Solutions | Products | Ordering | Support | Partners | Training | Corporate

Tech Notes

Windows Networking Design Implementation Guide

Contents

Help us help you.

Please rate this et:

○ Excellent

○ Good

○ Average

○ Fair

○ Poor

his et reete:a : ase:

○ Yes

○ No

estis r ireet:

(256 character limit)

tial tat irati:

Name:

Email:

Send

Introduction

The term "networking" covers a broad range of technologies, which, combined together, allow computers to share information. Networking components can be segmented into end-system applications, network operating systems, and networking equipment.

A network operating system is software run on all interconnected systems. Examples include Novell NetWare, Sun's NFS (Network File System), AppleShare, and Microsoft's implementation of a network operating system commonly called Windows Networking. Windows Networking is now extensively deployed with millions of nodes.

This design guide explains the basic concepts of Windows Networking and provides insight on how to design networks (LANs and WANs) to best utilize this operating system. The guide also explains protocols, naming, and scaling issues associated with Windows Networking.

What Is Windows Networking?

Windows Networking refers to the networking system shared by the software that comes with all the following Microsoft operating systems or servers:

- Microsoft LAN Manager
- MS-DOS with LAN Manager client
- Windows for Workgroups
- Windows 95, 98, and ME
- Windows NT and 2000

Microsoft LAN Manager, the LAN Manager client for MS-DOS, and Windows NT 3.1 are not discussed in this document except in an historical context.

Domains versus Workgroups

Windows Networking has three concepts of a group of related computers- workgroups, domains and a domain hierarchy. Workgroups can be any logical collection of computers; any computer on the network can join an existing workgroup or create a new one. More formal entities, domains are created and managed by a primary domain controller (PDC) process that runs on a Windows NT or Windows 2000 server. A domain has security and administrative properties that a workgroup does not. Each domain must have at least one NT or 2000 server, which is responsible for the PDC process, user account information in the domain, and security within the domain. Windows Networking domains are not the same as Internet domain names as used by the Domain Name System (DNS). A domain hierarchy or Active Directory Hierarchy is a collection of domains organized into parent-child relationships. This convention, introduced with Windows 2000, enables easier searching through multiple domains in a single query (among other things). This hierarchy maps closely to a DNS namespace.

What Protocol Does It Use?

Prior to Windows 2000, Windows Networking used the NetBIOS protocol for file sharing, printer sharing, messaging, authentication, and name resolution. A pure Windows 2000 installation would require NetBIOS only for interoperability with earlier versions of Windows Networking using the flat NetBIOS namespace. NetBIOS is a session-layer protocol that can run on any of the following transport protocols:

- NetBEUI (NetBIOS over LLC2)
- NWLink (NetBIOS over Internetwork Packet Exchange [IPX])
- NetBIOS over TCP (NBT)

Although Microsoft recommends that clients use only one transport protocol at a time for maximum performance, this setup is only the default for Windows 2000. You should pick a protocol to use for your entire network, preferably TCP/IP, and then turn the other protocols off because the NetBIOS name service maintains information about computer names (a name space) separately for each transport. Name spaces do not interact with each other; each transport operates as a separate network.

NetBEUI (NetBIOS over LLC2) is the least scalable of the three protocols because it must be bridged. NetBEUI is included only to support very old services (for example, old versions of LAN Manager). NetBEUI does not require any client address configuration. There is no fixed limit to the number of Windows clients can have with NetBEUI, but it is common for this solution to run into performance problems as the number of clients in a single bridge group goes above 50 to 100 users. The flat topology and reliance on broadcasts does not scale, especially when traffic must traverse a WAN link.

NWLink is recommended only for networks already running IPX that cannot be upgraded to use TCP/IP. Similar to NetBEUI, NWLink requires no client address configuration. NWLink uses IPX type-20 packets to exchange registration and browsing information. To forward type-20 IPX packets across Cisco routers, you must configure **ipx type-20 propagation** on each interface on every router on your network.

It is recommended to utilize NetBIOS over TCP (NBT) for most networks, or anytime the network includes a WAN. Since NBT uses TCP/IP, each computer must be configured to use a static IP address, or to fetch an IP address dynamically with the Dynamic Host Configuration Protocol (DHCP). For ease of network administration, it is highly recommended to use DHCP; for optimum network performance, it is highly recommended to use a (Windows Internet Name Service) WINS server as well. A WINS server allows clients to get browsing information without having to broadcast requests everytime. There is a direct correlation between the number of broadcasts in a network and network performance; broadcasts are necessary for a network to function, but minimizing them can be critical.

Cisco recommends that most customers use TCP/IP for Windows Networking. The bulk of this design guide focuses on designs using NBT.

Dynamic IP Addressing

What Is DHCP?

Manually addressing TCP/IP clients is both time consuming and error prone. To solve this problem, the Internet Engineering Task Force (IETF) developed DHCP, the Dynamic Host Configuration Protocol. DHCP is designed to automatically provide clients with a valid IP address and related configuration information (see the section DHCP Options below). Each range of addresses that a DHCP server manages is called a scope.

DHCP Scopes

You must configure a range of addresses for every IP subnet where clients will request a DHCP address; each range of addresses is called a DHCP scope. You can configure a DHCP server to serve several scopes since the DHCP server or servers do not need to be physically connected to the same network as the client. If the DHCP server is on a different IP subnet from the client, then you need to use DHCP relay to forward DHCP requests to your DHCP server.

