

Chapter  
2

**PLANNING  
AND GETTING  
STARTED**

*Get on the  
Fast Track!*



TM

**SYS-ED\  
COMPUTER  
EDUCATION  
TECHNIQUES, INC.**

**Objectives:**

You will learn:

- C To appreciate the hardware requirements and prospective problem areas.
- C Plan for system requirements: RAM and hard disk space.
- C Be ready to install a PDC, BDC, and domain server.
- C Become knowledgeable with the four domain models.
- C Understand the role of trust relationships.
- C Synchronization of domains.
- C Adding and removing computers in a domain.
- C Understand the Browser service.

---

## 1 Hardware Preliminaries

When all of the hardware is new and listed on the Windows NT Hardware Compatibility List (HCL) there should be minimal problems with the hardware being recognized and immediately functional.

Notwithstanding a 100% utilization of HCL approved hardware, the PCI 2.1 standard is an important system standard to be considered when buying a server and other network components. PCI 2.1 is an excellent benchmark for video cards, network interface card, and any other hardware that will go into your server.

The implementation of the PCI 2.1 standard virtually eliminates all hardware interrupt conflicts among network components.

---

### 1.1 Interrupts

Dealing with interrupt conflicts can be a confounding experience, which until resolved can prevent your server and network from becoming operational.

An interrupt is signal sent by the interrupt controller to a PC's CPU when an event occurs which needs responding to.

There are two interrupt controllers that are responsible for monitoring sixteen IRQ lines, numbered 0 to 15.

- C The first controller responds to IRQs 0 to 7.
- C The second controller handles 8 to 15.

Only the first controller is actually allowed to "talk" to your computer's processor. If the second controller receives an interrupt, it signals this event to the first controller by triggering IRQ number 2 and passing the true IRQ number (8 to 15) to the first controller.

Except for PC which utilize IBM's Micro Channel Architecture, no devices in a PC should ever share IRQ's.

Most PCs use the following default IRQ assignments:

IRQ	Common Use	IRQ	Common Use
0	System Timer	8	Real Time Clock
1	Keyboard	9	Available
2	Cascade	10	Available
3	COM2 (Communications Port 2)	11	Available
4	COM1 (Communications Port 1)	12	PS/2 Style Mouse
5	LPT2 (Printer Port 2)	13	Math Coprocessor
6	Diskette Controller	14	Hard Disk Controller
7	LPT1 (Printer Port 1)	15	Available

## 1.2 Port I/O Address

Most devices in a PC require a range of memory addresses (usually 8 bytes) located low in the range of possible addresses. There are called port I/O addresses, and for shorthand, they are typically recorded using just one three-digit number.

Port I/O addresses are locations in memory where a PC's processor can place information to be received by a device or read information to be retrieved from a device.

For example, COM2 normally use the port I/O addresses 02F8 through 02FF (hexadecimal), but often the documentation for a device that can use a COM2 assignment refers to the address range required as 2F8 (referred to as a base address, or base I/O address).

One of the available eight port I/O addresses used by COM2 is used for receiving information from a modem and a second location is used to pass information on to the modem, to be sent out. Each device that requires port I/O addresses may not use all available port I/O addresses, but nonetheless, port I/O addresses are reserved in blocks of eight.

No other device in your PC can share another device's port I/O addresses.

COM ports use by default the following port I/O addresses:

Device	Port I/O Address Block
COM1	3F8 to 3FF
COM2	2F8 to 2FF
COM3	3E8 to 3EF
COM4	2E8 to 2EF

---

### 1.3 Memory Address Space

In the PC design, a range of memory addresses - typically from the hexadecimal A000:00 to DFFF:FF was set aside for the use of add-in adapters (including video).

Adapters can use banks of memory (of varying sizes) in this range to allow your PC's processor to run programs from ROM (Read Only memory) located on the adapter and to communicate with the adapter.

Video cards, SCSI adapters, video capture cards, network cards, and sound cards commonly use memory address space in this region.

---

### 1.4 DMA - Direct Memory Access

DMA - direct memory access channels are used by devices that need to access a PC's main memory (RAM) directly, without requiring attention from a PC's processor.

Using DMA can help increase the responsiveness of your system, freeing your PC's processor to do other things.

Like IRQs, DMA channels are numbered 0 to 15, but all sixteen are available (none are cascaded). DMA channel 2 is normally reserved for the diskette controller. Most others are available for use by some SCSI adapters, network cards, sound cards, video capture cards, tape backup controllers, some CD-ROM adapters, and other devices.

As with any other PC resource, DMA channels cannot be shared.

Conflicts will cause a system to stop working.

---

## 2 Protocols

There are decisions and trade-offs involved in selecting an access protocol.

The three primary protocols are:

- C IPX/SPX
- C NETBEUI
- C TCP/IP

### IPX/SX

Unless an Internet connection is being installed immediately, IPX/SPX should be selected as one of the options when installing Windows NT Server. It is simple to establish and provides better performance than NetBEUI.

If there is a requirement for migrating a Windows NT Server network with a previously installed NetWare network, IPX/SPX will be required in order for the users on each network to "talk" to each other and share printers across networks.

### NETBEUI

Although selecting NetBEUI is an option on the setup screens for Windows NT Server, Microsoft doesn't migrate it. The objective is to convert from an old LAN Manager networks or integrate with LAN Manager or other older networks.

### TCP/IP

Select TCP/IP as one of your options if you plan to immediately establish a connection to the Internet. TCP/IP will provide the best overall transport in terms of flexibility, no matter how large your network gets.

The drawback to initially using TCP/IP is that you need to be assigned specific Internet addresses from an Internet Service Provider (ISP).

