Designed for

Microsoft®
Windows®98
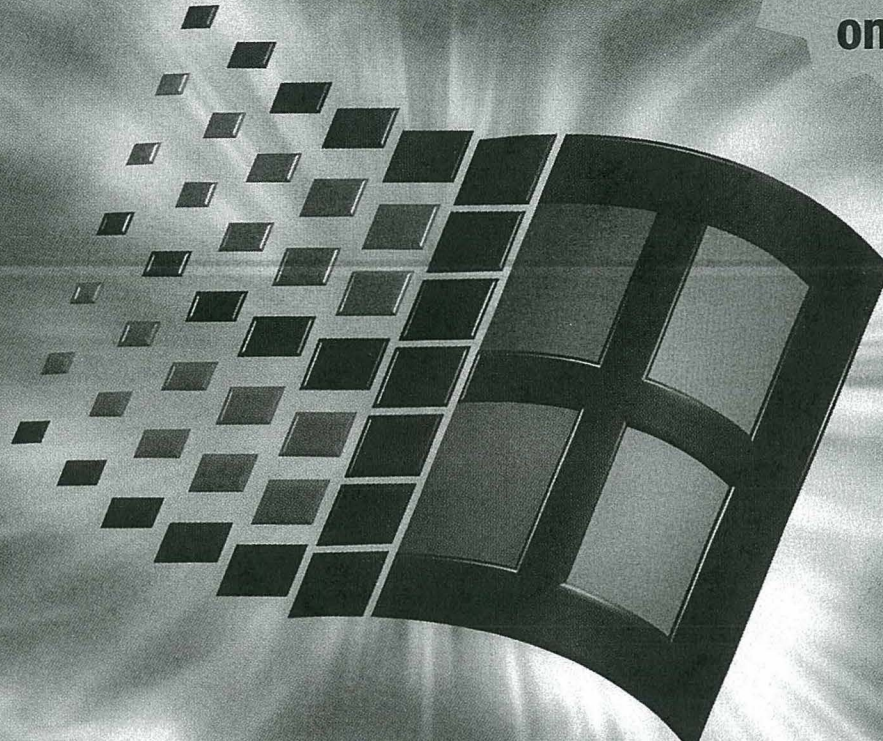
CD-ROM
Included

**Valuable tools included on CD!**

*The Technical Guide to Deploying, Configuring, and Supporting Windows 98 in Your Organization*

# Microsoft Windows®98 ResourceKit

## The Professional's Companion to Windows 98

**Microsoft** Press

# Microsoft® Windows® 98 Resource Kit

**Microsoft** Press

Material appearing in chapters 17 and 18 is based on material originally created as:
*Novell-Supplied NetWare Clients: The Benefits,*
Copyright © 1997, 1998 Novell, Inc. All rights reserved.
Used, reproduced, and distributed with permission from Novell, Inc.

# CHAPTER 9

# Security

This chapter presents an overview of security features provided in Microsoft Windows 98. It describes their use, together with security features of Internet Explorer version 4.0, in a networking environment. It is intended for system administrators and others who have authority to set security levels for network clients, and for those who need secure communication over the Internet.

**In This Chapter**

**See Also**

# Overview of Security Features

*Computer security* refers to the protection of all components—hardware, software, and stored data—of a computer or a group of computers from damage, theft, or unauthorized use. A computer security plan that is well thought out, implemented, and monitored makes authorized computer use easy and unauthorized use or accidental damage difficult or impossible.

Personal computing depends increasingly on computers connected through networks, and more often through the Internet and intranets. You can use Windows 98 security to prevent unauthorized access to shared resources on computers in a network. The security features built into Windows 98 are described briefly in this section, and in more detail later in the chapter.

## Logon Security

Windows 98 allows users to log on fully. In a networking environment, you can set your system up so that when a name and password pair have been validated against the security authority of a network server, the Windows 98 user interface is displayed.

### Logon Password

A user can log on to all networks and Windows 98 at the same time. If a user's password for Windows 98 or for another network is the same as the password for the primary logon client, Windows 98 automatically logs the user on to Windows 98 and all networks using that password.

---

**Note** A unified password prompt does not enhance security, but eases logging on to the system. As the system administrator, you can require additional passwords for a more secure system.

---

For more information about the logon prompt, see "Using the Windows 98 Logon Password" later in this chapter. Once users log on to their machines, they have the option to cache their passwords. These passwords are cached in a file with a .pwl extension. The file name is the same as the user's name. See "Password Caching" later in this chapter.

### Network Validation

With system policies, you can prevent users from logging on to Windows 98 if their Windows NT or Novell NetWare network logon is not validated. This causes the network logon dialog to appear before, or instead of, the Windows 98 logon prompt. Also, the user list may not be network wide, but specific to a server, and may be different for different servers.

For more information about logon security, see "Network Security" later in this chapter. For more information about system policies, see "Using System Policies to Enforce Password Security" later in this chapter, and Chapter 8, "System Policies."

# Shared-Resource Security

When a computer is running Windows 98 with file and printer sharing services, other users can connect to shared printers, volumes, directories, and CD-ROM drives on that computer. To protect these shared resources, Windows 98 provides user-level and share-level security.

## User-Level Security

With user-level security, a user's request to access a shared resource is passed through to a security provider, such as a Windows NT or NetWare server. The security provider grants or denies the request by checking the requestor's user name and password against a network-wide or server-wide stored list. User-level security does not require file and printer sharing services. These accounts must be created on the machine providing user-level authentication, such as a Windows NT or NetWare server. Windows 98 cannot act as an authentication server for user-level security.

This type of security allows fine-grained control over per-user access and allows individual accountability. The disadvantages are that you must create a user account for each user you want to grant access to, and you must grant that user the access.

## Share-Level Security

With share-level security, users assign passwords to their shared resources. Any user who can provide the correct password is permitted to access the shared resource. The password is stored and checked by the computer where the resource resides. Share-level security requires file and printer sharing services.

---

**Note**  Any subfolders of the shared folder, if they are also shared, must be set with the same level of security as the parent folder.

---

The advantage of this type of security paradigm is that it allows granting access to a broad range of people with very little effort. However, it is not as secure as user-level security, because the password is widely distributed and there is no notion of personal accountability.

> **Note** You cannot use share-level security on NetWare networks, because the File and Printer Sharing for NetWare Networks utility does not support passwords. You can limit access, however, by defining a resource as read-only.

# Password Controls

In addition to setting up passwords for security, Windows 98 also provides password caching, Password List Editor, and system policies.

## Password Caching

Like unified logon, password caching provides a convenient and secure way to access protected resources. The first time a user connects to the resources and saves the password, Windows 98 caches the password in a PWL file. Whenever the user logs on again, the logon password unlocks the PWL file and the resource passwords it contains, and the user then has free access to those resources. If password caching is disabled, users must type the password each time they connect to a password-protected resource.

## Password List Editor

Password List Editor lets you view resources on a password list. It also lets a user view or edit his or her own password file (PWL). You may then delete a password (you cannot view the actual password) so that it can be replaced.

## System Policies

System policies let you enforce a password policy with some or all of these restrictions:

- Disable password caching.
- Require an alphanumeric Windows 98 logon password.
- Require a minimum Windows 98 logon password length.

You can also define system policies that prevent users from enabling peer resource sharing services and that enforce other security techniques, such as preventing users from configuring system components.

For more information, see "Using System Policies to Enforce Password Security" later in this chapter, and Chapter 8, "System Policies."

# Internet and Intranet Security

The Internet is an effective way to communicate and share information with others, but with its use comes a greater need for security. The following security features make it easier for you to protect your computer and your privacy when using the Internet.

## Internet Explorer

Internet Explorer 4.0 has new security options that let you configure a security level to a specific Web site according to how much you trust the content of that Web site. Four security zones are set up in Internet Explorer 4.0. They are:

- An Internet zone that by default contains all Internet sites.
- A Trusted sites zone to which you can assign Web sites you trust.
- A Restricted sites zone to which you can assign Web sites you do not trust.
- A Local intranet zone for computers connected to a local area network.

## Outlook Express

Outlook Express includes tools to protect you from fraud, ensure your privacy, and prevent unauthorized access to your computer. These tools enable you to send and receive secure e-mail messages and to control potentially harmful e-mail messages through security zones.

## Distributed Component Object Model

A distributed application consists of multiple processes that cooperate to accomplish a single task. The Distributed Component Object Model (DCOM) can be used to integrate distributed applications in a network, thus allowing specified users to have access to certain processes.

## Firewalls

A firewall enforces a boundary between networks. The boundary prevents unauthorized access of private networks by preventing the passage of packets between networks.

# Security Planning Checklist

You need to determine the type of exposure or risk you potentially have, and develop a security policy that reflects this level of risk. On the basis of that analysis, choose products, network technology, and business practices for the installation, integration, and management of your system.

Before you integrate Windows 98 security into your network security model, consider the following issues:

**What kind of logon security do you need?** Do you allow users to log on to Windows 98 and the network with the same password? Do you want to require alphanumeric or minimum-length passwords for the Windows 98 logon password? Do you want to require that users be validated by the network security provider before being able to log on to Windows 98? For both Windows NT and NetWare networks, you can use system policies to require validation by a Windows NT or NetWare server before allowing access to Windows 98 and to specify other Windows 98 password restrictions.

**What kind of resource protection do you need on Microsoft networks?** If you enable peer resource sharing, you must decide how to protect those resources with share-level or user-level security. User-level security provides greater security because the network security provider must authenticate the user name and password before access to the resource is granted. Share-level security is not available for NetWare networks.

For more information about NetWare networks, see Chapter 17, "Windows 98 on Third-Party Networks."

**What kinds of access rights will users have to resources protected by user-level security?** You can specify the types of rights users or groups of users have to resources by setting Sharing properties for the shared resource (such as a folder or drive). For example, you can restrict other users to read-only access to files or give them read-access and write-access to files.

**How do you want to enable user-level security?** You can enable security in a setup script or in system policies. If you enable user-level security in either a setup script or Control Panel, remote administration is enabled by default for domain administrators on a Windows NT network and for supervisors on a NetWare network.

**Should password caching be allowed?** You can use system policies to disable password caching and thus require users to type a password each time they access a password-protected resource.

**Should users be able to change Control Panel settings?** You can use system policies to restrict users' ability to change the configuration of system components, their desktops, applications, or network connections in the Control Panel folder.

**Does a particular hard disk need extra protection?** Windows 98 security obstructs hacking over the network; but if a person has physical access to the computer, critical data could still be taken from the hard disk where it resides by using Safe Mode or a floppy disk to start the workstation. If specific data requires greater levels of security, you should store critical files on a secure server. If computers require greater levels of security, Windows NT Workstation is recommended, because it provides a means to protect resources on a hard disk based on a user's identity.

**Are there applications that should not be run?** You may need to restrict access to some applications while supplying access to other applications in your system. To implement this type of security, use system policies. You can also restrict access to parts of an application by using DCOM.

**Do certain processes of an application need protection?** If security is required for a distributed application—that is, one whose component processes are distributed over more than one computer in the network—use DCOM. DCOM provides the structure to share applications at the component level between a server and clients. The components can be shared over the Internet or an intranet. Using DCOM to set a security level for the application automatically applies that security level to each component, wherever located.

**Should Internet or intranet access be limited?** You may need to limit access to certain sites on the Internet and on your intranet. To implement this type of security, use Internet Explorer security features.

# Network Security

Windows 98 allows users to log on fully. The first thing most users encounter after booting their Windows 98 systems is a logon dialog box, which varies depending on the type of network. Once the proper user name and password are validated against the security authority of the network server, the Windows 98 user interface is displayed.

System administrators can configure the Windows 98 system to allow entry into the operating system with no network access (this configuration is the default). As an alternative solution to this problem, system administrators can specify guest accounts that have limited network access.

The Windows 98 user logon should not be construed as a mechanism to fully secure personal computers. Because personal computers are still vulnerable to a floppy boot, all data stored on their disks is potentially available. The underlying file system in Windows 98 is the MS-DOS file allocation table (FAT) file system, which has no built-in encryption or other security mechanisms.

Network resources are secured under Windows 98 using the same security mechanisms employed by network servers on corporate networks. The user name and password in Windows 98 can be configured to be the same as those used by the network server. By doing this, the network manager can control network access, provide user-level security for access to shared resources on the local computer, control the various agents in Windows 98, and limit who has remote administration authority on this Windows 98 system. In this fashion, Windows 98 leverages the existing investment in network servers, management tools, utilities, and infrastructure. System administrators can manage user accounts centrally on the server, just as they always have. They can also use familiar tools for managing user accounts.

## Implementing Network Security

Implementing security in a Windows 98 networking environment involves the following types of activity:

- Define user accounts on a network server or domain controller for user-level security. For more information, see the documentation for the software on the network security provider.

- Install file and printer sharing services, and then enable user-level or share-level security.

- Define access rights for resources protected by user-level security.

- Make the Windows 98 logon password and network logon password the same. Disable password caching if you do not want this feature. For more information, see "Using the Windows 98 Logon Password" and "Using the Windows 98 Password Cache" later in this chapter.

- Define system policies to restrict users' ability to configure the system or shared resources, and to enforce password policies.

- Define Internet and intranet security zones. For more information, see "Setting Up Security Zones" later in this chapter.

## Sharing Resources

Windows 98 provides share-level or, alternatively, user-level security for protecting shared resources on computers running Windows 98 (the share level requires file and printer sharing services).

Share-level security protects shared network resources on the computer running Windows 98 with individually assigned passwords. For example, you can assign a password to a folder or a locally attached printer. If other users want to access it, they need to type in the appropriate password. If you do not assign a password to a shared resource, every user with access to the network can access that resource.

User-level security protects shared network resources by requiring that a security provider authenticate a user's request to access resources. The security provider, such as a Windows NT domain controller or a NetWare server, grants access to the shared resource by verifying that the user name and password are the same as those on the user account list stored on the network security provider. Because the security provider maintains a network-wide list of user accounts and passwords, each computer running Windows 98 does not have to store a list of accounts.

**Note**  For Microsoft networks, the security provider must be a Windows NT domain or workstation. For NetWare networks, it must be either a NetWare 4.*x* server running bindery emulation or a NetWare 3.*x* server.

Figure 9.1 shows how user-level security works for Microsoft networks. The reference numbers are explained after the illustration.
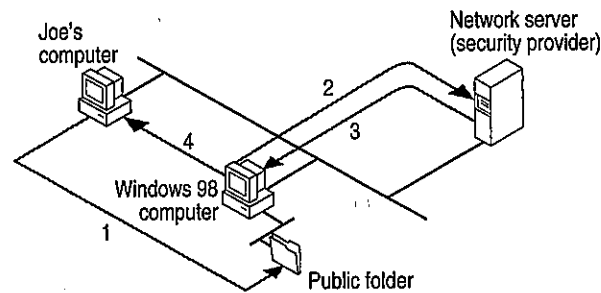


**Figure 9.1   User-level security**

1. Joe's computer is running Windows 98. Joe enters a password to access a shared resource protected by user-level security.

2. The Windows 98 computer passes a request to the server (security provider) to authenticate Joe's identity.

3. The security provider sends a verification to the computer if Joe's name and password combination are valid.

4. Windows 98 grants access to the shared resource according to rights assigned to Joe on the Sharing property sheet for that resource.

Joe's password is stored on his computer's PWL file to be used for authentication when he accesses that resource again. He will not be prompted for the password again during that session. When he logs off, the computer will erase his password from the file.

# Setting Up Security for Shared Resources

Before a user can share a resource on a computer running Windows 98, the computer must be configured for share-level or user-level security, and file and printer sharing services must be installed by using the Network option in Control Panel. Configuring share-level or user-level security is described briefly in the following sections, and in Chapter 18, "Logon, Browsing, and Resource Sharing."

**Note**  Share-level security is not available on NetWare networks.

▶  **To set up share-level security**

1. Install File and Printer Sharing for Microsoft Networks, as described in the "Installing Peer Resource Sharing" section of Chapter 18, "Logon, Browsing, and Resource Sharing."

2. On the computer that hosts the resource to be shared, in Control Panel, double-click Network, and then click the **Access Control** tab.

3. Click **Share-level access control**, and then click **OK**.

▶  **To set up user-level security on a Microsoft network**

1. Install File and Printer Sharing for Microsoft Networks, as described in the "Installing Peer Resource Sharing" section of Chapter 18, "Logon, Browsing, and Resource Sharing."

2. In Control Panel, double-click Network, and then click the **Access Control** tab.

3. Click **User-level access control**.

4. In the **User-level access control** box, type the name of the Windows NT domain or Windows NT workstation where the user accounts reside.

5. Click **OK**.

▶  **To set up user-level security on a NetWare network**

1. Install File and Printer Sharing for NetWare Networks, as described in the "Installing Peer Resource Sharing" section of Chapter 18, "Logon, Browsing, and Resource Sharing."

2. In Control Panel, double-click Network, and then click the **Access Control** tab.

3. Click **User-level access control**.

4. In the **User-level access control** box, type the name of the NetWare server.

5. Click **OK**.

For information about specifying values for security in custom setup scripts, see Appendix D, "Msbatch.inf Parameters for Setup Scripts." For information about using System Policy Editor to set user-level security and other security options, see Chapter 8, "System Policies."

## Using Share-Level Security

You can restrict access to resources such as a shared folder or a printer by either defining it as read-only or assigning a password to it.

▶ **To share a folder or printer with share-level security**

1. In Windows Explorer, right-click the folder or printer to be shared, and then click **Properties**.

2. In the **Properties** menu, click the **Sharing** tab.

3. Click **Shared As**, and type the resource's share name.

   The shared resource name will be the computer name plus the share name. For example, in the following screen shot, if the computer name is mycomputer, this shared resource is \\mycomputer\mydocuments.
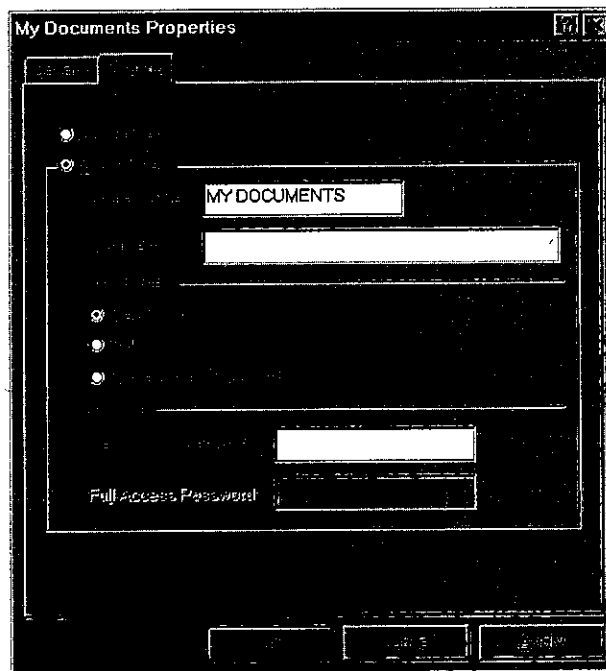
4. Specify whether you want users to have read-only or full access to this resource.

---

**Note**  There is no read-only share-level access for a printer or remote administration.

---

5. Type the password for the specified access, and click **OK**.

---

**Tip**  You can share a folder but hide it from the Network Neighborhood browsing list by adding a dollar sign ($) to the end of its share name (for example, PRIVATE$).

---

## Using User-Level Security

Windows 98 uses the logon process to provide user-level security for a variety of services beyond network resource access, including the following services that are remotely accessible:

- File and printer sharing.
- Dial-up network access gateway control.
- Backup.
- Network and system management.

Pass-through security is implemented in Windows 98 as the mechanism to enable user-level security. *Pass-through* literally means that Windows 98 passes authentication requests through to a Windows NT or NetWare server. Windows 98 does not implement its own unique user-level security mechanism but instead uses the services of an existing server on the network.

Enabling pass-through security is a two-step process. First, user-level security must be enabled using the Control Panel. Second, the device must be shared, and users with access privileges must be specified. Right-clicking the drive C icon in My Computer and selecting **Properties** from the Shortcut menu displays a property sheet that shows which shares already exist and which users have access. It also allows new devices to be shared and new users to be added to specific shares. The Windows NT server or the NetWare bindery supplies the user names listed in this property sheet.

For more information about file and printer sharing, see Chapter 18, "Logon, Browsing, and Resource Sharing."

The Remote Administration function of a Windows 98 personal computer specifies the users or groups who have authority to manage the Windows 98 system, including the following:

- Dial-up network access gateway control.
- Backup.
- Remote access to the registry.
- Remote NetWatcher access.
- Remote system performance monitoring.

Remote Administration is controlled through the Passwords option in Control Panel. For more information about Remote Administration, see Chapter 23, "System and Remote Administration Tools."

For each network resource governed by user-level security, there is a list of users and groups that can access that resource.

▶ **To share a resource with user-level security**

1. In Windows Explorer or My Computer, right-click the icon for the resource to be shared, and then click **Properties**.
2. In the **Properties** menu, click the **Sharing** tab.
3. Click **Add**.
4. In the **Add Users** dialog box, click a user or group, and then assign access rights as described in the following paragraphs.

   Assign, for each user, a set of rights for the resource. The kinds of rights that you assign depend on the kind of resource you are securing:

   - For shared directories, you can let a user have read-only access, full access, or custom access. Within custom access, you can grant the user any or all of the following rights: read, write, create, list, delete, change file attributes, and change access rights.
   - For shared printers, a user either has the right to access the printer or not.
   - For remote administration, a user either has the right to be an administrator or not as defined in the Passwords option in Control Panel.

   Permissions are enforced for a resource as follows:

   - If the user has explicit rights to the resource, those rights are enforced.
   - If the user does not have explicit rights to the resource, the permissions are determined by taking all of the rights of each group to which the user belongs.
   - If none of the groups to which the user belongs has any rights to that resource, the user is not granted access to the resource.

When you do not explicitly assign access rights to a file or folder, Windows 98 uses implied rights. *Implied rights* are those assigned to the nearest parent folder of a file or folder. If none of the parent folders (up to and including the root directory of the drive) have explicit rights, no access is allowed.

**Note** Implied rights are displayed automatically on the property sheet for the shared file or folder.

## Specifying Folder Access Rights in User-Level Security

Access rights specify what a user can do in a folder protected by user-level security. The access rights you define for a folder apply to all of its subfolders. You cannot, however, assign access rights to individual files in Windows 98. (Both Windows NT and NetWare let you assign access rights to files.)

**Note** Any subfolders of the shared folder, if they are also shared, must be set with the same level of security as the parent folder.

For each folder, you can assign read-only, full, or custom access. Custom access lets you further specify exactly what each user or group can do in the folder, as specified in Table 9.1.

**Table 9.1 Custom access options**

| File operation | Required permissions |
| --- | --- |
| Read from a closed file | Read files |
| See a file name | List files |
| Search a folder for files | List files |
| Write to a closed file | Write, create, delete, change file attributes |
| Run an executable file | Read, list files |
| Create and write to a file | Create files |
| Copy files from a folder | Read, list files |
| Copy files to a folder | Write, create, list files |
| Make a new folder | Create files |
| Delete a file | Delete files |
| Remove a folder | Delete files |
| Change folder or file attributes | Change file attributes |
| Rename a file or folder | Change file attributes |
| Change access rights | Change access control |

▶ **To define custom access**

1. Open the **Add Users** dialog box in a shared resource's properties (described in the procedure, "To share a resource with user-level security" earlier in this chapter).

2. In the **Add Users** dialog box, click a user or group, click **Custom**, and then click **OK**.

3. In the **Add Users** dialog box, click a user or group from the **Name** list, and then click **Custom**.

4. In the **Change Access Rights** dialog box, click the type of rights the user or group of users may have in the folder, and then click **OK**.

5. To remove a user or group of users, click that user or group, and then click **Remove**.

6. To edit the access rights for a user or group of users, click that user or group, and then click **Edit**.

## Managing User Lists

Windows 98 user-level security depends on a list of accounts and groups located on a security provider. You cannot add or remove users and groups from the security provider list by using Windows 98 tools. However, you can do this by running User Manager for a Windows NT domain, SYSCON for NetWare 3.*x*, and NETADMIN for NetWare 4.*x* in a NetWare bindery environment. You can use these tools on a computer running Windows 98. These tools are provided by the respective vendors and not by Windows 98. Under Windows 98, you specify what rights users have to specific resources on the local computer as described in "Using Share-Level Security" earlier in this chapter. For more information about changing a user's access rights, see "Specifying Folder Access Rights in User-Level Security" earlier in this chapter.

---

**Note**  Although Windows NT networks allow multiple domains, a computer running Windows 98 can specify only one domain for user-level security. However, you can set permissions for users or groups from any domain in the Sharing properties for the shared resource, as long as the two domains have a proper trust relationship. Also, rights may include user accounts from different trusted domains. To use a trust relationship to access multiple domains, you should consult the *Microsoft Windows NT Server 4.0 Concepts and Planning Guide*, part of the Windows NT Server documentation set.

---

### Managing Security for Windows 98 in NetWare Bindery Environments

NetWare 3.x servers store all the information about users, groups, passwords, and rights in a database stored on the server called the *bindery*. NetWare 4.x servers can appear to have a bindery through bindery emulation, a feature that is enabled by default. There is a separate bindery for each NetWare server. Windows 98 can use the bindery of only one NetWare server as the security provider. It is common for a company to have one or more NetWare servers per department, where users log on to the server for their department. This scenario can pose a problem when the bindery differs from one NetWare server to another. For example, Sue and Bob log on to the Sales server, and Fred logs on to the R&D server. Because Sue is running Windows 98 and can specify only one server for pass-through validation, she specifies Sales (the server she uses for logon). She can now grant access to shared resources on her computer to Bob but cannot grant access to Fred.

The only way to solve this problem is to include all user accounts for all servers on one NetWare server. This server should be specified as the security provider for every computer running Windows 98 with File and Printer Sharing for NetWare Networks.

---

**Note**  Windows 98 supports only bindery emulation to obtain user lists on NetWare 4.x servers. It does not support user lists obtained with NetWare Name Service (NNS) or other add-on services for that purpose.

---

# Passwords

A good password policy helps users protect their passwords from other individuals. This helps to reduce the probability of someone logging on with another user's password and gaining unauthorized access to data.

The following guidelines should help you create a basic security policy:

- Tell users not to write down their passwords.
- Tell users not to use obvious passwords, such as their names, their spouses' names, their children's names, and so on.
- Do not distribute user accounts and passwords in the same communication. For example, if you are sending a new user's account name and password in writing, send the user name and the password at different times.

You can use the following Windows NT and NetWare security features to enhance Windows 98 security:

**Enforce a reasonable minimum password length.**   This policy increases the number of permutations needed to guess someone's password randomly or programmatically. Additionally, you can enforce an alphanumeric password combination to achieve the same security.

**Enforce maximum and minimum password age.**   This policy forces the user to change the password, preventing someone else from discovering it as a result of the password being in use for a long time. A minimum password age prevents a user from immediately reverting to a previous password after a change.

**Enforce password uniqueness and maintain password history.**   This policy prevents users from toggling between their favorite passwords. You can specify the number of unique passwords that a user must have before that user can use a previously used password.

For more information about using Windows NT and NetWare security features, see the documentation for those products, or see the *Microsoft Windows NT Server Networking Guide* in the *Windows NT Server Resource Kit* (for Windows NT Server version 4.0) (ISBN 1-57231-343-9).

## Using the Windows 98 Logon Password

With Windows 98, users can log on to all networks and Windows 98 at the same time. The first time a user starts Windows 98, logon dialog boxes appear for Windows 98 and for each network client on that computer. This is useful for you as a network administrator, because you can use existing user accounts on a network security provider to validate access to the network for users running Windows 98. For more information, see Chapter 18, "Logon, Browsing, and Resource Sharing."

If a user's password for Windows 98 or for another network is the same as the password for the primary logon client, Windows 98 logs the user on to Windows 98, and then the network automatically uses that password. When a user logs on to other networks with different passwords and chooses to save them, the passwords are stored in the password list file. The Windows 98 password unlocks this file. Thereafter, Windows 98 will use the passwords stored in the password list file to log a user on to other networks, so that no additional passwords need to be typed. This single logon provides a solution to the problem of password proliferation.

The Passwords option in Control Panel provides a way to synchronize logon passwords for different networks. This allows users to use the password for whatever logon dialog box appears first (the primary network logon client or Windows 98 logon) for logging on to all other network clients.

▶ **To change a password for a network resource to be the same as the Windows 98 logon password**

1. In Control Panel, double-click Passwords, and then click **Change Windows Password.**

2. In the **Change Windows Password** dialog box, select the other passwords you would like to change to use the same password as the Windows 98 password, and then click **OK.**

   To appear in this list, the related software must include a function that lets its password be changed.

3. In the second **Change Windows Password** dialog box, type the current (old) Windows 98 password, type a new password, and then, in the **Confirm new password** box, type the new password again. Click **OK.**

---

**Note** The Windows Screen Saver passwords option appears here only if the Windows screen saver has been turned on and the password-protected option has been selected.

---

You can maintain separate passwords for a network resource and require users to type a password each time they access it.

▶ **To change a password for a network resource**

1. In Control Panel, double-click Passwords, and then click **Change Other Passwords.**

2. In the **Select Password** dialog box, select the password you want to change, and then click **Change.**

3. In the **Change Password** dialog box, type the current (old) network password, type a new password, and then, in the **Confirm new password** box, type the new password again. Click **OK.**

   You must now type the new password to access the resource.

---

**Note** You can also use the Passwords option to change individual passwords to other network resources to be different from the Windows 98 logon password.

---

# Using Windows 98 with NetWare Passwords

To log on to a NetWare network, you must type the name of the preferred server on which the related user account is stored. After the user name and password are validated by the network server, you can use resources shared on that server. If you are not validated, you will be prompted to enter a password whenever connecting to a NetWare server during this work session.

The first time you attempt to connect to a NetWare server other than the preferred server, Windows 98 searches for an appropriate user name and password in the PWL file. If no matching set of credentials is found, Windows 98 tries to log on using the Windows 98 password. If this fails, Windows 98 displays a NetWare logon prompt for you to enter a valid user name and password, which can then be stored in the PWL file.