DHCP Relay

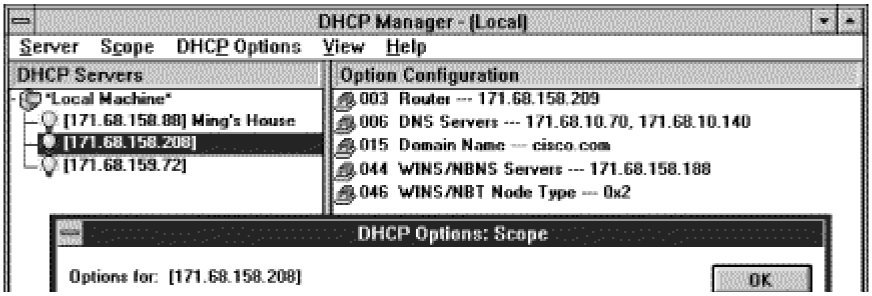
DHCP relay typically runs on a router and the relay support is available on Windows NT Server version 4.0 and Windows 2000 Server. On Cisco 700 series routers, you can turn on DHCP relay with the **set dhcp relay** command. You can turn on DHCP relay on a Cisco IOS router by configuring **ip helper-address** with the address of the DHCP server on each interface that will have DHCP clients. The **ip helper-address** command forwards many other IP broadcasts, including DNS, Trivial File Transfer Protocol (TFTP), and NetBIOS name service packets. To forward only DHCP requests, see the following example configuration. For more information, see the "Configuring Broadcast Handling" section in the Network Protocols Configuration Guide, Part 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
```

DHCP Options

In addition to its IP address, a DHCP client can get other TCP/IP configuration information from a DHCP server, including the subnet mask, default gateway, and DNS information. These pieces of information, called DHCP options, can be configured in the DHCP Manager on your Windows NT or Windows 2000 DHCP server.

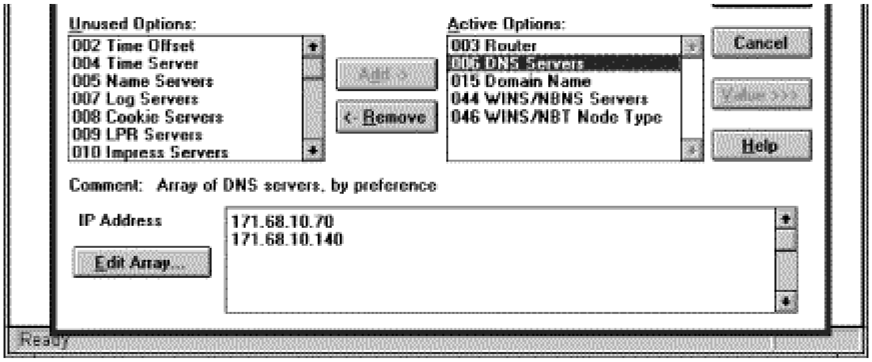
Figure 1: Microsoft's DHCP Manager



Local Machine
[171.68.158.88] Ming's House
[171.68.158.208]
[171.68.159.72]

003 Router --- 171.68.158.209
006 DNS Servers --- 171.68.10.70, 171.68.10.140
015 Domain Name --- cisco.com
044 WINS/NBNS Servers --- 171.68.158.188
046 WINS/NBT Node Type --- 0x2

Options for: [171.68.158.208]



Comment: Array of DNS servers, by preference

IP Address
171.68.10.70
171.68.10.140

If your clients are using Windows Internet Name Service (WINS) for name resolution (discussed later), you should configure the address of the WINS server and the WINS node type. A brief list of node types is included in the "Name Resolution" section. The node type p-node (**0x2**) is strongly recommended.

Cisco DHCP Servers

Cisco currently has an integrated DHCP and DNS server for Windows NT, Windows 2000 and UNIX; the server has a graphical interface, support for secondary addressing, and many other enterprise features. The Cisco 700 series routers (in Release 4.1 and later) and Cisco IOS routers (in Release 11.2(7)F and later) also include a DHCP server that can assign addresses on local network segments. Both styles of router include network and port-level address translation.

Name Resolution

Name resolution is the process of associating a convenient name, such as FRED or fred.domain.com, with a network address (often an IP address). For present purposes, this discussion applies to the way that Windows Networking resolves a NetBIOS unique workstation name (described as *WORKSTATION*<00> in a later section) to an IP address. This process should not be confused with the related but different process of browsing (which uses other types of NetBIOS names). As of the release of Microsoft Windows 2000, Windows Networking clients use up to five methods of name resolution:

- NetBIOS name cache
- IP Subnet Broadcasts
- LMHOSTS
- WINS
- Internet DNS

NetBIOS Name Cache

Windows Networking keeps a small cache of recently used NetBIOS names to IP address mappings. These entries are added after successful name resolution and then are removed after some period of time. Additional entries can be preloaded at system startup and made permanent by creating an entry in the LMHOSTS file with the **#PRE** tag (see the LMHOSTS section below).

IP Subnet Broadcasts

IP subnet broadcasts can be used for name resolution. Broadcasts are received by all computers on a subnet, requiring processing time at each computer. Windows Networking also maintains a designated browse master that maintains a list of all resources available on a subnet. An election process that uses broadcasts determines this browse master because registrations, browser elections, and name queries could all generate broadcasts, use of the broadcast name resolution method is not recommended.

LMHOSTS

Windows Networking can consult a static table in a file called LMHOSTS. To use this method, the PDC should maintain at the least a static list of all computers and their IP addresses in that domain and the names and addresses of the PDCs for all other domains in the network. All clients must then have an LMHOSTS file with the IP address of their PDC and the path to the master LMHOSTS file on the PDC.

Windows Internet Name Service

WINS was created to allow clients on different IP subnets to dynamically resolve addresses, register themselves, and browse the network without sending broadcasts. Clients send unicast packets to the WINS server at a well-known address. For compatibility with older Microsoft Networking clients, however, broadcast name resolution is still turned on by default, even when WINS is also configured.

To repeat what was stated above, it is highly recommended for optimum network performance to use WINS. Again, there is a direct correlation between the number of broadcasts in a network and network performance; broadcasts are necessary for a network to function, but minimizing them can be critical.

Internet DNS

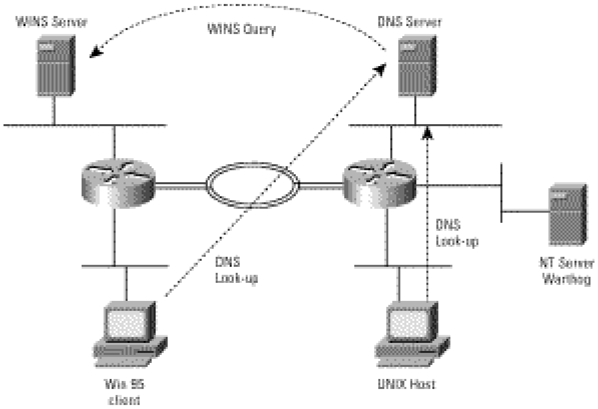
Any DNS server can be configured statically to answer queries for computers with fixed IP addresses. This scenario is useful if computers in your network have fixed IP addresses. When Windows systems use DHCP to get an IP address and WINS to register a NetBIOS name, you can set up a Windows DNS server to query a WINS server for names or addresses that were not entered statically. In both cases, Windows and non-Windows systems can resolve IP addresses correctly.

If an administrator configures each Windows Networking server with a static IP address, it may be convenient to enter each server in the DNS system and use DNS for name resolution. Occasionally (for example, when using a dial-on-demand link) it is convenient to register clients with WINS and make queries with DNS. The Microsoft NT 3.51 Resource Kit, Windows NT 4.0 Server and Windows 2000 all include a DNS server that can answer DNS queries by querying a WINS server in the background. For more information about how to configure this architecture, see Appendix A.

With Windows 2000, DNS servers can also be dynamically configured with address to name mappings. DHCP clients, DHCP Servers and Dynamic DNS servers work together to update name to address mappings in the DNS server. The DHCP server will perform this update for non-Windows

2000 DHCP clients.

Figure 2: Windows and non-Windows systems both send DNS lookups for a Windows NT server named Warthog. The DNS server does not have an entry for Warthog, so it queries the WINS server and returns the IP address.



Name Lookup Order

Windows networking components sends name resolution queries in a different order, depending on the NetBIOS node type. If the system is Windows NT 4.0 and the name is longer than 15 characters, then Windows NT sends only a DNS query. Other networking components and services may also use a different order depending upon the API called to perform name resolution. For example, a sockets application calling gethostbyname() will use DNS for name resolution first. Otherwise name lookup is performed in the following order:

- Check the NetBIOS name cache.
- Send a broadcast query or a WINS query name, depending on the current NetBIOS node type.
- Check the LMHOSTS file.
- Check the HOSTS file (if "resolve using DNS" is checked).
- Send an Internet DNS query (if resolve using DNS is checked).

