Designing Networks with Windows Networking

Design Implementation Guide

Rohan Mahy
rohan@cisco.com
Product Marketing Engineer
Cisco Systems, Inc.

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 over 100 million 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 Windows Networking. The guide also explains Windows 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
- Windows NT

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

Domains versus Workgroups

Windows Networking has two concepts of a group of related computers—workgroups and domains. 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 server. A domain has security and administrative properties that a workgroup does not. Each domain must have at least one NT server. Windows Networking domains are not the same as Internet domain names as used by Domain Naming System (DNS).

What Protocol Does It Use?

Windows Networking uses the NetBIOS protocol for file sharing, printer sharing, messaging, authentication, and name resolution. NetBIOS is a session layer protocol that can run on any of these transport protocols:

- NetBEUI
- NWLink (NetBIOS over IPX)
- NetBIOS over TCP (NBT)

Although Microsoft recommends that clients use only one transport protocol at a time for maximum performance, this is not the default. You should pick a protocol to use for your entire network, and then turn the other protocols off.

NetBEUI is the least scalable of the three protocols because it must be bridged. NetBEUI is only inluded to support very old services (for example, old versions of LAN manager). NetBEUI does not require any client address configuration.

NWLink is recommended for small to medium sized networks, especially if they are already running IPX. Like 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.

Microsoft recommends NetBIOS over TCP (NBT) for medium-sized and large networks, or anytime the network includes a wide-area network (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).

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 DHCP Options). 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.

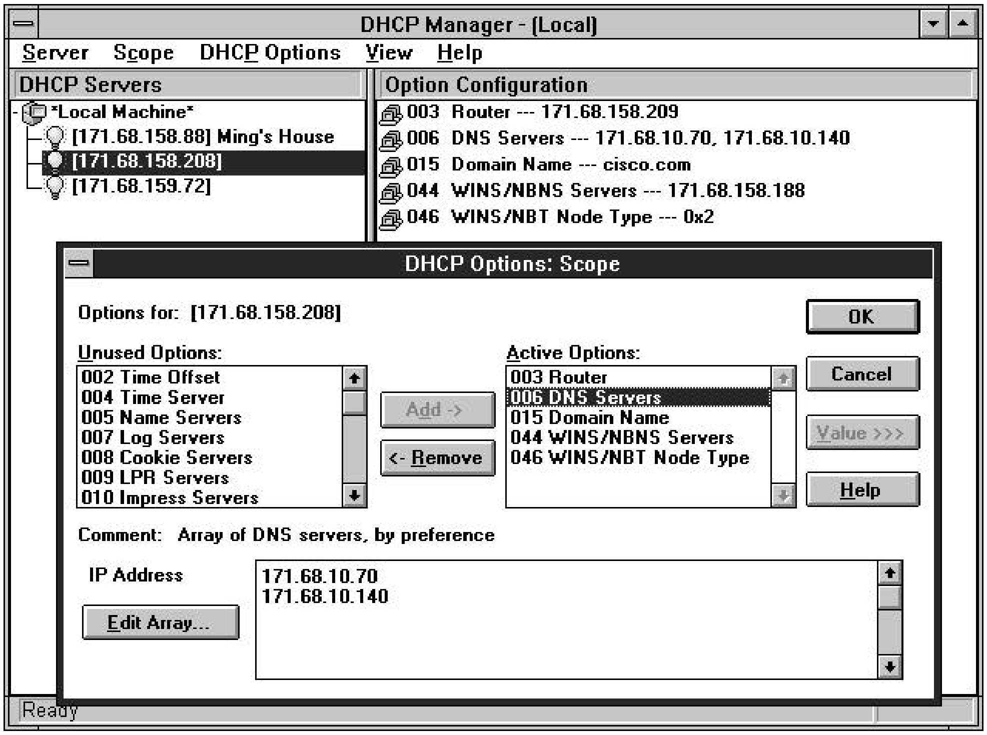
DHCP Relay

DHCP Relay typically runs on a router. You can turn on DHCP Relay on a Cisco Internetwork Operating System (Cisco IOS™) router by configuring **ip helper-address** with the address of the DHCP server on each interface that will have DHCP clients. To prevent forwarding other broadcasts to the DHCP server, add the **ip forward-protocol udp bootpc** global command to the router configuration. DHCP Relay on the Cisco 700 series is planned for the last quarter of 1996.

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 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]

Unused Options:
002 Time Offset
004 Time Server
005 Name Servers
007 Log Servers
008 Cookie Servers
009 LPR Servers
010 Impress Servers

Active Options:
003 Router
006 DNS Servers
015 Domain Name
044 WINS/NBNS Servers
046 WINS/NBT Node Type

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, as 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. p-node (0x2) is strongly recommended.