▶ **To avoid use of automatic NetWare logon**

- Use system policies to enable the policy named **Disable Automatic NetWare Login.**

▶ **To change your password on a NetWare server**

1. At the command prompt, use the **net use** command to connect to the NetWare server's SYS volume. For example, for a server name NWSVR2, you would type:

   **net use * \\nwsvr2\sys**

2. At the command prompt, change to the drive for the NetWare server, and then make the Public folder the current folder. For example, if the drive is mapped to drive N, type:

   **n:**

   Then type:

   **cd \public**

   ---

   **Note**  If you want to change your password on more than one server, connect to all affected servers before running the **setpass** command. Setpass is a utility provided by Novell and is not part of Windows 98.

   ---

3. At the command prompt, type **setpass.**

   If the server on which you want to change your password is different from the one on the current drive, type **setpass** and the name of the server.

   For example, to change your password on the server named NWSERVE1, type:

   **setpass nwserve1**

4. When you are prompted, type your old password, and then type and confirm the new password.

5. If you are connected to other NetWare servers that also use your old password, these servers are listed, and you are asked if you want to change your password on these servers also.

# Using the Windows 98 Password Cache

Keeping track of multiple passwords can be a problem for users. Often, they either forget the passwords or write them down and post lists of passwords near their computers. When this happens, the security policy is no longer doing the job it was meant to do—to allow access to those who should have it and to deny access to those who should not.

Windows 98 solves this problem by storing passwords for resources in a password list file (PWL). This file stores passwords for the following network resources:

- Resources on a computer running Windows 98 that are protected by share-level security.

- Password-protected applications that have been specifically written to the password-caching application programming interface (API).

- Windows NT computers that do not participate in a domain.

- A Windows NT logon password that is not the Primary Network Logon.

- NetWare servers.

The password list file is stored in the Windows folder on the local computer by using an encryption algorithm. An unencrypted password is never sent across the network.

---

**Caution**  If you delete PWL files, you will lose all previously stored passwords. You will need to retype each password.

---

Password caching is enabled by default when you install Windows 98. When you access a password-protected resource for the first time, make sure the **Save this password in your password list** option is selected (it should be selected by default) to save the password to the password list file.

---

**Note**  If, during log on, you click **Cancel** to bypass the logon screen, the cache will not be opened, and you will be prompted for a password each time you attempt to use a protected resource.

---

You can disable password caching by using System Policy Editor, which is shipped on the Windows 98 compact disc but not automatically installed onto your system during Setup. Use the Add/Remove Programs option in Control Panel to install System Policy Editor.

▶ **To install System Policy Editor**

1. In Control Panel, double-click Add/Remove Programs, click the **Windows Setup** tab, and then click **Have Disk**.

2. In the **Install From Disk** dialog box, click **Browse** and specify the Tools\Admin\Poledit folder on the Windows 98 compact disc.

3. Click **OK**, and then click **OK** again in response to the dialog boxes.

4. In the **Have Disk** dialog box, click **System Policy Editor**, and then click **Install**.

▶ **To disable password caching by using system policies**

1. On the **Start** menu, click **Run**.

2. Type **poledit**, and then click **OK**.

3. In System Policy Editor, double-click the Local Computer icon.

4. In the Local Computer Properties, click **Network**.

5. Click **Passwords**.

6. Click the policy named **Disable Password Caching**.

For more information, see Chapter 8, "System Policies."

---

**Note**  If you have any share-level security servers and you disable password caching and are running Client for Microsoft Networks, you should not use the **Quick Logon** feature in the Network option in Control Panel.

---

# Using Password List Editor

If password caching is enabled, Windows 98 caches passwords in the password list file when you connect to a password-protected network resource. Password List Editor (Pwledit) lets you view the resources listed in a user's password list (PWL) file. It does not let you view the actual passwords, but lets you remove specific password entries if problems are encountered using a cached password.

Password List Editor works only if the password list file is unlocked, that is, if the user is logged on. It can be used to view only the contents of the logged-on user's password list file, so you should run it on the user's computer.

**Note**  Only users themselves can view or edit their own PWL files.

Password List Editor can be found in the Netadmin\Pwledit folder on the Windows 98 compact disc.

▶  **To install Password List Editor**

1. In Control Panel, double-click Add/Remove Programs, click the **Windows Setup** tab, and then click **Have Disk.**

2. In the **Install From Disk** dialog box, click **Browse.**

3. Type the path name to Netadmin\Pwledit\Pwledit.inf, and then click **OK.**

4. In the **Have Disk** dialog box, click **Password List Editor,** and then click **Install.**

▶  **To run Password List Editor**

• On the **Start** menu, click **Run.** Type **pwledit,** and then click **OK.**

## Using System Policies to Enforce Password Security

You can use system policies to increase security by requiring users to follow specific password guidelines. Using system policies, you can enforce password policies.

For information about restricting settings with system policies, see Chapter 8, "System Policies."

# Internet Explorer Security

Internet Explorer 4.0 adds several security features to Windows 98, including support for security zones, Secure Socket Layer (SSL) versions 2.0/3.0 and Private Communication Technology (PCT) version 1.0 protocols, client and server authentication, and the Platform for Internet Content Selection (PICS) rating system. These security features make it easier for you to protect your computer and your privacy while using the Internet.

**Security zones.**  You can divide the Web into zones and have Internet Explorer 4.0 provide different levels of security depending on which zone you have assigned to a Web site.

When you install Windows 98, you configure the following Internet Explorer settings:

- Internet zone
- Trusted sites zone
- Restricted sites zone
- Local intranet zone

A fifth zone, My Computer, is also created, but it is not configurable through the security options.

This system lets the administrator divide the Web content a browser can visit into groups, each of which can have a security level associated with it. The Web content can be anything from a Hypertext Markup Language (HTML) file to a graphic, an ActiveX control, a Java applet, or an executable file.

**Authenticode technology.**   An Authenticode certificate identifies who published a piece of software and verifies that it has not been tampered with.

**Certificate management.**   System administrators can control which Java applets, ActiveX controls, and other software can be run on their intranets, based on who published the software.

**Capabilities-based Java security (sandboxing).**   The Internet Explorer 4.0 security model for Java makes it easy for you to control how Java applets interact with your computer system. You can decide what capabilities and levels of access to your computer or system you want to give Java applets. You can offer full access to applets from trusted sources while restricting applets from unknown sources to safe "sandboxes" where they cannot harm files.

**Privacy protection.**   Internet Explorer 4.0 supports all standard Internet security protocols to ensure private communication over the Web. Internet Explorer prompts you before user names or passwords are sent to Web sites not designated as trusted. For trusted sites, you can choose not to be prompted before personal information is transmitted. Outlook Express—the Internet mail and news component of Internet Explorer 4.0—lets you encrypt messages and ensures that no one can falsely assume your identity on the Internet.

The following sections explain how to configure these settings.

# Setting Up Security Zones

Internet Explorer 4.0 has security options that let you configure a security level to a specific Web site according to how much you trust the content of that Web site. Five predefined security zones, four of which have configurable security settings, are set up in Internet Explorer 4.0:

- Internet zone that by default contains all Internet sites.
- Trusted sites zone to which you can assign Web sites you trust.
- Restricted sites zone to which you can assign Web sites you do not trust.
- Local intranet zone for computers connected to a local area network.
- Local machine called My Computer, unsecured, providing full access to all aspects of the machine, not configurable.

**Note**  Because security works differently in Internet Explorer 4.0, any existing Internet Explorer 3.0 settings are not preserved.

Using the **Internet Properties** dialog box in the Internet option in Control Panel, you can set the security options you want for Internet, Trusted sites, Restricted sites, and Local intranet, and then add or remove sites from the zones depending on your level of trust in each site.

In corporate environments, administrators can set up zones for users and can add or remove authentication certificates of software publishers that they do or do not trust so that users do not have to make security decisions while they are using the Internet.

For each security zone, you can choose a High, Medium, Low, or Custom security setting. Use the High setting for sites in a zone of untrustworthiness and Low in a trusted zone. The Custom option gives advanced users and administrators even more control over all security options, including the following:

- Access to files, ActiveX controls, and scripts.
- The level of capabilities given to Java applets.
- Whether sites must be identified with SSL authentication.

▶ **To set up security zones**

1. In Control Panel, double-click Internet.
2. Click the **Security** tab.
3. Configure the settings according to your security needs.

## Setting Up the Internet Zone

By default, the Internet zone is set to the Medium security level. If you are concerned about security problems as users browse the Internet, change this setting to High. When this level is set to High, some Web pages may not be allowed to perform certain operations that can potentially compromise security.

For more advanced and detailed security control, use the Custom settings to configure each individual security setting for the zone.

▶ **To set up custom settings for the Internet zone**

1. In the **Security** tab, select **Custom**, and then click **Settings.**

2. Configure the settings according to your security needs.

## Adding Sites to the Trusted and Restricted Zones

You can classify Web sites into two categories, according to how much you trust their contents:

- Trusted sites zone
- Restricted sites zone

By default, the Trusted sites zone is set to the Low security level. When you add a site to the Trusted sites zone, the site is allowed to perform more operations, and Internet Explorer will ask you to make fewer security decisions when you access the site. Add a site to this zone only if you trust all of its content never to do anything that may harm your computer. For the Trusted sites zone, it is strongly recommended that you use the HTTPS protocol so that you can securely connect to the site.

By default, the Restricted sites zone is set to the High security level. When you add a site to the Restricted sites zone, the site is allowed to perform only minimal, very safe operations. Add sites that you do not trust to this zone.

▶ **To add sites to the Trusted sites zone or Restricted sites zone**

1. In the **Security** tab, select either the **Trusted sites zone** or **Restricted sites zone** in the Zone list.

2. Click **Add Sites**, select the desired sites for that zone, and then click **OK.**

## Setting Up the Local Intranet Zone

To be secure, the Local intranet zone must be set up in accordance with the proxy server and firewall configuration. All sites in the zone should be "inside the firewall," and proxy servers should be configured so that they do not allow an external Domain Name System (DNS) to be resolved in this zone.

By default, the Local intranet zone consists of local domain names and those set in proxy override in the **Connection** tab. Make sure that these settings are indeed secure for the installation; if they are not, adjust them as needed. You can check that the Local intranet zone is configured correctly by browsing various intranet and Internet pages and checking that the correct zone is shown in the status bar.

After you have checked that the Local intranet zone is secure, you can change the zone's security level to Low to allow a wider range of operations and make the Web pages more functional. You can also adjust individual security settings in the **Security Settings** dialog box as explained in "Setting Up the Internet Zone" earlier in this section.

If parts of your intranet are not secure or do not meet your security standards, you can exclude them from the Intranet zone by adding them to the Restricted sites zone.

The Local intranet zone is designed to be configured using the *Microsoft Internet Explorer Administration Kit*; however, you can also use the **Security** tab in the **Internet Properties** dialog box.

## Summary of Authenticode Technology

When users download signed code to their computers, *Authenticode* verifies both its publisher and its integrity (that it has not been tampered with since the author published it). No software can be guaranteed to be 100 percent safe under all circumstances, but Authenticode uses public key technology to sign objects digitally and help you make informed decisions about blocking the execution of certain code. Authenticode works with all common types of downloadable code, including Java applets, ActiveX controls, and plug-ins.

Authenticode checks to see that a piece of software is digitally signed during the valid lifetime of the publisher's certificate.

Authenticode can also automatically check to make sure a software publisher's certificate has not been revoked. Publishers can have their certificates revoked if they abuse their code-signing agreement by, for example, creating malicious code that harms users' computers.

## Summary of Certificate Management

Authentication certificates are a key tool in providing Internet security. Certificate management eases the administration of network security. The certificates, which are assigned to software publishers who meet defined levels of integrity and security in their code, give users a way to identify the origin of a piece of software on the Internet. This identification mechanism forms the basis of Authenticode. Certificate Management lets system administrators control which Java applets and ActiveX controls are allowed to run on their networks based on who published the applets or controls.

**Example**

### Certificate Management

You can let users open and run all internally created controls, but keep all controls that originate from outside your corporate firewall from loading and running on company computers.

---

Site certificates verify that you are really connected to the Web sites that you believe you are connected to. Viewing information may not present a security risk, but sending information can. Security certificates are issued to particular organizations for specific periods of time. Before you send information, certificates are sent from the secure Web sites to Internet Explorer 4.0. These certificates provide certain information about security at those sites. Internet Explorer 4.0 verifies that the Internet address stored in the certificate is valid and that the current date precedes the expiration date.

---

**Note** Site Certificates are active only for Uniform Resource Locators (URLs) using HTTPS. Communication to and from Web sites using HTTPS are kept private through encryption when this mode is active.

---

▶ **To see the site certificates stored in Internet Explorer 4.0**

1. Start Internet Explorer.
2. Click the **View** menu, and then click **Internet Options**.
3. Click the **Content** tab, and then click **Authorities**.

   By default, the **Certificate Authorities** dialog box contains a list of authorities that are allowed to issue certificates to sites.

If you are connected to a site with a certificate, a lock icon appears on the bottom right corner of the browser window.

## Summary of Java Security (Sandboxing)

Support for *sandboxing*, the Java security model, was built into Internet Explorer 3.0 and has been enriched in Internet Explorer 4.0. Running a Java applet in a sandbox prevents it from accessing a computer or network resource and also greatly restricts what it can do. Internet Explorer lets you control access of applets to users' resources, such as their hard disks and network connections. It presents users with a range of security options, such as allowing a Java applet to access a specific amount of hard disk space on a client computer.

# Summary of Privacy Protection

The following list describes the kinds of privacy protection built into Internet Explorer 4.0.

**Secure channel services.**  Support for Secure Socket Layer (SSL) versions 2.0/3.0 and Private Communication Technology (PCT) version 1.0 ensures that personal or business communications using the Internet or an intranet are private. The SSL and PCT protocols create a secure channel so that no one can eavesdrop on communications. With secure communications guaranteed, users can buy consumer goods, reserve plane tickets, or conduct personal banking on the Internet.

**Transport Layer Security.**  Transport Layer Security (TLS) is a new secure channel protocol under development by the Internet Engineering Task Force. TLS builds on existing protocols to create an improved Internet secure channel protocol.

**Personal Information Exchange.**  The Personal Information Exchange (PFX) is a set of public key-based security technologies that is part of the Microsoft Internet security framework. PFX supports such Internet standards as X.509 and PKCS#12 certificate formats. Microsoft has submitted PFX for consideration as a new Public Key Cryptography Standard (PKCS).

**Cookie privacy.**  Some Web sites use *cookie technology* to store information on client computers. These cookies are usually used to provide Web site personalization features. With Internet Explorer 4.0, you can choose whether or not to store a cookie.

---

**Tip**  You can decline cookies from a site by selecting **Prompt before accepting cookies** on the **Advanced** tab in the **Internet Options** dialog box of the Internet Explorer **View** menu.

---

**SOCKS firewall support.**  Many corporations provide their employees with access to the Internet through firewalls that protect the corporation from unwanted access. SOCKS is a standard protocol for traversing firewalls in a secure and controlled manner. Internet Explorer 4.0 is compatible with firewalls that use the SOCKS protocol.

**Windows NT Server challenge/response.**  Corporations can take advantage of the Microsoft Windows NT LAN Manager challenge/response authentication that might already be in use on their Windows NT Server network. Users enjoy increased password protection and security while still able to use their existing Internet information servers.

**CryptoAPI version 2.0.**  CryptoAPI provides the underlying security services for secure channels and code signing. Through CryptoAPI, developers can easily integrate strong cryptography into their applications. Cryptographic Service Provider (CSP) modules interface with CryptoAPI and perform functions, including key generation and exchange, data encryption and decryption, hashing, digital signatures, and signature verification. CryptoAPI is included as a core component of Windows 98 and Windows 95. Internet Explorer 4.0 automatically provides this support for earlier versions of Windows.

**Microsoft Wallet.**  Microsoft Wallet supports securely storing important and private information, such as credit cards, electronic driver's licenses, ATM cards, and electronic cash. No application or person can view this information without a user's permission. In addition, a user decides where to store the information (on a computer, smart card, or floppy disk). Users have to enter password or account information only once and do not have to remember many different passwords. Users have complete control over who can see or use this information. Wallet allows information to be securely transferred to any computer and used with any application through the use of PFX technology. Designed for the future, Wallet supports additional payment methods (such as Internet cash) as well as other credentials and confidential information.

**PICS standards for Internet content.**  Parents want the assurance that children can be blocked from visiting sites that display inappropriate information. Corporations have similar concerns, wanting to block the use of sites that offer no business value to their customers. Microsoft has been working closely with the Platform for Internet Content Selection (PICS) committee to help define standards for rating Internet content.

**Forget your password?**  With Internet Explorer 4.0, you do not have to type your user name and password every time you want to access a subscription Web service. Instead, Internet Explorer 4.0 functions as your virtual wallet, flashing your personal certificate to Web servers that want to verify your identity. It works the other way, too. You can also store certificates of Web servers in Internet Explorer 4.0. This means you can verify the identity of any Web merchant or other Web server before you purchase goods or communicate with them.

# Security Features in Outlook Express

As the use of e-mail and electronic commerce becomes more widely adopted, the amount of confidential information being exchanged over the Internet is growing rapidly. As a result, there is a need to make e-mail messages secure and private. In addition, with the growing popularity of ActiveX controls, scripts, and Java applets, there is an increased chance that the HTML content you receive in an e-mail message could damage or compromise files on your computer.

Outlook Express includes tools to protect you from fraud, ensure your privacy, and prevent unauthorized access to your computer. These tools enable you to send and receive secure e-mail messages and to control potentially harmful e-mail messages through security zones.

## Using Security Zones for Outlook Express

Outlook Express enables you to choose which Internet Explorer security zone your incoming e-mail messages are in—either the Internet zone or the Restricted sites zone. Which zone you decide to select depends on how concerned you are about active content (e.g., ActiveX controls, scripts, and Java applets) weighed against the freedom to run that content on your computer. In addition, for each security zone, you can choose a High, Medium, Low, or Custom security level setting.

For more information about security zones, see "Setting Up Security Zones" earlier in this chapter.

**Caution**  Changing the settings for the Internet zone or Restricted sites zone will also change this setting for Internet Explorer and vice versa.

▶ **To change the security zones settings for Outlook Express**

1. In Outlook Express, click the **Tools** menu.
2. Click **Options**, and then click the **Security** tab.
3. Configure the settings according to your security needs.

## Using Digital IDs

To use secure e-mail in Outlook Express, you need a digital ID. Digital IDs (also called certificates) provide a means for proving your identity on the Internet, much as a driver's license or other ID cards identify you.

Digital IDs let you sign your e-mail messages, so that the intended recipients can make sure that the message actually came from you and has not been tampered with. Also, a digital ID allows other people to send you encrypted messages.

For more information, see Outlook Express Help.

## Getting a Digital ID

You obtain your digital ID from a certifying authority, an organization responsible for issuing digital IDs and continuously verifying that digital IDs are still valid.

## Using Your Digital ID

Before you can send signed e-mail messages, you must associate your digital ID with the e-mail account you want to use it with.

▶ **To associate your digital ID with an e-mail account**

1. In Outlook Express, click the **Tools** menu, and then click **Accounts.**

2. Select the account you want to use your ID with, click **Properties,** and then click the **Security** tab.

3. Select **Use a digital ID when sending secure messages from.**

4. Click **Digital ID,** and then select the digital ID you want to associate with this account.

---

**Note**  Only the digital IDs with the same e-mail address as the e-mail address for the account will be shown.

---

## Backing Up Your Digital ID

Part of your digital ID is an irreplaceable private key stored on your computer. If the private key is lost, you will no longer be able to send signed e-mail messages or read encrypted e-mail messages with that digital ID. You are strongly encouraged to make a backup of your digital ID in case the files containing it are damaged or made otherwise unreadable.

▶ **To back up your digital ID**

1. In Internet Explorer, click the **View** menu, and then click **Internet Options.**

2. Click the **Content** tab, and then click **Edit Profile.**

3. Click the **Digital IDs** tab.

4. The **Import** and **Export** buttons let you manage your digital IDs. Use **Export** to back up your digital ID.

# Sending Secure E-mail Messages

Now that you have a digital ID, you can send secure e-mail messages. Secure e-mail messages in Outlook Express protects your Internet communications through both digital signatures and encryption. Using digital signatures, you can sign your e-mail message with a unique ID that assures the person receiving the message that you are the true sender of the message and that it was not tampered with in transit. Encrypting e-mail messages that you send can ensure that no one except the intended recipient can read the contents of the message while it is in transit.

Because Outlook Express uses the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard, other people can read secure e-mail messages that you compose, using programs that support this technology. Likewise, you can read messages composed by other people by using e-mail programs that support S/MIME technology.

## Sending and Receiving Signed E-mail Messages

Signed e-mail messages let recipients verify your identity. To send signed e-mail messages, you must have a digital ID of your own.

▶ **To digitally sign an e-mail message**

1. In Outlook Express, click the **Tools** menu.
2. Click **Options**, and then click the **Security** tab.
3. Select **Digitally sign all outgoing messages.**

   –Or–

   Use the **Digitally sign message** button on the message toolbar.

Signed e-mail messages from others lets you verify the authenticity of a message —that the message is from the supposed sender and the message has not been tampered with during transit. Signed e-mail messages are designated with special signed e-mail icons. Any problems with signed e-mail messages that you receive (described in Outlook Express security warnings) could indicate that the message has been tampered with or was not from the supposed sender.

## Sending and Receiving Encrypted E-mail Messages

Encrypting an e-mail message prevents other people from reading it when it is in transit. To encrypt an e-mail message, you need the digital ID of the person you are sending the e-mail message to. The digital ID must be part of the person's entry in the Address Book.

▶ **To send encrypted e-mail messages**

1. In Outlook Express, click the **Tools** menu.

2. Click **Options**, and then click the **Security** tab.

3. Select **Encrypt contents and attachments for all outgoing messages**.

   –Or–

   Use the **Encrypt message** button on the message toolbar.

When you receive an encrypted e-mail message, you can be reasonably confident that the message has not been read by anyone else. Outlook Express automatically decrypts e-mail messages, provided that you have the correct digital ID installed on your computer.

## Sending and Receiving Digital IDs

For others to be able to send you encrypted e-mail messages, they need your digital ID. To send it to them, simply send them a digitally signed e-mail message, and Outlook Express will automatically include your digital ID.

To send others encrypted e-mail messages, you need their digital ID. Outlook Express lets you retrieve digital IDs via directory services.

▶ **To find a digital ID**

1. In Outlook Express, click the **Edit** menu, and then click **Find People**.

2. Select a directory service that supports digital IDs (for example, the VeriSign directory service).

3. Enter the recipient's name or e-mail address in the appropriate search field, and then click **Find Now**.

4. Select a listing from the results pane, and then click **Add to Address Book**.

## Changing Trust Status on Digital IDs

When you add someone's digital ID to your Address Book, it has a trust status associated with it that indicates whether you trust the individual, group, or corporation to whom the digital ID was issued. If a digital ID owner warns you that he or she suspects that the digital ID's private key has been compromised, you may want to change the trust status to "Explicitly Distrust."

▶ **To change the trust status of a digital ID**

1. In the Address Book, double-click the name of the contact.

2. Click the **Digital IDs** tab, select the digital ID whose trust level you want to change, and then click **Properties**.

3. Click the **Trust** tab, and then select an option in the Edit Trust area.

For more information, see Outlook Express Help.

# Firewalls

An Internet firewall lets you take advantage of the services offered on the Internet, while limiting exposure to attack. A *firewall* may consist of a collection of hardware and software components that collectively provide a protected channel between networks with differing security. Potential paths to the private network are limited by configuring the firewall to accept only packets from Internet Protocol (IP) addresses and/or ports of the Transmission Control Protocol/Internet Protocol (TCP/IP) that have been designated by the system administrator.

For more information, see Chapter 20, "Internet Access and Tools."

## Understanding Proxy Servers

The most critical component of your firewall is your proxy server. A *proxy server* listens to the computers on your internal network. When a client application makes a request, a proxy server responds by translating the request and passing it to the Internet. When a computer on the Internet responds, the proxy server passes that response back to the client application on the computer that made the request.

Proxy servers make a firewall safely permeable to users behind the secured entrance, while closing entryways in the private network to potential attacks. The proxy server must act as both a server and client. It serves proxy clients when accepting approved requests for external servers, and requests services from those servers on behalf of its clients. Proxy servers are commonly used by administrators of corporate networks connected to the Internet and by Internet Service Providers (ISPs).

Microsoft Proxy Server provides an easy, secure, and cost-effective way to bring Internet access to every desktop in an organization. Microsoft Proxy Server routes requests and responses between the Internet and client computers, acting as a liaison between them. In addition to routing requests, Microsoft Proxy Server provides a cache of frequently requested Internet sites, blocks access to specified sites, and provides secure access between your internal network and the Internet. It also offers firewall features.

## Configuring Proxy Servers

Access to Web sites secured by Windows NT Challenge and Response requires that firewalls and proxy servers be configured to permit passage of Windows NT Challenge and Response.

If you want to use a proxy server or firewall to protect your local area network (LAN) from being accessed by others on the Internet, carry out the following steps, which set up your computer to gain access to the Internet through a firewall.

▶ **To set up a LAN proxy server or firewall**

1. Run the Internet Connection Wizard.

   Click **Start**, point to **Programs**, point to **Internet Explorer**, and then click **Connection Wizard**.

2. Configure your computer to connect to the Internet by using TCP/IP on your LAN.

3. When you are prompted for the gateway address, type an address only if your organization uses gateways for routing information over the network.

   ---

   **Note**  The gateway computer is not the same as the proxy server or firewall computer that protects your LAN from the Internet, so do not type your proxy server or firewall address here.

   ---

4. In Control Panel, double-click Internet, and then click the **Connection** tab.

5. In the Proxy server area, select the **Access the Internet using a proxy server** check box.

6. Click **Advanced**.

7. In the first text box, type the Hypertext Transfer Protocol (HTTP) server address for the computer you want to use as the proxy server. In the second text box, type the port number. An example of a proxy server and port number is **http://myproxy.mycompany.com:80**.

   In this example, you would type **http://myproxy.mycompany.com** in the first text box, and **80** in the second text box.

   You can use a different proxy for different types of addresses. However, if you want to use the same proxy for all types of addresses, make sure you select the **Use the same proxy server for all protocols** check box.

8. In the Exceptions area, click the text box, and then type the names of the computers, domains, and ports on the Internet that, when accessed, will not go through the proxy server. Separate each item you type with a semicolon (;). Local addresses are defined as those in which the server name does not have a period (.) in it.

   For example:

   - http://internalweb/ is a local address.

   - http://www.microsoft.com/ is not a local address.

   For Help on these items, click the ? in the title bar, and then click the item.

9. When you have finished changing settings, click **OK**.

10. Click **OK** to close the Internet properties in Control Panel.

If you are running Internet Explorer, restart your computer so that the new proxy settings can take effect.

---

**Note**  If you are setting up Internet Explorer with a SOCKS proxy server, you must set it up separately from other proxy information (for example, HTTP, FTP, or Gopher). In most cases, this means that all other proxy fields should be left blank and the SOCKS field should contain the address of your SOCKS proxy server. The only exception is when you are using a SOCKS proxy server and a different proxy (for example, HTTP) on the same connection.

---

For more information about proxy servers and firewalls, see *Microsoft Proxy Servers Installation and Administration Guide.*

# Distributed Component Object Model

The Component Object Model (COM) defines how components and their clients interact. The *Distributed Component Object Model* (DCOM) extends the COM infrastructure that underlies ActiveX, transparently and naturally adding support for reliable, secure, and efficient communication between ActiveX controls, scripts, and Java applets residing on different machines on a LAN, a wide area network (WAN), or the Internet. With DCOM, applications can be distributed across locations that make the most sense to your customer and to the application.

Because DCOM is a seamless evolution of COM, you can leverage your existing investment in all ActiveX applications, components, tools, and knowledge to move into standards-based distributed computing. As you do so, DCOM handles the low-level details of network protocols. DCOM enables component applications to operate across the Internet, because it works natively with such Internet technologies as TCP/IP and Java. It provides the "object glue" that allows business applications to work across the Web.

Figure 9.2 shows the overall DCOM architecture. The COM run-time provides object-oriented services to clients and components and uses the remote procedure call (RPC) and the security provider to generate standard network packets that conform to the DCOM wire protocol standard. COM provides sophisticated mechanisms for the marshaling and unmarshaling of method parameters that build on the RPC infrastructure defined as part of the distributed computing environment (DCE) standard. DCE RPC defines a standard data representation for all relevant data types, the Network Data Representation (NDR).
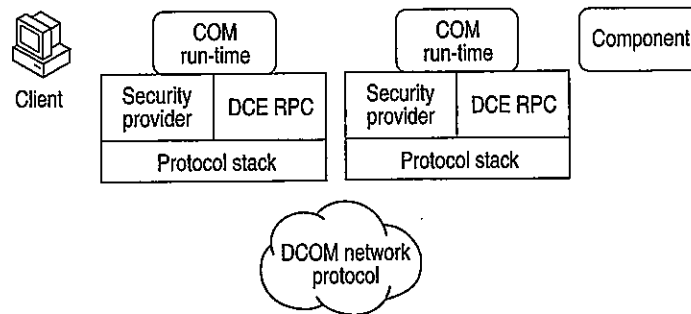


**Figure 9.2   Overall DCOM architecture**

A distributed application consists of multiple processes that cooperate to accomplish a single task. A distributed application can accommodate different clients with different capabilities by running components on the client side when possible and running them on the server side when necessary. A distributed application is also much more scalable than its monolithic counterparts, and easier to administer and deploy.

Designing a distributed application poses several challenges to the developer. One of the most difficult design issues is security: Who can access which objects? Which operations is an object allowed to perform? How can administrators manage secure access to objects? How secure does the content of a message need to be as it travels over the network?

Mechanisms to deal with security-related design issues have been built into DCOM from the ground up. DCOM provides an extensible and customizable security framework upon which developers can build when designing applications.

Different platforms use different security providers, and many platforms even support multiple security providers for different usage scenarios or for interoperability with other platforms. DCOM and RPC are built in such a way that they can simultaneously accommodate multiple security providers.