## 2.1 Transport Selection Guidelines

Application	NetBEUI	Transport IPX/SPX	TCP/IP
Integrate w/NetWare		X	
Connect to Internet			X
Work with UNIX			X
Route the Transport (WAN)			X
Big Network			X
Small Network	X	X	X

## 2.2 Other Network Protocols

Two other protocols are available to be installed from the network properties:

DLC protocol	<p>Used primarily to access IBM mainframe computers. DLC also is used to connect to printers that are connected directly to a LAN, rather than to a specific printer.</p> <p>Windows NT DLC allows Windows NT computers to connect to IBM mainframes using 3278 emulators and to IBM AS/400 computers using 5250 emulators.</p> <p>The DLC protocol works with Windows NT-based programs and MS-DOS-based and 16-bit Windows-based programs.</p>
Point-to-point Tunneling Protocol	<p>Networking technology that supports multiprotocol virtual private networks (VPNs), enabling remote users to access corporate networks across the Internet by dialing into an internet service provider or by connecting directly to the Internet</p>

### 3 Resource Allocation

#### 3.1 Choosing the Right Amount of RAM

The amount of random access memory in a server is one of the key factors in a server's performance. Windows NT Server holds as many active files as possible in RAM so it doesn't have to keep accessing the hard disk to get information into the CPU to be acted upon. The bottom line is the more RAM, the better the performance.

Given a finite budget, a more reasonable approach calls for calculating the amount of RAM which will provide for sufficient, if not excellent performance.

Factors			Total RAM
System Memory	(Minimum required 16 MB)	A =	A
User Data	Average size of data files open per user.	B =	D
	Number of users.	C =	
	Multiply B by C.	D =	
Applications	Average size of executables being run off the server.	E =	G
	Number of applications being run off the server.	F =	
	Multiply E by F.	G =	
<b>Total System Memory Recommended for this Configuration</b>			<b>A+D+G</b>

#### 4 Choosing the Right Amount of Hard Disk Space

The amount of random access memory in a server is one of the key factors in a server's performance.

The following generic hard disk calculation is provided by Microsoft.

Factors			Hard Disk Size (MB)
System Disk Drive (C: Drive)	Greater of 250 MB -or- 150 MB + Server Memory + 12MB	A =	A
Applications	Size of each application installation.	B =	D
	Number of applications being run off the server.	C =	
	Multiply B by C.	D =	
Applications	Budgeted disk space per user.	E =	G
	Number of users.	F =	
	Multiply by 110% to get an extra 10% margin for error.	G = 1.1	
	Multiply E by F by G.	H	
<b>Total System Memory Recommended for this Configuration</b>			A+D+G

---

## 5 Workgroups and Domains

All Microsoft networks conform to a workgroup model or a domain model of network organization.

### Workgroups

Workgroups are associated with Windows NT's, Windows 95/98, and Windows for Workgroups built-in peer-to-peer networking capabilities.

When a Windows NT workstation needs to share its resources with other users or access shared resources on other computers, it participates in either a workgroup or domain. In a workgroup environment, the security accounts manager (SAM) database on each Windows NT system hold information about how other users can access files and resources.

Windows 95/98, Windows for Workgroups, and MS-DOS clients have limited networking capabilities compared to Windows NT Workstation.

To participate in a workgroup, a workstation will require a computer name and a workgroup name. The primary purpose of the workgroup name is to organize computers into groups for browsing purposes.

The workgroup model often works better for small organizations where computer resources and user accounts are maintained by individual users.

No central point of administration is provided. If a user wants access to other computers in the workgroup, the user must be explicitly added as a user account on each of the computers that is to be accessed.

---

### 5.1 Joining/Creating a Workgroup

A computer can belong to any workgroup on the network.

To change from one workgroup to another:

1. Open the Control Panel.
2. Double-click the Network icon.
3. Click Change on the Identification page of the Network property sheet.
4. Specify a workgroup name.

If the workgroup doesn't exist, this will effectively serve to create a new workgroup. Workgroups simplify network browsing, but they do not simplify system administration.

Redundant user accounts become necessary to share resources between several users and computers. In addition, each user is responsible for permitting or refusing access to his own computer resources. In a large organization, this scheme can become quite unwieldy.

## Domains

As a network grows, keeping track of and supporting resources and users can become exceedingly complex. Even on smaller networks, distributed resources can be difficult to manage.

Domains are associated with the Windows NT Server product and provide enhanced security on large multi-server networks. Domains enable centralization of account access and account management while still enabling users to access the network and its resources from any point in the network.

In a domain, security information is stored on a central Windows NT Server computer called the Primary Domain Controller (PDC). The master user account database is placed on this server.

Other servers in the domain can be installed as Backup Domain Controllers (BDCs), meaning they replicate the user account database on the PDC.

Unlike a workgroup, in which a user must have an account on the computer being logging on to, with a domain a user can log on from any workstation in the domain.

When users log on to a domain, they are authenticated by the PDC and can gain access to other servers based on the PDC information, rather than user account information at each server.

The domain model provides a central point of administration for:

C	user accounts	C	resource sharing
C	access rights	C	permissions

Domains allow users to log on to the network only once while gaining access to all network resources, even in a multiple-server environment.

If there are multiple domains, each has its own master user account database and users must have an account on each. However, Windows NT Server domains can trust each other. With a trust relationship between domains, the authenticated user will be able to access the trusting domain.

Users can then log onto one computer and access other computers without logging onto each computer separately.

Trust relationships link together two or more domains.

- C Windows NT Servers can only be members of a domain.
- C Windows NT Workstation computers can become members of a workgroup or a domain, as is the case for both Windows for Workgroups 3.x and Windows 95/98 computers.