Table 1: NetBIOS Names Are Searched Differently Based on The NetBIOS Node Type

NetBIOS Node Type	**Name Search Order**
b-node (**0x1**)	Broadcast only
p-node (**0x2**)	WINS only
m-node (**0x4**)	Broadcast, then WINS
h-node (**0x8**)	WINS, then broadcast

The Microsoft LAN Services Browser

Windows Networking was originally designed to run on a single LAN segment or a bridged (flat) network. At that time, only the NetBEUI protocol was supported.

Microsoft developed the LAN Services Browser to enable the user to browse a list of all computers available on the network. Each Windows Networking client registered its NetBIOS name periodically by sending broadcasts.

Every computer also had to send broadcasts to elect a browse master for the network. The browse master (and several backup browse masters) maintained the list of computers and their addresses. When a user browsed the network, the client sent a broadcast request and one of the browse masters responded.

Eventually Microsoft added support for NetBIOS over IPX and NetBIOS over TCP/IP, but Windows Networking still assumed that all clients and servers were on the same logical IPX network or IP subnet---they still sent broadcasts to register and find computers on the network.

This architecture, although simple to implement, generated an enormous burden on the network and on the CPU of each client on the network. Because of these scalability problems, Microsoft began to offer other methods of browsing and name resolution---ways for clients to map a name to the IP address of other computers on the network. Eventually Microsoft also provided a way to browse and resolve names without broadcasts.

The rest of this section explains how browsing works in various environments. The previous section explained how individual NetBIOS names are resolved. These two activities are similar but distinct. Users browse the network when opening the network neighborhood, using the net view command, or logging into a Windows NT domain at startup. Name resolution is the process of resolving names previously known, or found when browsing. Please note that this discussion is unrelated to Web browsers.

NetBIOS Names

NetBIOS names are 15-character, uppercase names that have a special identifier added to the 16th byte. As well, NetBIOS names can apply to a single IP address (unique), or to more than one (group). Some name types can be either unique or group names. Some of the most common of these last characters are listed as follows (all values are in hexadecimal):

Table 2: A Partial Table of Special NetBIOS Names and their Descriptions

Registered Special Names	Description
User Names	
<USERNAME><00>	Used to register the name of the currently logged on user in the WINS database, so that users can receive **net send** commands sent to their user names.
Computer Names	

<COMPUTER><00>	Used by Microsoft networking workstations to receive second class mailslot requests. All workstations must add this name in order to receive mailslot requests. This is the computer name registered for workstation services by a WINS client.
<COMPUTER><03>	Used as the computer name that is registered for the messenger service on a computer that is a WINS client.
<COMPUTER><20>	Used as the name that is registered for the peer server service on a Windows 95 computer (or the server service on a Windows NT computer) that is a WINS client.
<COMPUTER><Be>	Used as the unique name that is registered when the Network Monitor agent is started on the computer.
<COMPUTER><Bf>	Used as the group name that is registered when the Network Monitor agent is started on the computer. If this name is not 15 characters in length, it is padded with plus (+) symbols.
<COMPUTER><1f>	Used as the unique name that is registered for network dynamic data exchange (DDE) when the NetDDE service is started on the computer.
Group Names	
<01><02>MSBROWSE<02><01>	Used by master browser servers to periodically announce their domain on a local subnet. This announcement contains the domain name and the name of the master browser server for the domain. In addition, master browser servers receive these domain announcements to this name and maintain them in their internal browse list along with the announcer’s computer name.
<DOMAIN><00>	Used by workstations and servers to process server announcements to support Microsoft LAN Manager. Servers running Windows 95, Windows NT, Windows NT Server, and Windows for Workgroups do not broadcast this name unless the LMAnnounce option is enabled in the server’s properties.
<DOMAIN><1b>	Used to identify the domain master browser name, which is a unique name that only the primary domain controller (PDC) can add. The PDC processes GetBrowserServerList requests on this name. WINS assumes that the computer that registers a domain name with the <1b> character is the PDC.
<DOMAIN><1c>	Used for the internet group name, which the domain controllers register. The Internet group name is a dynamic list of up to 25 computers that have registered the name. This is the name used to find a Windows NT computer for pass-through authentication.

<DOMAIN><1d>	Used to identify a master browser (not a domain master browser). The master browser adds this name as a unique NetBIOS name when it starts. Workstations announce their presence to this name so that master browsers can build their browse list. For workgroups, this name has the form <WORKGROUP><1d>.
<DOMAIN><1e>	Used for all workgroup or domain-wide announcements by browser servers in a Windows network workgroup or Windows NT Server domain. This name is added by all browser servers and potential servers in the workgroup or domain. All browser election packets are sent to this name. For workgroups, this name has the form <WORKGROUP><1e>.

The Startup Process

On startup, any networked system sends a series of packets to discover network addresses, register itself, authenticate itself, and discover services. Windows Networking systems that log into a Windows NT domain must contact a domain controller to authenticate. This process uses name resolution and browsing.

First the startup system must register a computer name (*WORKSTATION*<00>). If the LMAnnounce parameter is on (for compatibility with LAN Manager servers), then the system also registers *DOMAIN*<00>. Next the system locates a domain controller for the login domain by trying to resolve *DOMAIN*<1C>. Prior to Windows 2000, this worked only with broadcast, LMHOSTS, or WINS name resolution methods. With Windows 2000, DNS is tried first. Next, the system logs on to the domain controller using NetBIOS-based mailslot messages, which are sent on User Datagram Protocol (UDP) port 138. Finally, after login is successful, the system registers the user who logged on (*USERNAME*<03>) so the messenger service can find that user.

Finding a Computer

When a user requests a resource on a computer by name (for example: **net use \\fred\someshare,** or finds FRED), the local system attempts to resolve the computer name. This query is for a unique NetBIOS name of type <00>, or a DNS or HOSTS file entry.

Viewing the Network Neighborhood

When a user opens the network neighborhood to request a list of domains, the system will attempt to get a list of backup browsers, either through broadcasting to the master browser name, or directly connecting to the domain master browser (or both). Once a list of backup browsers is retrieved, the system will choose a backup browser, connect to that system and retrieve the list of domains. Subsequent requests for servers within a domain are forwarded to the same backup browser.