Cisco DHCP Server

Cisco will ship an integrated DHCP and DNS server for Windows NT, UNIX, and OpenVMS in the third quarter of 1996. This server will have a graphical interface, support for secondary addressing, and many other enterprise features.

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 would send a broadcast request and one of the browse masters would respond.

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.

Name Resolution

As of the release of Microsoft Windows NT 3.51, Windows Networking clients have a choice of any of four methods of name resolution:

- Broadcasts
- LMHOSTS
- WINS
- Internet DNS

Broadcasts

By sending broadcasts on a subnet, Windows Networking clients cause a browser election. The designated browse master maintains a list of all the resources available on that subnet. Because registrations, browser elections, and name queries all generate broadcasts, use of this method is not recommended.

Since this method is used by default on all Microsoft products, it is strongly recommended that you turn this feature off by setting the BrowseMaster setting to Disabled (the default is Automatic). For specific details, see Appendix A.

LMHOSTS

Windows Networking can consult a static table in a file called LMHOSTS. To use this method, the Primary Domain Controller (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.

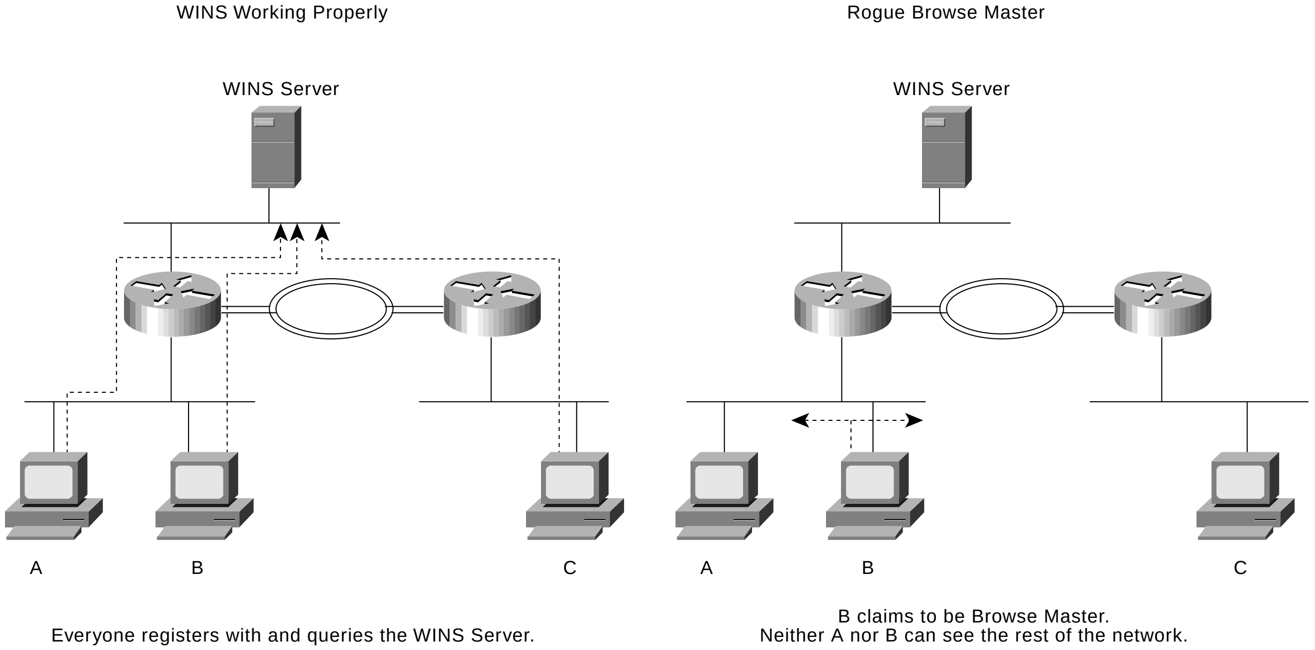
Using this method alone, however, does not allow clients to browse the network. Because of the obvious administrative burden, this method of resolving NetBIOS names is recommended only if you are using a router running EveryWare (Cisco 700 series) and you need to control line charges. (See the Dial-on-Demand Routing section for more details.)

Windows Internet Name Service

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

Important: Browsing will not work on a subnet if any Windows 3.1 or Windows 95 computer on the subnet has broadcast name resolution turned on (that is, Browse Master setting to Automatic). Individual servers, however, are still reachable by name.

Figure 2.


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

In Windows for Workgroups 3.11, broadcasts are turned off by adding a command to the system.ini file. (See Appendix A for details.) In Windows 95 the Browse Master setting in Advanced File and Print Sharing Properties must be set to Disabled. 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 is below.