---

## 6 Domain Components

---

### 6.1 Primary and Backup Domain Controllers

Each domain includes one primary domain controller (PDC), and can (optionally) include one or more backup domain controllers (BDCs).

#### Primary Domain Controller - PDC

The PDC stores the account and security database, and responds to access requests from workstations and servers in the domain. The PDC checks the validity of the account and password provided by the remote process, then approves or disapproves the access request.

Changes to the user account database are made only on the primary domain controller and then propagated automatically to the backup domain controllers, where read-only copies of the database are maintained.

The administration of the user accounts and privileges, is done at the PDC. The administrator, however, does not have to be logged on physically to the PDC. Rather, the administrator can log on from any computer in the workgroup, including through a dial-up networking connection.

#### Backup Domain Controller - BDC

Often, especially in large organizations, a domain will have at least one other server known as a Backup Domain Controller (BDC).

The BDC provides a backup to the PDC. The PDC replicates the user account database and related information to all BDCs on the network.

A BDC can perform most PDC network tasks, such as validating logon requests, but does not promote itself to PDC and does not become domain master browser in the event of a failure.

If the PDC is unable to respond to an access request, the BDC handles the request.

Although it isn't a requirement that there be a BDC on the network, it is a good practice to create one.

---

### 6.2 Domain Server

A third type of server can also exist in a domain: a server.

A domain server does not authenticate user logons. Its only purpose is to run application programs or to act as a dedicated application server for products like SQL Server, Exchange Server, or other back-end client/server applications.

---

### **6.3 Workstations**

Workstations can be any of the following:

- C MS-DOS
- C Microsoft Windows 3.x
- C Microsoft Windows for Workgroups
- C Microsoft Windows 95/98
- C Microsoft Windows NT Workstation
- C OS/2
- C Macintosh



## 7 Cross Domain Management in Windows NT Networks

In Windows NT Server a trust relationship is a link between two domains. It allows one domain (the trusting domain) to trust another (the trusted domain). This means that the trusting domain can recognize all user and global group accounts from the trusted domain.

Establishing trust relationships between domains on a network enable user accounts and global groups to be used in domains other than the domain where they are located.

Administration becomes easier because a user account only needs to be created once on the entire network, yet can be given access to any computer on the network.

Trust relationships are controlled with the User Manager for Domains.

Trust relationships can be one-way or two-way. A two-way trust relationship is a pair of one-way relationships, where each domain trusts the other.

When established correctly, trust relationships allow each user to have only one user account in the network (defined in the user's home domain), yet have access to network resources in other domains.

### 7.1 Domain Models

Large-scale enterprise networks must choose from one of four major Windows NT Server domain models:

Domain Model	Description
Single Domain	For networks that don't have too many users and don't need to be logically divided for effective management, one single large domain may suffice.  Obviously, no trust relationships are required.
Master Domain	All user accounts and global groups are created in one domain, the master domain, whose main purpose is to manage the network's accounts.  All other domains trust this master domain, and users in the master domain can use the user accounts and global groups defined within the user domains.
Multiple Master Domain	Suitable for larger networks, this network type contains several master domains; all user accounts on the network are created in one or another of the master domains.  Each master domain has a two-way trust relationship with all other domains. All other domains trust each master domain, but may or may not trust each other, depending on the needs of the network.

Domain Model	Description
Complete Trust	<p>Each domain on the network has a two-way trust relationship with every other domain. Every domain administrator can manage his or her own domain and define its own users and global groups.</p> <p>Because of the multiple trust relationships, these users and global groups can be used on all domains in the network.</p>

---

## 7.2 Trust Relationships

A trust relationship is a special logical relationship between domains.

In a trust relationship, one domain trusts another domain's users. The trusting domain allows users who have accounts in the trusted domain, and domain B is the trusted domain. A user from domain B can access resources in domain A.

A trust relationship can be unidirectional or bidirectional. Just because domain A trusts domain B doesn't mean that domain B trusts domain A.

Domain trust relationships are not transitive. This means that trust does not pass from one domain to another.

- C If domain A trusts domain B, and domain B trusts domain C, that doesn't mean that domain A trusts domain C.
- C If domain A is to trust domain C, the relationship between domain A and domain C must be explicitly set up.

---

## 8 Creating a Domain

The process of creating and managing a domain requires that a primary domain controller be created for each domain. Optionally, a backup domain controllers can be created.

A domain can be created in two ways:

- When installing Windows NT Server create a new primary domain controller.
- Use the Network property sheet which is accessed from the Network icon in the Control Panel to change the name of the domain on a primary domain controller to a new domain name.

### Security IDs

Windows NT Server assigns a Security ID (SID) to a PDC when the PDC is created. The SID then becomes a key component of the domain's security mechanism.

As BDCs and computers are being added to the domain, the PDC's SID is prefixed to those computers' names. When those other computers connect to the domain, they do so using SID.

Performing an upgrade on the PDC retains the SID and doesn't cause a loss of domain identity.

---

### 8.1 Creating a Domain During Setup

During the installation of Windows NT Server, Setup prompts for the designation of the security role of the computer.

The choice can be made between domain controller:

<input type="radio"/> PDC: Primary Domain Controller	<input type="radio"/> BDC: Backup Domain Controller	<input type="radio"/> Server
---	--	------------------------------

If the computer is specified to be a PDC, the name of the domain that the server will control is entered. Setup then searches the network to verify that the domain name which has been specified does not already exist.

Setup proceeds only if the name specified is a new domain name.

---

## 8.2 Moving a Domain Controller to a New Domain

A new domain can be created by moving an existing domain controller to a new domain.

The following steps have to be implemented:

1. Open the Control Panel and double-click the Network icon.
2. Click the Identification tab of the Network property sheet to display the Identification page.
3. Click the Change button to open the Identification Changes dialog box.
4. In the Domain Name text box, type the name for the new domain.
5. If the server's computer name is to be changed, type a new name in the Computer Name text box.
6. Choose OK.