Common to all these security providers is their providing a means of identifying a security principal (typically a user account), a means of authenticating a security principal (typically through a password or private key), and a central authority that manages security principals and their keys. If a client wants to access a secured resource, it passes its security identity and some form of authenticating data to the resource, and then the resource asks the security provider to authenticate the client. Security providers typically use low-level custom protocols to interact with clients and protected resources.

# Configuring Applications to Use DCOM

The DCOM Configuration tool can be used to configure 32-bit COM and DCOM applications.

▶ **To run the DCOM Configuration tool**

- Click **Start**, click **Run**, and then type **dcomcnfg**.

---

**Note**  Before you can use an application with DCOM, you must use DCOM Configuration to set application properties, such as security and location.

---

# Distributed Applications for the Internet or an Intranet

You can use DCOM to integrate client/server applications across multiple computers. DCOM provides the infrastructure that enables client/server applications to share components over the Internet or intranet.

▶ **To set default permissions for all DCOM applications**

1. Run dcomcnfg to open the DCOM Configuration tool.
2. Click the **Default Security** tab.
3. Click **Edit Default** for Default Access Permissions.
4. If necessary, click **Add** to add other user accounts to the **Name** box.

▶ **To set permissions for a DCOM application**

1. Run dcomcnfg to open the DCOM Configuration tool.
2. Click the application you want to configure, and then click **Properties**.
3. Click the **Security** tab.
4. Select **Use Custom Access Permissions** for launch, access, or configuration, and then click **Edit**.
5. If necessary, click **Add** to add other user or group accounts to the **Name** box.

▶ **To grant permissions that apply to all applications**

1. Run dcomcnfg to open the DCOM Configuration tool.
2. Click the **Default Security** tab.

▶ **To set the location of a DCOM application**

1. Run dcomcnfg to open the DCOM Configuration tool.
2. Click the application you want to configure, and then click **Properties.**
3. Click the **Location** tab, and specify the location of the application.

# Troubleshooting Security

To make it easy for customers to contact Microsoft with any potential security issues, an e-mail address has been created: secure@microsoft.com. Please use this address to report security issues with a Microsoft product. Microsoft product teams respond to security issues you bring to their attention.

### No Windows or Network logon dialog box appears at startup.

When you start Windows 98, you might not receive a Windows or a Network logon dialog box, or you might receive one of the following error messages:

```
No network provider accepted the given network path.
```

```
The operation being requested was not performed because the user has not
logged on to the network. The specified service does not exist.
```

Another symptom of this problem is the absence of the **Change Passwords** tab in the **Passwords Properties** dialog box.

This problem occurs if any of the following conditions are true:

- The primary network logon field is not set correctly.
- The following entry appears in the **HKEY_LOCAL_MACHINE\Software \Microsoft\Windows\CurrentVersion\Network\Real Mode Net** registry key:

```
AutoLogon=<x>
```

where <x> is a number.

- You are logging on to a Novell NetWare network, and the server you log on to is running multiple frame types.
- You are logging on to a Microsoft or NetWare network, and you have cached your network password.
- The network adapter is improperly configured.

### Find Fast does not index password-protected files.

Because password-protected files are encrypted, they cannot be indexed. Find Fast does not index password-protected documents because they are not searchable files. Any references to file properties or content will not be addressed in the index. The behavior of Find Fast is, by design, to uphold the security and protection of your documents.

### File and Printer Sharing for Microsoft Networks is unavailable.

When you use the right mouse button to click a drive, folder, or printer, there may be no Sharing command on the menu that appears even though File and Printer Sharing for Microsoft Networks is installed. The cause may be that Nwserver.vxd is loading even though File and Printer Sharing for NetWare Networks is not installed in network properties. If this service is installed and you do not use NetWare networks, you need to remove the Microsoft Client for NetWare Networks by clicking Network in Control Panel, clicking **Client for NetWare Networks**, and then clicking **Remove**. Click **OK**, and then restart your computer when you are prompted.

### The user list with user-level security is incomplete.

Your Windows 98 system is configured for user-level security with a Windows NT system as the security provider, but when you try to add a user in a shared folder's properties, you may not see a full list of users. Or some users on the network who do not have an account in the user list from the security provider may be able to gain access to your shared Windows 98 computer.

This problem can occur when the security provider is a Windows NT Workstation that is a member of a Windows NT domain. The user list in the **Add Users** dialog box is the list of local user accounts defined on the Windows NT Workstation, but access to the Windows 98 computer is controlled by the accounts in the Windows NT domain.

Use the list of user and group accounts from the Windows NT domain. To do so, specify the name of the domain instead of the Windows NT Workstation on the **Access Control** tab of the Network option in Control Panel.

### The selected security provider cannot be found.

When you select user-level security and enter the name of a server to use as a security provider, you may receive the following error message:

```
Window could not find the specified security provider on the network. Do
you wish to use the name you typed anyway?
```

This error message can occur for any of the following reasons:

- You specified an incorrect server name.
- The server type does not match the services selected for file and printer sharing. For example, you specified a NetWare server but File and Printer Sharing for Microsoft Networks is installed.
- The server is not operational.
- The network has not been started.
- You are not logged on to the Microsoft LAN Manager or the Windows NT domain.

▶ **To resolve this problem**

1. Verify that the server name you entered is correct.
2. Verify that the server type you specified matches the network services you are running. For example, if you are running File and Printer Sharing for NetWare Networks, make sure to specify a NetWare server.
3. Verify that the server is operational.
4. After you verify the previous items, if the network has not been started, restart the computer.

### No logon servers are available.

When you attempt to connect to a share on a Windows 98 computer that is using a Microsoft Windows NT domain to provide user-level security, you may receive the following error message:

```
There are currently no logon servers available to service the logon
request.
```

This problem may occur regardless of which users have been given access to the share you are connecting to and which access rights each user has been given. It does not occur when the Windows 98 computer you are connecting to is configured for share-level security.

This problem can occur when your user account is configured so that you can log on only to certain computers in the domain. If your user account is configured in this manner and the Windows 98 computer you are attempting to connect to is not one of the specified computers, you are unable to connect to resources on that computer.

To work around the problem, configure the Windows 98 computer you are attempting to connect to for share-level security.

▶ **To configure Windows 98 for share-level security**

1. In Control Panel, double-click Network, and then click the **Access Control** tab.

2. Click **Share-level access control**, and then click **OK**.

3. Restart the computer when prompted.

---

**Note** After you change the type of access control a computer is using, any resources that were shared on that computer are no longer shared. You must share resources again to allow other people access to them.

---

### Additional Resources

| For more information about | See this resource |
|---|---|
| Windows NT | *Microsoft Windows NT Server Networking Guide* in the *Microsoft Windows NT Server Resource Kit* (for Microsoft Windows NT Server version 4.0) |
| | *Microsoft Windows NT Server 4.0 Concepts and Planning Guide* |
| Internet security | *Microsoft Internet Explorer Administration Kit* |
| Proxy servers | *Microsoft Proxy Servers Installation and Administrator's Guide* |
| | **http://www.microsoft.com/security/** |

CHAPTER 1 5

# Network Adapters and Protocols

15

This chapter describes technical issues related to network adapters and protocols for Microsoft Windows 98 and explains how to install and configure network adapters and protocols. It also presents some technical notes and tips for networking.

**In This Chapter**

**See Also**
- For an overview of network configuration, see Chapter 14, "Introduction to Networking Configuration."
- For more information about using Windows 98 on Microsoft networks, see Chapter 16, "Windows 98 on Microsoft Networks."
- For more information about using Windows 98 on third-party networks, see Chapter 17, "Windows 98 on Third-Party Networks."
- For more information about logon, browsing, and resource sharing, see Chapter 18, "Logon, Browsing, and Resource Sharing."
- For more information about Dial-Up Networking, see Chapter 19, "Remote Networking and Mobile Computing."
- For more information about network architecture, see Chapter 29, "Windows 98 Network Architecture."

# Overview of Network Adapter Drivers and Protocols

A network adapter (sometimes called a network interface card, or NIC) is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable.

Every networked computer must also have a network adapter driver, which controls the network adapter. Each network adapter driver is configured to run with a certain type of network adapter.

A networked computer must also have one or more protocol drivers (sometimes called a transport protocol or just a protocol). The protocol driver works between the upper-level network software and the network adapter to package data to be sent on the network.

In most cases, for two computers to communicate on a network, they must use identical protocols. Sometimes, a computer is configured to use multiple protocols. In this case, two computers need only one protocol in common to communicate. For example, a computer running File and Printer Sharing for Microsoft Networks that uses both NetBEUI and TCP/IP can communicate with computers using only NetBEUI or only TCP/IP. Common protocols are not necessary if the computers are using an intermediary device or application such as the gateway. For a brief explanation of gateways, see "Using Gateways for Connectivity" in Chapter 17, "Windows 98 on Third-Party Networks."

In Windows 98, you configure all network adapter drivers and protocols supporting protected-mode clients by using the Network option in Control Panel rather than by manually editing configuration files. Configuration values are stored in the registry.

Windows 98 Setup automatically configures a computer to use protocols and drivers to match network components that are running when Setup is started.

If you are setting up Windows 98 for a new networking option, you must choose which types of network adapter drivers and protocols to use. Because Windows 98 has an open architecture, you have a lot of flexibility in this decision. Windows 98 supports both network driver interface specification (NDIS) and transport driver interface (TDI) standards, allowing Windows 98 to communicate with many other networking products and making it possible to choose from a variety of network adapters and protocols.

This section describes basic issues for choosing network adapter drivers and protocols to support your networking needs.

## Choosing Adapters and Drivers for Best Performance

Network adapters have become exceptionally reliable and inexpensive. The low cost of Ethernet adapters, including new Plug and Play hardware, means that usually the cost-effective way to improve network performance is to replace an older network adapter with a new model. The cost of the new hardware is offset almost immediately by savings in support time and improved performance. Also, you should buy an adapter that matches one of your computer's buses. For example, peripheral component interconnect (PCI) network adapters are available for use in PCI computers.

## Choosing Protected-mode Protocols and Adapter Drivers

Microsoft recommends that you choose separate 32-bit, protected-mode protocols and drivers rather than real-mode protocols and drivers. However, Windows 98 includes mapping technology for users who must continue to use real-mode NDIS 2 or Open Datalink Interface (ODI) drivers.

# Overview of Protocols

Windows 98 network protocols are implemented as 32-bit, protected-mode virtual device drivers (VxDs) that offer high performance. Windows 98 can support multiple protocols simultaneously, and protocol stacks can be shared among the installed network clients. For example, the Internet Packet Exchange/Sequenced Packet Exchange (IPX/SPX)–compatible protocol can support both Client for NetWare Networks and Client for Microsoft Networks. The following protocols are included with Windows 98:

- TCP/IP
- IPX/SPX-compatible
- NetBEUI
- 32-bit DLC

All four protocols are Plug and Play–compliant, so they can be loaded and unloaded automatically. For example, if a PC Card network adapter is removed from the computer so that the network is no longer available, the protocols are unloaded automatically after any dependent applications have been notified.

Windows 98 can support multiple network protocols and can share a protocol among the network providers that are installed. You might choose more than one protocol to ensure communication compatibility with all systems in the enterprise. However, choosing multiple protocols can cause more network traffic, more memory used on the local computers, and more network delays.

The following sections briefly describe the benefits of using each protocol and issues to consider when using each protocol.

## Microsoft TCP/IP Protocol

This is a complete implementation of the standard, routable Transmission Control Protocol/Internet Protocol (TCP/IP) protocol. Windows 98 includes only protected-mode support for this protocol. Microsoft TCP/IP provides the following benefits:

- Support for Internet connectivity and the Point-to-Point Protocol (PPP).
- Connectivity across interconnected networks with different operating systems and hardware platforms, including communication with many non-Microsoft systems, such as Internet hosts, Apple Macintosh systems, IBM mainframes, UNIX systems, and Open VMS systems.
- Support for automatic TCP/IP configuration using Dynamic Host Configuration Protocol (DHCP) servers such as Windows NT servers.
- Support for automatic IP-address-to-NetBIOS computer name resolution using Windows NT Windows Internet Naming Service (WINS) servers.
- Support for Windows Sockets 1.1 and 2.0, which are used by many client/server applications and many public-domain Internet tools.
- Support for the NetBIOS interface, commonly known as NetBIOS over TCP/IP.
- Support for many commonly used utilities, which are installed with the protocol.

Consider the following issues when using this protocol:

- TCP/IP in general has been known to require careful planning and management of the Internet Protocol (IP) address space. However, this problem is vastly reduced when you use DHCP servers to manage assignment of IP addresses for computers running Microsoft TCP/IP.
- If you want to take advantage of DHCP for private IP addressing or use WINS for name resolution on computers running Windows 98, the appropriate DHCP servers must be in place on the network.
- The Microsoft TCP/IP stack does not bind to NetWare client; therefore, you cannot use TCP/IP as a substitute for NetWare/IP when connecting to a NetWare server.

## Microsoft IPX/SPX-compatible Protocol

This protocol is compatible with the Novell NetWare Internetwork Packet Exchange/Sequential Packet Exchange (IPX/SPX) implementation. Windows 98 includes both 32-bit, protected-mode and real-mode support for this protocol. This protected-mode protocol provides the following benefits:

- Works with Microsoft Client for NetWare Networks and Novell Client for Windows 95/98.

- Supports packet-burst mode to offer improved network performance.

- Supports the Windows Sockets, NetBIOS, and ECB programming interfaces.

- Support for automatic detection of frame type, network address, and other configuration settings.

- Routable connectivity across all network bridges and routers configured for IPX/SPX routing.

Consider the following issues when using this protocol:

- This protocol is required for Microsoft Client for NetWare Networks and installed automatically with the client. When Windows 98 Setup determines that it cannot install Client for NetWare Networks on a computer running a Novell-supplied network client, Setup still tries to install this protected-mode protocol. For information about how Setup determines whether to install this protocol automatically, see Chapter 17, "Windows 98 on Third-Party Networks."

- This protocol cannot be used to configure Windows 98 to support NetWare over ArcNet. Instead, you must use real-mode IPX drivers with NetBIOS support on ArcNet network adapters.

- With this protocol, it is not necessary to load the Novell-supplied Vipx.386 driver, because the Microsoft protocol provides virtualized services to all virtual machines (VMs) and applications.

## Microsoft NetBEUI Protocol

This protocol is compatible with existing networks that use the NetBIOS extended user interface (NetBEUI), including Windows for Workgroups peer networks, Windows NT Server, LAN Manager, and other networks, and includes support for the NetBIOS programming interface. Windows 98 provides both protected-mode and real-mode support for this protocol.

NetBEUI was first introduced by IBM in 1985, when it was assumed that LANs would be segmented into workgroups of 20 to 200 computers and that gateways would be used to connect one LAN segment to other LAN segments or to a mainframe. NetBEUI is optimized for high performance when used in departmental LANs or LAN segments. Microsoft NetBEUI under Windows 98 is completely self-tuning.

One common method for setting up a network is to use NetBEUI plus a protocol such as TCP/IP on each computer that needs to access computers across a router. If you set NetBEUI as the default protocol, Windows 98 uses NetBEUI for communication within the LAN segment and uses TCP/IP for communication across routers to other parts of the WAN.

Consider the following issues when choosing this protocol:

- NetBEUI is a nonroutable protocol that cannot cross routers, although it can cross bridges and source routing bridges.
- NetBEUI is optimized for high performance only for use in departmental LANs or LAN segments.

## Microsoft DLC Protocol

The 32-bit DLC protocol provides connection and communication with mainframe computers using DLC. With the 32-bit Data Link Control (DLC) protocol, you can establish multiple connections to different IBM host and AS/400 computers over the same network token-ring, FDDI, or Ethernet adapter. Host terminal emulation programs use the 32-bit DLC to communicate directly with host computers. The 32-bit DLC protocol also allows multiple 32-bit applications to use the same network adapter at the same time to connect to different host computers. You can also use the 32-bit DLC protocol to provide connectivity to local area printers connected directly to the network.

The 16-bit DLC protocol is also available; however, in most cases, it is recommended that you use the 32-bit DLC protocol.

## Microsoft TCP/IP Protocol

Microsoft Transmission Control Protocol/Internet Protocol (TCP/IP) provides communication across interconnected networks that use diverse hardware architectures and various operating systems. TCP/IP can be used to communicate with computers running Windows 98, with devices using other Microsoft networking products, or with non-Microsoft systems such as UNIX.

Microsoft TCP/IP in Windows 98 extends the functionality that Microsoft TCP/IP offered in Windows 95. In Windows 95, Microsoft TCP/IP provided the following elements:

- Core TCP/IP protocols, including the Transmission Control Protocol (TCP), Internet Protocol (IP), User Datagram Protocol (UDP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Domain Name System Protocol (DNS). This suite of Internet protocols provides a set of standards for how computers communicate and how networks are interconnected.

- Support for application programming interfaces (APIs), including Windows Sockets and NetBIOS.

- TCP/IP diagnostic tools to detect and resolve TCP/IP networking problems, including **arp, ftp, nbtstat, netstat, ping, route, telnet, tracert**, and **ipconfig**, plus Windows-based Telnet and IP Configuration (**winipcfg**) utilities.

- Client for DHCP, for automatic configuration of computers running TCP/IP on networks that have DHCP servers.

- Client for WINS, for dynamic resolution of IP addresses to computer names on networks that have WINS servers.

- Point-to-Point Protocol (PPP) for asynchronous communication, as described in Chapter 19, "Remote Networking and Mobile Computing."

With Windows 98, the following enhancements are added:

- Automatic private IP addressing by the client, as described in the section "Configuring IP Addresses Using Automatic Private IP Addressing" later in this chapter.

- Multihoming, as described in the section "Configuring Multihoming" later in this chapter.

- Windows Sockets 2 support, as described in "Enhancements to TCP/IP in Windows 98" later in this chapter.

- Support for IP Multicast (Request for Comments [RFC] 1112), including support for Internet Draft for IGMP version 2.

- Support for Internet Control Message Protocol (ICMP) Router Discovery (RFC 1256).

- Performance enhancements for certain types of high-speed, high-bandwidth networks. These include support for TCP Large Windows (RFC 1323), support for Selective Acknowledgments (RFC 2018), and support for TCP Fast Retransmit and Fast Recovery.

- DHCP enhancements, including address assignment conflict detection and longer timeout intervals.

For information about the Resource Reservation Protocol (RSVP) and Generic Quality of Service (GQoS) architecture, see Chapter 29, "Windows 98 Network Architecture." For more information about GQoS, see also the specification on **ftp://ftp.microsoft.com/bussys/winsock/winsock2/**. For more information about RSVP, see also the Internet Engineering Task Force (IETF) RSVP specification at **http://www.ietf.org**.

For other RFCs and Internet drafts listed above, see **http://www.ietf.org**.

# Planning for TCP/IP

This section gives a broad overview of IP addressing. Then it presents a few common types of networks and explains issues you might want to consider when implementing each type of network.

For information about the architecture of TCP/IP and its Windows Sockets 2 socket API, see Chapter 29, "Windows 98 Network Architecture."

For more conceptual information about TCP/IP, information about routing, and information about using TCP/IP in a large installation with Windows NT Server, see the following publications:

- *Microsoft Windows NT Server Networking Guide for Microsoft Windows NT Server version 4.0.*

- *Network Supplement for Microsoft Windows NT Server version 4.0.*

- *Networking with Microsoft TCP/IP* by Drew Heywood (New Riders Publishing, 1996).

See also the TCP/IP white paper "Microsoft TCP/IP and Windows 95 Networking" at **http://www.microsoft.com/win32dev/netwrk/**.

For TCP/IP shareware tools such as *finger*, *chat*, *whois*, and *nslookup*, visit the following Web sites:

- **http://www.download.com**
- **http://www.shareware.com**
- **http://www.tucows.com**
- **http://www.windows95.com**

## Understanding IP Addressing

Each workstation needs an IP address to communicate on a TCP/IP network such as the corporate network or the global public Internet. The section "Configuring IP Addresses" later in this chapter describes IP addresses in more detail, but for now it is just important to understand that there are two kinds of IP addresses, globally unique IP addresses and private IP addresses.

- Globally unique IP addresses, which you can use on the global Internet.

  On the Internet, the Internet Assigned Numbers Authority (IANA) assigns groups of IP addresses to organizations. The organizations can then assign IP addresses within those groups to individual computers. This prevents multiple computers from having the same IP address.

  For a computer to be visible on the Internet, it must be reachable through a globally unique IP address.

- Private IP addresses, which you cannot use on the global Internet.

  The IANA has reserved a certain number of IP addresses that will never be used on the global Internet. You can use these addresses for computers that will never be used to access the Internet.

  In some cases, you can also use these addresses for computers that need partial connectivity to the Internet but do not need to be directly reachable from the Internet. For example, if you need only Web browsing and e-mail connectivity on a computer, that computer does not necessarily have to be directly reachable from the Internet.

  However, in order to enable computers to use private IP addresses, you must deploy a firewall with proxy or Network Address Translator (NAT) capabilities. A proxy or NAT sits between a private network (a network of computers using private IP addresses) and the Internet. The firewall has a globally unique IP address that can be used on the Internet. When a computer on the private network sends a packet to the Internet, the NAT substitutes the source IP address on that packet for the NAT's own IP address. Thus, the packets appear to originate from the NAT.

  This configuration provides flexibility and a certain level of security: hosts on the Internet cannot directly send IP packets to the computer on the private network because they do not know and cannot use its IP address. The firewall can provide a level of administrative control for which machines and which applications can reach computers on the Internet, and vice versa.

  For more information about private IP addresses, see Request for Comments (RFC) 1918. For more information about NATs, see RFC 1631.

Depending on your needs, you can use either private IP addresses or globally unique IP addresses for each workstation. You could also use both a private IP address and a globally unique IP address if you have a multihomed computer (a computer that has two different adapters, each connected to a different network). For example, a workstation could be connected both to the corporate network (using an adapter that is configured with a private IP address) and to the Internet (using a dial-up adapter that is configured with a globally unique IP address). For information about multihoming and this type of special configuration, see the section "Configuring Multihoming" later in this chapter.

Regardless of the type of IP address you choose, you have two options for configuring the IP addresses:

- Dynamic IP addressing.

   With dynamic IP addressing, the IP address can be configured automatically. This method is much simpler, decreases your management time, and enables you to reuse IP addresses. It is recommended for all sizes of networks.

   In Windows 95, two types of dynamic IP addressing were available. For corporate networks, if there was a Dynamic Host Configuration Protocol (DHCP) server on the network, the computer could automatically obtain the IP address from the DHCP server. And for dial-up Internet connections, some Internet Service Providers (ISPs) automatically assigned your computer a dynamic IP address.

   Windows 98 provides a third option, automatic private IP addressing. This option is recommended for simple networks that have one LAN (subnet) and no DHCP servers. With automatic private IP addressing, if no DHCP server is available, the computer automatically assigns itself a private IP address. (If a DHCP server later becomes available, the computer obtains an IP address from the DHCP server instead.) Computers using private IP addresses can communicate only with other computers using private IP addresses, on the same subnet. They are not directly reachable from the Internet.

- Static IP addressing.

   With static IP addressing, you must manually configure the IP address. This method is time-consuming, especially on medium to large networks. It is not recommended except as a last resort.

For more information about automatic private IP addressing, see "Configuring IP Addresses Using Automatic Private IP Addressing" later in this chapter.

For more information about DHCP, see "Automatically Configuring IP Addresses with DHCP" later in this chapter.

## Planning for a Dial-Up Networking Connection to the Internet

If you plan to use Dial-Up Networking to connect to the Internet, you must configure the Dial-Up Networking connection. Your ISP might automatically assign you an IP address. If not, you must configure information such as the following:

- An IP address
- A default gateway (default router)

For more information about creating a Dial-Up Networking connection, see Chapter 19, "Remote Networking and Mobile Computing."

For more information about configuring an IP address for a Dial-Up Networking connection, see Chapter 20, "Internet Access and Tools."

## Planning for Small Networks

Figure 15.1 shows an example of a small (single-subnet) network that is connected to the Internet by a gateway. In this example, all the computers use globally unique IP addresses and are all visible on the Internet.
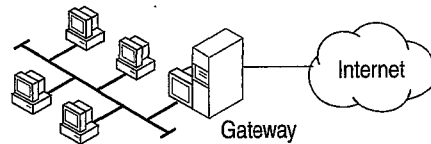


**Figure 15.1   Small network with gateway**

For this type of network, you must obtain a network ID that is valid on the Internet. You must also configure a gateway to reach the Internet, and each computer needs the address of the gateway in order to reach the Internet. A Windows 98 computer cannot be configured to act as a gateway.

For addressing, you should add a DHCP server and let it automatically assign IP addresses. You could also use static IP addressing, but to do so you must manually configure each computer not only now but whenever you make a change to your network that requires new IP addresses.

Now, suppose that the network includes a NAT. You must still obtain a network ID that is valid on the Internet, configure a gateway to reach the Internet, and configure each computer with the address of the gateway. Also, you can still use either DHCP or static addressing. However, because the NAT shields the IP addresses on your network from the Internet, you can also use private IP addressing. On a simple LAN you can use either DHCP to assign private IP addresses, or you can use the automatic private IP addressing feature to let the computer assign itself a unique private address on the LAN.

## Planning for Large Networks

Figure 15.2 shows an example of a large network that is divided into several subnetworks and is connected to the Internet by a gateway.
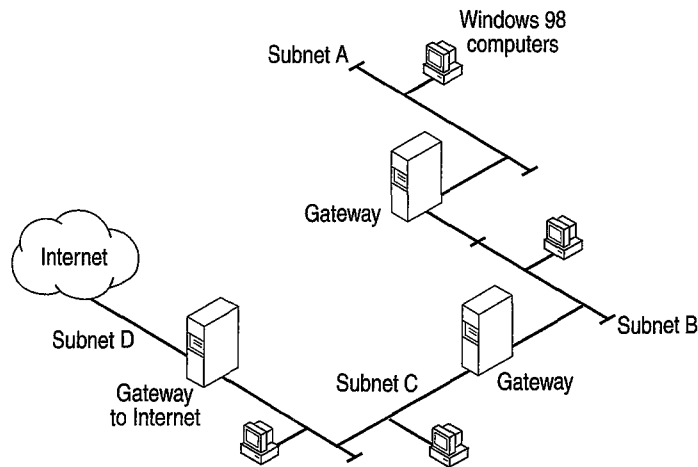
**Figure 15.2 Large network with gateway**

As with the previous example, you must obtain a network ID that is valid on the Internet. You must also set up one or more gateways. If you have multiple gateways, at least one must be configured as the *default gateway* (the gateway that is used to connect to the rest of the network). For more information about default gateways, see the section "Configuring Multihoming" later in this chapter.

For this type of network, you should use DHCP addressing. If your network does include a NAT, you can assign private IP addresses to each computer, but you should not do so using the Windows 98 automatic private IP addressing feature because the automatic private IP addressing feature guarantees uniqueness only on a LAN-per-LAN basis. Computers that use the automatic private IP addressing feature can communicate only with computers in their immediate subnet. Thus, you should use DHCP when there are routers on the network, even if each computer uses private IP addresses. You could, however, use the automatic private IP addressing feature as a backup method if your DHCP server fails.

If your computer does not include a proxy server or a NAT firewall and you want your machines to communicate on the Internet, you must use DHCP for IP address assignment and not the automatic private IP addressing feature.

# Installing Microsoft TCP/IP

Setup installs Microsoft TCP/IP by default if you are installing Windows 98 (instead of upgrading to Windows 98) and you have a network adapter or modem in your computer. If you are upgrading to Windows 98, however, Setup generally keeps your network configuration and you will need to install Microsoft TCP/IP if you want to use it.

If your original Windows installation included a third-party TCP/IP protocol stack, Setup keeps the existing TCP/IP protocol stack instead of installing Microsoft TCP/IP. However, you might want to use Microsoft TCP/IP instead. For example, many third-party TCP/IP stacks do not yet support Windows Sockets 2. If you want to use Microsoft TCP/IP instead of your third-party stack, you must uninstall the third-party stack by using the uninstall utility provided by your network vendor, then install Microsoft TCP/IP.

▶   **To install Microsoft TCP/IP after Windows 98 Setup**

1. In Control Panel, double-click Network.

2. On the **Configuration** tab, click **Add**.

3. Select **Protocol**.

4. Click **Add**.

5. In **Manufacturers**, select Microsoft.

6. In **Network Protocols**, select TCP/IP.

7. Click **OK**.

# Configuring TCP/IP

This section discusses the following topics:

- Configuring IP addresses.

- Configuring a multihomed computer.

- Using the route table to view your IP configuration and to add routes to hosts on the network.

## Configuring IP Addresses

Every computer on a TCP/IP network is identified by a unique 32-bit *IP address*, which also specifies routing information in an internetwork. An IP address looks like this:

```
172.16.94.97
```

This is referred to as dotted decimal notation, with each eight bits of an IP address (called an octet) separated from the next eight bits by a period. An IP address is a single value that contains two pieces of information:

- The *network ID*, which is the portion of the IP address that identifies a group of computers and other devices that are all located on the same logical network.

- The *host ID*, which identifies a particular computer within a particular network ID. A *host*, or node, is any device that is attached to the network and uses TCP/IP.

Each host on the network uses the network ID and host ID to determine which packets it should receive or ignore, and to determine the scope of its transmissions (only hosts with the same network ID accept each other's IP-level broadcasts).

The Internet community uses *address classes* to differentiate networks of various sizes. The network class can be determined from the first octet of its IP address. Table 15.1 summarizes the relationship between the first octet of an IP address and its network ID and host ID, using *w.x.y.z.* to designate the four octets of the IP address. As Table 15.1 shows, the value of the first octet determines which portion of the IP address will be the network ID and which portion will be the host ID.

For example, the first octet of the sample IP address 172.16.34.1 is 172. The **w values** portion of Table 15.1 shows that if the first octet has a value of 128-191, it is a Class B address. Thus, the sample IP address is a Class B address. Its first octet (172) is the network ID, and the remaining octets (16.34.1) are its host ID.

---

**Note** The sample IP addresses used in this chapter are private IP addresses, not IP addresses that are valid on the global Internet.

---

The table also identifies the total number of network IDs and host IDs for each address class that participates in the Internet addressing scheme.