Subnet Browsing

In the 1980s, most networks were "flat," or had only a few subnets. NetBEUI and NWLink use this model, and IP broadcasts can be bridged or helped across a small number of subnets. The following discussion assumes the case of a flat network.

Each subnet has a subnet master browser per domain or workgroup and may have some subnet backup browsers (also per domain or workgroup). After bootup, backup browsers and nonbrowsers send broadcast announcements at increasing intervals of 1, 2, 4, and 8 minutes; they eventually broadcast announcements only every 12 minutes. Subnet master browsers listen to these announcements to build a browse list.

Subnet master browsers and backup browsers are responsible for answering browse queries from other computers. Master browsers can answer these requests directly from the browse list. Backup browsers also keep a browse list, which they request from the subnet master browser every 15 minutes.

Broadcast Browsing across Subnets

In reality, most networks today have several subnets. Domains often span subnets and subnets sometimes contain systems in more than one domain. The browser software on some systems can communicate with a domain master browser (usually the PDC) to exchange browse lists from many subnets, but it needs to know the unicast address of the domain master browser. A subnet master browser can get the unicast address of the PDC from an LMHOSTS file (for a detailed description, see the Name Resolution section) or from WINS (see next section).

LMHOSTS is a text file that the browser software can read to find the unicast address of a PDC. A sample follows. First is the unicast IP address of the PDC, next the NetBIOS name of the PDC (**ENG_PDC**), a tag which stores this line in the NetBIOS name cache, (**#PRE**) and finally, a tag that marks this system as a domain controller for the ENG domain (**#DOM**).

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

When a subnet master browser knows the unicast address of the domain master browser, the browsers exchange browse lists every 15 minutes (using IP unicast packets). Because a master browser is consulted, clients can browse only domains that have a system on the local subnet (a subnet master browser). In practice, this scenario works well enough to find a login server at startup, but does not allow users to browse using the network neighborhood.

Important note: Because of a bug in some versions of Windows for Workgroups 3.11 and Windows 95, these systems cannot function as a subnet master browser or backup browser. The bug prevents the subnet browser from contacting the domain master browser. This bug has been fixed in Windows 95 OSR (OEM Service Release) 2. As a result, browsing on the subnet fails if there are Win31 or Win95 master or backup browsers on the subnet.

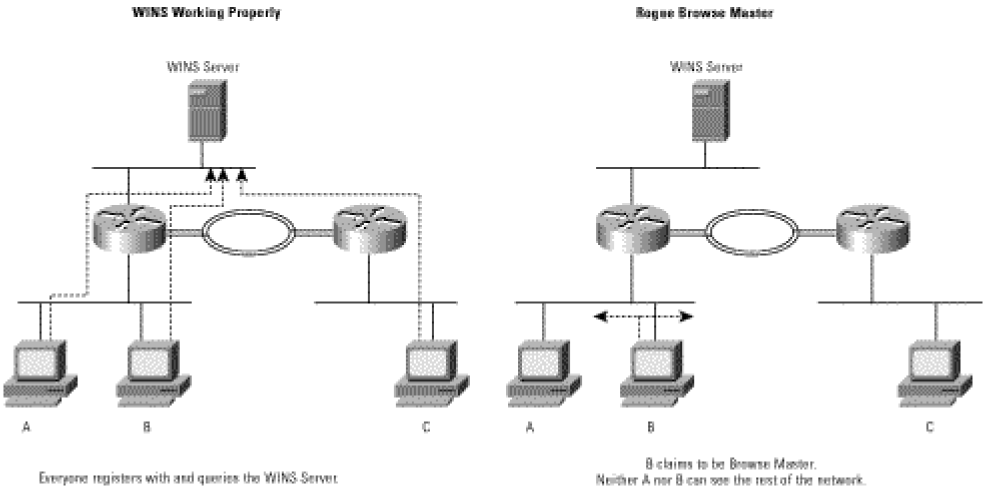
Browsing Any Domain with WINS

In an organization with several domains, it is not reasonable to architect a network based on the restrictions outlined in the previous section. When WINS is running, the subnet browser can be a WINS client and can get the unicast IP address of the domain master browser (the PDC) for any domain. However, broadcasts are still sent frequently and repeatedly by default (see table describing WINS node types in the following section) on the chance that there may be some non-WINS clients on the subnet. The best solution in most networks is to turn off broadcast browsing.

Turning Off Broadcasts

The biggest challenge when turning off broadcasts is avoiding rogue browse masters, which cause havoc on a subnet because they disrupt the browsing process.

Figure 3: Rogue Browse Master


WINS Working Properly
WINS Server
A
B
C
Everyone registers with and queries the WINS Server.
Rogue Browse Master
WINS Server
A
B
C
B claims to be Browse Master.
Neither A nor B can see the rest of the network.

You can disable broadcast name resolution by setting the BrowseMaster setting to Disabled. In Windows for Workgroups 3.11, broadcasts are turned off by adding a command to the SYSTEM.INI file. (See Appendix B for details.) In Windows 95/98, the BrowseMaster setting in Advanced File and Print Sharing Properties must be set to Disabled. In Windows NT, it is not necessary to turn off browsing in most cases, although it may be desirable. In Windows NT, set the **Hkey_local_machine\system\CurrentControlSet\Services\Browser\Parameters\MaintainServerLi** registry key to No. Administrators can control broadcasts sent by DHCP clients by selecting the appropriate WINS node type (p-node: **0x2**). A complete list of WINS node types follows.

Table 3: List of WINS Node Types

WINS Node Type	Name Search Order
b-node (**0x1**)	Broadcast only
p-node (**0x2**)	WINS only
m-node (**0x4**)	Broadcast, then WINS
h-node (**0x8**)	WINS, then broadcast

Scaling to Larger Networks

Trusted Domains

When planning a Windows network, consideration of what domain model to use is important. The following paragraphs discuss the benefits and drawbacks of several domain models. If you have several domains, you probably want to exchange data with other domains in your network. Trust relationships are a way to gain or grant access to a domain without having to manage each user individually. Each relationship permits trust in one direction only. For more information, see the *Windows NT 4.0 Server Resource Kit*, volume 2, chapter 4.

Single Domain

This domain model is the simplest---the network has only one domain. This setup works for small or medium-sized installations without a WAN.

Global Trust

Designed for companies without a central administrative or IS organization, the global trust model is the easiest to understand and the most difficult to manage. Every domain trusts every other domain.

Master Domain

In this model, a master domain is trusted by all other domains, but the master domain trusts no one. This option is beneficial when departments or divisions want administrative control over their own services, but still want to authenticate centrally.

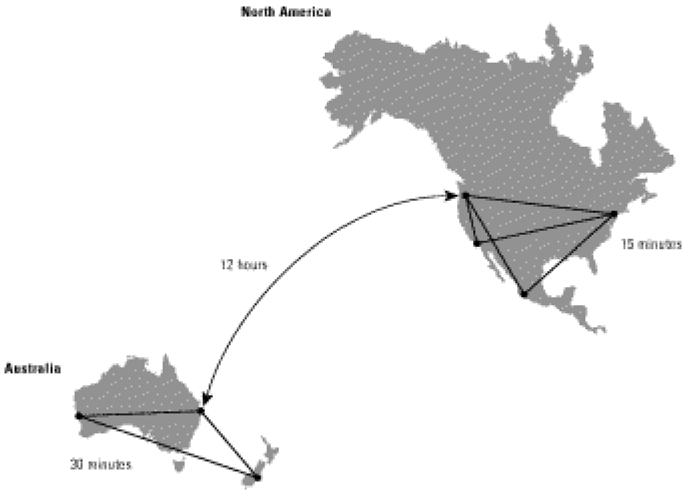
Multiple Master Domains

This model is designed to be a larger version of the master domain model. Several master domains all trust each other, and each of the master domains is, in turn, trusted by each departmental domain.

Replicating WINS

For redundancy or to optimize WAN traffic, sometimes having several WINS servers is desirable. Windows NT and Windows 2000 servers can replicate or resynchronize WINS databases in either or both directions. In Figure 4, a large multinational company has several distributed WINS servers, so WINS queries do not have to travel across continents.

Figure 4: Example of an Enterprise-Wide Configuration for WINS Replication



Modem Access

Windows NT and Windows 2000 come with Microsoft's remote-access server (RAS), which uses the Point-to-Point Protocol (PPP). Customers may want to use Cisco access servers instead of NT RASs for their dial-in pools because of the better dial-in density and performance available on Cisco access servers.

Windows supports TCP/IP, IPX, and NetBEUI (IP Control Protocol [IPCP], IPX Control Protocol [IPXCP], and NetBIOS Frames Control Protocol [NBFCP] control protocols for PPP). NetBEUI dial-in support was added to the Cisco IOS software in Release 11.1. For NetBEUI dial in, use the **netbios nbf** command (as shown in the following example) on each async interface or on a group-async interface on the access server.