---

## 8.3 BDC: Backup Domain Controller

A BDC can only be created when installing Windows NT Server. A Backup Domain Controller (BDC) receives a copy of the user account database from the PDC, and handles requests for authentication when the PDC is unavailable.

For example, when shutting down the PDC for maintenance, a BDC on the network should be promoted to PDC. Doing so with the PDC online automatically causes the PDC to be demoted to a BDC. The BDC can then handle logon authentication for the domain.

A BDC is an important consideration in designing a network.

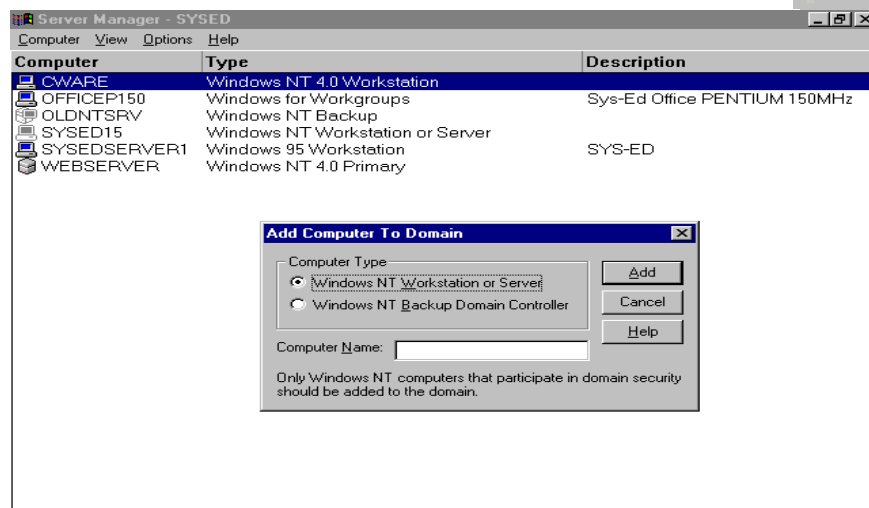
---

## 8.4 Administration Issues

The following issues are central to effective planning and administration of a Windows NT network.

C	the domain model to be used.	C	BDC's - promoting/demoting a BDC to PDC.
C	planning/establishing trust relationships.	C	synchronization

## 9 Adding and Removing Computers in a Domain



Workstations and servers can be added to a domain through the Server Manager, which then enables the user of that workstation or server to join that domain.

It is also possible for an administrator with domain privileges to add a workstation to a domain.

To add computers to a domain, follow these steps:

1. Log on the server as Administrator, then open the Server Manager.
2. Choose computer, Add to Domain; the Add Computer to Domain dialog box appears.
3. Specify the function of the computer to be added by selecting the appropriate option button.
4. Type the name of the computer being added in the Computer Name text box.
5. Choose Add.
6. Repeat steps 3 through 5 for other computers to be added.
7. After having finished adding computers, choose Close.

---

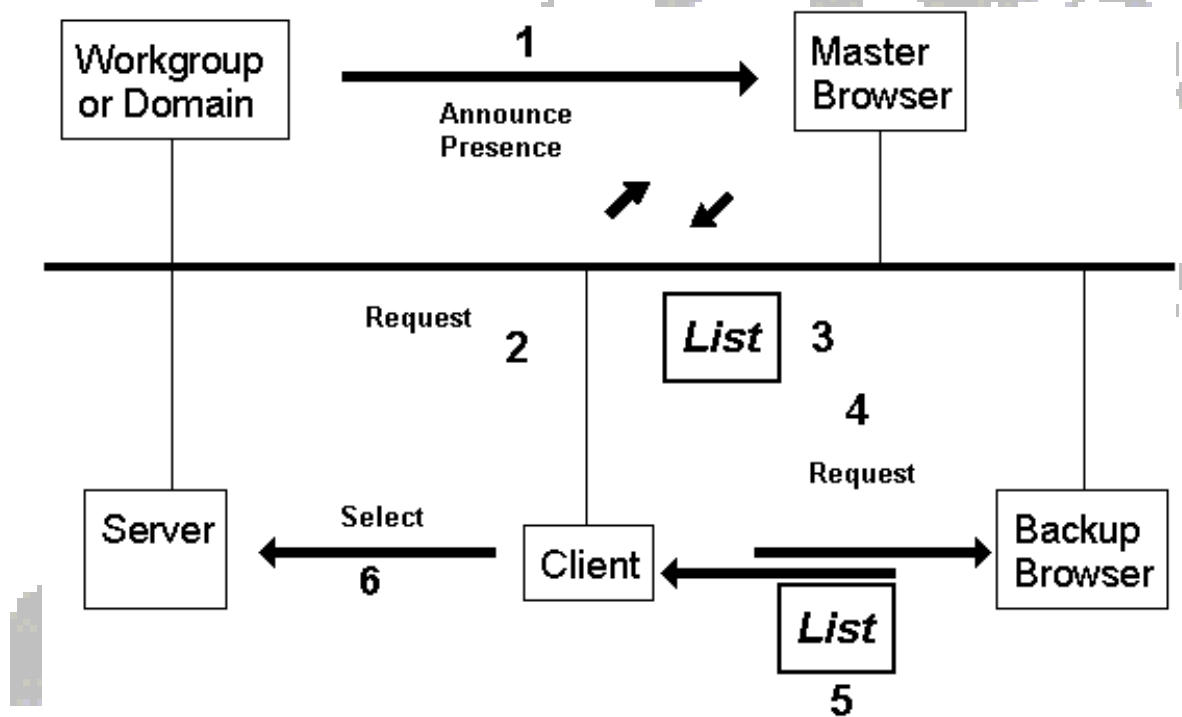
## 10 Browser Service

Windows NT provides the Computer Browser service to display a list of currently available resources.

