.com. (
			1	; Numéro de série
			10800	; Régénérez [3h]
			3600	; Relance [1h]
			604800	; Expirent [7d]
			86400)	; Minimum [1d]
@	DANS	GAGNE 1.1.4.6 1.2.7.4		
wins-serveur	DANS	1.1.4.6		
wins-server2	DANS	1.2.7.4		

[1]Albitz, Paul et grillon Liu. Sébastopol, CA : O'Reilly et associés, 1992.

Informations connexes

- Support technique - Cisco Systems