```
interface ethernet 0

netbios nbf

interface group-async 0

group-range 1 16

netbios nbf
```

To configure IPX dial in, use the **ipx ppp-client** command (as shown in the following example) on each async interface or on a group-async interface on the access server. This command requires you to configure an IPX network address on a loopback interface. Dial-in clients do not need to hear Service Advertisement Protocol (SAP) messages, so these messages should be turned off with the **ipx sap-interval 0** command.

```
Interface loopback 0

ipx network <network number>

interface group-async 0

group-range 1 16

ipx ppp-client loopback 0

ipx sap-interval 0
```

In order to assign IP addresses to dial-in clients, Cisco access servers can use a pool of local addresses or act as a proxy for a DHCP server. The access server requests an address from the DHCP server and uses that address during PPP negotiation. The client can also negotiate the address of its WINS server.

```
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

Dial-on-Demand Routing

Dial-on-demand routing (DDR) provides network connections across the Public Switched Telephone Network (PSTN). Traditionally, WAN connections have been dedicated leased lines. DDR provides low-volume, periodic network connections, allowing on-demand services and decreasing network costs. Integrated Services Digital Network (ISDN) is a circuit-switched technology. Like the analog telephone network, ISDN connections are made only when there is a need to communicate.

Cisco routers use DDR to determine when a connection needs to be made to another site. Packets are classified as either interesting or uninteresting, based on protocol-specific access lists and dialer lists. Uninteresting packets can travel across an active DDR link, but they do not bring the link up, nor do they keep the link up.

Windows for Workgroups and Windows 95/98 clients that share files or printers register themselves with WINS every twelve or fifteen minutes by sending a unicast packet to the WINS server (on UDP port 137---the NetBIOS name service port).