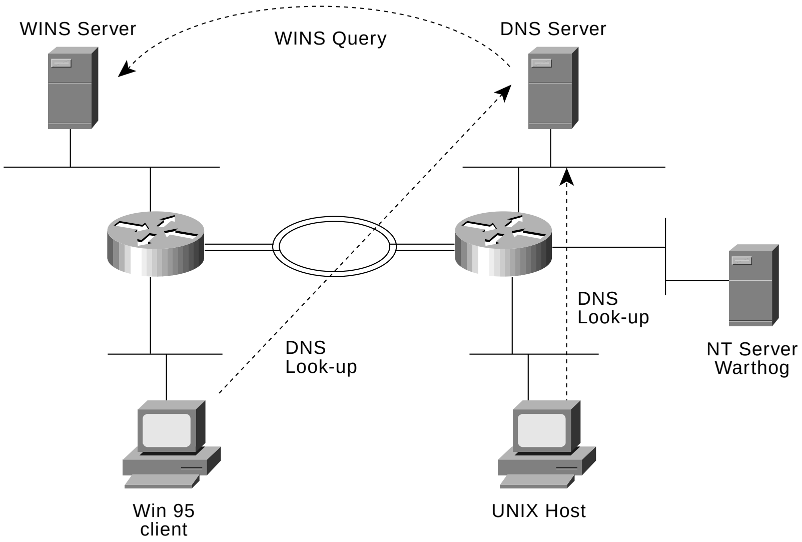
WINS Node Type	Name Search Order
b-node (0 x 1)	Broadcast only
p-node (0 x 2)	WINS only
m-node (0 x 4)	Broadcast, then WINS
h-node (0 x 8)	WINS, then broadcast

Internet DNS

Any DNS server can be configured statically to answer queries for computers with fixed IP addresses. This 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 setup a Windows NT 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 and Windows NT 4.0 server both 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 B.

Figure 3. 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.



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 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.

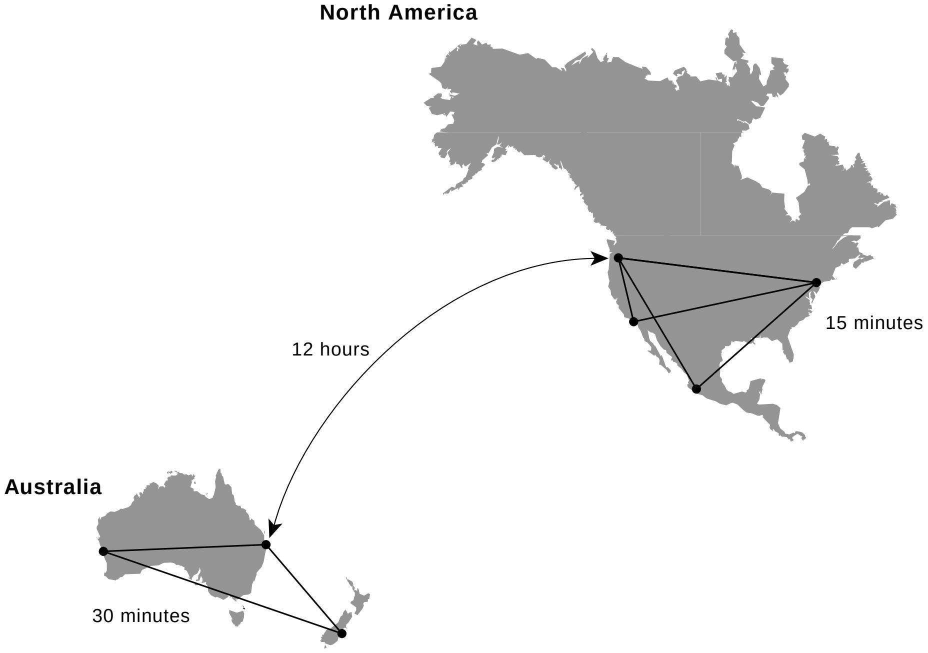
Multiple Master Domains

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 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 that WINS queries do not have to travel across continents.

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



Modem Access

Windows NT comes with Microsoft's remote-access server (RAS), which uses the Point-to-Point Protocol (PPP). Customers often 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.