**Table 15.1  IP address classes**

| Class | w values[1,2] | Network ID | Host ID | Available networks | Available hosts per net |
|---|---|---|---|---|---|
| A | 1–126 | *w* | *x.y.z* | 126 | 16,777,214 |
| B | 128–191 | *w.x* | *y.z* | 16,384 | 65,534 |
| C | 192–223 | *w.x.y* | *z* | 2,097,151 | 254 |

[1] Inclusive range for the first octet in the IP address.

[2] The address 127 is reserved for loopback testing and interprocess communication on the local computer; it is not a valid network address. Addresses 224 and above are reserved for special protocols (IGMP multicasting and others), and cannot be used as host addresses.

Because the sender's IP address is included in every outgoing IP packet, the receiving computer can derive the originating network ID and host ID from the IP address field. This is done by using *subnet masks*, which are 32-bit values that allow the recipient of IP packets to distinguish the network ID and host ID portions of the IP address.

The value of a subnet mask can also be represented in dotted decimal notation. Subnet masks are determined by assigning ones to bits that belong to the network ID and zeroes to bits that belong to the host ID. When the bits are in place, the 32-bit value is converted to dotted decimal notation, as shown in Table 15.2.

**Table 15.2   Default subnet masks for standard IP address classes**

| Address class | Bits for subnet mask | Subnet mask |
|---|---|---|
| Class A | 11111111 00000000 00000000 00000000 | 255.0.0.0 |
| Class B | 11111111 11111111 00000000 00000000 | 255.255.0.0 |
| Class C | 11111111 11111111 11111111 00000000 | 255.255.255.0 |

The result allows TCP/IP to determine the host ID and network ID of the local computer. For example, if the IP address is 172.16.34.1 and the subnet mask is 255.255.0.0, then the network ID is 172.16 and the host ID is 34.1.

Subnet masks are also used to further segment an assigned network ID among several local networks. For example, a network using the Class B network address 10.100 is one of over 16,000 Class B addresses capable of serving more than 65,000 nodes each. But if this corporate network includes 12 international LANs with 75 to 100 nodes each, it is better to use subnetting to make effective use of 10.100 than to apply for 11 more network IDs. In this case, the third octet of the IP address can be used as a subnet ID, using the subnet mask 255.255.255.0, which splits this Class B address into 254 subnets: 10.100.1 through 10.100.254, each of which can have 254 nodes. Any of these network addresses could be assigned to the 12 international LANs in this example. Within each LAN, each computer is assigned a unique host ID, and they all have the subnet mask 255.255.255.0.

---

**Note** All systems connected to the same local area network must have the same subnet mask.

Host IDs 0 and 255 should not be assigned to a computer; they are used as broadcast addresses that are typically recognized by all computers.

---

Windows 98 provides three methods of IP addressing:

- DHCP addressing, in which DHCP servers such as computers running Windows NT Server 3.5 or later automatically assign IP addresses to Windows 98 clients.

- Automatic private IP addressing, in which the computer automatically assigns itself an IP address.

- Static IP addressing, in which network administrators manually configure IP addresses for all the computers on the network.

The following sections describe each of the three configurations.

## Automatically Configuring IP Addresses with DHCP

In an effort to make implementing the TCP/IP protocol more manageable, Microsoft worked with other industry leaders to create an Internet standard called Dynamic Host Configuration Protocol (DHCP) for the automatic allocation of IP addresses. DHCP is not a Microsoft standard, but a public Request for Comments (RFC 1541) that Microsoft has implemented.

DHCP allows you to establish a range of valid IP addresses to be used per subnetwork. An individual IP address from the range is assigned dynamically to any DHCP client requesting an address. DHCP also allows you to establish a lease time that defines how long an IP address is to remain valid. Other configuration parameters can also be assigned using DHCP, such as subnet mask, DNS and WINS server identification, and so on.

A computer running Windows 98 cannot be a DHCP server. A DHCP server runs as a service on Windows NT Server 3.5 or later. If DHCP is available company-wide, users can move from subnet to subnet and always have a valid IP address. The IP Configuration utility (**winipcfg**) allows users or administrators to examine the current IP address assigned to the computer, the IP address lease time, and other useful data about the TCP/IP configuration.

When TCP/IP is installed, Windows 98 automatically enables the option to obtain an IP address from a DHCP server. You can disable this option if you want to manually enter IP addresses; however, in general you should not need to disable DHCP.

▶   **To disable DHCP**

- You disable DHCP by configuring static IP addresses, following the instructions outlined in the section "Manually Configuring IP Addresses" later in this chapter.

If Microsoft TCP/IP is configured to obtain an IP address from a DHCP server when a DHCP server is not available on the network, an error message announces that the DHCP client could not obtain an IP address and your Windows 98 computer automatically assigns itself a private IP address (using automatic private IP addressing). When the DHCP server becomes available again, it will assign your computer an IP address.

## Configuring IP Addresses Using Automatic Private IP Addressing

With Windows 98, Microsoft TCP/IP provides a new mechanism for automatic IP address assignment for simple LAN-based network configurations, called automatic private IP addressing. With automatic private IP addressing, DHCP clients can automatically assign themselves an IP address if a DHCP server is not present. This might happen, for example, on very small networks without a DHCP server, or on any size network if a DHCP server is temporarily down. The DHCP client can use B-node NetBIOS naming to assign the adapter a unique IP address from a special address space. These IP addresses must lie in the following range:

169.254.*x.x*

These addresses are used only for private, internal addressing and are not valid for hosts that are visible on the global Internet.

After the adapter has been assigned an IP address, the computer can use the TCP/IP protocol to communicate with any other computer that is connected to the same LAN hub and that also uses automatic private IP addressing. However, the computer cannot communicate with computers on other subnets, or with computers that do not use automatic private IP addressing.

A Windows 98 computer that is configured for automatic private IP addressing can assign itself a private IP address if either of the following circumstances applies:

- A computer that is not configured as a laptop can assign itself a private IP address at boot time if the computer does not have a valid DHCP lease, and no DHCP server is found on the network.

- If the computer is configured as a laptop, the computer can assign itself a private IP address if no DHCP server is found on the network, regardless of whether it has a DHCP lease. This is useful, for example, for a computer that is sometimes located on a network with a DHCP server, and sometimes located on a network without a DHCP server.

In either case, if a DHCP server is later found, the computer stops using the private IP address and instead uses the IP address assigned by the DHCP service.

Automatic private IP addressing is automatically enabled. You might want to disable it in the following cases:

- Your network uses routers.
- Your network is connected to the Internet without a NAT or proxy server.

Unless you have turned DHCP messages off, DHCP messages inform you when you change between DHCP addressing and automatic private IP addressing. If you do accidentally turn DHCP messages off, you can turn them back on by changing the value of the registry entry **PopupFlag** from 00 to 01 in the following registry location:

**HKEY_LOCAL_MACHINE\System**
    **\CurrentControlSet\Services\VxD\DHCP**

You must reboot for the change to take effect.

You can also determine whether your computer is using automatic private IP addressing by using **winipcfg**, as the following procedure explains.

▶  **To determine whether automatic private IP addressing is currently enabled**

- Click **Start**, click **Run**, type **winipcfg**, and then click **More info**. The resulting screen identifies your IP address and other information. Look at the box immediately beneath your adapter address. If the name of the box is "IP Autoconfiguration Address" and the IP address lies in the 169.254.*x.x* range, automatic private IP addressing is enabled. If, on the other hand, the name of the box is "IP Address," automatic private IP addressing is not currently enabled.

You can disable automatic private IP addressing in one of two ways:

- You can manually configure TCP/IP by following the procedure outlined in the section "Manually Configuring IP Addresses" later in this chapter. However, this method also disables DHCP.

- You can disable automatic private IP addressing (but not DHCP) by editing the registry.

You disable automatic private IP addressing but not DHCP by adding the **IPAutoconfigurationEnabled** registry entry with a value of DWORD 0x0 in the following registry location:

**HKEY_LOCAL_MACHINE\System**
    **\CurrentControlSet\Services\VxD\DHCP**

Use the Registry Editor to add this entry, then shut down and restart the computer.

---

**Caution**  Using Registry Editor incorrectly can cause serious problems that may require you to reinstall Windows 98. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

---

You can change this registry entry for your entire network by creating an Msbatch.inf file. For more information about Msbatch.inf, see Chapter 3, "Custom Installations."

## Manually Configuring IP Addresses

If you cannot use DHCP or automatic private IP addressing for automatic configuration, the network administrator must configure TCP/IP manually. Or, if custom setup scripts are used to install Windows 98, the correct values can be defined in the setup script. The required values include the following:

- The IP address and subnet mask for each network adapter installed on the computer.

- The IP address for the default gateways (hardware routers or servers running routing software with the ability to interpret IP addresses, usually used to find remote destinations).

- Whether the computer will use Domain Name System (DNS) and, if so, the IP addresses of the DNS servers on the internetwork.

- WINS server addresses, if WINS servers are available on the network.

The following procedure describes the basic configuration options for TCP/IP. If you want to configure the computer to use DNS or WINS for name resolution, see the procedures in "Using DNS for Name Resolution" later in this chapter and "Using WINS for Name Resolution" later in this chapter.

▶ **To configure the TCP/IP protocol manually**

1. In Control Panel, double-click Network.

2. Double-click the instance of the TCP/IP protocol that is bound to your network adapter.

---

**Note**   If your computer has multiple network adapters, the list includes an instance of TCP/IP for each network adapter. You must configure each adapter with its own IP address, subnet mask, and gateway. There is one exception: you should configure TCP/IP settings for your dial-up adapter from your Dial-Up connection icon.

All other settings apply system-wide.

---

3. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.

4. Select the **Specify an IP address** check box.

5. Type an IP address and subnet mask in the respective boxes.

   The network administrator must provide these values for individual users, based on the network ID and the host ID plan for your site.

   - The value in the **IP Address** box identifies the IP address for the local computer or, if more than one network adapter is installed, for the network adapter selected in the **Configuration** dialog box.

   - The value in the **Subnet Mask** box identifies the network membership and its host ID for the selected network adapter. The subnet mask defaults to an appropriate value, as shown in the following list.

| Address class | Range of first octet in the IP address | Subnet mask |
| --- | --- | --- |
| Class A | 1–126 | 255.0.0.0 |
| Class B | 128–191 | 255.255.0.0 |
| Class C | 192–223 | 255.255.255.0 |

6. To view or specify which network clients are bound to the TCP/IP protocol, click the **Bindings** tab.

   - To keep a network client from using the TCP/IP protocol, make sure the check mark beside the client name is cleared.

   - If the network client for which you want to use TCP/IP does not appear in this list, that client might not be installed properly. Return to the **Configuration** tab in the **Network** dialog box and reinstall that network client.

---

**Note**  The only network client provided with Windows 98 that can use Microsoft TCP/IP is Client for Microsoft Networks. Client for NetWare Networks does not use Microsoft TCP/IP.

NetWare/IP from Novell allows the NetWare Core Protocol (NCP) request to be sent over an IP header. You can use NetWare/IP only with a Novell-provided client.

---

7. Click the **Gateway** tab. Type at least one IP address for the default gateway (IP router) on the network, and then click **Add**.

8. To specify an IP address for an additional gateway, type the IP address in the **New gateway** box, and then click the **Add** button.

   The first gateway in the list is the default gateway, which is used to reach destinations on remote networks. Gateway addresses can be prioritized by dragging the IP address in the list of installed gateways. Windows 98 attempts to connect to other gateways only if the primary gateway is unavailable.

9. Click **OK**.

10. Restart the computer for changes to take effect.

If you are using Dial-Up Networking to connect to the Internet, you can manually configure DNS and IP addresses for each connection that you define. For more information about defining IP addresses for each connection and about IP addresses on TCP/IP networks, see Chapter 20, "Internet Access and Tools." For more information about TCP/IP registry entries, see Chapter 31, "Windows 98 Registry."

## Configuring Multihoming

When a computer is configured with more than one IP address, it is referred to as a *multihomed system*. With Windows 98, network administrators create multihomed configurations for purposes such as the following:

- To connect a computer simultaneously to the local network and (through Dial-Up Networking or PPTP) to the Internet.

- To connect to different subnets when the computer is on a single physical network that contains multiple logical IP networks.

- To allow a computer to communicate simultaneously on two otherwise isolated networks.

For example, in the most common configuration, a computer might have a LAN connection and a dial-up (PPP) or Point-to-Point Tunneling Protocol (PPTP) connection to the Internet or another IP network.

For more information about this configuration, see Chapter 19, "Remote Networking and Mobile Computing."

As another example, a computer on the local area network at a branch office that also requires a network connection to certain computers on the corporate enterprise network might require a multihomed configuration. Such a configuration might be used, for example, by financial or human-resources personnel who must access servers on a private subnet.
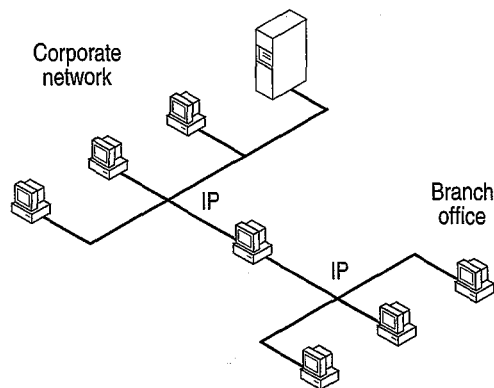


Figure 15.3   Multihomed Windows 98 computer connected to two separate networks

This section provides information about configuring multihomed computers running Windows 98.

---

**Note**  Multihoming on a Windows 98 computer is suitable only as a limited solution for connecting a single computer to other networks. For corporate computing environments that require routing among subnetworks, you should use dedicated routers such as a Cisco routers, UNIX hosts, or a computer running Windows NT Server 3.5 or later.

---

## Configuring TCP/IP on Multihomed Computers

You can configure multihoming by using multiple network adapters on a single computer, multiple media, or multiple IP addresses for a single network adapter.

For a multihomed computer that uses multiple network adapters for physical connections to the LAN, or a dial-up adapter for remote access, there is an instance of Microsoft TCP/IP for each adapter in the Network option in Control Panel.

Instances of Microsoft TCP/IP
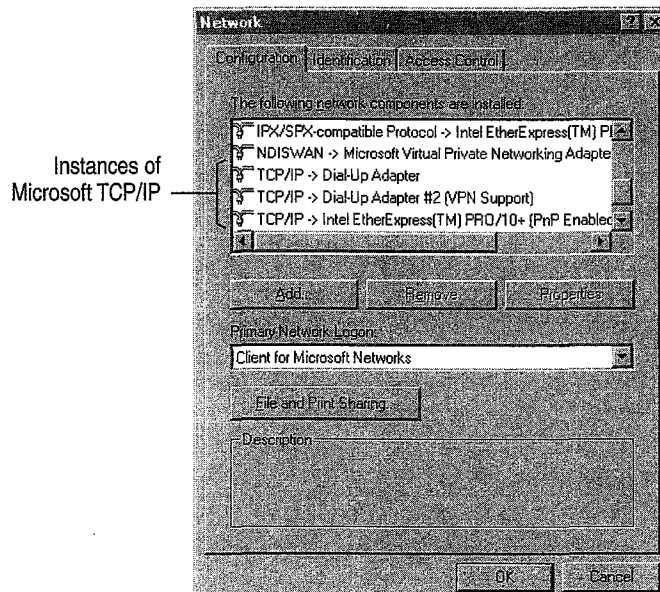


### Configuring multiple network adapters per physical network.

Windows 98 places no restrictions on such configurations, so you can add as many network adapters as the computer hardware can accommodate, and assign each a separate address. However, you can only have six instances of TCP/IP and four instances of IPX/SPX installed on the system.

► **To configure a multihomed system using multiple network adapters**

- Add TCP/IP configuration information for each network adapter in the Network option in Control Panel, either by using DHCP or by entering information for static IP addresses.

**Caution**  You should not use this method to configure a multihomed system for a Dial-Up or virtual private networking connection. When Dial-Up Networking or virtual private networking are installed, adapters are automatically added and appear automatically in the Network option in Control Panel.

### Configuring multiple networks and media types.

You can have only six instances of TCP/IP and four instances of IPX/SPX. This means that only six adapters can bind to TCP/IP and only four to IPX/SPX. Otherwise, there are no restrictions for this type of configuration other than hardware and media support. Microsoft TCP/IP supports the following:

- Ethernet (and 802.3 SNAP).
- Token-ring (802.5).
- Fiber distributed data interface (FDDI), using NDIS 2 real-mode network adapter drivers (only a few protected-mode adapter drivers are available for FDDI supporting TCP/IP).
- WAN, using switched virtual-circuit wide-area media such as ISDN, X.25, and dial-up or dedicated asynchronous lines.

### Configuring multiple IP addresses per network adapter.

This option is not supported through the Network option in Control Panel. Additional addresses can be added directly in the registry. However, this is not a recommended method for configuring TCP/IP. NetBIOS name registration using NetBIOS over TCP/IP supports only one IP address per network adapter. Moreover, if DHCP is enabled for configuring TCP/IP, only one DHCP-assigned address can be provided per adapter.

### Issues When Implementing Multihoming

If TCP/IP is configured for multiple network adapters, or for both LAN and Dial-Up connections, you must consider the following issues:

### A unique IP address and subnet mask are defined for each adapter.

For each network adapter or dial-up adapter, an instance of TCP/IP is bound to the adapter. You can choose to have IP addresses dynamically assigned by DHCP or automatic private IP addressing or defined manually as static addresses.

### Domain Name System (DNS) configuration settings are global.

The settings on the **DNS Configuration** tab in TCP/IP properties are used for all adapters on the computer. For example, if you change the DNS settings in the TCP/IP properties for the dial-up adapter to enable DNS, then DNS is also enabled for every LAN adapter on the computer.

However, the settings on the **WINS Configuration** tab are used only for the adapter you are configuring. If you enable the option named **Use DHCP For WINS Resolution** for a LAN adapter, this option is enabled only for that adapter, not for the dial-up adapter or for other LAN adapters on the computer.

Therefore, for a multihomed computer, you must carefully define options for DNS that are applicable for all adapters using TCP/IP. Usually, this means that you want the following:

- If you want to use DNS or the Hosts file for name resolution with any TCP/IP connection, then make sure DNS is enabled.

---

**Note** In the case when WINS is used for name resolution on the network (including using WINS servers for host-name resolution) and when DNS is used only for dial-up connections, it is easy for a user to mistakenly disable DNS in the TCP/IP properties for the LAN adapter, without realizing that this also disables DNS for the remote connection. The result would be an inability to find remote hosts when using the remote connection.

---

### The default gateway can be different for each adapter.

For multiple physical connections to the WAN, you can assign a different default gateway for each network connection; however, a Windows 98 computer uses only one default gateway at a time. The default gateway for the dial-up adapter is assigned by the access provider. You can also assign different gateways for a Dial-Up Networking connection by using the Make New Connection Wizard.

### Only one default gateway is used at a time.

Although you can have a different default gateway for each adapter, Windows 98 uses only one default gateway at a time. This means that only certain hosts are reachable:

- Hosts on the local subnet
- Hosts that are reachable by the default gateway

As a result, in some cases you may lose network connectivity. For example, suppose your computer is first connected to the corporate TCP/IP network and you make a PPP dial-up connection to the Internet. Your computer stops using the default gateway that connects your computer to the corporate network and instead uses the default gateway that connects your computer to the Internet. Therefore, you can reach hosts on your local subnet, but you cannot reach other hosts on your network.

For a detailed example of a computer changing default gateways, see Chapter 19, "Remote Networking and Mobile Computing."

If you want to restore connectivity to the corporate network, you can use one of the following three methods:

- You can manually add routes to destinations on your local network. For information about adding routes, see "Using the Route Table" later in this chapter.

- In the properties for your dial-up connection, you can deselect the option named **Use default gateway on remote network**, then manually add routes to dial-up destination. For information about how to do this, see Chapter 19, "Remote Networking and Mobile Computing."

- If any of the routers on your corporate network uses the Routing Information Protocol (RIP), you can configure your computer to listen in on those broadcasts. For information about this configuration, see "Support for RIP Listening" later in this chapter.

## Using the Route Table

The route table controls where IP packets are sent. It is maintained automatically in most cases, but in some cases you may want to manually add a route. This section describes the route table and explains how to add routes.

To see the route table for your computer, at the command prompt type **route print**.

---

**Note**  You can reach the command prompt from the **Start** menu, either by clicking **Run** or by clicking **Programs**, and then clicking **MS-DOS Prompt**.

---

The following table is a sample route table from a single-homed computer.

**Table 15.3    Route table sample**

| Network address | Netmask | Gateway address | Interface | Metric |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 172.16.34.1 | 172.16.34.232 | 1 |
| 127.0.0.0 | 255.0.0.0 | 127.0.0.1 | 127.0.0.1 | 1 |
| 172.16.34.0 | 255.255.255.0 | 172.16.34.232 | 172.16.34.232 | 1 |
| 172.16.34.232 | 255.255.255.255 | 127.0.0.1 | 127.0.0.1 | 1 |
| 172.16.255.255 | 255.255.255.255 | 172.16.34.232 | 172.16.34.232 | 1 |
| 10.0.0.0 | 10.0.0.0 | 172.16.34.232 | 172.16.34.232 | 1 |
| 255.255.255.255 | 255.255.255.255 | 172.16.34.232 | 172.16.34.232 | 1 |

Table 15.3 shows a computer with the IP address 172.26.34.232. The table contains the following seven entries:

1. The first line is the default route. This is the route to which the computer sends IP packets if the other route entries do not specify where to send them.

2. The second line is the loopback address. This is the address a host uses to send packets to itself. The loopback address is always 127.0.0.0, and the netmask is always 255.0.0.0.

3. The third line is a network route.

4. The fourth line is a host route for the local host (the route for this host computer).

5. The fifth line is the subnet broadcast address.

6. The sixth line is the IP multicast address. This is the address the computer sends packets to in order to reach an IP multicast group.

7. The seventh line is for limited broadcast address. This is the address a host uses to reach all other addresses on the subnet.

## Network Address

The network address in the route table is the destination address. The network address column can have four different types of entries, listed here in the order in which they are searched for a match.

1. Host address (a route to a single, specific destination IP address).
2. Subnet address (a route to a subnet).
3. Network address (a route to an entire network).
4. Default gateway (a route used when there is no other match).

If no match is found, the packets are discarded.

## Netmask

The *netmask* defines which portion of the network address must match in order for that route to be used. When the mask is written in binary, a 1 is significant (must match) and a 0 need not match.

For example, the mask of all 255s (all 1s) means that the destination address of the packet to be routed must exactly match the network address in order for this route to be used. For another example, the network address 172.20.232.0 has a netmask of 255.255.255.0. This netmask means that the first three octets must match exactly, but the last octet need not match.

## Gateway Address

The gateway address is where the packet must be sent. This can be the local network card or the address of a gateway (router) on the local subnet.

## Interface

The interface is the address of the network card over which the packet should be sent. 127.0.0.1 is the software loopback address.

## Metric

The metric is the number of hops to the destination. Anything on the local subnet is one hop, and each router crossed after that is an additional hop. The metric is used to determine the best route.

## Configuring Routes for a Multihomed Computer

If your computer is multihomed and has connections to two separate IP networks, such as the corporate network and the Internet, the default gateway for only one network is used. For the computer to be able to communicate with the other network, routes must be added to the route table. This can be accomplished in one of two ways:

1. If a router on the network sends RIP broadcasts and your computer is configured to listen to RIP broadcasts, routes will be added automatically. (For more information about configuring your computer to listen to RIP broadcasts, see the section "Support for RIP Listening" later in this chapter.)

2. You can manually add static routes to the route table.

   To add static routes, use the following format:

   ```
   Route add [subnet] mask [netmask] [gateway] metric [metric]
   ```

   The following is an example route:

   ```
   Route add 172.20.255.0 mask 255.255.255.0 172.20.234.232 metric 2
   ```

   The route in this example means that to get to the subnet 172.20.255.0 with a mask of 255.255.255.0, use gateway 172.20.234.232, and that the gateway is 2 hops away.

# Configuring TCP/IP Name Resolution

Computers use IP addresses to identify each other, but users usually find it easier to work with computer names. A name resolution mechanism must be available on a TCP/IP network to resolve names to IP addresses.

Windows 98 provides several different types of name resolution, including DNS, WINS, broadcast name resolution, and name resolution using Hosts or LMHosts files. Generally, a Windows 98 computer uses a combination of these name resolution types, summarized in this section.

**Domain Name System name resolution.** Domain Name System (DNS) is a global, distributed database based on a hierarchical naming system. DNS name resolution is used on the Internet to map friendly names to IP addresses, and vice versa. Notice that DNS replaces the functionality of the Hosts file. For more information, see "Using DNS for Name Resolution" later in this chapter.

**Windows Internet Naming Service.** Windows Internet Naming Service (WINS) name resolution provides static and dynamic mapping of names to IP addresses. (This contrasts with DNS name resolution, which provides only static mapping.) Computers running Microsoft TCP/IP can use WINS if one or more Windows NT Server computers configured as WINS servers are available. WINS can be used in conjunction with broadcast name resolution for an internetwork, where other name resolution methods are inadequate. Notice that WINS is a dynamic replacement for the LMHosts file. For more information, see "Using WINS for Name Resolution" later in this chapter.

**Broadcast name resolution.**  Computers running Microsoft TCP/IP can use local broadcast name resolution, which is a NetBIOS-over-TCP/IP mode of operation defined in RFC 1001/1002 as b-node. It is restricted to only one subnet. This method relies on a computer making IP-level broadcasts to register its name by announcing it on the network. Each computer in the broadcast area is responsible for challenging attempts to register a duplicate name and for responding to name queries for its registered name.

**Hosts or LMHosts files.**  Hosts and LMHosts files, also called *host tables*, are files that Windows 98 can use for local name resolution if other methods are not available. An LMHosts file specifies the NetBIOS computer name and IP address mappings. When WINS in not available, it is used as a WINS equivalent to resolve NetBIOS names to IP addresses. Likewise, a Hosts file specifies the DNS name and IP address. It is used as a local DNS equivalent to resolve host names to IP addresses. You must manually enter the name-to-IP address mappings in Hosts and LMHosts files.

For more information about creating and editing Hosts and LMHosts files, see Appendix F, "Hosts and LMHosts Files for Windows 98."

Windows 98 provides support for multiple DNS servers and up to twelve WINS servers. Support for either service can be configured automatically from a DHCP server or after Windows 98 Setup by using the Network option in Control Panel.

---

**Note**  To ensure that both the name and the address are unique, the computer using Microsoft TCP/IP registers its name and IP address on the network during system startup.

---

## Using DNS for Name Resolution

This section provides an overview of DNS, then describes how to configure your Windows 98 client to use DNS.

### Understanding DNS

Although TCP/IP uses IP addresses to identify and reach computers, users typically prefer to use host names. For example, users prefer the friendly name **ftp.terrafirminc.tld** instead of its IP address 172.16.23.55. Domain Name System, defined in Requests for Comments (RFCs) 1034 and 1035, is the naming service used on the Internet to provide standard naming conventions for IP computers.

Although DNS may seem similar to WINS, there are two major differences. First, DNS requires static configuration of IP addresses for name-to-address mapping. WINS, on the other hand can provide name-to-address mapping dynamically and requires far less administration.

Second, whereas WINS uses a flat name space (all names are located in the same domain), DNS uses a tree structure called the domain name space, where each node or domain is named and can contain subdomains. DNS is a global, distributed database based on a hierarchical naming system. The naming system was developed to provide a method for uniquely identifying hosts on the Internet.

In Windows 98, the DNS name consists of two parts—the domain name and the host name—known together as the fully qualified domain name (FQDN). For example, using the fictional domain name of Terrafirminc, an FQDN for a workstation in the nursery division could be **jeff.nursery.terrafirminc.tld**. Note that the DNS name can actually be multipart with a period (.) separating each part. Also note that the host portion of the name, **jeff**, is analogous to a NetBIOS computer name.

---

**Note**  In Windows 98, a computer's globally known system name is its host name (for example, **jeff**), appended with a DNS domain name (for example, **nursery.terrafirminc.tld**). The host name defaults to the computer name (NetBIOS name) defined during Windows 98 Setup. The default name can be changed in the **DNS Configuration** tab when you are configuring TCP/IP properties.

---

The top-level domains were assigned organizationally and by country. These domain names follow the International Standard 3166. Two-letter and three-letter abbreviations are used for countries, and various abbreviations are reserved for use by organizations, as shown in Table 15.4.

**Table 15.4   DNS domain names**

| DNS domain name | Type of organization |
| --- | --- |
| com | Commercial (for example, microsoft.com) |
| edu | Educational (for example, mit.edu for Massachusetts Institute of Technology) |
| gov | Government (for example, nsf.gov for the National Science Foundation) |
| org | Noncommercial organizations (for example, fidonet.org for FidoNet) |
| net | Networking organizations (for example, nsf.net for NSFNet) |

DNS uses a client/server model, where the DNS servers contain information about a portion of the DNS database and make this information available to clients, called *resolvers*, that query the name server across the network. DNS *name servers* are programs that store information about parts of the domain name space called *zones*. The administrator for a domain sets up name servers that contain the database files with all the resource records describing all hosts in their zones. DNS resolvers are clients that use name servers to gain information about the domain name space.

All the resolver software necessary for using DNS on the Internet is installed with Microsoft TCP/IP. Microsoft TCP/IP includes the DNS resolver functionality used by NetBIOS over TCP/IP and Windows Sockets connectivity applications such as File Transfer Protocol (FTP) and Telnet to query the name server and interpret the responses.

The key task for DNS is to present friendly names for users and then resolve those names to IP addresses, as required by the internetwork. If a local name server does not contain the data requested in a query, it then queries the other name servers until it finds the specific name and address it needs. This process is made faster because name servers continuously cache the information learned about the domain name space as the result of queries.

## Configuring DNS

You need to determine whether users should configure their computers to use DNS. Usually you will use DNS if you are using TCP/IP to communicate over the Internet or if your private internetwork uses DNS to distribute host information. You can use DNS either instead of or in conjunction with WINS, which is described in the next section.