Windows NT systems may also send a variety of other periodic packets, which can cause high WAN costs. These periodic packets include browser synchronization, WINS replication, SAM (user account database) replication, printer browsing, and DHCP. Many of these services have registry keys that may be tuned to bring up the dial-on-demand connection less frequently. For more information, see the *Microsoft Knowledge Base*, article: Q134985. Important registry entries include:

Hkey_local_machine\system\CurrentControlSet\Services\Browser\Parameters\MasterPeriodicity

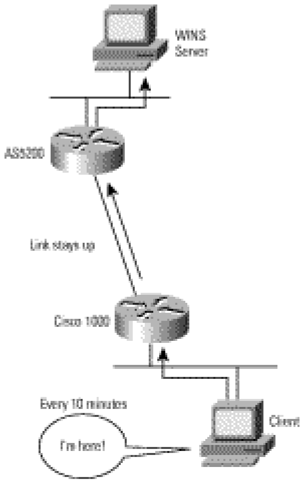
Hkey_local_machine\system\CurrentControlSet\Services\Browser\Parameters\BackupPeriodicity

Hkey_local_machine\system\CurrentControlSet\Services\Replicator\Interval

Hkey_local_machine\system\CurrentControlSet\Services\Netlogon\PulseMaximum

Hkey_local_machine\system\CurrentControlSet\Services\Control\Print\DisableServerThread

Figure 5: Dial-on-Demand Link Up All the Time



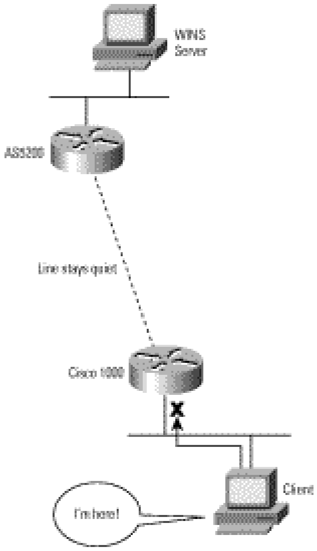
Sending a packet to the WINS server normally brings up the dial-on-demand link. If, however, this port is classified as uninteresting to the Cisco IOS software, then the router neither brings up nor keeps up the link.

```
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: UDP Port 137 Is Uninteresting, Link Is Down



Filters for the Cisco 700 series are available in Release 4.1(2). An example filter to make Windows NT SAM traffic uninteresting follows:

```
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
```

ISDN Access

This section covers ISDN cards and terminal adapters (TAs). For information about using Windows networking with ISDN routers, see the previous section on dial-on-demand routing.

Adtran

Because Adtran and Cisco have worked closely during interoperability testing, Adtran is a good candidate to consider for external TAs. Adtran TAs support Multilink PPP (MP), Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), synchronous or asynchronous serial interfaces, and the Automatic Service Profile Identifier (AutoSPID) configuration.

Motorola BitSURFR

The simplest way to make a BitSURFR connected to a PC interoperate with a Cisco router is to turn on async/sync conversion with the command **AT%A2=95** (for more information, see page 7-1 of the BitSURFR manual). If you are using a BitSURFR Pro and want to use both B channels, you must use PAP authentication. The BitSURFR Pro cannot correctly answer the CHAP challenge sent when bringing up the second B channel. To place a call using two B channels, you must enter the phone number twice. For example, if the phone number is 555-1212, you would enter ATD555-1212&555-1212. The following table lists the commands to enter for several types of connections:

Table 4: Useful Configuration Commands for the Motorola BitSURFR

Type of Connection	**Command**
Connect Using PPP	**%A2=95**
Use Both B Channels (MP)	**@B0=2**
Use PAP Authentication	**@M2=P**
Data Termination Equipment (DTE) Speed (PC COM port)	**&M**
Place 64-kbps Calls	**%A4=0**
Place 56-kbps Calls	**%A4=1**
Place Voice Calls	**%A98**

Client Software

CiscoRemote Lite

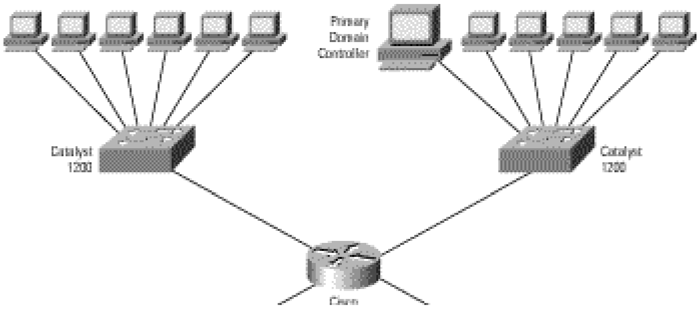
CiscoRemote Lite is a free TCP/IP stack and dialer application for Windows 3.1 and Windows for Workgroups. CiscoRemote supports PPP and Serial Line Internet Protocol (SLIP) protocols.

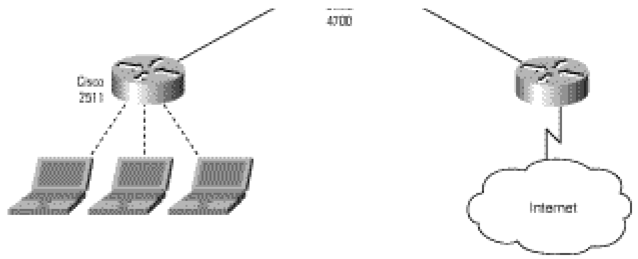
Examples

Example 1

Example 1 shows a small, single-domain network using NWLink (NetBIOS over IPX). Figure 7 shows a graphic of the setup.

Figure 7: Small, Single-Domain Network Using NWLink





Configuration of Cisco 4700 Router

```
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 of Cisco 2511 Access Server

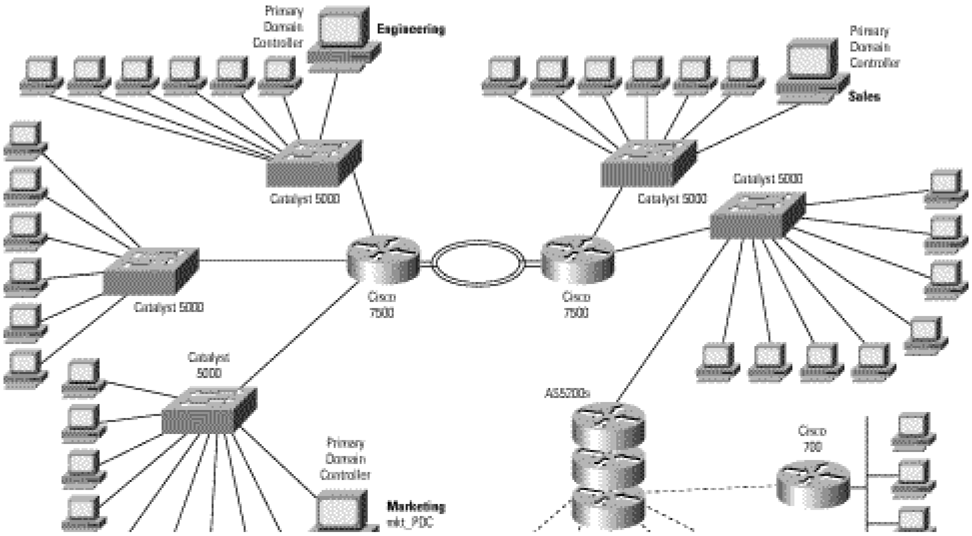
```
hostname 2511

ipx routing

!

interface ethernet 0
```

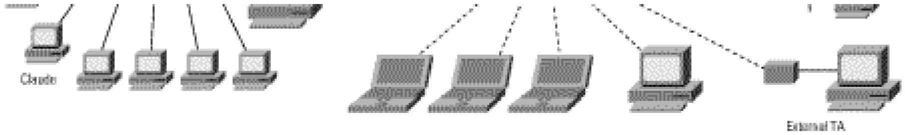
```
ipx network 98

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
```

Example 2

Example 2 shows a medium-sized network using NBT (NetBIOS over TCP) and static name resolution (LMHOSTS). Figure 8 shows a graphic of the setup.