NT supports TCP/IP, IPX, and NetBEUI (IPCP, IPXCP, and NBFCP control protocols for PPP). NetBEUI dial-in support was added to the Cisco IOS 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 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-server p.p.p.p
ip address-pool dhcp-proxy-client
!
interface group-async 0
 group-range 1 16
 peer default ip address dhcp
```

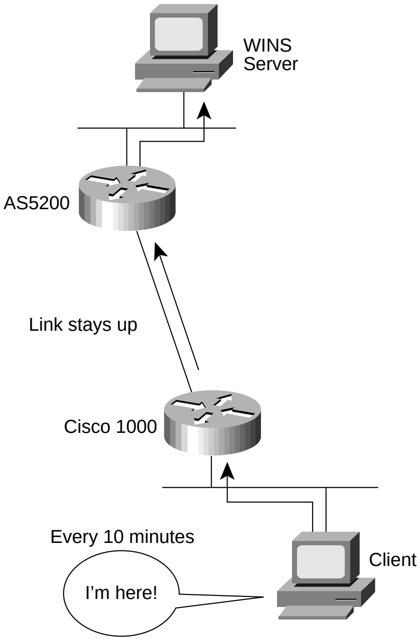
Dial-on-Demand Routing

Dial-on-demand routing (DDR) provides network connections across Public Switched Telephone Networks (PSTNs). Traditionally, WAN connections have been dedicated leased lines. DDR provides low-volume, periodic network connections, allowing on-demand services and decreasing network costs. 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 dial-on-demand routing (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, or keep the link up.

Windows for Workgroups and Windows 95 clients using WINS try to register themselves on the network every ten minutes by sending a unicast packet to the WINS server (on User Datagram Protocol [UDP] port 137—the NetBIOS Name Service port).

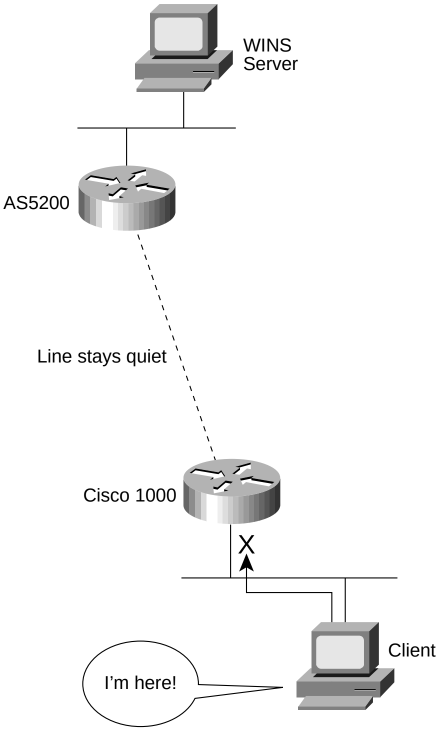
Figure 5. Dial-on-Demand Link Up All the Time



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 will neither bring up nor keep up the link. This feature is not currently available on the Cisco 700 series.

```
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



Unfortunately, making NetBIOS name service packets uninteresting can cause initial logins to time out, or fail completely. The only reliable way to ensure that Windows for Workgroups and Windows 95 logins succeed while controlling line usage is to use the DNS method of NetBIOS name resolution.

Windows NT workstations and servers regularly send security messages to the domain controllers in their domain. This traffic is not spoofable. To prevent this traffic from keeping your dial-on-demand connection up, Cisco recommends that you create a separate trusted domain at the remote site. You may also want to use separate WINS servers on each side of the ISDN line and periodically replicate them.

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.

Cisco 200

The Cisco 201 and 202 are ISDN cards for Industry-Standard Architecture (ISA) bus computers. Open Data-Link Interface (ODI) drivers are available for Windows 3.1 and Windows 95, which support IP and IPX dial-on-demand routing. Network driver interface specification (NDIS) 3.1 drivers and drivers for the ISDN accelerator pack (both for Windows 95) should be available in September 1996. Windows NT drivers are scheduled for release in the third quarter of 1996.

Adtran

Because Adtran and Cisco have worked closely during interoperability testing (PPP bakeoffs, for example), Adtran is a good candidate to consider for external terminal adapters. Adtran TAs support Multilink PPP (MP), Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP), synchronous or asychronous 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:

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 and CiscoRemote Lite

CiscoRemote™ Lite is a free TCP/IP stack and dialer application for Windows 3.1 and Windows for Workgroups.

CiscoRemote is a complete set of applications for “dial-up” remote computing in one package for the PC Windows and Apple Macintosh environments. All applications are optimized, tested, and supported by Cisco. This single product will link PCs with other computing resources within an enterprise network or across the worldwide Internet. CiscoRemote also includes the industry’s first remote node accelerator to dramatically improve dial-up performance.

Cisco TCP/IP Suite 100

This TCP/IP stack for Windows 3.1 and Windows 95 directly replaces the Microsoft stack and adds features like router discovery and extensive configuration and management facilities. The full suite of TCP/IP applications include a Serial Line Internet Protocol (SLIP) and PPP dialer; a graphical File Transfer Protocol (FTP) client (with passive-mode support); a Telnet client with full VT420, tn3270, and tn5250 emulation and Kerberos support; a World Wide Web browser; Post-Office Protocol (POP) mail client; a Network File System (NFS) client; line printer daemon (LPD), Stream and PCNFSd printing; and best-in-class technical support.