You also need to determine whether or not you want to use DHCP for automatic configuration. (For information about circumstances in which you might want to use DHCP, see "Planning for TCP/IP" earlier in this chapter.) If you use DHCP for automatic configuration, a DHCP server can automatically configure the list of DNS servers the client should use. If you do not use DHCP, however, you will need to configure these parameters yourself.

### Using DNS with WINS Lookup

If you are already using WINS servers for local name resolution but you want to make those servers visible to the global Internet, you can do so without configuring configure DNS on each computer. Windows NT Server 4.0 and later includes a feature called DNS with WINS Lookup. If you configure a Windows NT Server 4.0 and later to use DNS with WINS Lookup, that Windows NT Server can query the WINS servers for the "friendly names" of your computers, then use the information to construct a name that can be used on the global Internet.

For example, suppose the network **terrafirminc.tld** contains a Windows 98 computer named Annuals. On the internal network, the Windows NT Server is using DHCP to automatically assign IP addresses and WINS to resolve those IP addresses to the computer's "friendly names." You want Internet users to be able to connect to Annuals using the fully qualified domain name **annuals.terrafirminc.tld**. If you have Windows NT Server 4.0 or later, you can configure Microsoft DNS server on that computer to query WINS for the IP address for Annuals. WINS returns the IP address, and DNS then successfully resolves the IP address to the FQDN **annuals.terrafirminc.tld**.

For more information about this configuration, see the *Microsoft Windows NT Resource Kit* (for Microsoft Windows NT Server version 4.0).

This section describes how to configure a Windows 98 computer to use DNS for name resolution. You only need to follow the procedures outlined in this section if you are not using DHCP to configure name resolution. If you are using DHCP to configure name resolution, you need only configure DHCP by following the steps in "Automatically Configuring IP Addresses with DHCP" earlier in this chapter.

Figure 15.4 shows sample DNS configuration settings.
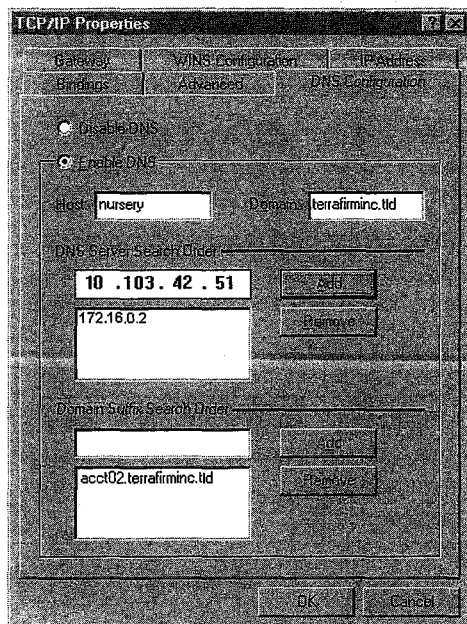


**Figure 15.4    Sample DNS configuration settings**

▶ **To configure a computer to use DNS for name resolution**

1. In Control Panel, double-click Network.

2. Double-click the TCP/IP protocol that is bound to your network adapter.

3. In the **TCP/IP Properties** dialog box, click the **DNS Configuration** tab.

4. If a DNS server is available, click **Enable DNS**. Then specify a host name and complete the other configuration information as described in the following procedure.

---

**Tip**  You must enable DNS on each computer that needs to use Hosts for name resolution.

---

The host name is used to identify the local computer for authentication by some utilities. Other TCP/IP-based utilities can use this value to learn the name of the local computer. Host names are stored on DNS servers in a table that maps names to IP addresses for use by DNS.

▶ **To set the host name for DNS**

- Type a name in the **Host** box.

  The name can be any combination of the letters A through Z, the numerals 0 through 9, and the hyphen (-), plus the period (.) character used as a separator. By default, this value is the Microsoft networking computer name, but the network administrator can assign another host name without affecting the computer name.

---

**Note**  Some characters that can be used in computer names, especially the underscore, cannot be used in host names. This is a limitation imposed in the character set defined by the Internet Engineering Task Force (IETF) standard for DNS. For more information, see RFC 1123.

---

▶ **To set the DNS domain name**

- Optionally, type a name in the **Domain** box.

  This is usually an organization name followed by a period and an extension that indicates the type of organization, such as **microsoft.com**. The name can be any combination of the letters A through Z, the numerals 0 through 9, and the hyphen (-), plus the period (.) character used as a separator.

This DNS domain name is appended to the host name (or short name) to create the fully qualified domain name (FQDN) for your computer. If you have not specified a domain in the Domain Suffix Search Order and you are querying for a short name, then this DNS domain name is appended to your query.

---

**Note**  A DNS domain is not the same as a Windows NT or LAN Manager domain. A DNS domain is a hierarchical structure for organizing TCP/IP hosts and provides a naming scheme used on the Internet. A Windows NT or LAN Manager domain is a grouping of computers for security and administrative purposes.

---

You can add up to three IP addresses for DNS servers. For a given DNS query, Windows 98 attempts to get DNS information from the first IP address in the list. If no response is received, Windows 98 goes to the second server in the list, and so on. To change the order of the IP addresses, you must remove them and retype them in the order that you want the servers to be searched.

▶   **To set the DNS server search order**

1. In Control Panel, double-click Network.

2. Double-click the TCP/IP protocol that is bound to your network adapter.

3. In the **TCP/IP Properties** dialog box, click the **DNS Configuration** tab.

4. In the **DNS Server Search Order** box, type the IP address of a DNS server that will provide name resolution. Then click the **Add** button to add the IP address to the list.

   The network administrator should provide the correct values for this parameter, based on the IP address assigned to the DNS server used at your site.

5. To remove an IP address from the list, select it, and then click the **Remove** button.

---

**Note**  If you have two servers listed in this dialog box, Windows 98 checks the second server only if no response is received from the first server. If Windows 98 attempts to check a host name with the first server and receives a message that the host name is not recognized, the system does not try the second DNS server.

---

The Domain Suffix Search Order specifies the DNS domain suffixes to be appended to short names during name resolution. For example, with the DNS configuration settings shown in Figure 15.4, the domain name acct02.terrafirminc.tld would be appended to the short name to create an FQDN. However, if the Domain Suffix Search Order list is blank, the domain name terrafirminc.tld would be appended instead.

You can add up to five domain suffixes. Place domain suffixes in the list in the order you want them to be searched.

▶   **To set the domain suffix search order**

1. In Control Panel, double-click Network.

2. Double-click the TCP/IP protocol that is bound to your network adapter.

3. In the **TCP/IP Properties** dialog box, click the **DNS Configuration** tab.

4. In the **Domain Suffix Search Order** box, type the domain suffixes to add to your domain suffix search list, and then click the **Add** button.

5. To remove a domain name from the list, select it, and then click the **Remove** button.

## Using WINS for Name Resolution

Windows Internet Naming Service (WINS) is a service that runs on Windows NT Server to optimize NetBIOS name resolution. It provides a distributed database for registering and querying dynamic computer name-to-IP address mappings in a routed network environment. You can use WINS either alone or in conjunction with DNS.

WINS reduces the use of local broadcasts for name resolution and allows users to locate computers on remote networks automatically. Furthermore, when dynamic addressing through DHCP results in new IP addresses for computers that move between subnetworks, the changes are updated automatically in the WINS database. Neither the user nor the network administrator needs to make manual accommodations for name resolution in such a case.

WINS consists of two components: the WINS server, which handles name queries and registrations, and the client software (NetBIOS over TCP/IP), which queries for computer name resolution. A WINS server is a Windows NT Server 3.5 or later computer with WINS server software installed. When Microsoft TCP/IP is installed under Windows 98, WINS client software is installed automatically.

On a Windows-based network, users can browse transparently across routers. To allow browsing without WINS, you must ensure that the users' primary domain has Windows NT Server computers on both sides of the router to act as master browsers. These computers need to contain correctly configured LMHosts files with entries for the domain controllers across the subnet.

With WINS, such strategies are not necessary, because the WINS servers and proxies provide the support necessary for browsing Windows NT domains across routers. For a technical discussion of how WINS works and how it can be set up on the network, see *Windows NT Server 4.0 TCP/IP* in the Windows NT Server 4.0 documentation set.

If there are WINS servers installed on your network, you can use WINS in combination with broadcast name queries to resolve NetBIOS computer names to IP addresses. If you do not use this option, Windows 98 can use name query broadcasts (b-node mode of NetBIOS over TCP/IP) plus the local LMHosts file to resolve computer names to IP addresses. Broadcast resolution is limited to the local network, as described earlier in this section.

If DHCP is used for automatic configuration, these parameters can be provided by the DHCP server. Otherwise, you must configure information about WINS servers manually. WINS configuration is global for all network adapters on a computer.

### Configuring WINS

The following procedure describes how to configure WINS and how to enable DHCP.

▶ **To configure a computer to use WINS for name resolution**

1. In Control Panel, double-click Network.

2. Double-click the TCP/IP protocol that is bound to your network adapter.

3. In the **TCP/IP Properties** dialog box, click the **WINS Configuration** tab.

4. If a DHCP server is available that is configured to provide information on available WINS servers, select the **Use DHCP For WINS Resolution** check box.

   – Or –

   If a WINS server is available but not a DHCP server, select **Enable WINS Resolution** and type the IP addresses of the Primary and Secondary WINS servers. These values should be provided by the network administrator, based on the IP addresses assigned to these Windows NT Server computers.

5. If WINS is enabled, in the **Scope ID** box, type the computer's scope identifier, if required on an internetwork that uses NetBIOS over TCP/IP.

   Usually this value is left blank. Scope IDs are used only for communication based on NetBIOS over TCP/IP. In such a case, all computers on a TCP/IP internetwork must have the same scope ID. A scope ID can be assigned to a group of computers if those computers communicate only with each other and not with computers outside the group. Such computers can find each other if their scope IDs are identical.

### Enabling WINS Persistent Connection Attempts

Windows 98 includes an enhancement to the WINS client (called NetBIOS over TCP/IP, or NetBT), a session-layer network service that performs name-to-IP address mapping for name resolution. (For more information, see the following section, "WINS Technical Notes.") In Windows 95, NetBT queried only one WINS server, and returned a failure for a setup session attempt if the first IP address it tried to use failed to establish a session. This caused a problem because replication delays between two or more WINS servers on the network can cause WINS servers to return stale IP addresses when queried.

You can configure Windows 98 to work around this problem by configuring NetBT to continue querying multiple WINS servers if it failed to establish the initial session. Thus, it first queries the primary WINS server for an IP address and tries to establish a connection using that IP address. If this fails, it tries to get another IP address from the next WINS server, or by using broadcast name resolution. It will continue to query WINS servers until either all of the WINS servers specified have been queried or a connection is established.

To enable WINS persistent connection attempts, set the registry entry **TryAllNameServers** (String data type) to a value of 1. **TryAllNameServers** is found in the following registry key:

**HKEY_LOCAL_MACHINE\System**
    **\CurrentControlSet\Services\Vxd\MSTCP**

## WINS Technical Notes

The WINS protocol is based on and is compatible with the protocol defined for WINS server in Requests for Comments (RFCs) 1001 and 1002, so it is interpretable with any other implementations of these RFCs.

Microsoft TCP/IP uses NetBIOS over TCP/IP as specified in RFCs 1001 and 1002, which define a software interface that supports name resolution for NetBIOS client and server programs in the WAN environment.

RFCs 1001 and 1002 define the following four node types:

- B-node, which uses broadcasts to resolve names.
- P-node, which uses point-to-point communications with a NetBIOS server to resolve names.
- M-node, which uses broadcasts first (b-node), then name queries (p-node) if broadcasts are not successful.
- H-node, which uses name queries first (p-node), and then uses broadcasts (b-node) if the name server is unavailable or if the name is not registered in the WINS database.

If WINS is enabled on a Windows 98 computer, the system uses h-node by default. Without WINS, the system uses b-node by default. Non-WINS clients can access WINS through proxies, which are WINS-enabled computers that listen to name query broadcasts and then respond for names that are not on the local subnet or are h-nodes.

▶ **To see which node type is configured on a Windows 98 computer**

1. Click **Start**, click **Run**, and then, type **winipcfg**.
2. Click the **More info** button.
3. In **Host Information**, look at the **Node type** box.

## Viewing Your WINS and DNS Configuration

Regardless of how you configure your computer to use name resolution, you can view your settings using the **winipcfg** utility. For instructions on using **winipcfg**, see "Using Diagnostic Utilities to Troubleshoot," later in this chapter.

# Technical Notes on TCP/IP

This section discusses technical information about TCP/IP. First it describes the enhancements to TCP/IP in Windows 98. Next, it lists the supported standards. Finally, it lists and briefly describes TCP/IP command-line utilities.

For information about using these utilities to troubleshoot TCP/IP problems, see "Troubleshooting TCP/IP" later in this chapter.

## Enhancements to TCP/IP in Windows 98

Microsoft TCP/IP in Windows 98 includes many enhancements over the version of Microsoft TCP/IP that was included in Windows 95. It includes performance enhancements, support for Windows Sockets 2 and multimedia applications, and greatly improved support for IP multicast. Additionally, it includes RIP listening, a feature that can improve network connectivity for multihomed computers in large corporate networks. This section describes some of the enhancements to Microsoft TCP/IP in Windows 98.

### Support for Windows Sockets 2

In Windows 98, Windows Sockets 2 is the preferred application programming interface (API) for TCP/IP socket programming.

Microsoft TCP/IP contains the following enhancements to support Windows Sockets 2:

- Support for Resource Reservation Protocol (RSVP), and Quality of Service (QoS). For more information, see the next section.

- Support for IP multicast, as described in Request for Comment (RFC) 988. This includes support for the Internet Draft for IGMP version 2 and for RFC 1256, ICMP Router Discovery. For more information, see "Support for IP Multicast" later in this section.

- Support for raw sockets, enabling application developers to write applications that directly access Windows Sockets 2. Raw sockets can be used if an application does not want to use either UDP or TCP but instead wants to encapsulate its data in an IP packet to send it.

For more information about Windows Sockets 2, see Chapter 29, "Windows 98 Network Architecture." For information about troubleshooting setup problems associated with Windows Sockets 2, see Chapter 5, "Setup Technical Discussion." For information about incompatibilities between Windows Sockets 2 and third-party networking clients, see Chapter 17, "Windows 98 on Third-Party Networks."

## Support for Quality of Service and Resource Reservation Protocol

Microsoft TCP/IP supports the Generic Quality of Service (GQoS) and Resource Reservation Protocol (RSVP) APIs.

The GQoS APIs let applications request certain characteristics for a network connection. The GQoS APIs can request attributes such as the following:

- Peak bandwidth (average or peak bit rate available).
- Latency (the maximum acceptable delay between transmission of a bit and its receipt by the receiver).
- Delay variation (the difference between a packet's minimum and maximum delay).

RSVP is a signaling protocol that is used to establish connections with the requested GQoS characteristics. It handles QoS requests, reserving network bandwidth when possible and when requested, then ensuring that the network can provide that bandwidth.

GQoS is available only if you have the most recent version of Microsoft TCP/IP (which includes Windows Sockets 2).

For more information about the RSVP and QoS architecture, see Chapter 29, "Windows 98 Network Architecture." For more information about GQoS, see also the specification on **ftp://ftp.microsoft.com/bussys/winsock/winsock2/**. For more information about RSVP, see also the Internet Engineering Task Force (IETF) RSVP specification at **http://www.ietf.org**.

For more information about installing Microsoft TCP/IP, see the section "Installing Microsoft TCP/IP" earlier in this chapter.

## Support for IP Multicast

With Windows 98, Microsoft TCP/IP supports RFC 1112 IP Multicast, or the transmission of IP packets to a group of zero or more hosts in a multicast group. Windows 98 computers can create, join, and leave multicast groups, and they can send IP packets to groups they belong to.

Microsoft TCP/IP also supports the Internet Draft for IGMP version 2. IGMP version 2 specifies a way for hosts to quickly report termination of multicast group membership. This is useful for low-bandwidth connections. For example, suppose a user is listening to a radio broadcast over a slow dial-up link and wants to change the channel to listen to a different radio station. With IGMP 2, the computer can send a message to the upstream multicast router to stop forwarding the group's packets.

## Support for ICMP Router Discovery

Microsoft TCP/IP supports Internet Control Message Protocol (ICMP) Router Discovery, described in RFC 1256. ICMP Router Discovery enables hosts attached to broadcast networks to learn IP addresses of neighboring routers.

## Performance Enhancements

With Windows 98, Microsoft TCP/IP includes several features that improve network performance. These features include the following:

- Support for TCP Large Windows and time stamps
- Support for Selective Acknowledgments
- Support for Fast Retransmission and Recovery

### Support for TCP Large Windows

Windows 98 TCP/IP supports TCP Large Windows (TCPLW) and time stamps as documented in RFC 1323. Time stamps enable computers to measure round trip times and to reject old duplicate packet segments. TCPLW and time stamps are useful for networks that have high bandwidth and high delay, such as high-speed transcontinental connections or satellite links.

Support for TCPLW and time stamps are enabled by default. By default, TCPLW will be used if an application requests a Windows Sockets 2 socket to use a buffer size greater than 64 KB or if a **DefaultRcvWindow** size of more than 64 KB is used in the registry. To change the default value, you must add the registry entry **Tcp1323Opts** to the following location:

**HKEY_LOCAL_MACHINE\System
    \CurrentControlSet\Services\VXD\MSTCP\Parameters**

The registry entry **Tcp1323Opts** is a string value type. The values for the key are:

    0 - No window scaling and time stamp options

    1 - Window scaling options but no time stamp options

    2 - Time stamp but no window scaling options

    3 - Window scaling and time stamp options

### Support for Selective Acknowledgments

Windows 98 TCP supports Selective Acknowledgments (SACK) as documented in RFC 2018. Selective Acknowledgments allows TCP to recover from IP packet loss without resending packets that were already received by the receiver. Selective Acknowledgments is most useful in combination with TCPLW and time stamps. SACK support is enabled by default. To disable SACK support, you must add the registry entry **SackOpts** to the following location:

**HKEY_LOCAL_MACHINE\System
\CurrentControlSet\Services\VXD\MSTCP\Parameters**

The registry entry **SackOpts** is a string value type. The values for the entry are:

0 - No SACK options

1 - SACK option enabled

The default value is 1 - SACK option enabled.

### Support for Fast Retransmission and Fast Recovery

Windows 98 TCP/IP supports Fast Retransmission and Fast Recovery on TCP connections that are incurring IP packet loss. These mechanisms allow a TCP sender to quickly infer a single packet loss and resend the packet after receiving duplicate acknowledgments for a previously sent and acknowledged TCP/IP packet. This mechanism is useful when the network is intermittently congested and intervening routers or switches are dropping packets.

By default, the sender must receive three duplicate acknowledgments before resending the last unacknowledged TCP/IP packets. You can change this default value by adding a registry entry to the following location:

**HKEY_LOCAL_MACHINE\System
\CurrentControlSet\Services\VXD\MSTCP\Parameters**

The registry entry **MaxDupAcks** is data type DWORD and accepts integer values from 2 to N. The value data of MaxDupAcks indicates the number of duplicate acknowledgments the sender receives before resending the last unacknowledged TCP/IP packet.

### Support for RIP Listening

In some large networks, a computer might be configured as a multihomed system and connected to two different networks. Figure 15.3 (earlier in this chapter) shows this configuration.

To communicate with both networks at the same time, the computer must be able to communicate with both routers. However, as the section "Configuring Multihoming" described, Windows 98 computers can use only one default gateway at a time.

There is a solution to this problem. If one or both of the routers uses the Routing Information Protocol (RIP) to send routing information, the computer can be configured to "listen in" to the RIP messages. Your computer can learn other routes on the network, by listening to RIP messages, and then add their IP addresses to the route table. Thus, you do not need to manually add routes to the route table. This process is called *RIP listening* or *silent RIP*. Figure 15.5 shows an example of a multihomed host that uses RIP listening.
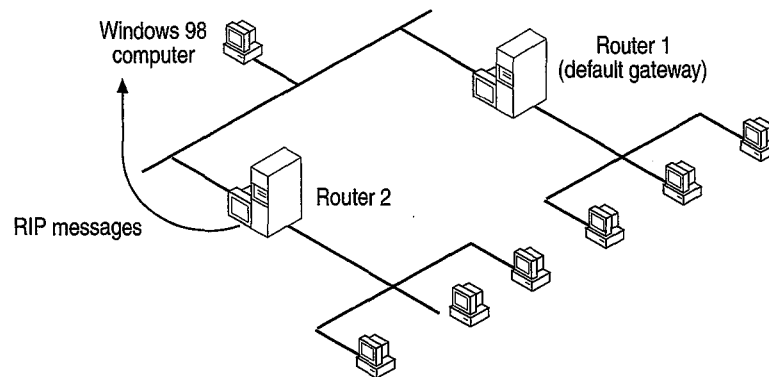
**Figure 15.5   Multihomed host using RIP listening**

Router 2 sends RIP messages, and the Windows 98 computer listens in on those messages. Router 1 does not send RIP messages, so the Windows 98 computer is configured to use Router 1 as the default gateway. Thus, the Windows 98 computer can communicate with hosts on both networks.

The following procedure describes how to enable RIP listening.

▶ **To enable RIP listening**

1. In Control Panel, double-click **Network**, and then click **Add**.

2. In **Select Network Component Type**, select **Service**, and then click **Add**.

3. Click **Have Disk**, and then type the location of the RIP listening files. They are located on the Windows 98 CD, in the \Tools\RIP directory. Select the file Irip.inf, and then click **OK**.

You must restart your computer for the changes to take effect.

## Supported Standards

TCP/IP standards are defined in Requests for Comments (RFCs) published by the Internet Engineering Task Force (IETF) and other working groups. Table 15.5 lists the RFC standards supported by Microsoft TCP/IP. To find these standards, visit **http://www.ietf.org/**.

**Table 15.5   Request for Comments standards supported**

| RFC number | RFC standard |
| --- | --- |
| 768 | User Datagram Protocol (UDP) |
| 783 | Trivial File Transfer Protocol (TFTP) |
| 791 | Internet Protocol (IP) |
| 792 | Internet Control Message Protocol (ICMP) |

**Table 15.5    Request for Comments standards supported** (*continued*)

| RFC number | RFC standard |
| --- | --- |
| 793 | Transmission Control Protocol (TCP) |
| 816 | Fault Isolation and Recovery |
| 826 | Address Resolution Protocol (ARP) |
| 854 | Telnet Protocol (TELNET) |
| 862 | Echo Protocol (ECHO) |
| 863 | Discard Protocol (DISCARD) |
| 864 | Character Generator Protocol (CHARGEN) |
| 865 | Quote of the Day Protocol (QUOTE) |
| 867 | Daytime Protocol (DAYTIME) |
| 894 | IP Over Ethernet |
| 919,922 | IP Broadcast Datagrams (broadcasting with subnets) |
| 950 | Internet Standard Subnetting Procedure |
| 959 | File Transfer Protocol (FTP) |
| 1001,1002 | NetBIOS Service Protocols |
| 1034,1035 | Domain Name System (DNS) |
| 1042 | IP over Token-Ring |
| 1055 | Transmission of IP over Serial Lines (IP-SLIP) |
| 1122,1123 | Host Requirements (communications and applications) |
| 1134 | Point-to-Point Protocol (PPP) |
| 1144 | Compressing TCP/IP Headers for Low-Speed Serial Links |
| 1157 | Simple Network Management Protocol (SNMP) |
| 1179 | Line Printer Daemon Protocol |
| 1188 | IP over Fiber Distributed Data Interface (FDDI) |
| 1191 | Path Maximum Transmission Unit (MTU) Discovery |
| 1201 | IP over ArcNet |
| 1231 | IEEE 802.5 Token-Ring MIB (MIB-II) |
| 1323 | TCP Extensions for High Performance |
| 1332 | PPP Internet Protocol Control Protocol (IPCP) |
| 1334 | PPP Authentication Protocols |
| 1518 | An Architecture for IP Address Allocation with Classless Inter-Domain Routing (CIDR) |
| 1519 | Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy |
| 1533 | Dynamic Host Configuration Protocol (DHCP) Options and Bootstrap Protocol (BOOTP) Vendor Extensions |

**Table 15.5    Request for Comments standards supported** (*continued*)

| RFC number | RFC standard |
| --- | --- |
| 1534 | Interoperation between DHCP and BOOTP |
| 1541 | Dynamic Host Configuration Protocol (DHCP) |
| 1542 | Clarifications and Extensions for the Bootstrap Protocol (BOOTP) |
| 1547 | Requirements for Point-to-Point Protocol (PPP) |
| 1548 | The Point-to-Point Protocol (PPP) |
| 1549 | PPP in High-level Data Link Control (HDLC) Framing |
| 1552 | PPP Internetwork Packet Exchange Control Protocol (IPXCP) |
| 1553 | IPX Header Compression |
| 1570 | Link Control Protocol (LCP) Extensions |
| 2018 | TCP Selective Acknowledgment Options |
| 2131 | Dynamic Host Configuration Protocol (DHCP) |
| Draft RFCs | NetBIOS Frame Control Protocol (NBFCP); PPP over ISDN; PPP over X.25; Compression Control Protocol |

## TCP/IP Utilities

The TCP/IP utilities offer network connections to non-Microsoft hosts such as UNIX system computers. You must have the TCP/IP network protocol installed to use the TCP/IP utilities. The tools listed in Table 15.6 are installed automatically when you install Microsoft TCP/IP.

**Table 15.6    Tools installed with TCP/IP**

| Command | Purpose |
| --- | --- |
| **arp** | Displays and modifies the IP-to-Ethernet address translation tables. |
| **ipconfig** | Command-line utility that displays IP address and other configuration information |
| **ftp** | Transfers files to and from a node running **ftp** service. |
| **nbtstat** | Displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP. |
| **netstat** | Displays protocol statistics and current TCP/IP connections. |
| **ping** | Verifies connections to a remote host or hosts. |
| **route** | Manually controls network routing tables. |
| **telnet** | Starts terminal emulation with a remote system running a Telnet service. Windows 98 provides a graphical version of this utility as well as the older, MS-DOS-based version. |
| **tracert** | Determines the route taken to a destination. |
| **Winipcfg** | Graphical utility that displays IP address and other configuration information |

**Important** The FTP and Telnet utilities rely on password authentication by the remote computer. Passwords are not encrypted before being sent over the network. This allows another user equipped with a network analyzer on the same network to steal a user's remote account password. For this reason, it is strongly recommended that users of these utilities choose different passwords for their workgroups, computer, or domain from the passwords used when connecting to computers that are not on Microsoft networks.

The following describes most of the TCP/IP commands included with Windows 98. For information about the syntax of those commands, use the help provided in the MS-DOS virtual machine.

For information about **winipcfg**, see "Using Diagnostic Utilities to Troubleshoot," later in this chapter.

▶ **To get help on TCP/IP utilities**

- At the command prompt, type the command name followed by a space and -?. For example, type **arp -?** to get help on the **arp** command. For some commands, you do not need to type the dash and question mark.

## Arp

This diagnostic command displays and modifies the IP-to-Ethernet or IP-to-token-ring address translation tables used by the Address Resolution Protocol (ARP).

## Ftp

This connectivity command transfers files to and from a computer running a File Transfer Protocol (FTP) service. The **ftp** command can be used interactively or by processing ASCII text files.

▶ **To use the ftp command**

- At the command prompt, type **ftp** plus any desired switches and press ENTER.

  For example, you might type **ftp -s:myfile.scr**

▶ **To get help with the ftp command**

- From within FTP, type **help** *command*, where *command* is the name of the command you need help with. For a list of commands, simply type **help**.

Table 15.7 shows the FTP commands available when Microsoft TCP/IP is installed on a computer.

**Table 15.7   FTP commands in Microsoft TCP/IP**

| Command | Purpose |
|---|---|
| ! | Runs the specified command on the local computer. |
| ? | Displays descriptions for **ftp** commands. Identical to **help**. |
| append | Appends a local file to a file on the remote computer, using the current file type setting. |
| ascii | Sets the file transfer type to ASCII, the default. |
| bell | Toggles a bell to ring after each file transfer command is completed. By default, the bell is off. |
| binary | Sets the file transfer type to binary. |
| bye | Ends the FTP session with the remote computer and exits **ftp**. |
| cd | Changes the working directory on the remote computer. |
| close | Ends the FTP session with the remote server and returns to the command interpreter. |
| debug | Toggles debugging. When debugging is on, each command sent to the remote computer is printed, preceded by the string --->. By default, debugging is off. |
| delete | Deletes files on remote computers. |
| dir | Displays a list of a remote directory's files and subdirectories. |
| disconnect | Disconnects from the remote computer, retaining the **ftp** prompt. |
| get | Copies a remote file to the local computer, using the current file transfer type. Identical to **recv**. |
| glob | Toggles file name globbing. Globbing permits use of wildcard characters in local file or path names. By default, globbing is on. |
| hash | Toggles hash-mark (#) printing for each 2048 bytes data block transferred. By default, hash-mark printing is off. |
| help | Displays descriptions for FTP commands. |
| lcd | Changes the working directory on the local computer. By default, the current directory on the local computer is used. |
| literal | Sends arguments, verbatim, to the remote FTP server. A single FTP reply code is expected in return. Identical to **quote**. |
| ls | Displays an abbreviated list of a remote directory's files and subdirectories. |
| mdelete | Deletes multiple files on remote computers. |
| mdir | Displays a list of a remote directory's files and subdirectories. Allows you to specify multiple files. |
| mget | Copies multiple remote files to the local computer using the current file transfer type. |

**Table 15.7    FTP commands in Microsoft TCP/IP** (*continued*)

| Command | Purpose |
|---------|---------|
| **mkdir** | Creates a remote directory. |
| **mls** | Displays an abbreviated list of a remote directory's files and subdirectories. |
| **mput** | Copies multiple local files to the remote computer, using the current file transfer type. |
| **open** | Connects to the specified FTP server. |
| **prompt** | Toggles prompting. During multiple file transfers, **ftp** provides prompts to allow you to selectively retrieve or store files; **mget** and **mput** transfer all files if prompting is turned off. By default, prompting is on. |
| **put** | Copies a local file to the remote computer, using the current file transfer type. Identical to **send**. |
| **pwd** | Prints the current directory on the remote computer. |
| **quit** | Ends the FTP session with the remote computer and exits **ftp**. |
| **quote** | Sends arguments, verbatim, to the remote FTP server. A single FTP reply code is expected in return. Identical to **literal**. |
| **recv** | Copies a remote file to the local computer, using the current file transfer type. Identical to **get**. |
| **remotehelp** | Displays help for remote commands. |
| **rename** | Renames remote files. |
| **rmdir** | Deletes a remote directory. |
| **send** | Copies a local file to the remote computer, using the current file transfer type. Identical to **put**. |
| **status** | Displays the current status of FTP connections and toggles. |
| **trace** | Toggles packet tracing; displays the route of each packet when running an FTP command. |
| **type** | Sets or displays the file transfer type. |
| **user** | Specifies a user to the remote computer. |
| **verbose** | Toggles verbose mode. If on, all FTP responses are displayed; when a file transfer completes, statistics regarding the efficiency of the transfer are also displayed. By default, verbose is on. |

## Nbtstat

This diagnostic command displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.