Figure 8: Medium-Sized Network Using NBT and LMHOSTS





LMHOSTS Configuration on Claude (a Client in the Marketing Domain)

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

LMHOSTS Configuration on mkt_PDC (Primary Domain Controller for the Marketing Domain)

1.1.1.3	eng_PDC	#PRE #DOM:eng
1.1.4.5	sales_PDC	#PRE #DOM:sales
1.2.1.4	sleepy	-
1.2.1.5	sneezy	-
1.2.6.2	martin	-
1.2.6.78	theresa	-
1.2.6.89	claude	-

Configuration of Cisco 7500 Router

```
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 of an AS5200 in a Stack Group

```
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
```

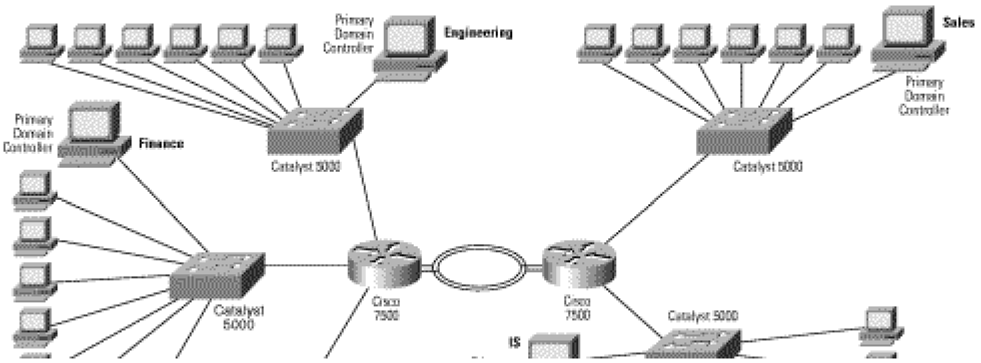
Configuration of Cisco 700 Router

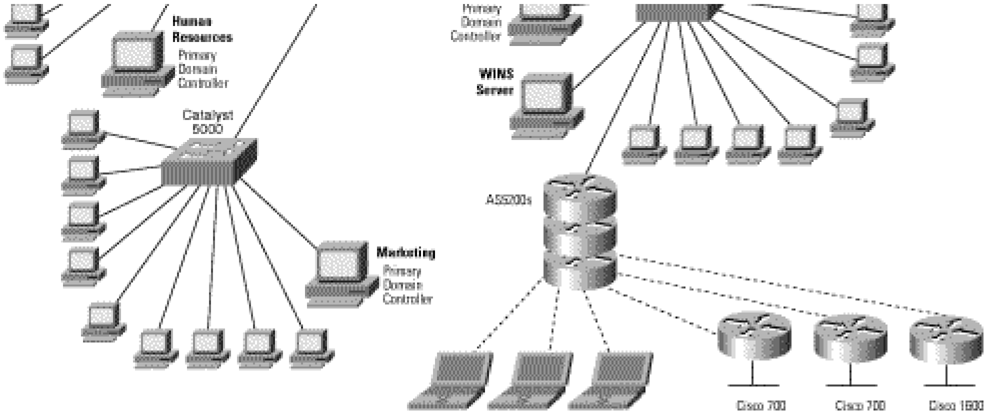
```
set system 700

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
```

Example 3

Example 3 shows a medium-sized network using NBT (NetBIOS over TCP) and a single WINS server. Figure 9 shows a graphic of the setup.

Figure 9: Medium-Sized Network Using NBT (NetBIOS over TCP) and a Single WINS Server





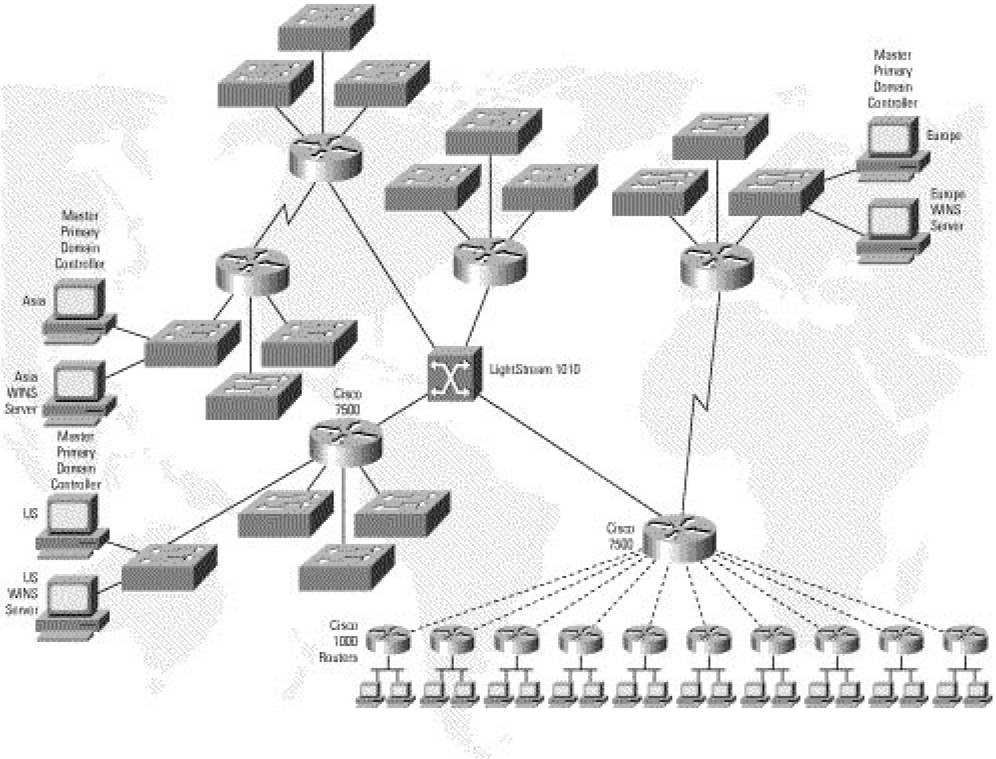
Configuration of a Cisco 1600