The Browser services maintains a centralized list of available network resources. This list is distributed to specially assigned computer that perform browsing services, along with their other normal services.

By assigning the browser role to specific computer, the browser service lowers the amount of network traffic required to build and maintain a list of all shared resources on the network.

This also frees the CPU time each computer would have had to use in creating a network resource list.



## 10.1 Browser Server Roles

Role	Explanation
Non Browser	<p>A computer configured so that it will not maintain a browse list.</p> <p>Client computers are commonly non browsers.</p>
Potential Browser	<p>A computer that is capable of maintaining a browse list and can be elected as a master browser.</p> <p>A master browser can designate a potential browser to act as a potential browser.</p>
Preferred Master Browser	<p>An administrator can configure a specific computer to be the preferred master browser. When this computer is started, it designates itself as the master browser for the domain or workgroup.</p> <p>If there already is a master browser and other computers were up and running in the workgroup before this one was turned on, the preferred master browser forces an election. The election process ensures that there is only one master browser per workgroup or domain. The result is that the preferred master browser assumes the role of the master browser.</p> <p>A preferred master browser will not win an election over a Primary Domain Controller.</p>
Backup Browsers	<p>A computer that receives a copy of the browse list from the master browser. It then distributes the list to the browser clients upon request.</p> <p>Computers running Windows NT Workstation, Windows for Workgroups, or Windows 95/98 can be backup browsers if there are fewer than three Windows NT Server computers performing backup-browser functions for the domain.</p> <p>Backup browsers call the master browser for every 15 minutes to get the latest copy of the browse list and a list of domains. Each backup browser caches these lists and returns the list of servers to any clients that send a remote NetServerEnum API call to the backup browser.</p> <p>If the backup browser cannot find the master browser, it forces an election of the master browser.</p> <p>The data limit for the list of servers maintained on computers running a version of Windows NT prior to version 4.0, Windows for Workgroups, or Windows 95/98 is 64K.</p> <p>This limits the number of computers in a browse list for a single workgroup or domain to between 2,000 and 3,000 computers</p>

Role	Explanation
Master Browser	<p>Is the computer that collects and maintains the master list of available network resources. The browse list includes all servers in the master browser's domain or workgroup, and the list of all domains on the network. It also distributes the browse list to the backup browsers.</p> <p>When a domain spans more than one subnetwork, the master browser will do the following tasks:</p> <ul style="list-style-type: none"><li>• Maintain the browse list for the portion of the domain on its subnetwork.</li><li>• Provide lists of backup browsers on the local subnetwork of a TCP/IP-based network to computers running Windows NT Server, Windows NT Workstation, and Windows for Workgroups.</li></ul>

If a TCP/IP-based subnetwork is comprised of more than one domain, each domain has its own master browser and backup browsers.

On networks using the NWlink IPX/SPX-compatible network protocols, name queries are sent across routers, ensuring that there is always one master browser for each domain.

NetBEUI (NBF) is not designed for a routed network and requires a separate master browser per subnet.

When a computer starts and its MainServerList registry entry is set to Auto, the master browser must tell that computer whether or not to become a backup browser.

#### C Domain Master Browser

The domain master browser is responsible for collecting announcements for the entire domain, including any network segments, and for providing a list of domain resources to master browsers.

The domain master browser is always the primary domain controller (PDC) of a domain.

The PDC of a domain is given priority in browser elections to ensure that it becomes the master browser. The Windows NT Browser service running on a PDC has the additional role of being the domain master browser.

For a domain that uses TCP/IP and spans more than one subnetwork, each subnetwork functions as an independent browsing entity with its own master browser and backup browsers.

NWLink and NBF transports don't use the domain master browser role because those transport have only a single master browser for the entire network. Browsing across the wide area network (WAN) to other subnetworks requires at least one browser running Windows NT Server, Windows NT Workstation, or Windows for Workgroups 3.11b on the domain for each subnetwork.

A PDC typically functions as the domain master browser on its subnetwork.

When a domain spans multiple subnetworks, the master browser of each subnetwork announces itself as the master browser to the domain master browser, using a directed MasterBrowserAnnouncement datagram. The domain master browser merges the server list from each subnetwork master browser with its own server list, forming the browse list for the domain. The process is repeated every 15 minutes to ensure that the domain master browser has a complete browse list of all the servers in the domain.

The master browser on each subnetwork also sends a remote NetServerEnum API call to the domain master browser to obtain the complete browse list for the domain. This browse list is available to browser clients on the subnetwork.

### **Caveat**

Windows NT workgroups cannot span multiple TCP/IP subnetworks. Any Windows NT workgroup that spans subnetworks actually functions as two separate workgroups with identical names.

---

## **10.2 Multiple Browser Roles**

A single computer may play multiple browser roles. For example, the master browser may also be the domain master browser.

---

## **10.3 Browser Operation**

The Windows NT Computer Browser Service operates as follows:

1. After startup, all computers that are running the Server service announce their presence to the master browser in the workgroup or domain.
2. The first time a client computer attempts to locate available network resources, it contacts the master browser of the domain or workgroup for a list of backup browsers.
3. The client then requests the network resource list from a backup browser.
4. The backup browser responds to the requesting client with a list of domains and workgroups and the list of servers local to the client's domain or workgroup.

5. The user at the client selects a local server, a domain, or a workgroup to view available servers.
6. The user selects the appropriate server, searches for the resource on which he/she wants to establish a session to use that resource, and contacts the appropriate server.