### Notes on Nbtstat

The column headings generated by the **nbtstat** utility have the following meanings.

Input
> Number of bytes received.

Output
> Number of bytes sent.

In/Out
> Whether the connection is from the computer (outbound) or from another system to the local computer (inbound).

Life
> The remaining time that a name table cache entry will live before it is purged.

Local Name
> The local NetBIOS name associated with the connection.

Remote Host
> The name or IP address associated with the remote host.

Type
> This refers to the type of name. A name can either be a unique name or a group name.

*<03>*
> Each NetBIOS name is 16 characters long. The last byte often has special significance, because the same name can be present several times on a computer. This notation is the last byte converted to hexadecimal. For example, <20> is a space in ASCII.

State
> The state of NetBIOS connections as shown in Table 15.8

**Table 15.8   NetBIOS connection states**

| State | Meaning |
| --- | --- |
| Accepting | An inbound session is currently being accepted and will be connected shortly. |
| Associated | A connection endpoint has been created and associated with an IP address. |
| Connected | The session has been established. |
| Connecting | The session is in the connecting phase where the name-to-IP address mapping of the destination is being resolved. |
| Disconnected | The local computer has issued a disconnect, and it is waiting for confirmation from the remote computer. |
| Disconnecting | A session is in the process of disconnecting. |
| Idle | This endpoint has been opened but cannot receive connections. |

**Table 15.8    NetBIOS connection states** (*continued*)

| State | Meaning |
| --- | --- |
| Inbound | An inbound session is in the connecting phase. |
| Listening | This endpoint is available for an inbound connection. |
| Outbound | A session is in the connecting phase where the TCP connection is currently being created. |
| Reconnecting | A session is trying to reconnect if it failed to connect on the first attempt. |

## Netstat

This diagnostic command displays protocol statistics and current TCP/IP network connections.

### Notes on Netstat

The **netstat** utility provides statistics on network components. Table 15.9 outlines these statistics.

**Table 15.9    Netstat statistics**

| Statistic | Purpose |
| --- | --- |
| Foreign Address | The IP address and port number of the remote computer to which the socket is connected. The name corresponding to the IP address is shown instead of the number if the Hosts file contains an entry for the IP address. In cases where the port is not yet established, the port number is shown as an asterisk (*). |
| Local Address | The IP address of the local computer, and the port number the connection is using. The name corresponding to the IP address is shown instead of the number if the Hosts file contains an entry for the IP address. In cases where the port is not yet established, the port number is shown as an asterisk (*). |
| Proto | The name of the protocol used by the connection. |
| (state) | Indicates the state of TCP connections only. The possible states are the following: |

close_wait      fin_wait_1      syn_received
closed           fin_wait_2      syn_send
established     listen           timed_waitlast_ack

## Ping

This diagnostic command verifies connections to one or more remote hosts.

### Notes on Ping

The **ping** command verifies connections to a remote host or hosts, by sending Internet Control Message Protocol (ICMP) echo packets to the host and listening for echo reply packets. The **ping** command waits for up to 1 second for each packet sent and prints the number of packets transmitted and received. Each received packet is validated against the transmitted message. By default, 4 echo packets containing 64 bytes of data (a periodic uppercase sequence of alphabetic characters) are transmitted.

You can use the **ping** utility to test both the host name and the IP address of the host. If the IP address is verified but the host name is not, you may have a name resolution problem. In this case, be sure that the host name you are querying is in either the local Hosts file or in the DNS database.

## Route

This diagnostic command manipulates network routing tables.

## Telnet

This connectivity command starts terminal emulation with a remote system running a Telnet service. Telnet provides Digital Equipment Corporation (DEC) VT 100, DEC VT 52, or TTY emulation, using connection-based services of TCP.

To provide terminal emulation from a Windows 95 computer, the foreign host must be configured with the TCP/IP program, the Telnet server program or daemon, and a user account for the computer running Windows 95.

The Telnet application is found in the Accessories program group if you install the TCP/IP connectivity utilities. Telnet is a Windows Sockets–based application that simplifies TCP/IP terminal emulation with Windows 98. HyperTerminal can also be used as a Telnet client.

---

**Note**  Microsoft does not provide the Telnet server daemon (**telnetd**).

---

### Tracert

This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying Time-To-Live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router is supposed to send back an ICMP Time Exceeded message to the source system. The **tracert** command determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Notice that some routers silently drop packets with expired TTLs and are invisible to **tracert**.

#### Notes on Tracert

When you type **tracert** *destination*, where *destination* is the host you wish to reach, four columns are displayed. The first column is the hop number, which is the TTL value set in the packet. Each of the next three columns contains the round-trip times in milliseconds for an attempt to reach the destination with that TTL value. An asterisk (*) means that the attempt timed out. The fourth column is the host name (if it was resolved) and IP address of the responding system.

# IPX/SPX-compatible Protocol

The Microsoft Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)–compatible protocol (nwlink.vxd) supports the 32-bit Windows Sockets 1.1 programming interface, so that any Win32-based Windows Sockets 1.1 application can run on IPX/SPX with Windows 98. (There are no 16-bit Windows Sockets applications using IPX/SPX.)

The IPX/SPX-compatible protocol can be used by Client for NetWare Networks to communicate with NetWare servers or computers running File and Printer Sharing for NetWare Networks.

This protocol can also be used by Client for Microsoft Networks to communicate with computers running Windows for Workgroups 3.11 or Windows NT that are also running IPX/SPX.

The IPX/SPX-compatible protocol uses the nwnblink.vxd module to support computers that use NetBIOS over IPX and to support the NetBIOS programming interface. This protocol can also use NetWare servers configured as routers (and other IPX routers) to transfer packets across LANs.

# Configuring the IPX/SPX-compatible Protocol

The Microsoft IPX/SPX–compatible protocol is installed automatically when Client for NetWare Networks is installed. You can also install this protocol to support other network clients, including Client for Microsoft Networks.

▶ **To install the IPX/SPX-compatible protocol**

1. In Control Panel, double-click Network, and then click **Add**.

2. In the **Select Network Component Type** dialog box, click **Protocol** and then click the **Add** button.

3. In **Manufacturers**, click **Microsoft**, and then in **Network Protocols**, click **IPX/SPX-compatible Protocol**, and then click **OK**.

4. Click **OK**. Setup copies the files you need.

When you install the IPX/SPX-compatible protocol, Windows 98 automatically detects and sets appropriate values for the frame type, network address, and other settings. However, in some cases you might need to configure settings for this protocol manually.

▶ **To configure the IPX/SPX-compatible protocol**

1. In Control Panel, double-click Network.

2. Double-click the instance of **IPX/SPX-compatible Protocol** that is bound to your network adapter.

> **Note**  If the computer has multiple network adapters, the list will contain an instance of the IPX/SPX-compatible protocol for each network adapter. You must configure each adapter with its own settings. You can only have four instances of IPX/SPX on your system, so if you have more than four adapters are installed, you should bind IPX/SPX only to the adapters that will use this protocol.

3. Click the **Advanced** tab.

4. Most values have correct defaults in typical installations. If you need to change a value for a particular purpose, select the item in the **Property** list and specify a setting in the **Value** list based on the information in the Table 15.10.

**Table 15.10    IPX/SPX configuration values**

| Property | Value |
|---|---|
| Force even-length IPX packets | Enabled only for Ethernet 802.3 on monolithic implementations that cannot handle odd-length packets. |
| Frame type[1] | Specifies the frame type based on detection. This value is used for network adapters that support multiple frame types. The possible values are:<br><br>■ Auto-detect (recommended)<br>■ Ethernet 802.2 (default for NetWare 3.12 and later)<br>■ Ethernet 802.3<br>■ Ethernet II<br>■ Token-ring<br>■ Token-ring Subnetwork Access Protocol (SNAP) |
| Maximum connections | Specifies the maximum number of connections that IPX will allow. Configured dynamically. |
| Maximum sockets | Specifies the maximum number of IPX sockets that IPX assigns. Configured dynamically. |
| Network address | Specifies the IPX network address as a four-byte value. Configured dynamically. |
| Source routing[2] | Specifies the cache size to use with source routing. This parameter is used only on token-ring networks, where it is used to turn on source routing.<br><br>**Important** Cache size is specified by entry count, not byte count. The recommended value of 16 entries is the most efficient and best setting for most installations. |

[1] Each time the computer starts, Windows 98 detects the frame type by sending a general RIP request in each frame format. Based on the responses received from routers, Windows 98 determines the most prevalent frame type used and sets that as the default frame type.

[2] Source routing is a method of routing data across bridges. For NetWare networks, this means forwarding NetWare frames across an IBM token-ring bridge. With NDIS protocols, source routing is done by the protocol. With ODI-based protocols, source routing is configured with the network adapter driver or using the NetWare route.com utility.

You should not need to change bindings in most circumstances. However, you can disable the bindings for a protocol if you do not want other computers using that protocol to see this computer. At least one protocol, however, must be bound to the network client for the computer to communicate with the network.

▶ **To change bindings for the IPX/SPX-compatible protocol**

1. In Control Panel, double-click Network.

2. Double-click the instance of **IPX/SPX-compatible Protocol** that is bound to your network adapter.

**Note**  If the computer has multiple network adapters, the list will contain an instance of the IPX/SPX-compatible protocol for each network adapter. You must configure each adapter with its own settings. You can only have four instances of IPX/SPX on your system, so if you have more than four adapters are installed, you should bind IPX/SPX only to the adapters that will use this protocol.

3. Click the **Bindings** tab.

4. Click any network component to change its bindings.

   If the option is checked, it is bound to the protocol. If it is not checked, that network component is not using the IPX/SPX-compatible protocol. For more information, see "Configuring Network Adapters" earlier in this chapter.

**Note**  Microsoft Client for NetWare Networks is always bound only to the IPX/SPX-compatible protocol. This network client cannot use another protocol.

## Using NetBIOS over IPX

NetBIOS is an interface used by network applications to communicate with other NetBIOS-compliant applications. The NetBIOS interface is responsible for the following:

- Establishing logical names on the network.

- Establishing connections (called sessions) between two computers by use of their logical names on the network.

- Transmitting data between networked computers.

Windows 98 provides a 32-bit, protected-mode driver to support NetBIOS services over IPX (Vnetbios.386). This implementation is compatible with the Novell NetBIOS support driver. Performance enhancements include acknowledgment of previous frames in response frames (called PiggyBackAck), plus a "sliding window" acknowledgment mechanism.

These NetBIOS enhancements are used only when the computer is communicating with other computers using IPX over NetBIOS, such as other computers running Windows 98, Windows NT, or NetWare when running Lotus Notes or other NetBIOS applications. NetBIOS over IPX is not necessary for computers running Windows 98 to be able to communicate with each other. The redirector and server networking components in Windows 98 communicate with the IPX protocol directly without NetBIOS.

Novell provides a terminate-and-stay resident (TSR) NetBIOS driver named Netbios.exe, which is a Level 1 NetBIOS provider that consumes about 40K of conventional memory. This driver acknowledges each frame received, thus increasing the amount of traffic generated when NetBIOS is used. With the Microsoft implementation of NetBIOS over IPX, you can remove the real-mode Netbios.exe TSR.

---

**Note** A Windows 98 computer that uses IPX without NetBIOS can connect to a Windows NT 3.5 or later server that uses IPX without NetBIOS. However, the Windows NT 3.5 or later computer service can only connect to a Windows 98 computer running File and Printer Sharing for Microsoft Networks when the Windows 98 computer is using NetBIOS over IPX.

---

▶ **To use the IPX/SPX-compatible protocol with NetBIOS on a computer**

1. In Control Panel, double-click Network.
2. Double-click the instance of **IPX/SPX-compatible Protocol** that is bound to your network adapter.

---

**Note** If the computer has multiple network adapters, the list will contain an instance of the IPX/SPX-compatible protocol for each network adapter. You must configure each adapter with its own settings. You can only have four instances of IPX/SPX on your system, so if you have more than four adapters are installed, you should bind IPX/SPX only to the adapters that will use this protocol.

---

3. Click the **Bindings** tab.
4. Click the **NetBIOS** tab, and then click **I want to enable NetBIOS Over IPX/SPX**.

## Technical Notes on IPX/SPX on NetWare Networks

- There is no need to enable source routing on token-ring networks if the communication is on the same ring, even if one computer has it enabled.
- SPX-II is a protocol definition for windowing and transmitting large packets over SPX. The IPX/SPX-compatible protocol included with Windows 98 (Nwlink.vxd) does not support SPX-II. Some third-party dynamic-link libraries (DLLs) provide SPX-II support when you are using Nwlink.vxd. However, if you are using a third-party DLL that provides SPX-II support and a program communicates directly with Nwlink.vxd, SPX-II support will not be available for that program.

- When you install Windows 98 with the IPX/SPX-compatible protocol, parameters in Net.cfg and Shell.cfg will be moved to the registry if they are not already there. (If you are upgrading over an installation of Windows 95 that included the IPX/SPX-compatible protocol, those parameters will already have been moved to the registry.)

- To determine the network address in IPX packets, Windows 98 checks the wire for RIP packets and chooses the most likely address. The network address is dynamic and changes when a new network address becomes more prevalent.

- All transport layer interface (TLI) libraries can run on the IPX/SPX-compatible protocol in Windows 98. TLI is similar to TDI in Microsoft networking as a layer between the protocol and network adapter driver; this implementation is similar to STREAMS and provides a STREAMS environment for NetWare, but Windows 98 uses Windows Sockets instead.

# Microsoft NetBEUI Protocol

Windows 98 provides the NetBIOS extended user interface (NetBEUI) protocol for compatibility with existing networks that use NetBEUI. Because NetBEUI is nonroutable and was designed for smaller LANs, you should use the TCP/IP or IPX/SPX-compatible protocol for enterprise-wide networks that require a routable protocol.

NetBEUI in Windows 98 provides two types of traffic:

1. Unreliable connectionless traffic, in which the sender sends packets to the receiver without setting up a connection and with no guarantee that the packets will arrive. NetBEUI connectionless traffic are used for name resolution, datagrams, and miscellaneous traffic.

2. Reliable connection-oriented traffic, in which the sender and receiver establish a reliable connection before sending data. NetBEUI connection oriented traffic is used for commands such as **net use**, **net view**, and **net start**.

NetBEUI in Windows 98 supports a NetBIOS programming interface that conforms to the IBM NetBEUI specifications and includes several performance enhancements. The NetBEUI module, Netbeui.vxd, is accessible through the NetBIOS interface.

If Windows 98 Setup detects NetBEUI during installation, it installs support for Microsoft NetBEUI automatically. If you are upgrading from a computer that did not have NetBEUI, Windows 98 does not automatically install it; however, you can add it at any time.

▶ **To install NetBEUI**

1. In Control Panel, double-click Network.

2. On the **Configuration** tab, click **Add**.

3. In the **Select Network Component Type** dialog box, click **Protocol**, and then click the **Add** button.

4. In **Manufacturers**, click **Microsoft**, and then in **Network Protocols**, click **NetBEUI**, and then click **OK**.

5. Click **OK**. Setup copies files from your original installation media and prompts you to restart your computer.

The **Advanced** properties for NetBEUI affect only real-mode NetBEUI. These values are set dynamically for protected-mode NetBEUI.

▶ **To configure real-mode NetBEUI manually**

1. In Control Panel, double-click Network.

2. On the **Configuration** tab, double-click the instance of **NetBEUI** that is bound to your network adapter.

---

**Note** If your computer has multiple network adapters, an instance of NetBEUI appears for each network adapter. You must configure each adapter with its own settings.

---

The **Bindings** tab shows which clients and services are currently using the NetBEUI protocol. For information about configuring bindings, see "Configuring Network Adapters" later in this chapter.

3. Click the **Advanced** tab to modify settings for **Maximum Sessions** and **NCBs** for the real-mode NetBEUI. The following list outlines the options in NetBEUI advanced configuration.

| Option | Description |
|---|---|
| Maximum Sessions | Used to identify the maximum number of connections to remote computers that can be supported from the redirector. This is equivalent to the **sessions=** parameter formerly specified in Protocol.ini. |
| NCBs (network control blocks) | Used to identify the maximum number of NetBIOS commands that can be used. This is equivalent to the **ncbs=** parameter formerly specified in Protocol.ini. |

4. Click **OK**. Then shut down and restart the computer.

# Microsoft DLC Protocol

Windows 98 includes both a protected-mode DLC driver (Dlc.vxd), which supports 32-bit and 16-bit DLC applications, and a real-mode DLC driver (Msdlc.exe), which supports only 16-bit applications. Microsoft DLC is used primarily to access IBM mainframe computers and Hewlett-Packard network-ready printers. Microsoft recommends that you use the protected-mode driver in most cases. However, some 16-bit DLC applications will work only with the real-mode DLC driver. For more information about applications that require the 16-bit DLC, see "Using 32-bit DLC for Connectivity" later in this chapter.

The following sections how to use 32-bit, protected-mode DLC protocol and the 16-bit, real-mode DLC protocol.

## Using 32-bit DLC for Connectivity

The 32-bit DLC protocol provides connection and communication with mainframe computers using DLC. With the 32-bit Data Link Control (DLC) protocol, you can establish multiple connections to different IBM host and AS/400 computers over the same network token-ring, FDDI, or Ethernet adapter. Host terminal emulation programs use the 32-bit DLC to communicate directly with host computers. The 32-bit DLC protocol also allows multiple 32-bit applications to use the same network adapter at the same time to connect to different host computers.

You can also use the 32-bit DLC protocol to provide connectivity to local area printers connected directly to the network. For example, you can use the DLC protocol to print to a printer that uses an adapter to connect directly to the network rather than to a port on a print server. The DLC protocol must be installed and running on the print server for the printer. The protocol does not need to be installed on the computers that send print jobs to the print server. To take advantage of the DLC protocol device driver, you must create a network printer in the printers folder by using a third-party utility such as Hewlett Packard's Jet Administration Utility.

The 32-bit DLC protocol software supports the following 32-bit and 16-bit DLC programs:

- Windows-based 32-bit programs that use Command Control Block 2 (CCB2).
- 16-bit programs that use Command Control Block 1 (CCB1).

Microsoft recommends that in most cases you use the 32-bit DLC protocol rather than the 16-bit DLC protocol or IBM's LAN Support drivers, because it supports both 32-bit applications and most 16-bit applications, provides better performance, and can access protected memory.

However, the 32-bit DLC protocol does not support certain 16-bit DLC applications. Some 16-bit DLC applications load TSRs to check the existence of DLC before Windows 98 loads. If you need to run any of those applications, you may want to use the 16-bit DLC protocol. For more information about the 16-bit programs the 32-bit DLC protocol does not support, see "Running 16-bit Applications" later in this chapter. The 32-bit DLC protocol also does not support 32-bit programs created to run under OS/2.

Client for Microsoft Networks does not use the 32-bit DLC protocol to communicate with the Microsoft network. Also, the 32-bit DLC protocol does not have a NetBIOS interface. 32-bit terminal emulation programs usually call the protected-mode DLC protocol by loading a TSR that acts as an interface to the DLC protocol. A 16-bit terminal emulation program can call the 32-bit DLC protocol by using the Int 0x5C (NetBIOS) interrupt vector. The 32-bit DLC protocol can coexist with other protocols, and it conforms to the network driver interface specification (NDIS) 3.1 and later.

Windows 98 supports the Ethernet multivendor standard DIX 2.

The following sections describe how to install the Microsoft 32-bit DLC protocol and how to configure it with Novell NetWare ODI drivers and IBM LAN Support.

For information about the architecture of Microsoft DLC, see Chapter 29, "Windows 98 Network Architecture."

## Installing the 32-bit DLC Protocol

Before you install the 32-bit DLC protocol, you must perform the following tasks:

- Make sure you have access to your original Windows 98 setup files.

- If you are installing the 32-bit DLC protocol over the IBM LAN Support program (DXM mode drivers), first remove the existing IBM DLC from the Network option in Control Panel.

- If you are installing the 32-bit DLC protocol over an existing Madge Smart.exe (token-ring), you must first remove the existing ODI driver from the Network option in Control Panel. Then you must add the NDIS 3.1 or later Madge driver and the Microsoft 32-bit DLC protocol stack.

▶ **To install the 32-bit DLC protocol**

1. In Control Panel, double-click Network.

2. On the **Configuration** tab, click **Add**.

3. Click **Protocol**, and then click **Add**.

4. In the **Manufacturers** box, click **Microsoft.**

5. In the **Network Protocols** box, click **Microsoft 32-bit DLC.**

6. Click **OK**.

7. Setup prompts you to shut down and reboot your computer.

Windows 98 Setup removes any previous configuration settings for 16-bit Microsoft DLC, and adds an entry in the Autoexec.bat file for Dlchlp.exe, the file that supports 16-bit DLC programs. If no 16-bit DLC programs are used, you can save real-mode and 32-bit DLC protected-mode memory by disabling 16-bit support. For more information about disabling 16-bit support, see "Disabling 16-bit Support" later in this chapter.

Windows 98 setup also associates a unique CCB adapter number to the adapter that is bound to the DLC protocol.

For information about changing the CCB adapter number, see "Configuring the 32-bit DLC Protocol" later in this chapter.

For information about using multiple CCB adapter numbers, see "Adding a Second Network Adapter" later in this chapter. After you have installed the 32-bit DLC protocol, you can verify that the protocol is bound to the adapter by using the following procedure.

▶ **To verify bindings**

1. In Control Panel, double-click Network, and then click the name of your adapter.

2. Click **Properties.**

3. Click the **Bindings** tab.

4. Make sure **Microsoft 32-bit DLC** is selected.

---

**Note**  You cannot check the bindings by clicking the 32-bit DLC protocol, because only clients and services can be bound to protocols.

---

# Configuring the 32-bit DLC Protocol

After you have installed the 32-bit DLC protocol, you can configure adapter settings and settings for the 32-bit DLC protocol.

For information about configuring adapter settings, see Chapter 15, "Network Adapters and Protocols."

This section covers the following topics:

- Configuring settings for the 32-bit DLC protocol.
- Configuring Service Access Points (SAPs) and link stations.
- Configuring timer values.
- Adding a second network adapter.
- Disabling 16-bit support.

## Configuring Settings

This section describes the 32-bit DLC settings you can manually configure.

---

**Note** In most cases, you do not need to change the default values. However, if you are loading multiple terminal emulation sessions, you might want to increase values for SAPs and link stations.

---

▶ **To configure 32-bit DLC settings**

1. In Control Panel, double-click Network.
2. Click the **Microsoft 32-bit DLC** protocol.
3. Click **Properties**.
4. Click the **Advanced** tab.

Table 15.11 shows the default settings you can change. Applications can also change these settings.

**Table 15.11   DLC configuration settings**

| 32-bit DLC parameter | Description | Range | Default |
|---|---|---|---|
| CCB Adapter Num (equivalent to LANA-number in NCB) | Specifies a unique number used by 32-bit DLC to identify each instance of a driver that is associated with a network card. [1] | 1-15 | 0 |
| Ethernet DIX | Sets the frame format. For 802.3 Ethernet format, set the value to 0. For Ethernet DIX 2.0 (Ethertype 0x80D5) format, set the value to 1 (enable). (Ethernet DIX frames have an extra type field.) | 0- 1 (Boolean) | 0 |

**Table 15.11   DLC configuration settings** (*continued*)

| 32-bit DLC parameter | Description | Range | Default |
|---|---|---|---|
| Max Grp Member | Specifies the maximum number of SAPs that can belong to each Group SAP. | 1- 127 | 0 |
| Max Grp SAPs | Specifies the maximum number of Group SAPs that can be opened simultaneously. | 1- 126 | 0 |
| Max Links | Indicates the number of link stations that can be opened simultaneously. [2] | 1- 255 | 20 |
| Max SAPs | Indicates a service access point. [3] | 1- 255 | 3 |
| Maximum Adapters | Indicates the maximum number of network adapter cards you can have in your computer. | 1- 16 | 4 |
| Maximum Frame Size | Indicates the maximum size of a frame that can be sent across the network. The maximum value of this setting depends on the network type. [4] | 96-17960 bytes | 4464 |
| Maximum Users | Indicates the maximum number of logical adapters that can be open at the same time. Typically, each 32-bit program opens a logical adapter of its own. | 1-40 | 5 |
| NDIS Pkt Descriptors | Specifies the number of packets that the adapter driver can store in its packet buffer before sending them to the network. | 24-128 | 24 |
| Support CCB1 | If this setting is set to 1, 16-bit programs that use CCB1 are supported. If it is set to 0, only 32-bit DLC programs are supported. [5] | 0-1 (Boolean) | 1 |
| Swap Addr Bits | When DLC is bound to an Ethernet or token-ring driver, set this parameter to 1 (enable) to turn on address bit-swapping. | 0- 1 (Boolean) | 1 |
| Timer T1 (1) | Sets the retransmission-timer "short tick" value. This timer determines the delay (in units of 40 milliseconds) before retransmitting a link-level frame if no acknowledgment is received. [6] | 1- 255 | 5 |
| Timer T1 (2) | Sets the retransmission-timer "long tick" value. This timer determines the delay (in units of 40 milliseconds) before retransmitting a link-level frame if no acknowledgment is received. | 1- 255 | 25 |
| Timer T2 (1) | Sets the delayed-acknowledgment timer "short tick" value. This timer determines the delay (in units of 40 milliseconds) before acknowledging a received frame when the receive window has not been reached. | 1- 255 | 1 |
| Timer T2 (2) | Sets the delayed-acknowledgment timer "long tick" value. This timer determines the delay (in units of 40 milliseconds) before acknowledging a received frame when the receive window has not been reached. | 1- 255 | 10 |

**Table 15.11   DLC configuration settings** (*continued*)

| 32-bit DLC parameter | Description | Range | Default |
|---|---|---|---|
| Timer Ti (1) | Sets the inactivity-timer "short tick" value (in units of 40 milliseconds). This timer determines how often DLC checks an inactive link to see whether it is still operational. | 1- 255 | 25 |
| Timer Ti (2) | Sets the inactivity-timer "long tick" value (in units of 40 milliseconds). This timer determines how often DLC checks an inactive link to see whether it is still operational. | 1- 255 | 125 |
| Trace Mask | Indicates the default mask setting used by the Trcdlc.exe command-line utility. [7] | – | – |

[1] For more information about setting the CCB number for an alternate or secondary network card, see "Adding a Second Network Adapter" later in this chapter.

[2] For more information about link stations, see "Determining Links and SAPs Settings" later in this chapter.

[3] For a description of SAPs, see the *IBM Local Area Network Technical Reference*. For more information about SAPs, see "Determining Links and SAPs Settings" later in this chapter.

[4] For example, token ring networks can support frame sizes of up to 4 kilobits per second (Kbps), whereas Ethernet networks can support frame sizes of less than 2 Kbps. For more information about the maximum frame size, see your network documentation.

[5] For more information about CCB1, see "Disabling 16-bit Support" later in this chapter.

[6] For more information about timer settings, see "Configuring Timer Settings" later in this chapter.

[7] For more information about Trdlc.exe, see "Installing the 32-bit DLC Protocol" earlier in this chapter.

## Choosing 16-bit DLC Protocol Settings

Table 15.12 shows 16-bit DLC protocol settings that are still available with the 32-bit DLC protocol. Note that the names have changed.

**Table 15.12   Available 16-bit DLC protocol settings**

| 16-bit DLC | 32-bit DLC |
|---|---|
| Swap | Swap Addr Bits |
| UseDIX | Ethernet DIX |
| SAPs | Max SAPs |
| Stations | Max Links |

## Determining Links and SAPs Settings

Each program requires a certain number of Service Access Points (SAPs) and link stations. Because each SAP or link station takes up memory, you should provide just enough for your program to run.

If you do not know the number of SAPs and link stations your program requires, and you want to minimize the memory your terminal emulation programs use, start with large values and gradually reduce them until the program no longer works.

The Microsoft 32-bit DLC protocol uses defaults of 5 SAPs and 20 link stations. This should be sufficient for most programs. If needed, you can increase the number of SAPs and link stations. For more information about configuring 32-bit DLC settings, see "Configuring Settings" earlier in this chapter.

For information about which SAP and link station settings to use with your DLC programs, see the documentation for those programs.

### Configuring Timer Settings

The Microsoft DLC protocol uses three timers:

- t1 (retransmission)
- t2 (acknowledgment)
- ti (inactivity)

Each timer has a "short tick" rate and a "long tick" rate that individual commands use to determine timer values. A command such as Dlc.Open.Sap specifies a timer value with a number range of 1 through 10 units of milliseconds.

For example:

- When the number is in the range of 1 through 5 units of milliseconds, the actual timer value is:

  ```
  (number selected) * (short-tick value) * 40 milliseconds
  ```

- When the number is in the range of 6 through 10 units of milliseconds, the actual timer value is:

  ```
  (number selected  - 5) * (long-tick value) * 40 milliseconds
  ```

Some network programs adjust these timer entries automatically. The Dlc.Open.Adapter command overrides the default value.

### Adding a Second Network Adapter

If you add a second DLC32-compatible network adapter to your computer, a new copy of the 32-bit DLC protocol is created and automatically bound to your secondary network adapter. When you restart your computer, the CCB adapter number setting for that copy of the 32-bit DLC protocol automatically changes to a unique number.