```
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
```

Example 4

Figure 10 shows a large network using NBT (NetBIOS over TCP) with multiple master domains and replicated WINS servers.

Figure 10: Large Network Using NBT with Multiple Master Domains and Replicated WINS Servers



Appendix A: Turning Off Broadcast Name Resolution

When Using Windows for Workgroups 3.11

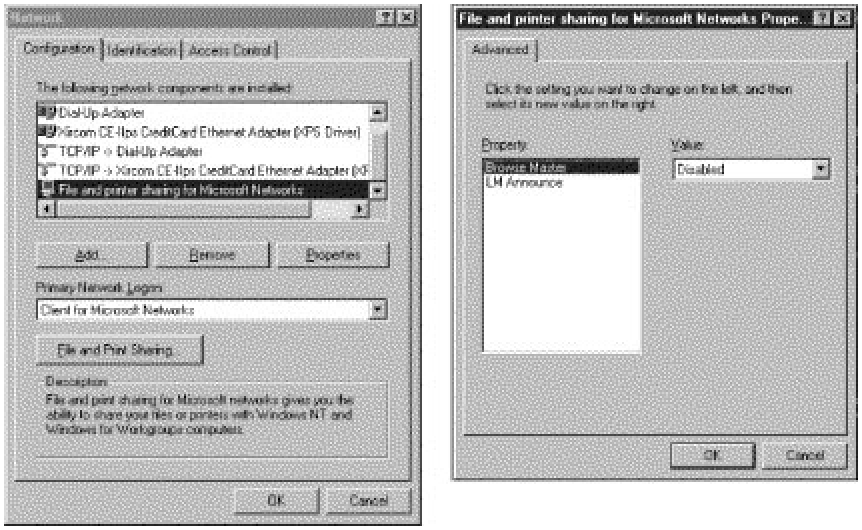
When using Windows for Workgroups 3.11, a new browser file, **VREDIR.386**, which is included with Windows NT 3.5, must be used to allow browsing to work correctly. Windows 95/98 already includes this modified browser. The VREDIR.386 file is typically located in the **C:\WINDOWS\SYSTEM** directory.

Windows for Workgroups clients should make the following change to the SYSTEM.INI file:

```
; SYSTEM.INI

;

[Network]

MaintainServerList=No
```

Windows 95/98

Figure 11: Turning Off Browse Master in Windows 95/98



Network

The following network components are installed:

- Dial-Up Adapter
- Xircom CE-IIps CreditCard Ethernet Adapter (XPS Driver)
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Xircom CE-IIps CreditCard Ethernet Adapter (XF
- File and printer sharing for Microsoft Networks

Primary Network Logon: Client for Microsoft Networks

Description: File and print sharing for Microsoft networks gives you the ability to share your files or printers with Windows NT and Windows for Workgroups computers.

File and printer sharing for Microsoft Networks Prope...

Click the setting you want to change on the left, and then select its new value on the right.

Property: Browse Master, LM Announce

Value: Disabled

Windows NT 3.51

Windows NT 3.51 workstations and servers that are configured for WINS name resolution do not send broadcasts unless other computers on the network request a browser election. No action is required.

Windows NT Registry Entries

These entries in the **hkey_local_machine\system\currentcontrolset\services\browser\parameters** area of the registry should be set as follows: **MaintainServerList** should be set to Yes, and **IsDomainMaster** should be set to False. These are the default settings.

The **MasterPeriodicity** setting (in seconds) specifies how often subnet browse servers query the domain master to obtain a browse list. When subnet browse servers and the domain master are separated by a low-speed or charge-per-packet link, you can set this to an hour or more.

Finding Rogue Browse Masters

Windows 3.1 and Windows 95/98 workstations cannot function as browse masters in a Windows NT network because they do not handle NT server and domain information. Unfortunately, by default, Windows 95/98 attempts to become a browse master. A single workstation incorrectly claiming to be the browse master hinders browsing for every computer on that entire subnet. The priority for becoming a browse master is PDC, BDC, NT Server, NT Workstation, then Windows 95/98, which should prevent this from occurring.

The *Windows NT 4.0 Server Resource Kit* contains a utility called **BROWSTAT**. The easiest way to find a rogue broadcaster on a subnet is to run BROWSTAT on a Windows NT computer on the affected subnet.

Appendix B: Configuring DNS Resolution of WINS Names

Windows NT 4.0 Server and Windows 2000 both include a DNS server that can answer DNS queries by querying a WINS server in the background. The Windows 2000 DNS server also supports dynamic updates per RFC 2136. The WINS server and the DNS server do not need to be on the same Windows NT/2000 machine. All DNS queries to a subdomain (in this example, wins.cisco.com) should be delegated to the DNS/WINS server. Configuring a Windows NT/2000 DNS server using a boot file is not necessary or recommended by Microsoft. The DNS Manager provides a rich interface for the service.

The DNS Boot File

;BOOT	-	-
cache	**.**	**CACHE**
primary	**domain.com**	**domain.dom**
primary	**8.17.1.in-addr.arpa**	**1-17-8.rev**

The DNS File for domain.com

;domain.dom				
@	**IN**	**SOA**	**ns.domain.com.**	**rohan.domain.com. (**
			1	**; Serial Number**
			10800	**; Refresh [3h]**
			3600	**; Retry [1h]**
			604800	**; Expire [7d]**
			86400)	**; Minimum [1d]**
@	**IN**	**WINS 1.1.4.6 1.2.7.4**		
wins-server	**IN**	**A 1.1.4.6**		
wins-server2	**IN**	**A 1.2.7.4**		

[1] Albitz, Paul and Cricket Liu. Sebastopol, CA: O'Reilly and Associates, 1992.

Related Information

- **LAN Technologies Top Issues**
- **LAN Technical Tips**

Home | What's New | How to Buy | Login | Register | Feedback | Search | Map/Help