---

### 10.4 Browser Criteria

Browser criteria are a means of determining the hierarchical order of the different types of computer systems that are in the workgroup or domain.

Each browser computer has certain criteria, depending on the type of system it is.

The criteria are:

- C operating system
- C operating system version
- C current role in the browsing environment

---

### 10.5 Browser Election Process

The election process insures that only one master browser exists per workgroup or domain.

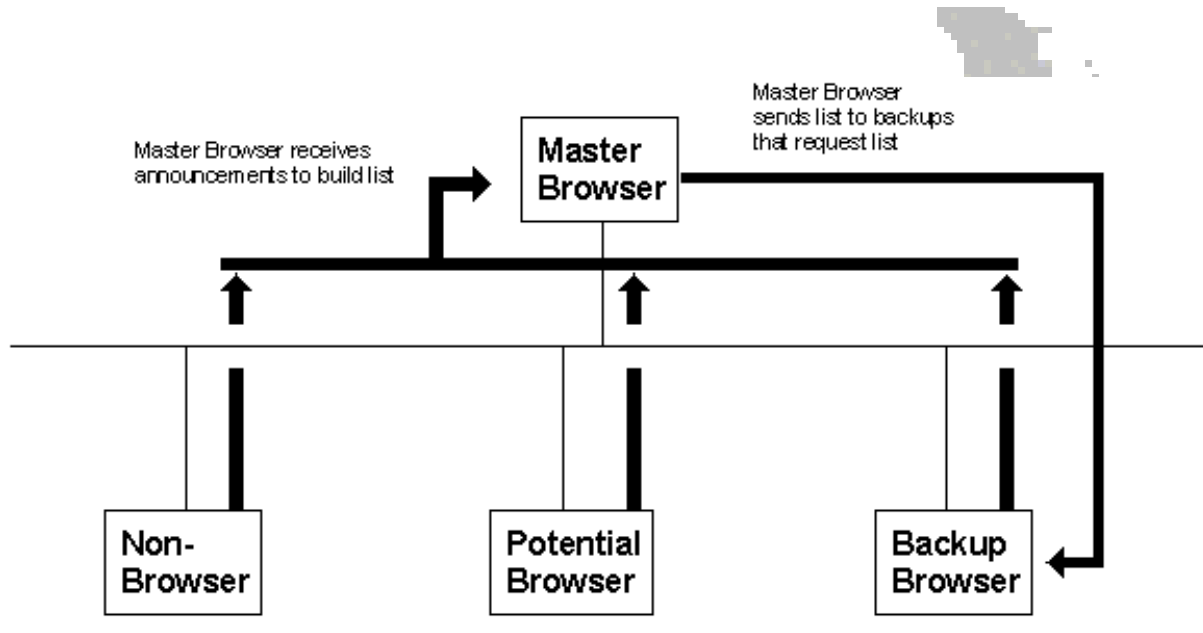
An election is initiated by a computer when any of the following occurs:

- C A client computer cannot locate a master browser.
- C A backup browser attempts to update its network resource list and cannot locate the master browser.
- C A computer that has been designated as a preferred master browser comes on line.

The following lists, arranged by criteria, state the hierarchy by which a computer in a Microsoft domain would win an election:

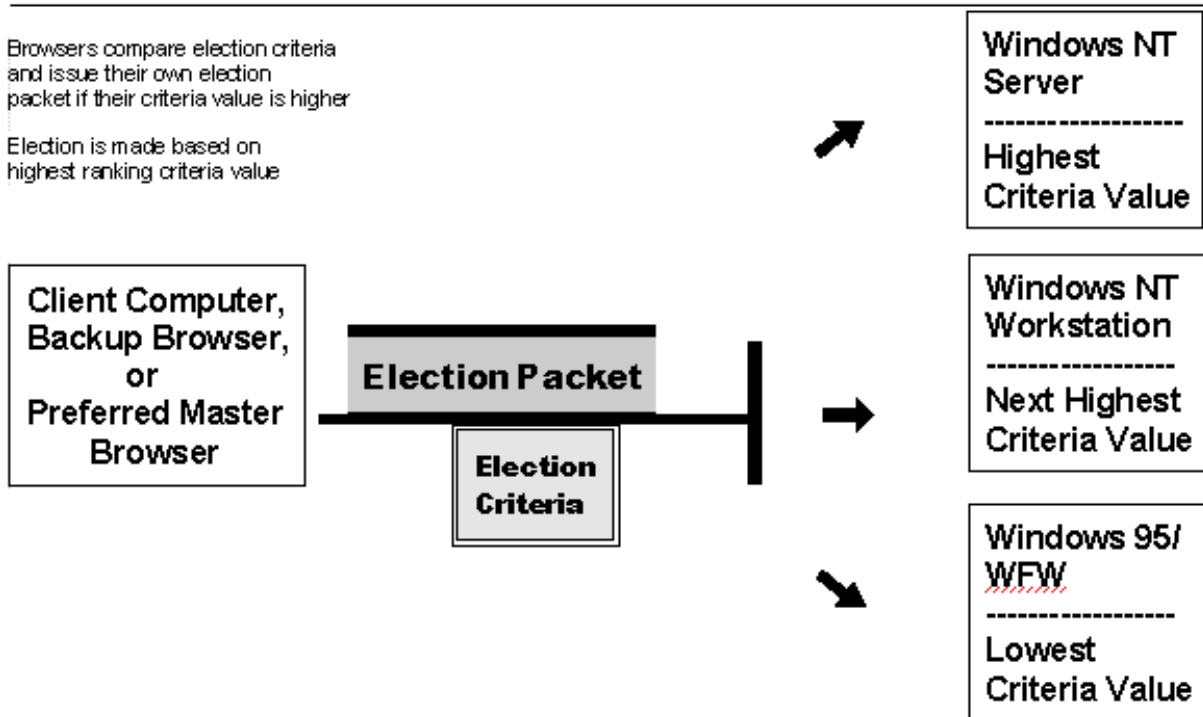
Operating System	Operating System Versions	Current Browser Role
- WNT Server - PDC - Windows NT Server	- 4.0 - 3.51	- Preferred Master - Master
- WNT Workstation - Windows 95/98	- 3.5 - 3.1	- Backup Browser - Potential Browser
- Windows for Workgroups		