---

**Note**  If you remove your primary network adapter, the CCB adapter number for the second adapter does not change.

---

### Disabling 16-bit Support

If your users will use only 32-bit network programs, you can disable support for 16-bit programs. This speeds up network access and saves real-mode and protected-mode memory.

▶  **To disable 16-bit support**

1. In Control Panel, double-click Network, and then click the Microsoft 32-bit DLC protocol for which you wish to disable 16-bit support.

2. Click **Properties**.

3. Click the **Advanced** tab.

4. Click the **Support CCB1** setting, and set it to 0. The reference in your Autoexec.bat file to Dlchlp.exe is removed.

**Caution**  Do not manually remove Dlchlp.exe from your Autoexec.bat file.

## Switching from IBM LAN Support

The 32-bit DLC protocol cannot be upgraded over IBM LAN Support. If you are adding the 32-bit DLC protocol to a computer that used IBM LAN Support, you must first remove the IBM DLC protocol from the Network option in Control Panel, then add the Microsoft 32-bit DLC protocol. Otherwise, you may not be able to connect to your host, and the Windows 98 computer could stop responding.

**Note**  Before upgrading over IBM LAN Support, record the parameters for the DXM driver line(s) so that you can configure the equivalent Microsoft 32-bit DLC protocol settings. If you are using an NDIS configuration with IBM LAN Support, you should also record the parameters for your Protocol.ini file.

Windows 98 Setup does not migrate the IBM LAN Support program settings will to the Microsoft 32-bit DLC protocol. You will need to make sure that the settings for the Microsoft 32-bit DLC properties correlate to the prior settings for IBM LAN Support. Table 15.13 shows how to convert the Xmit_swap setting in Dxme0mod.sys to the Swap Addr Bits and Ethernet DIX settings for the 32-bit DLC protocol.

**Table 15.13   IBM LAN Support program settings**

| Xmit_swap setting in Dxme0mod.sys | Swap Addr Bits setting | Ethernet DIX setting |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 1 | 1 |
| 2 | 0 | 0 |
| 3 | 0 | 1 |

**Note**   You can configure the alternate adapter by using the **CCB Adapter Num** setting. For more information about the **CCB Adapter Num** setting, see "Adding a Second Network Adapter" earlier in this chapter.

## Running 16-bit Applications

If you are running 32-bit Microsoft DLC with 16-bit applications that use DLC, you will need to update your Autoexec.bat file. Make sure that Net.exe is loaded before Dlchlp.exe.

Applications that require a terminate-and-stay-resident (TSR) program to connect to a host computer before starting Windows 98 will not work with the Microsoft 32-bit DLC protocol stack. The following applications require TSRs:

- IBM PC SUPPORT (versions V2R1 - V2R3)
- RELAY GOLD version 5.0 and 6.0a
- EICON ACCESS 5250 version 3.21

Contact your vendor for updated information about these applications.

## Technical Notes for the 32-bit DLC Protocol

Table 15.14 describes the files included with the 32-bit DLC protocol.

**Table 15.14   32-bit DLC files**

| File name | Description |
|---|---|
| Netdlc32.inf | The Windows 98 device information file, which provides settings used by Windows 98 setup to install DLC. |
| Dlc.vxd | The Windows 98 device driver for DLC. |
| Dlcapi.dll | The DLL file that supports 32-bit DLC programs. |
| Dlcndi.dll | A DLL file used by Windows 98 setup for custom installations. |

**Table 15.14   32-bit DLC files** (*continued*)

| File name | Description |
| --- | --- |
| Trcdlc.exe | A command-line trace utility for viewing DLC commands that are running 32-bit calls. This utility helps developers troubleshoot 32-bit DLC programs. |
| Dlchlp.exe | A TSR that allows 32-bit DLC to also support 16-bit DLC programs. This file is loaded in the Autoexec.bat file, but is not required if you do not need support for 16-bit DLC programs. |

**Note**  If you do not need support for 16-bit DLC programs, do not remove Dlchlp.exe from your Autoexec.bat file manually. Instead, disable support for 16-bit DLC programs by using the Support CCB1 setting.

# Using 16-bit DLC for Connectivity

The 16-bit DLC protocol provides connection and communication with mainframe computers using DLC. To provide connection and communication, the DLC protocol must be installed on the client computer that is running Windows 98. The Microsoft DLC protocol works with either token-ring or Ethernet network adapter drivers.

Microsoft DLC is also used to provide connectivity to local area printers connected directly to the network. For example, DLC can be used for printing to a printer such as an HP LaserJet 4Si that uses an HP JetDirect network adapter to connect directly to the network (rather than to a port on a print server). The DLC protocol must be installed and running on the print server for the printer. Computers sending print jobs to a print server for a DLC network printer do not need the DLC protocol—only the print server requires DLC. To take advantage of the DLC protocol device driver, you must create a network printer in the Printers folder.

In addition to the 16-bit DLC protocol, Windows 98 includes a 32-bit DLC protocol. In most cases, Microsoft recommends that you use the 32-bit DLC protocol. It provides better performance and can access protected memory. However, certain applications require Microsoft's 16-bit DLC because they require a TSR program to connect to a host computer before starting Windows 98. For more information about these applications, see "Running 16-bit applications" earlier in this chapter.

The following sections describe how to install the Microsoft DLC protocol and how to configure it with Novell NetWare ODI drivers and IBM LAN Support.

# Installing and Configuring Real-Mode Microsoft DLC

This section describes how to install the real-mode NDIS 2 Microsoft DLC protocol to bind with an NDIS 2 network adapter driver. This is an NDIS 2 protocol that, when installed, is bound to an NDIS 2 network adapter driver. The Windows 98 protected-mode protocols use the Ndis2sup.vxd module to coexist with and run over the real-mode NDIS 2 network adapter drivers.

When you install Windows 98, Windows 98 Setup detects whether the computer already has the Microsoft DLC protocol installed; if so, Setup migrates the protocol and its settings to Windows 98. Otherwise, you can add Microsoft DLC as a protocol after Windows 98 is installed.

---

**Note**  You must install the version of Microsoft DLC provided with Windows 98. You cannot use the Microsoft DLC INF file from Windows for Workgroups 3.*x* to install this protocol; Windows 98 uses a new INF file format.

You can also install Microsoft DLC using setup scripts, as described in Appendix D, "Msbatch.inf Parameters for Setup Scripts."

---

▶  **To install the Microsoft DLC protocol on a computer running Windows 98**

1.  In Control Panel, double-click Network.

2.  On the **Configuration** tab, click **Add.**

3.  In the **Select Network Component Type** dialog box, double-click **Protocol.**

4.  In the **Select Network Protocol** dialog box, click **Microsoft** in the Manufacturers list, and then click **Microsoft DLC** in the Network Protocols list. Then click **OK.**

5.  Shut down and restart the computer for the changes to take effect.

6.  Make sure that there is only one **net start** entry in Autoexec.bat, because Setup automatically adds an entry to support DLC, even if such an entry already exists.

The properties in Table 15.15 are set by default for real-mode Microsoft DLC. You can use the Network option in Control Panel to change these default values, or to set values for other parameters that you might use, in the Advanced properties for Microsoft DLC protocol.

**Table 15.15     DLC properties**

| Value | Description |
|-------|-------------|
| Saps | Indicates the number of SAPs that can be opened simultaneously. The range for SAPs is 1 to 255 inclusive. The default is 3. |
| | For a description of SAPs, see the *IBM Local Area Network Technical Reference*. |
| Stations | Indicates the number of link stations that can be opened simultaneously. The range for stations is 1 to 255 inclusive. The default is 20. |
| | Each application requires a certain number of SAPs and stations. Because each SAP or station takes up memory, you should provide only enough for your application to run. |
| Swap | Turns on address bit-swapping when it is enabled and Microsoft DLC is bound to an Ethernet driver. The default is 1 (enabled). |
| Usedix | Sets the frame format. By default, this value is 0 (disabled), which is the correct value for 802.3 Ethernet format. Set this value to 1 for Ethernet DIX 2.0 (Ethertype 0x80D5) format. Ethernet DIX frames have an extra type-field. |

The default values for SWAP and UseDIX are appropriate for most token-ring LAN environments. If the computer has an Ethernet adapter, then you should set the correct values for these parameters in the Advanced properties for Microsoft DLC. If you previously used the IBM Dxme0mod.sys driver, use Table 15.16 to map the Xmit_swap parameter to set values for the two Microsoft DLC parameters.

**Table 15.16     Mapping Xmit_swap parameters**

| Dxme0mod.sys xmit_swap | Microsoft DLC parameters |
|------------------------|--------------------------|
| 0 | swap=1<br>usedix=0 |
| 1 | swap=1<br>usedix=1 |
| 2 | swap=0<br>usedix=0 |
| 3 | swap=0<br>usedix=1 |

Table 15.17 shows some typical settings in Autoexec.bat and Protocol.ini for Microsoft DLC with an Intel EtherExpress PRO LAN NDIS 2 network adapter driver on an Ethernet network. Notice that the [msdlc$] section is added automatically by Windows 98 when the protocol is installed.

**Table 15.17      Sample configuration file settings for Microsoft DLC with NDIS 2 adapters**

| File name | Required settings |
|---|---|
| autoexec.bat | ```
net init
msdlc.exe
net start
``` |
| protocol.ini | ```
[netbeui$]
DriverName=NETBEUI$
Lanabase=0
sessions=10
ncbs=12
Bindings=EPRO$

[nwlink$]
DriverName=nwlink$
Frame_Type=4
cachesize=0
Bindings=EPRO$

[epro$]
DriverName=EPRO$
INTERRUPT=10
ioaddress=0x300

[protman$]
priority=ndishlp$
DriverName=protman$

[ndishlp$]
DriverName=ndishlp$
Bindings=EPRO$

[data]
version=v4.00.000
netcards=EPRO$,*PNP8132

[msdlc$]
DriverName=msdlc$
stations=20
saps=3
swap=0
usedix=1

Bindings=EPRO$
``` |

## Configuring Real-mode Microsoft DLC with ODI Drivers

For computers that are running Microsoft DLC with ODI drivers using the Novell-supplied Odinsup.exe file, Windows 98 Setup installs over this configuration and leaves entries for ODINSUP and MSDLC in Autoexec.bat. Microsoft does not provide direct support for Microsoft DLC used with Odinsup.exe.

If you must run a real-mode network redirector or TSR (Netx.exe, Vlm.exe, and so on), you need to configure Microsoft DLC by binding the Microsoft DLC protocol to an ODI network adapter driver. Otherwise, install Microsoft DLC over NDIS 2 with the protected-mode Microsoft Client for NetWare Networks. For information about these configurations, see "Architecture for DLC" in Chapter 29, "Windows 98 Network Architecture."

Table 15.18 shows settings used to configure Microsoft DLC with ODI drivers.

**Note**  This manual editing of Protocol.ini will remove "Microsoft DLC" from the Network Configuration dialog. The usage of Odinsup.exe prevents Windows 98 from correctly identifying the "Microsoft DLC" as being used by the Ethernet adapter and therefore will not be displayed even though the protocol will still function.

**Table 15.18    Configuration file settings for real-mode Microsoft DLC with ODI drivers**

| File name | Required settings | |
|---|---|---|
| autoexec.bat | lsl | ;Novell-supplied component |
| | *mlid_driver*.com | ;Novell-supplied component |
| | odihlp.exe | ;Windows 98 component |
| | odinsup.exe | ;Novell-supplied component |
| | msdlc.exe | ;Windows 98 component |
| | net start netbind | ;Windows 98 component |
| net.cfg | Protocol ODINSUP | |
| |    Bind EPROODI | |
| |    BUFFERED | |
| | Link Driver EPROODI | |
| |    Port 300 | |
| |    Frame Ethernet_802.2 | |
| |    Frame Ethernet_802.3 | |
| |    Frame Ethernet_II | |
| |    Frame Ethernet_Snap | |

**Table 15.18   Configuration file settings for real-mode Microsoft DLC with ODI drivers** (*continued*)

| File name | Required settings |
|---|---|
| protocol.ini | `[protman$]`<br>`priority=ndishlp$`<br>`DriverName=protman$`<br><br>`[ndishlp$]`<br>`DriverName=ndishlp$`<br>`Bindings=`<br><br>`[data]`<br>`version=v4.00.000`<br>`netcards=`<br><br>`[nwlink$]`<br>`Frame_Type=4`<br>`cachesize=0`<br>`DriverName=nwlink$`<br><br>`[msdlc$]`<br>`DriverName=msdlc$`<br>`xstations0=0`<br>`xstations1=0`<br>`stations=20`<br>`saps=3`<br>`xsaps0=1`<br>`xsaps1=1`<br>`swap=0`<br>`usedix=1`<br>`Bindings=EPROODI`<br><br>`[EPROODI]`<br>`Drivername=EPROODI`<br>`INTERRUPT=10`<br>`ioaddress=0x300` |

## Upgrading Existing IBM LAN Support Installations

If you are using DLC support supplied by IBM to connect to host computers, Windows 98 Setup can detect IBM DLC; it leaves the installation intact and configures Windows 98 to run over that configuration. Although support for IBM DLC can be installed using the Network option in Control Panel, the required components must be provided by your network vendor.

This section describes two typical IBM LAN Support configurations, using Dxmc0mod.sys and Dxme0mod.sys.

**DxmcOmod.sys, the monolithic IBM DLC driver.** For this configuration, Windows 98 Setup does one of two things:

- If the computer is running NetWare, Setup keeps the DxmcOmod.sys driver and related settings, and installs the Generic ODI driver plus Microsoft Client for NetWare Networks, or keeps the real-mode client.

- If the computer is running DxmcOmod.sys and no other networking components, Setups keeps the DxmcOmod.sys driver and does not install any Windows 98 networking components.

Table 15.19 shows a sample configuration for IBM DxmcOmod.sys with Microsoft Client for NetWare Networks.

**Table 15.19 Example of configuration settings for DxmcOmod.sys with ODI drivers**

| File name | Required settings | |
|---|---|---|
| autoexec.bat | lsl | ; Novell-supplied component |
| | lansup | ; Novell-supplied component |
| | odihlp.exe | ; Microsoft component |
| config.sys | device=*path*\dxmaood.sys | ;IBM-supplied component |
| | device=*path*\dxmcomod.sys | ;IBM-supplied component |

**DxmeOmod.sys, the NDIS driver for IBM DLC.**

For this configuration, Windows 98 Setup does one of three things:

- If the computer is running DxmeOmod.sys and no other networking components, Setup keeps the DxmeOmod.sys driver and does not install any Windows 98 networking components.

- If the computer is running DxmeOmod.sys and Novell NetWare, Setup installs an NDIS network adapter driver plus Microsoft Client for NetWare Networks, and leaves the DxmeOmod.sys driver intact.

- If the computer is running DxmeOmod.sys with the IBM MS-DOS LAN Requestor, Setup installs an NDIS 2 adapter driver, keeps the DxmeOmod.sys driver, installs Client for Microsoft Networks, and removes the IBM MS-DOS LAN Requestor redirector components.

Table 15.20 shows a sample configuration for IBM Dxme0mod.sys with Client
for Microsoft Networks using an NDIS 2 adapter driver. The same basic kinds of
settings are used for a computer running Microsoft Client for NetWare Networks
with an NDIS 2 adapter driver.

**Table 15.20   Example of settings for Dxmce0mod.sys with Client for Microsoft
Networks**

| File name | Required settings |
|---|---|
| autoexec.bat | `net start netbind` |
| config.sys | `device=c:\windows\protman.dos /i:c:\windows`<br>`device=c:\windows\epro.dos      ;ndis2 driver`<br>`device=c:\lsp\dxma0mod.sys      ;IBM-supplied`<br>`device=c:\lsp\dxme0mod.sys ,,3  ;IBM-supplied`<br>`device=c:\windows\ndishlp.sys   ;Windows 98` |
| protocol.ini | `[protman$]`<br>`priority=ndishlp$`<br>`DriverName=protman$`<br><br>`[ndishlp$]`<br>`DriverName=ndishlp$`<br>`Bindings=EPRO$`<br><br>`[data]`<br>`version=v4.00.000`<br>`netcards=EPRO$,*pnp8132`<br><br>`[netbeui$]`<br>`DriverName=NETBEUI$`<br>`Lanabase=0`<br>`sessions=10`<br>`ncbs=12`<br>`Bindings=EPRO$`<br><br>`[nwlink$]`<br>`DriverName=nwlink$`<br>`Frame_Type=4`<br>`cachesize=0`<br>`Bindings=EPRO$`<br><br>`[EPRO$]`<br>`DriverName=EPRO$`<br>`INTERRUPT=10`<br>`ioaddress=0x300` |

**Table 15.20    Example of settings for Dxmce0mod.sys with Client for Microsoft Networks** (*continued*)

| File name | Required settings |
|-----------|-------------------|
| protocol.ini (*continued*) | `[DXMAIDXCFG]`<br>`dxme0_nif=dxme0.nif`<br>`dxmj0mod_nif=dxmj0mod.nif`<br>`smcdosjp_nif=smcdosjp.nif`<br>`smcdosjp2_nif=smcdosjp.nif`<br>`smcdosat_nif=smcdosat.nif`<br>`smcdosat2_nif=smcdosat.nif`<br>`smcdosmc_nif=smcdosmc.nif`<br>`smcdosmc2_nif=smcdosmc.nif`<br><br>`[ETHERAND]`<br><br>`DriverName=DXME0$`<br>`Bindings=EPRO$` |

# Overview of Network Adapters

Windows 98 Setup automatically detects most network adapters, installs the appropriate driver for the adapter, and provides appropriate default settings to configure the adapter. If you add a new network adapter, its driver is bound automatically to all network driver interface specification (NDIS)–compatible protocols currently running on the computer. If any protocols are added later, they will also be bound automatically to the network adapter driver. TCP/IP can be bound to a maximum of six network adapters.

This section provides technical details for configuring network adapters, setting LAN adapter numbers, and other technical notes.

For specific information about PC Card adapters, see Chapter 24, "Device Management."

---

**Note**  For information about specific network adapters, see the Windows 98 Adapter Card Configuration Help File on the Microsoft Windows 98 Resource Kit compact disc.

---

## Understanding the Benefits of NDIS Adapter Drivers

The network driver interface specification (NDIS) describes the interface that network adapter drivers use to communicate with underlying hardware, with overlying protocol drivers, and with the operating system. All network adapter drivers and protocols provided with Windows 98 conform to NDIS. Windows 98 provides NDIS 5.0, an extension of NDIS 4.0 that supports NDIS versions 2.$x$ 3.1, 4.0, and 5.0 protocol and adapter drivers. Windows 98 also provides a replacement for version 3.0 drivers, which are incompatible with Windows 98.

You should use NDIS 3.1 or later drivers whenever possible with Windows 98. If you are using a Novell-supplied network client, you should use ODI-based client software rather than monolithic IPX drivers.

NDIS 5 drivers add to the functionality provided by NDIS 3.1 drivers. For example, by using NDIS 5 drivers, Windows 98 can support a wide range of network media, including Ethernet, fiber distributed data interface (FDDI), token-ring, asynchronous transfer mode (ATM), and WAN technology. The NDIS 5 specification accommodates Plug and Play features, so that in many cases network adapters can be added and removed dynamically while the computer is running. NDIS 5 drivers also provide performance improvements, and compatibility with Windows NT Server 5.0.

This section summarizes the related benefits.

For information about NDIS architecture, see Chapter 29, "Windows 98 Network Architecture." See also the introduction to NDIS at **http://www.microsoft.com /hwdev/devdes/ndis5.htm.**

**Plug and Play support for network protocols and adapters.** Windows 98 can automatically determine the adapters to which each protocol should bind. Additionally, if you are using a PC Card or CardBus adapter, and a Plug and Play event occurs, such as the removal of an adapter from a portable computer, the NDIS protocols and network adapters can detect the event and remove themselves from memory automatically.

**NDIS miniport driver model.** In releases of NDIS before 3.1, adapter drivers implemented not only the media access functionality that was specific to the network adapter, but also the media access functionality that is common to all NDIS drivers.

For NDIS 3.1 and later adapter miniport drivers, the Windows 98 NDIS wrapper implements the half of the media access functionality that is common to all NDIS drivers. Thus, the miniport driver provided by the adapter manufacturer must implement only the half of the media access layer that is specific to the network adapter. These include specific details such as establishing communications with the adapter, turning on and off electrical isolation for Plug and Play, providing media detection, and enabling any value-added features the adapter might contain.

The Windows 98 miniport drivers are binary-compatible with Windows NT 3.5 and later miniport drivers, which means they can be used on either operating system without being recompiled. (You can recognize a miniport driver by its .sys file name extension; other drivers have .vxd extensions.)

**Real-mode NDIS 2 support.** An NDIS 2.*x* protocol under Windows 98 must use an NDIS 2.*x* network adapter driver. Both the protocol and network adapter drivers must load and bind in real mode before Windows 98 runs. Values in Protocol.ini are used to load the real-mode NDIS drivers, as described in Chapter 16, "Windows 98 on Microsoft Networks." However, you still use the Network option in Control Panel to configure NDIS 2 adapters.

When you run a real-mode network, Windows 98 uses NDIS 2 versions of NetBEUI and IPX/SPX protocols. These protocols are not intended for everyday use, since Windows 98 supplies faster protected-mode versions of these protocols.

Windows 98 also supports existing ODI drivers with Novell NetWare–compatible network clients. For information, see Chapter 17, "Windows 98 on Third-Party Networks."

**Support for Windows Management Infrastructure.** Windows Management Interface (WMI) collects a wealth of information about the entire system as well as device configuration. This information is stored in the registry and made available through extensions to the Registry API.

NDIS 5 supports the Windows Management Infrastructure (WMI) for Web-Based Enterprise Management (WBEM) of NDIS miniports and their associated adapters, providing the architecture for user-mode management of NDIS drivers and network adapters. This will enable network administrators and support technicians to remotely monitor and control systems using NDIS 5 compliant drivers.

For more information about WMI, see **http://www.microsoft.com/hwdev /devdes/ndis5.htm**.

**Support for broadcast media.** NDIS 5 includes extensions to support Broadcast Architecture. It supports high-speed unidirectional broadcast media such as services provided by DirectTV, PrimeStar, and Intercast. The extensions include definitions for receiver tuning, multiple media stream negotiation, fast data streaming, and support for UDP/IP multicast packets using a Microsoft LAN Emulation driver.

For more information about Broadcast Architecture, see Chapter 13, "WebTV for Windows 98."

**Support for connection-oriented media.** In addition to supporting connectionless media such as Ethernet, token-ring, FDDI, Wireless WAN, and infrared, with NDIS 5 Windows 98 now supports raw access to connection-oriented media such as ATM, integrated services digital network (ISDN), X.25, and Frame Relay. This support is provided only if you are using miniport drivers.

For more information about NDIS support for connection-oriented networks, see Chapter 29, "Windows 98 Network Architecture."

# Plug and Play Networking

Plug and Play is an independent set of computer architecture specifications that hardware manufacturers use to produce computer devices that can be configured with no user intervention. With Windows 98, you can install Plug and Play–compliant devices such as network adapters simply by plugging in the device and turning on the computer. If Windows 98 has support for the device it automatically adds its configuration information to the registry, ensures that the correct files are installed, and ensures that the configuration options are set properly.

The networking components in Windows 98 are designed for dynamic Plug and Play operation with most ISA, EISA, PCI, IBM Micro Channel, CardBus, and PC Card network adapters. To take advantage of these features, the computer must be running all protected-mode networking components, including client, protocols, and network adapter drivers.

NDIS 3.1 and later supports adding and removing Plug and Play network adapters dynamically while the computer is running. For example, if you undock a portable computer (called *hot undocking*), the Windows 98 protocols can remove themselves from memory automatically.

Additional Plug and Play networking benefits are available when you use 32-bit socket services with PC Card cards. You can click the PC Card icon on the taskbar to remove the card without shutting down Windows 98 or turning off the computer. Clicking the PC Card icon causes the operating system to perform an orderly shutdown of the affected network components. Windows 98 notifies applications that the network is no longer available and automatically unloads any related drivers or protocols.

To help mobile users who might need to change adapters in their hardware, Windows 98 uses 32-bit Card and Socket Services to support hot removal and insertion of PC Cards, including network adapters. Support for hot docking means that users do not have to restart their computers each time they make a change to their hardware configuration by docking or undocking their computers. For information about using and configuring PC Cards, including how to enable 32-bit Card and Socket Services, see Chapter 30, "Hardware Management."

Network Plug and Play support in Windows 98 includes application-level support. An application created for Windows 98 might be designed with the ability to determine whether the network is available. Therefore, if a network adapter is removed, for example, the application automatically puts itself into "offline" mode to allow the user to continue to work, or it shuts down.

# Configuring Network Adapters

This section describes how to configure network adapters for Windows 98 computers. First, the section "Installing and Configuring Network Adapters" provides a brief overview of how to install both Plug and Play and legacy network adapters. Next, the section "Configuring Network Adapter Settings in Windows 98" explains how to configure network adapter driver properties from within Windows 98. Finally, the section "Binding Network Adapter Drivers to Protocols" describes how to bind network adapter drivers to protocols.

## Installing and Configuring Network Adapters

How you install your network adapter depends on what type of network adapter you have.

If you have a Plug and Play network adapter, Windows 98 automatically detects the adapter and performs most of the required configuration.

If you have a non-Plug and Play network adapter (also called a *legacy network adapter*), the Add New Hardware wizard starts and should automatically configure the network adapter. However, you might need to perform software or hardware configuration. For example, with some legacy network adapters you must set jumpers or switches on the hardware itself. With others, you must run a vendor-supplied software configuration program from within an MS-DOS window.

Note that this configuration is separate from the configuration you must do from within Windows 98. As the section "Configuring Network Adapter Settings in Windows 98" explains, you must configure settings from the Network option in Control Panel to match the settings you have configured using jumpers, switches, or a software configuration program.

## Configuring Network Adapter Settings

This section discusses how to configure properties for network adapter drivers.

The properties you must configure from within Windows 98 depend on whether you are installing Plug and Play or non-Plug and Play devices.

If you install a Plug and Play network adapter, Windows 98 should automatically configure it. You should not need to change most of the settings, including any of the settings described in "Configuring Network Adapter Resource Settings" later in this chapter. However, if your network configuration is not working properly, you might want to review this section.

If you install a non-Plug and Play network adapter, the Add New Hardware Wizard should automatically configure it. When asked whether you want Windows to search for your new hardware (that is, to perform hardware detection), make sure to click **Yes**. This helps Windows 98 choose the correct driver and resource assignments. If hardware detection fails, you might need to configure Windows 98 settings to match the settings for the network adapter itself. For example, if you used a software configuration utility to set an Interrupt Request (IRQ), you must configure Windows 98 to use the same IRQ for the network adapter.

If you experience problems with the settings for a network adapter, you should begin troubleshooting by removing the network adapter driver from the Network option in Control Panel. Then reboot, and if the card is not detected, use the Add New Hardware option to reinstall support for the network adapter, using hardware detection to ensure that Windows 98 determines the correct adapter driver and standard settings for that network adapter. If you experience problems after installing a Plug and Play device or after automatically detecting a non-Plug and Play device from the Add New Hardware option, you might need to manually configure properties for network adapter drivers.

## Specifying the Driver Type for a Network Adapter

Generally, you will not need to specify the driver type for a network adapter. In fact, some network adapters do not let you specify the driver type. However, if you need to use a real-mode driver you must specify the driver type.

▶ **To specify the driver type for a selected network adapter**

1. In Control Panel, double-click Network.

2. On the **Configuration** tab, select the name of the network adapter driver from the list of installed components.

3. Click the **Properties** button.

4. In the properties for the network adapter, click the **Driver Type** tab.

5. Click one of three options (if available for the specific adapter), as described in the following list.

| Network adapter driver type | Description |
|---|---|
| Enhanced mode (32-bit and 16-bit) NDIS driver | Installs an NDIS 3.1 or later–compliant driver. This is the preferred driver type for use with 32-bit, protected-mode network clients. |
| Real-mode (16-bit) NDIS driver | Installs an NDIS 2.x–compliant driver. |
| Real-mode (16-bit) ODI driver | Installs a real-mode driver created to support ODI for Windows 3.1 on NetWare networks. |

### Configuring Network Adapter Resource Settings

Windows 98 can determine hardware settings for Plug and Play network adapters. Thus, for Plug and Play network adapters you should let Windows 98 go through its Plug and Play installation process. You should not change any settings described in this section unless you are absolutely sure they are incorrect. In fact, you cannot change network adapter resource settings for most Plug and Play network adapters.

For non-Plug and Play network adapters, you should use the Add New Hardware option in Control Panel, using detection to determine the correct driver and resource settings. You should accept the proposed settings unless you are absolutely sure they are incorrect.

Most ISA devices cannot share IRQ settings, memory buffer addresses, or ROM addresses. Where possible, Windows 98 identifies and resolves conflicts. However, if one of the supported devices does not seem to work, the problem may be the particular hardware configuration. To make sure there are no conflicts among network adapters or other peripherals, or between the system board and adapters, check the settings in Device Manager.

For information about checking the settings in Device Manager, see Chapter 24, "Device Management."

If Device Manager shows that any of these settings conflict, you can use the Network option in Control Panel to make sure that the settings match the settings for your network adapter.

▶ **To configure resources in a network adapter's properties**

1. In Control Panel, double-click Network.

2. In the list of installed components, click the network adapter and then click the **Properties** button. Make sure to click the network adapter, not the protocol binding for that adapter.

3. In the properties for the network adapter, if a **Resources** tab appears, click it.

---

**Note** If a **Resources** tab does not appear, you cannot configure the network adapter's resources from the Network option in Control Panel.

---

4. Select a configuration from the **Configuration type** box. Confirm values for the listed settings by comparing the proposed settings with the values recommended in the documentation for the adapter.

5. To select from the available values for a setting, click the arrow beside the setting's current value.

- A hash (#) character appears by current settings.

- An asterisk (*) appears beside settings that conflict with another device in the system. You should avoid this setting or reconfigure the other devices to use different settings.

The settings available depend on the type of network adapter. For example, for Intel adapters, you cannot set the IRQ using the adapter's properties. Table 15.21 describes a few typical settings. Each setting must match the adapter's settings, as specified in the documentation for the adapter.