IPeXchange Gateways

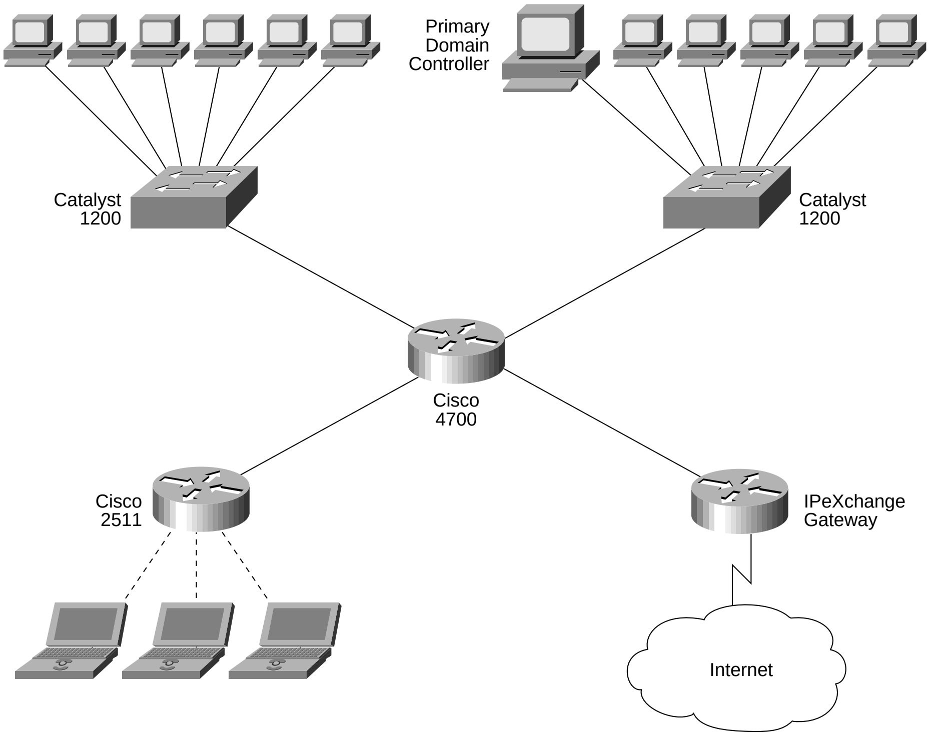
Customers using NWLink (NetBIOS over IPX) who want Internet access but do not want the complexity of configuring TCP/IP on each computer, can use a Cisco IPeXchange gateway to run TCP/IP applications on a computer configured only with IPX. Only the IPeXchange Gateway requires a TCP/IP address.