10.6 Browser Announcements



Browsers compare election criteria and issue their own election packet if their criteria value is higher

Election is made based on highest ranking criteria value



---

## 10.7 Number of Browsers

**Rules**

- C If there is currently a PDC in the domain, it will be the master browser for the domain.
- C Every BDC in the domain will be a backup browser for the domain. The only exception to this is if the BDC is needed as a master browser because the PDC has failed. In that case the BDC will be the master browser for the domain.
- C If a computer's MaintainServerList registry parameter is set to YES, this computer will be a backup browser for the domain or TCP/IP subnet.
- C If no backup browsers are selected for the domain based on the preceding rules, the master browser determines the number of backup browsers for the domain.
- C If a computer's MaintainServerList registry parameter is set to Auto, the master browser will select some of those computers to act as backup browsers based on the number of computers in the domain.

Number of Systems	Number of Backup Browsers	Number of Master Browsers
1	0	1
2 - 31	1	1
32 - 63	2	1

- C For each 32 additional computers added to the workgroup or domain, another backup browser is selected for the domain.
- C For the TCP/IP transport, each subnet independently enforces the preceding set of rules.

---

## 10.8 Browsing Failures

**Non-browser Failure**

If a non-browser computer fails to announce itself, it is eventually removed from the list. The configured announcement period is between 1 and 12 minutes.

If the non-browser has not announced itself after three announcement periods, the master browser removes the computer from the browse list. It can take up to 51 minutes before all browsers know of a non-browser's failure (12 x 3 minutes - non browser) and 15 minutes for all the backup browsers to retrieve the updated list from the master browser.

**Backup-browsers Failure**

If a backup browser fails, it is removed from the master browser browse list in the same amount of time as the as non-browser (up to 51 minutes).

If a browse list cannot be obtained from the missing backup browser, the client selects another backup browser from its cached list of three backups.

If all of the client's known backup browsers fail, the client attempts to get a new list of backup browsers from the master browser.

If the client is unable to contact the master browser, the client forces an election.

**Master-browser Failure**

When a master browser fails, a backup browser detects the failure within 15 minutes. When this happens a backup browser forces an election to select a new master browser.

If a client performs its browse request after a master browser fails but before a backup browser detects the failure, the client forces an election.

If a master browser fails and there are no backup browsers, browsing in the workgroup or domain will not function effectively.

During the gap between the master browser's failure and the election of a new master browser, the workgroup or domain can disappear from the lists that are visible to computers in other workgroups and domains.

**Server Shutdown or Failure**

If a backup browser shuts down properly, it sends an announcement to the master browser that it is shutting down. The backup browser does this by sending an announcement that does not include the Browser service in the list of running services.

If a Master Browser shuts down gracefully, it will send a ForceElection datagram so that a new master browser can be chosen.

When the computer is shut down normally, it makes an announcement that causes the master browser to remove it from the list.

If a backup browser shuts down properly, it sends an announcement to the master browser that it is shutting down.

**Domain Master-browser Failures**

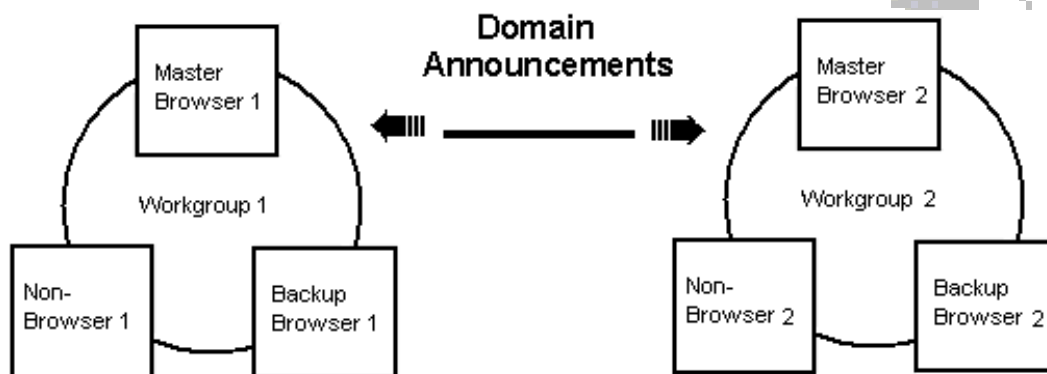
If the domain master browser fails, the master browser for each network segment provides a browse list, containing only the servers in local network segment. All servers that are not on the local network segment will eventually be removed from the browse list. Users will still be able to connect to servers on the other network segments if they know the name of the server. Because a domain master browser is also a PDC, administrator can correct the failure by promoting a BDC to PDC.

---

**10.9 Browser Announcement Intervals**

Type of Message	Protocol/Transport	Default Interval
PDC-BDC Message Replication	Any	Every 5 minutes.
Master Browser to backup Browser Replication	Any	Every 15 minutes.
Server Announcement to Master Browser	Any	Once each minute, then every 2 minutes, then: every 4 minutes, then every 8 minutes, then every 12 minutes, and every 12 minutes thereafter
NetBIOS Keepalive Message	TCP/IP	Every 60 minutes.
NetBIOS Keepalive Message	IPX/NetBEUI	Every 30 seconds.