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
```

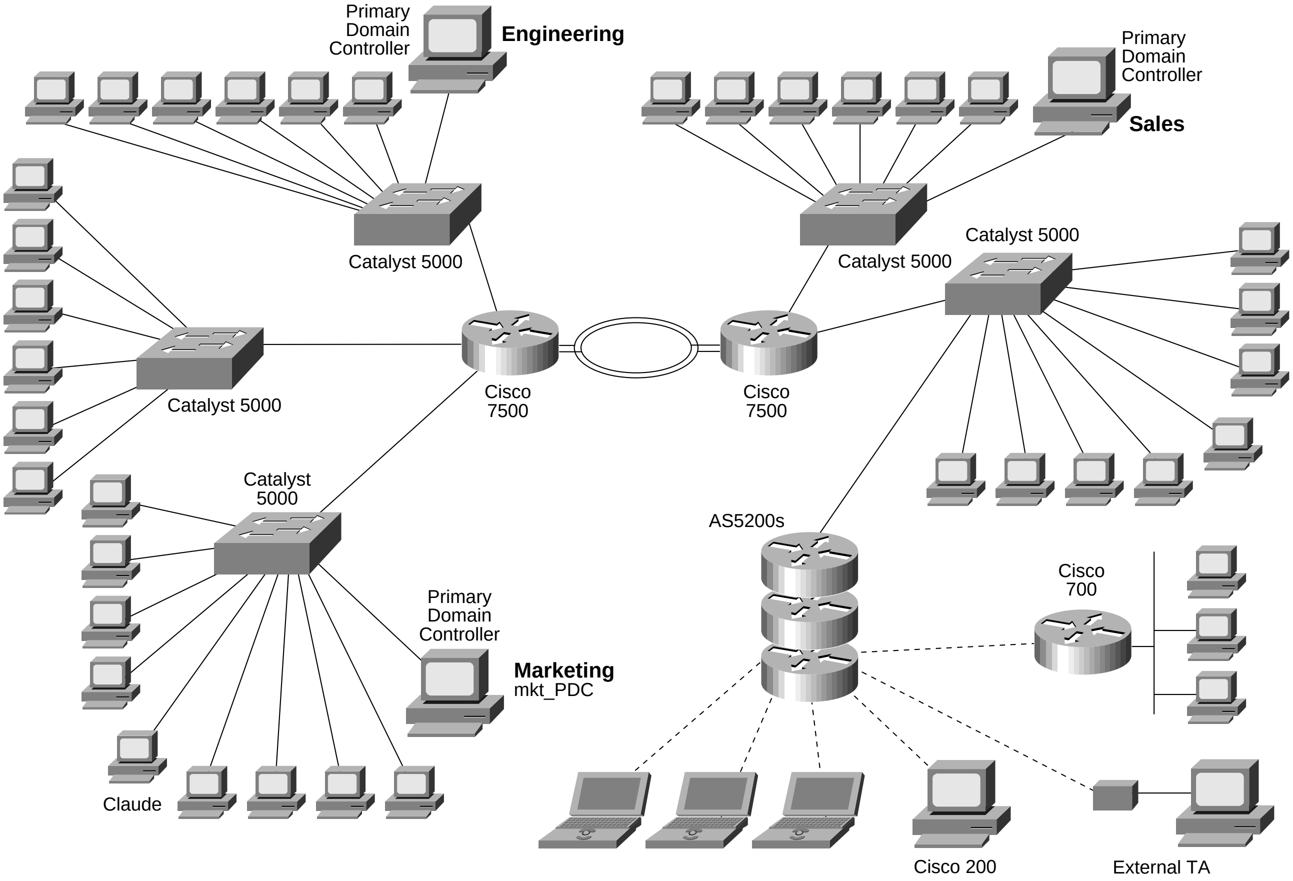
Configuration of Cisco 2511 Access Server

```
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-address n.n.n.n
...
interface ethernet 23
 ip address 1.5.56.1 255.255.255.0
 ip helper-address n.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-server n.n.n.n
ip wins-server m.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
```

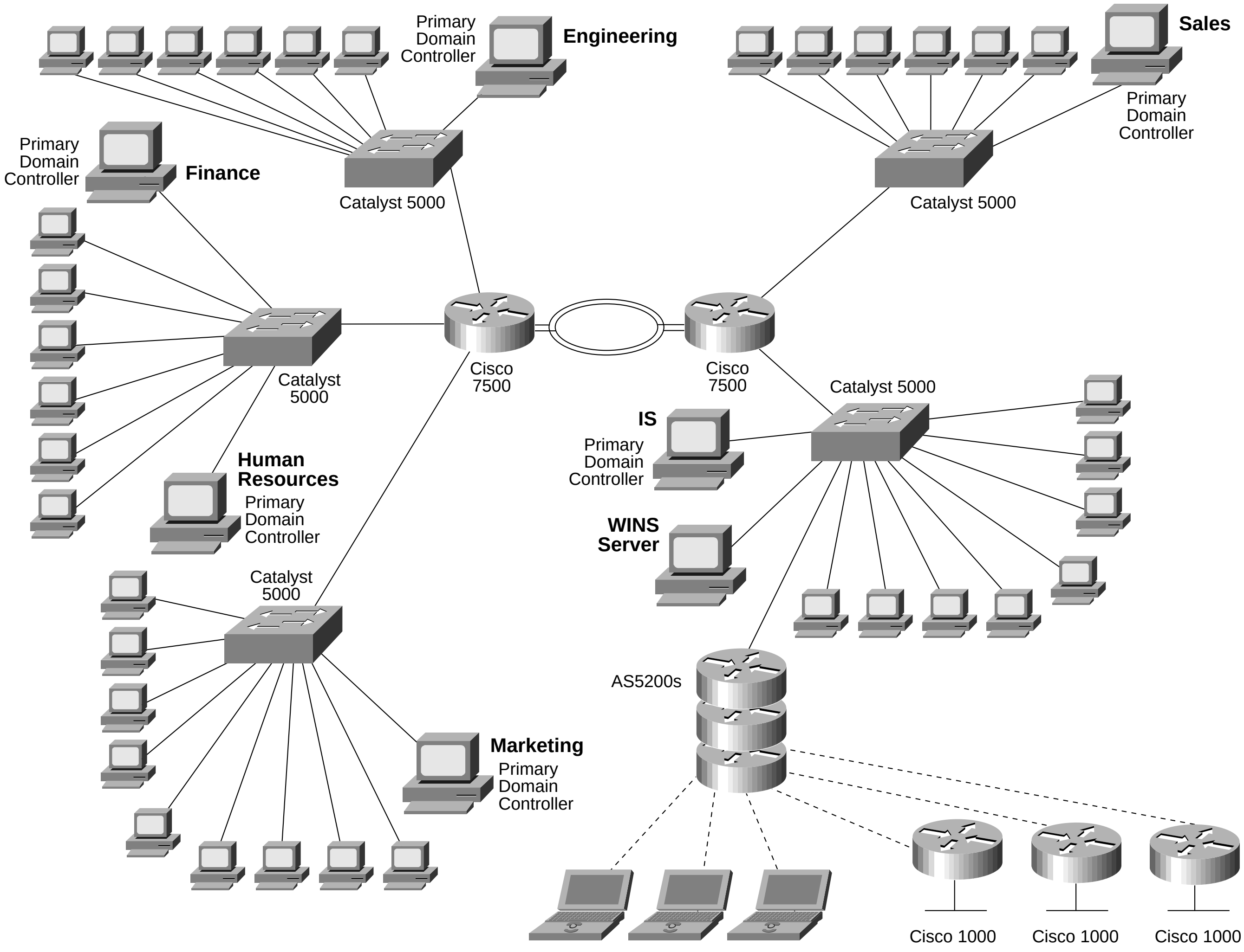
Configuration of Cisco 700 Router