---

**11 Browsing Multiple Workgroups / Domains**

Upon becoming a master browser, each master browser broadcasts a Domain announcement to each workgroup or domain every minute for the first five minutes of its life as master browser.

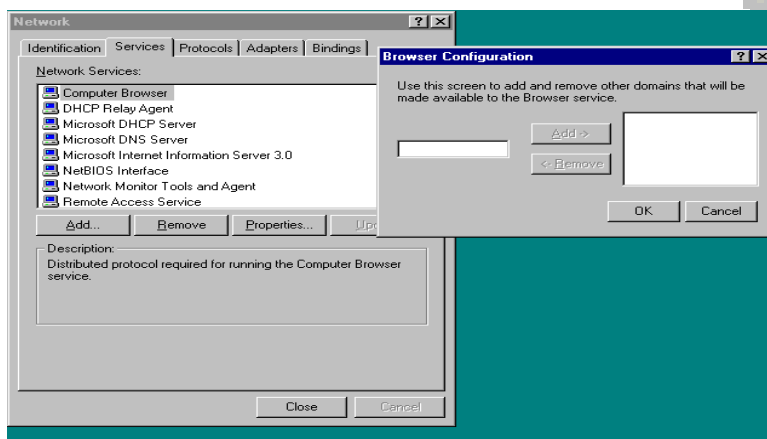
After the first five minutes, the master browser makes Domain announcement broadcasts once every 15 minutes. If a workgroup or domain has not announced itself for a period equaling three times the announcement period, the workgroup or domain is removed from the list of workgroups and domains.

Therefore, it is possible that a workgroup or domain will appear in the browse list for up to 45 minutes after the workgroup or domain has ceased operations.

It is the task of the master browser in each workgroup or domain to receive Domain Announcement packets from other workgroups and domains. The master browser uses these announcements to build a list of available workgroups and domains. This list is also given to backup browsers every 15 minutes so that they can return a list of network resources available in their workgroup or domain, as well as a list of other workgroups and domains.

The Domain Announcement packet contains the name of the domain, the name of the master browser for that domain, and whether the master browser is running Windows NT Workstation or Windows NT Server. In addition, if the master browser is running Windows NT Server, the Domain Announcement also specifies whether the system is the domain's PDC.

## 11.1 Windows NT Server - PDC: Browser Configuration



## 11.2 Browse Service Across a WAN

When using domains that are split across routers, each TCP/IP network segment functions as an independent browsing entity with its own master browser and backup browsers.

Browsers elections will occur within each network segment.

Domain master browsers are responsible for spanning network segments to collect computer-name information.

- C The domain master browser is the PDC of a domain.
- C The master-browser computers on the subnets can be running Windows NT Server, Windows NT Workstation, Windows for Workgroups version 3.11b, or Windows 95/98.

When a domain spans multiple network segments, the master browsers for each network segment use a directed datagram - MasterBrowserAnnouncement datagram - to announce themselves to the domain master browser.

The MasterBrowserAnnouncement datagram notifies the domain master browser that the sending computer is a master browser in the same domain and that the domain master browser needs to obtain a copy of the master browser's list. When the domain master browser receives a MasterBrowserAnnouncement datagram, it sends a request to the network segment's master browser, which announced itself in order to collect a list of the network segment's servers.

The domain master browser then merges its own server list with the server list from the master browser that issued the announcement. This process is done every 15 minutes and guarantees that the domain master browser has a complete browse list of all the servers in the domain. When a client issues a browse request to a backup browser, the backup browser returns a list of all the servers in the domain, regardless of the network segment on which they are located.

Workgroups using Windows NT or Windows for Workgroups cannot span multiple network segments. Any workgroup of either kind that does not span network segments will function as two separate workgroups with the same name.

---

### 11.3 Browsing with TCP

Browser-service communication relies on broadcasts.

TCP is commonly used in a WAN environment. In this type of environment, where domains are separated by routers, special broadcast problems will need to be addressed because broadcasts do not pass through routers.

The two basic issues are:

- C How a browser separated by a router perform browser functions.
- C How local clients browse remote domains that are not on their local network segment.

There are three methods that can be used for setting up WAN browsing with TCP/IP.

- C Windows Internet Name Service (WINS)

WINS resolves NETBIOS names to IP addresses so that datagrams can be sent to the targeted computer.

Implementing WINS eliminates the need to configure the LMHOSTS file or to enable UDP port 137.

- C LMHOSTS file

NetBIOS name resolution is typically performed through broadcasts, which will resolve names only on the local network segment. To resolve names of computers located on another network segment, the LMHOSTS file must be configured. The LMHOSTS file must contain a NetBIOS name-to-IP address mapping for all computers that are not on the local network segment.

To implement communication between network segments and the domain master browser, the administrator must configure the LMHOSTS file with the NetBIOS names and IP addresses of all browsers.

To ensure that the master browser for each network segment can access the domain's PDC, the PDC for each domain must exist in the LMHOSTS file on each master browser and have the #DOM tag.

To guarantee that the PDC can request the local browse list from the network segment's master browser, TCP/IP and all other WAN transports must cache the client's IP address.

C UDP Port 137 / NetBIOS Name Service Broadcasts

Some routers can be configured to forward specific types of broadcasts and filter out others.

All NetBIOS over TCP/IP (NetBT) broadcasts are sent to the UDP port 137, which is defined as the NetBT Name Service.

Routers normally filter out these frames because they are sent to the hardware and subnet broadcast addresses. However, some routers allow all frames sent to this particular UDP port - which is used only by NetBT - to be forwarded

This causes the to browser to look as if it is on one big network segment.

All domains and computers within the network segment are seen by all computers.