```
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



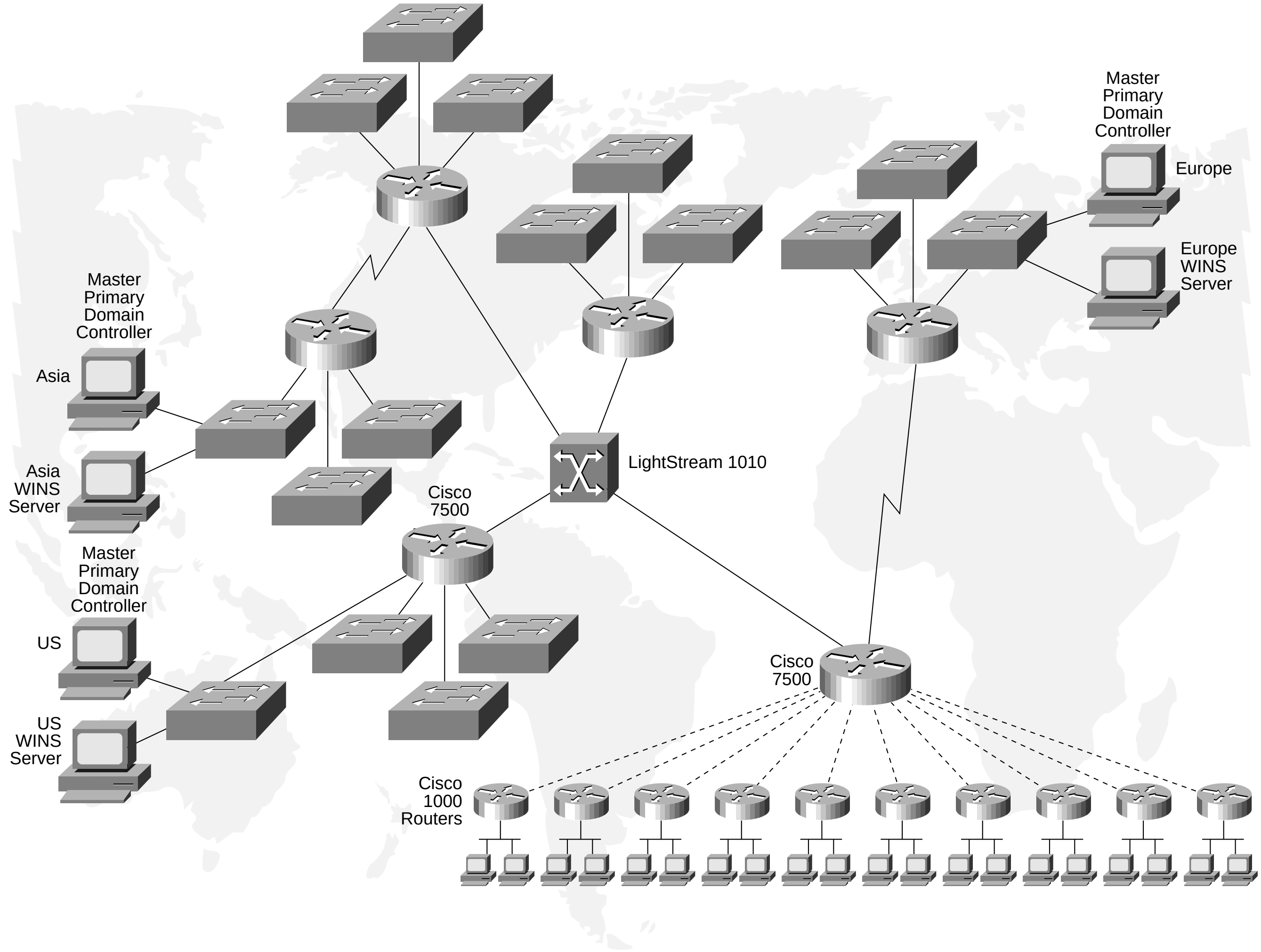
Configuration of a Cisco 1000

```
hostname 1000
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

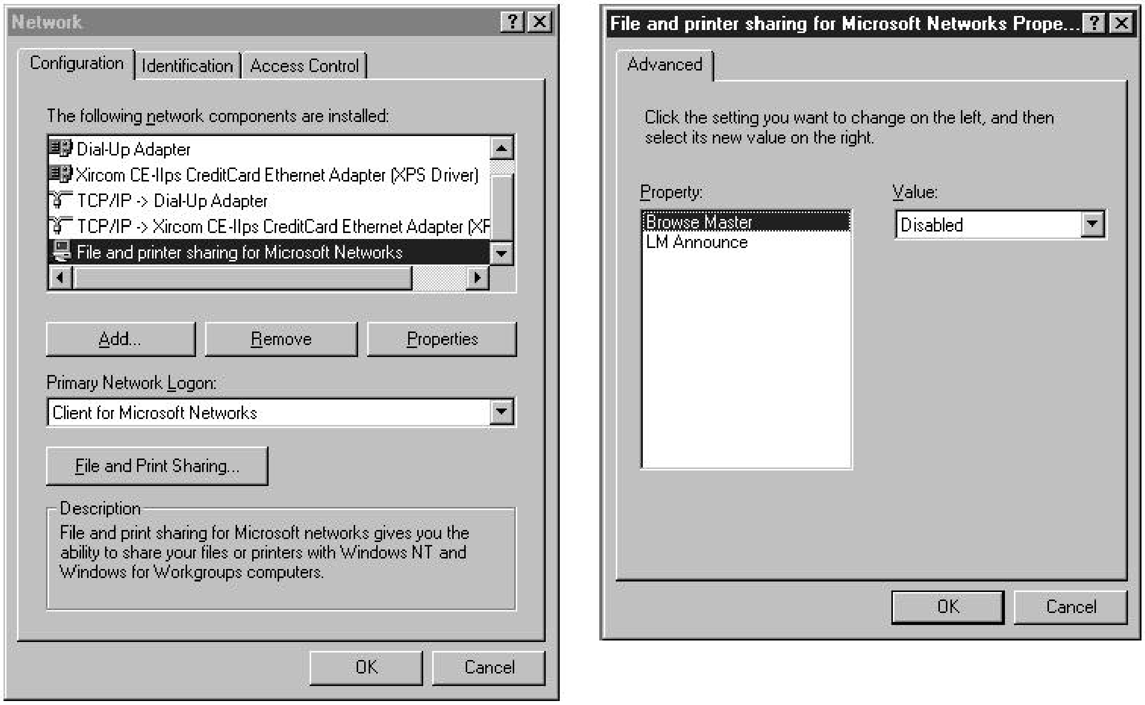
When using Windows for Workgroups 3.11, a new browser file, VREDIR.386, which is included with Windows NT 3.5, must be used to allow browsing to work correctly. Windows 95 already includes this modified browser. The VREDIR.386 file is typically located in the C:\WINDOWS\SYSTEM directory.

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

```
; SYSTEM.INI
;
[Network]
MaintainServerList=No
```

Windows 95

Figure 11. Turning Off Browse Master in Windows 95



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.

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 which 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 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 will attempt to become a browse master. A single workstation incorrectly claiming to be the browse master will hinder browsing for every computer on that entire subnet.

The Windows NT 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

The Microsoft NT 3.51 Resource Kit and Windows NT 4.0 server both include a DNS server that can answer DNS queries by querying a WINS server in the background. The WINS server and the DNS server must be on the same Windows NT machine. All DNS queries to a subdomain (in this example, wins.cisco.com) should be delegated to the DNS/WINS server.

For more information about DNS, see *DNS and Bind* by Paul Albitz and Cricket Liu (O’Reilly and Associates, 1992).

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 cisco.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
```

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
World Wide Web URL:
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Cisco Systems has more than 125 sales offices worldwide. To contact your local account representative, call Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

0896R