**Table 15.21   Example hardware resource settings for a network adapter**

| Setting type | Description |
| --- | --- |
| I/O Address Range | Specifies the reserved I/O address range (as a hexadecimal value). |
| Interrupt Request (IRQ) | Specifies the hardware line over which the device can send interrupts (requests for service) to the computer's CPU. |
| Memory Address | Specifies the base memory address (as a hexadecimal value) used by this network adapter. |

If the settings in the **Resources** tab do not match the adapter's settings, you must either change the settings in the **Resources** tab or, in some cases, change the adapter's settings. To determine how to change the adapter's settings, refer to the documentation for your network adapter.

---

**Note**  For some legacy adapters, it is possible that the adapter uses resources not listed with the Resource properties. For these adapters, the NDIS driver determines the resource settings directly from the adapter itself. Even though these resources do not appear in the list, they can still conflict with other devices. For example, the resource list for the IBM token-ring adapter shows only the I/O settings, but this adapter also uses IRQ and Memory resources.

---

## Configuring Advanced Properties for Network Adapters

You can configure Advanced properties for both Plug and Play and non-Plug and Play devices. The options available in the **Advanced** tab of the **Properties** dialog box vary, depending on the type of network adapter. For information about specific settings that appear for a selected network adapter, see the documentation provided by the manufacturer for the adapter and driver. The manufacturer can also provide guidelines for when to change the default values for advanced configuration options.

▶ **To specify advanced settings for the network adapter**

1. In Control Panel, double-click Network.

2. In the list of installed components, click the network adapter and then click the **Properties** button.

3. In the properties for the selected network adapter, click the **Advanced** tab.

   The following figure shows the advanced options for an Intel EtherExpress network adapter.



4. To change these values, select an item in the **Property** list, and then select a setting in the **Value** box.

5. Click the **OK** button.

6. Restart the computer.

Table 15.22 shows some typical settings for general types of network adapters. Network adapters that use the new, fast Ethernet technology might have many more settings. Examples of such adapters include SMC EtherPower 10/100 (9332) PCI Ethernet Adapter, DEC Etherworks 435, and Intel EtherExpress PRO/100. For an explanation of specific settings for a network adapter, see the documentation provided by the adapter manufacturer. You should not change the default settings unless you know they are incorrect.

**Table 15.22   Typical network adapter settings**

| Example setting | Description |
|---|---|
| **For Ethernet adapters:** | |
| Transceiver type (cable connector) | The transceiver is the device that connects a computer to the network, defined as one of the following values:<br>■ Thick Net, for an AUI or Digital/Intel/Xerox (DIX) connection.<br>■ Thin Net, for a BNC or coaxial (COAX) connection.<br>■ Twisted pair, for a TPE RJ-45 connection. |

**Table 15.22   Typical network adapter settings** (*continued*)

| Example setting | Description |
| --- | --- |
| **For token-ring adapters:** | |
| I/O port base address | This value specifies the base memory address used by the adapter. To set the I/O address of an IBM 4/16 token-ring adapter, select either Primary (A20) or Secondary (A24) for this value. In this case, the driver ignores the I/O settings in the **Resource** tab of the **Network Adapter Properties** dialog box. |
| Network Address | By default, Windows 98 network detection uses the address burned into the adapter. To use another network address, type the network address in hexadecimal form, in the format *XX-XX-XX-XX-XX-XX*; for example, 01-02-03-4E-2D-1F. |
| Ring speed | The ring speed is 4 or 16 megabits per second, and is set by changing a jumper on the adapter or by running the adapter's configuration utility. For example, for an Intel TokenExpress 16/4 adapter, this is set on the adapter itself. The value in Windows 98 should match the physical or software setting. |

## Binding Network Adapter Drivers to Protocols

For a protocol to communicate with each network adapter on your computer, the network adapter driver must be bound to the protocol. (This applies to both Plug and Play and non-Plug and Play network adapters.) The bindings define the relationships between networking software components. Windows 98 automatically binds the appropriate protocols to the network adapter.

You might want to change the bindings if you have multiple network adapters and you do not want to use a specific protocol with a particular network adapter. Or, if the computer is on a local area network and is also connected to the enterprise internetwork, you might not want the computer's shared resources to be seen on the internetwork. In that case, you can disable the binding between the related protocol and the adapter that connects the computer to the internetwork.

▶ **To configure bindings between a network adapter and installed protocols**

1. In Control Panel, double-click Network.

2. In the list of installed components, click the network adapter and then click the **Properties** button.

3. In the properties for the selected network adapter, click the **Bindings** tab.

   In the list, the protocols that are bound to the selected adapter are checked. If a particular protocol does not appear in the list, check that it is installed correctly by returning to the **Configuration** tab of the **Network** dialog box and reinstalling it.

4. If you do not want this network adapter to be bound to a particular protocol, clear the check box beside the protocol.

# Setting LAN Adapter Numbers

NetBIOS defines the interface between the network client and the protocol layers using a set of function calls that allow an application to use the protocol services. Because many network applications use NetBIOS to send commands to the protocol driver, the NetBIOS interface is supported by all protocols provided with Windows 98.

Each combination of a NetBIOS network protocol and a network adapter forms a logical network over which computers can communicate with each other. For example, a computer can have a token-ring adapter and an Ethernet adapter, and might use NetBEUI on the token-ring network and both NetBEUI and TCP/IP on the Ethernet network. In this case, the computer is connected to three logical networks, each of which is assigned a NetBIOS LAN adapter (LANA) number that Windows 98 uses for communication.

When Windows 98 uses multiple protocols, it transmits data first using one protocol, then again using the next protocol, and so on. When multiple protocols are installed on a computer, the first protocol to be used is called the primary protocol.

On a computer running Windows 98, each binding of a protocol to a network adapter has a LAN adapter number assigned to it. (For example, one protocol bound to two network adapters requires two LAN adapter numbers; two protocols each bound to two adapters requires four LAN adapter numbers.)

In Windows 98, LANA numbers are assigned dynamically in sequence of binding order for the protocols, beginning with 7 and then 0, 1, and so on. This accommodates dynamic Plug and Play events such as the removal of a network adapter while the computer is running. If you are running Windows 98 in such a dynamic environment, Windows 98 cannot guarantee that a given protocol will receive the same LANA number each time the system is started. If the computer's network hardware never changes, the LANA numbers might not change at each startup. However, the default protocol is always LANA 0.

You need to change a LAN adapter number only if you have a NetBIOS application that needs to know the LANA number. For example, Lotus Notes requires that you enter the LANA number that Lotus Notes will use. To configure Windows 98 to use Lotus Notes, set the default protocol to be the NetBIOS-based protocol on which you want to run Lotus Notes. (Setting the default protocol makes it LANA 0.) This protocol can be NetBEUI, IPX/SPX-compatible with NetBIOS support, or TCP/IP.

▶ **To select a default protocol for LANA settings**

1. In Control Panel, double-click Network.

2. Double-click the protocol you want to be the default.

3. In the protocol's **Properties** dialog box, click the **Advanced** tab.

4. Click the option named **Set this protocol to be the default protocol** so that the check box is checked. Then click **OK**, and shut down and restart the computer for the changes to take effect.

# Configuring Asynchronous Transfer Mode and LAN Emulation

Transport protocols such as TCP/IP and IPX are connectionless. That is, they do not need to establish a connection before transmitting data; computers using those protocols simply send packets out to the network. However, asynchronous transfer mode (ATM) is connection-oriented and must establish a connection before transmitting any data. LAN Emulation provides the bridge between the connectionless protocols and ATM, enabling them to function transparently over ATM networks.

This section describes how to configure LAN Emulation on Windows 98 computers.

For more information about the ATM and LAN Emulation architecture, see the section "Architecture for NDIS" in Chapter 29, "Windows 98 Network Architecture."

The following procedure describes how to configure a computer as a LAN Emulation client, so it can communicate with other devices on the ATM network.

**Note**  Windows 98 Setup automatically installs TCP/IP only if it detects a network adapter. However, it does not automatically install TCP/IP on computers that have only an ATM card. Thus, if you want to use TCP/IP over the ATM network, you must also install TCP/IP by following the procedures outlined in "Installing Microsoft TCP/IP" earlier in this chapter. If you want to use another network protocol instead, you must install it by following the procedures outlined in the section for that protocol, earlier in this chapter.

▶ **To configure a Windows 98 computer as a LAN Emulation client**

1. In Control Panel, double-click Network.

2. On the **Configuration** tab, click the **Add** button.

3. In the **Select Network Component Type** dialog box, click **Protocol**, then click the **Add** button.

4. In the **Manufacturers** box, click **Microsoft**.

5. In the **Network Protocols** box, click **ATM Call Manager**, and then click **OK**.

6. Repeat steps 2 through 4 one time.

7. In the **Network Protocols** box, click **ATM Emulated LAN**, and then click **OK**.

8. Repeat steps 2 through 4 one time.

9. In the **Network Protocols** box, click **ATM LAN Emulation Client** and then click **OK**.

The previous procedure configures the computer to be part of the *default emulated LAN*. An *emulated LAN* is a virtual network that acts like a traditional LAN. ATM networks can consist of one or more emulated LANs: for example, a network administrator might want to create different emulated LANs for users in the Marketing and Accounting departments. However, all ATM networks have one default emulated LAN, which is the emulated LAN that all computers belong to unless they have been specifically configured as part of a different emulated LAN. Thus, after you have configured your computer as a LAN Emulation client, it automatically belongs to the default emulated LAN and can communicate with other devices on the ATM network.

In some circumstances, the ATM network administrator might configure additional emulated LANs. If so, and if you are given the name of an emulated LAN to which you should belong, you can configure your computer to be part of that emulated LAN.

---

**Note**  When you are using ATM LAN Emulation, any network protocol that you will use on the emulated LAN must be installed on your computer. If you have not yet installed the network protocol you will use, you should do so now. For more information about installing network protocols, see the section for that protocol, earlier in this chapter.

---

▶ **To configure your computer as part of an Emulated LAN other than the default LAN**

1. In Control Panel, double-click Network.

2. In the list of installed components, select the network adapter binding for **ATM LAN Emulation Client**.

3. In the **Value** box, enter the name of the emulated LAN.

## Technical Notes on Network Adapters

NDIS 3.0 network adapter drivers that worked with Windows for Workgroups 3.11 do not work under Windows 98. You must use an NDIS 2.*x* real-mode driver, an ODI driver, or an updated NDIS 3.1 or later protected-mode driver for the network adapter. The driver must have a Windows 98 INF file. Many real-mode drivers, updated protected-mode drivers, and supporting INF files are included with Windows 98.

# Troubleshooting Network Adapters and Protocols

This section contains information about troubleshooting problems related to network protocols. For general information about troubleshooting the network installation, including how to use **net diag**, see Chapter 14, "Introduction to Networking Configuration." For information about troubleshooting procedures and tools provided with Windows 98, see Chapter 27, "General Troubleshooting."

## Correcting Problems with Network Adapters

This section describes specific problems you might encounter using network adapters with Windows 98.

For information about specific network adapters, see the Windows 98 Adapter Card Configuration Help File on the Windows 98 Resource Kit compact disc.

For general troubleshooting steps, see the "Troubleshooting Basic Networking Configuration" section in Chapter 14, "Introduction to Networking Configuration."

### Plug and Play card does not function with 16-bit network drivers.

If you are running Plug and Play with a 16-bit, real-mode driver, your Plug and Play network adapter might not function properly. If this happens, disable Plug and Play support for that network adapter.

▶ **To disable Plug and Play support for a network adapter**

1. Run the software setup utility that comes with your Plug and Play card.
2. Set the card to non-Plug and Play Mode.
3. In Control Panel, double-click System, and then click the **Device Manager** tab.
4. Expand the **Network adapters** tree, and then select your network card.
5. Click **Remove**.
6. In Control Panel, double-click Add New Hardware.
7. Manually reinstall the network adapter.

---

**Note**  For some network adapters, you will also need to install a non-Plug and Play driver.

---

If you later need to re-enable Plug and Play support, follow these steps:

▶ **To re-enable Plug and Play support for a network adapter**

1. In Control Panel, double-click System, and then click the **Device Manager** tab.
2. Remove the network adapter.
3. Run the software setup utility that comes with your Plug and Play card.
4. Set the card to Plug and Play Mode.
5. Reboot the computer. Windows 98 automatically detects the network adapter.

# Correcting Problems with TCP/IP

This section describes TCP/IP utilities that you can use to diagnose TCP/IP connectivity problems. Next, it discusses general troubleshooting methods to solve TCP/IP connectivity problems. Finally, it lists common problems you might experience.

## Using Diagnostic Utilities to Troubleshoot

Use the TCP/IP diagnostic utilities included with Microsoft TCP/IP to diagnose connectivity problems. The following list describes which MS-DOS utility helps to identify various problems. For a more detailed description of these utilities, see "TCP/IP Utilities" earlier in this chapter.

**Table 15.23　Using TCP/IP diagnostic utilities**

| Use this utility | To accomplish this action |
| --- | --- |
| **ipconfig /all** | Check host name, host IP address, and TCP/IP configuration. |
| | **Note:** The graphical utility **winipcfg**, described in this section, also provides this information. |
| **ping** | Verify physical connection and remote TCP/IP computer. |
| **arp** | Detect invalid entries in the ARP table on the local computer. |
| **nbtstat** | Check the state of NetBIOS over TCP/IP connections, update LMHosts cache, and determine registered name and scope ID. |
| **net view** | Determine if destinations on TCP/IP networks are reachable using WINS. |
| **netstat** | Display statistics and state of current TCP/IP connections. |
| **tracert** | Check the route to a remote computer. Also test connectivity to PPTP servers, which generally do not respond to ping requests. |

For more information about these utilities, see "TCP/IP Utilities" earlier in this chapter.

You can also use the graphical IP Configuration utility **winipcfg** to display, update, or release TCP/IP configuration values, including DHCP values.

**Winipcfg** can also show you whether or not your computer is using automatic private IP addressing for its IP address. For more information about automatic private IP addressing, see "Configuring IP Addresses Using Automatic Private IP Addressing" earlier in this chapter.

▶  **To use winipcfg**

1. Click Start, click Run, and then type:

   **winipcfg**

2. The resulting screen identifies your IP address and the IP address of your default gateway.

3. Click **More info**.

4. The resulting screen tells you your IP address, subnet mask, and default gateway for each of your network interfaces. It also shows your DNS and WINS settings.

▶  **To test TCP/IP using ping**

- Check the loopback address by typing **ping 127.0.0.1** and pressing ENTER at the command prompt. The computer should respond immediately. To determine whether you configured IP properly, use **ping** with the IP address of your computer, your default gateway, and a remote host. (If you are using DHCP, use **winipcfg** to find the IP address.)

If you cannot use **ping** successfully at any point, verify the following:

- The computer was restarted after TCP/IP was installed and configured.

- The local computer's IP address is valid and appears correctly in the **TCP/IP Properties** dialog box.

- The IP address of the default gateway and remote host are correct.

- IP routing is enabled on the router, and the link between routers is operational.

- The local computer's registry includes an entry for **lmhosts=c:\\***directory* that correctly indicates the location of LMHosts.

If you can **ping** other computers running Windows 98 on a different subnetwork but cannot connect using Windows Explorer, **net use** \\\\*server*\\*share*, or **net view** \\\\*server*\\*share*, verify the following:

- The host is functioning.
- The correct host computer name was used.
- Using **tracert**, make sure that a router path exists between your computer and the target computer.
- LMHosts contains correct entries, so the computer name can be resolved.
- The computer is configured to use WINS, the WINS server addresses are correct, and WINS servers are functioning.

You can use **winipcfg** to verify your TCP/IP configuration settings. For information about using **winipcfg**, see "Using Diagnostic Utilities to Troubleshoot," earlier in this chapter.

## Troubleshooting TCP/IP Gateway Problems

If a host computer on one subnet has problems communicating to computers on another subnet when using TCP/IP, the following information can help you determine whether the problem is with the gateway. For these troubleshooting steps, it does not matter whether the gateway that provides routing capabilities is a hardware router or a Windows NT or UNIX server configured to act as a router.

First, to troubleshoot gateway problems, you need a network map, plus the IP addresses and subnet masks for the host computer with problems, the near side of the hardware or software router that acts as the gateway, the remote side of the gateway, and the destination computer (node). For example, Figure 15.6 shows two subnets connected by a router.
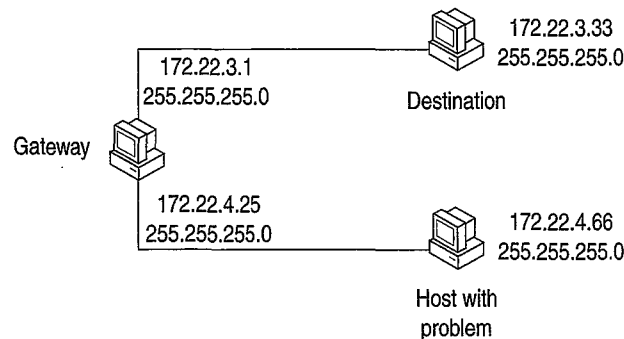


172.22.3.33
255.255.255.0

172.22.3.1
255.255.255.0

Destination

Gateway

172.22.4.25
255.255.255.0

172.22.4.66
255.255.255.0

Host with
problem

**Figure 15.6    Two subnets connected by a router**

The following example of troubleshooting steps uses the IP addresses from this illustration.

► **To troubleshoot possible gateway (router) problems**

1. Use **ping** to access the host computer that is having problems communicating outside the subnet. For example:

   ```
   ping 172.22.4.66
   ```

   If this works, this host is probably healthy at the IP level.

   If this does not work, use the usual methods to check the IP configuration and network connections on this host.

2. If the problem is not solved, use **ping** to access the near side of the router (that is, the default gateway). For example:

   ```
   ping 172.22.3.1
   ```

   If this works, this side of the router is healthy.

   If this does not work, use the usual methods to check the actual IP configuration and network connection for the near side of the router. Adjust the gateway settings on the problem host computer, if required.

   Notice, however, that if you can use **ping** to get a response from this address, it does not necessarily mean that this is actually a router.

3. If the problem is not solved, use **ping** to access the far side of the router. For example:

   ```
   ping 172.22.4.25
   ```

   If this works, the router is working.

   If this does not work, have another user use the same **ping** command from the destination node (172.22.4.66 in the example).

   If this works, the router is not working correctly.

4. If the problem is not solved, use **ping** to access the remote host. For example:

   ```
   ping 172.22.4.66
   ```

   If this works and all problems in the previous steps have been resolved, TCP/IP should be working fine.

   If this does not work, check the IP configuration and network connections on the destination computer. Typically, at this point the problem is that the remote computer has not route configured back to the original host computer. That is, the remote computer's routers or routing table does not contain the information necessary to send packets back to the original host computer.

When troubleshooting router connections, note the following:

- Do not use the host name when you are testing the router; instead, use the IP address. This will avoid any problems related to the Hosts or LMHosts files, DNS server, WINS server, or any other methods of name resolution.

- In most cases, the subnet mask should be the same for all hosts on the same side of the router.

- There could be two routers at separate sites performing the same job as described above; if this is the case, treat this situation the same as above, keeping in mind that each router could have a near and far side, depending on the configuration.

- If multiple routers exist between the source and destination, use **tracert** to see an ordered list of routers used. **Tracert** can also help you determine how many hops there are between the source and destination, and how much time it takes a packet to travel from the source to the destination.

---

**Tip for using SNMP for routing**   The TCP/IP utilities use the public interface provided by inetmib1.dll in both Windows NT and Windows 98. This API can be used with Simple Network Management Protocol (SNMP) for actions such as setting and getting routing information programmatically on Windows 98 computers. For information about the management information base (MIB) object types provided for Microsoft networking, see the *Microsoft Windows NT Server Resource Kit* (for Microsoft Windows NT Server version 4.0).

Notice, however, that you cannot use a Windows 98 computer to run the SNMPUTIL tool provided with the Windows NT Resource Kit utilities.

---

## Troubleshooting Other TCP/IP Problems

This section describes how to troubleshoot other problems with TCP/IP.

### Windows 98 does not retain primary WINS server IP address.

If the setting for your primary WINS server IP address is not retained when you reboot, check that a secondary WINS server IP address is also configured. If not, add a secondary WINS server IP address.

### Windows 98 does not send DHCP request packet.

If the DHCP key in the registry contains eight MAC address entries, Windows 98 cannot create a new entry for the current session and will not send a DHCP request packet. If this happens, use the Registry Editor to remove all keys except for the Dhcpinfo00 key from the following registry entry:

**HKEY_LOCAL_MACHINE\System**
    **\CurrentControlSet\Services\VxD\DHCP**

Then restart the computer.

### Windows 98 detects an IP address conflict.

If your Windows 98 computer uses static IP addressing (described in the section "Manually Configuring IP Addresses" earlier in this chapter) and you receive a message that Windows 98 has detected an IP address conflict, another computer on the network is using the same IP address and you must change the IP address.

▶ **To change your IP address**

1. In Control Panel, double-click Network.

2. Click your TCP/IP protocol.

3. Click the **Properties** button.

4. Click the **IP Address** tab.

5. Configure the protocol to use a different IP address that is not already in use on the network.

### Cannot log on to Windows NT domain.

If you cannot log on to a Windows NT domain, check that your computer uses NetBIOS name services. Windows 98 needs NetBIOS name services to log on to a Windows NT domain.

### IP address connects but host names do not.

Verify that the Hosts file and DNS settings have been configured for the computer by checking settings on the **DNS Configuration** tab.

- If you are using a Hosts file, verify that the DNS host name of the remote computer is identical—especially in terms of spelling and capitalization—to the name in the file and the application using it.

- If you are using DNS, verify that the IP addresses of the DNS servers are correct and in proper order. Use **ping** with the remote computer, and type both the host name and IP address to determine if the host name is resolved properly.

Use the **netstat -a** command to show the status of all activity on TCP and UDP ports on the local computer. A good TCP connection is usually established with 0 bytes in the send and receive queues. If data is blocked in either queue or if the state is irregular, there might be a problem with the connection. If not, you are probably experiencing network or application delays.

### Connect times are long after adding to LMHosts.

You might experience long connect times with a large LMHosts file if there is an entry at the end of the file. If so, mark the entry in LMHosts as a preloaded entry by following the mapping with the #PRE tag, or place the mapping higher in the LMHosts file. Then use the **nbtstat -R** command to update the local name cache immediately. The LMHosts file is parsed sequentially to locate entries without the #PRE keyword. You should place frequently used entries near the top of the file, and place the #PRE entries near the bottom.

### You see a message stating computer is unable to connect to a server.

This message appears if name resolution fails for a particular computer name. If the computer is on the local subnetwork, confirm that the target server name is spelled correctly and that the target server is running TCP/IP. If the computer is not on the local subnetwork, be sure that its name and IP address mapping are available in the LMHosts file or the WINS database. If all TCP/IP elements appear to be installed properly, use **ping** with the remote computer to be sure that its TCP/IP software is working.

Use the **nbtstat -n** command to determine what name (or names) the server registered on the network. The **nbtstat** command can also display the cached entries for remote computers from either #PRE entries in LMHosts or recently resolved names. If the remote computers are using the same name for the server, and the other computers are on a remote subnetwork, be sure that they have the computer's mapping in their LMHosts files.

# Correcting Problems with NetBEUI and IPX/SPX

This section describes problems that might occur with the NetBEUI and IPX protocols.

### You cannot connect using NetBEUI

- Use **net diag** to test for NetBIOS connectivity over the LANA that NetBEUI is using. If it fails, check the transceiver type, cabling, and adapter.
- Check the NetBEUI protocol bindings.
- Verify that routing is not involved.

### A NetBIOS application fails to start

This might be because the application is hard-coded to use the protocol on LANA 0 (such as Lotus Notes). You can force a particular protocol to always occupy LANA 0 by selecting it as the default protocol, as described in "Setting LAN Adapter Numbers" earlier in this chapter.

### You cannot connect using the IPX/SPX-compatible protocol

Verify that both computers trying to connect are using the same frame type and that other settings are correct for this protocol.

- Verify the following in the **Advanced** tab of the **IPX/SPX-compatible Protocol Properties** dialog box, as described in "Configuring the IPX/SPX-compatible Protocol" earlier in this chapter:

  - The correct frame type is set. The recommended setting is Auto, but this frame type only checks SAP broadcast traffic on the network and might be selecting an incorrect frame type in a mixed frame-type environment.

  - Source Routing is enabled and a cache size is set if needed.

  - The option named Force Even Length Packets is set properly. NetWare servers with older NetWare Ethernet drivers or older IPX routers may require even-sized packets. If required, change this setting to make sure the computer transmits only even-length IPX frames.

- On the IPX routers, check the setting for Type 20 Packets (NetBIOS packets). When using NetBIOS over IPX, the IPX packet type is set to 14h (decimal 20). Manufacturers of routers might consider all NetBIOS traffic as being nonroutable LAN traffic even when carried over the routable IPX protocol, and so, by default, will not pass Type 20 NetBIOS IPX packets. To use NetBIOS over IPX connectivity, Type 20 packet passing must be enabled on the router.

- Use **net diag** to test for IPX connectivity over the related LANA number used by NetBIOS over IPX.

- Use System Monitor to view statistics for the IPX/SPX-compatible protocol. Then retry network operation and check the activity. If there is none, remove and reinstall the protocol, and then retry and retest the operation.

# Correcting Connection Problems with Microsoft 32-bit DLC

This section describes common problems you might encounter while using the 32-bit DLC protocol.

### Windows 98 reports a Dlchlp error message.

This error message appears if you have removed or renamed your Autoexec.bat file, or removed the reference to Dlchlp.exe from your Autoexec.bat file. To correct this error, add the Dlchlp.exe entry to your Autoexec.bat file.

### Setting 32-bit DLC as the default protocol does not change the LANA number for NetBIOS protocols.

The 32-bit DLC protocol does not use a LANA number, so there is no reason to set DLC as the default protocol.

### The 32-bit DLC protocol does not bind to the Dial-Up adapter.

Currently, the Microsoft 32-bit DLC protocol cannot bind to the Dial-Up adapter. When the Dial-Up adapter is installed and you then install the 32-bit DLC protocol, the 32-bit DLC protocol appears to be bound to the Dial-Up adapter. However, after you restart your computer, Windows 98 removes the binding. This is by design.

### You cannot use Extra SAPs and Extra Stations settings.

Manual configuration of Extra SAPs and Extra Stations is no longer necessary with the Microsoft 32-bit DLC protocol.

### After removing an adapter driver, programs cannot connect to the host.

When your computer is configured with multiple network adapters, removing an adapter driver may prevent the DLC program from connecting properly to the host. The connection fails when the removed network adapter driver is the adapter for which the DLC program is configured. To prevent this problem, if the DLC program is configured for the primary adapter, make sure the CCB Adapter Num is set to 0. If the DLC program is configured for the alternate (or secondary) adapter, make sure the CCB Adapter Num is set to 1. The 32-bit DLC protocol allows CCB2 adapter numbers 0 through F.

### You cannot connect to the host over Ethernet after adding the 32-bit DLC protocol.

The most common issues you will face when using the DLC protocol on Ethernet are problems with bit swapping and Ethernet DIX. Check to see whether the host uses frame type 802.3 or Ethernet DIX 2.0, and whether address swapping is required on your network. For more information about configuring the 32-bit DLC protocol, see "Configuring the 32-bit DLC Protocol" earlier in this chapter.

**After you have installed the 32-bit DLC protocol on a token-ring network adapter, Windows 98 stops responding.**

Sometimes a token-ring network adapter has an RcvBufsize setting that is too small for the size of the frame being sent across the wire. If this happens, restart Windows 98 in Safe Mode, and increase the RcvBufSize setting for the network adapter driver. For more information about the appropriate settings for your network adapter, see the documentation for your network adapter. For information on getting to Safe Mode, see Chapter 27, "General Troubleshooting."

# Correcting Connection Problems with Microsoft 16-bit DLC

If you encounter problems using the real-mode Microsoft DLC protocol, check the following items:

- When adding the Microsoft DLC protocol, make sure that there is only one **net start** entry in Autoexec.bat. Setup adds an entry for Microsoft DLC, even if an entry already exists. Also, make sure that Autoexec.bat is configured properly, as described in "Installing and Configuring Real-Mode Microsoft DLC" earlier in this chapter.

- Do not make direct entries or changes in Protocol.ini for Microsoft DLC. Instead, make all changes in the **Advanced** properties for Microsoft DLC by using the Network option in Control Panel. If you make changes directly in Protocol.ini, the next time you change any values by using the Network option in Control Panel, all settings in Protocol.ini for Microsoft DLC will be overwritten.

- Some terminal emulation applications use TSRs to communicate with the Microsoft DLC protocol. If your emulation application uses a TSR that runs from Autoexec.bat, make sure that the entry for the TSR still exists (usually, the TSR entry occurs after the **msdlc** and **net start** lines). Windows 98 Setup removes or comments out many TSRs.

- The option named **Set This Protocol To Be The Default Protocol** in the **Advanced** properties for Microsoft DLC does not provide any functionality. This option should not be checked, because Microsoft DLC does not use LANA settings.

- Real-mode Microsoft DLC is an NDIS 2 protocol, so the network adapter must have an NDIS 2-compatible network adapter driver for use with Windows 98. Windows 98 includes many compatible drivers, but some Windows 98 drivers for certain PCI and PC Cards do not have a corresponding NDIS 2 driver to allow loading real-mode Microsoft DLC.

## Additional Resources

| For more information about | See this resource |
|---|---|
| Conceptual information about TCP/IP | *Networking with Microsoft TCP/IP* by Drew Heywood (New Riders Publishing, 1996). |
| Network adapters and protocols | *Microsoft Windows NT Server Networking Guide for Microsoft Windows NT Server version 4.0.* |
| | See also the *Network Supplement for Microsoft Windows NT Server version 4.0.* |
| GQoS specification | **ftp://microsoft.com/bussys/winsock/winsock2/** |
| Requests for Comments (RFCs) and Internet drafts | **http://www.ietf.org/** |
| TCP/IP White Paper | **http://www.microsoft.com/win32dev/netwrk/** |
| TCP/IP and Dial-Up Networking shareware and technical information | **http://www.download.com/** |
| | **http://www.shareware.com/** |
| | **http://www.tucows.com/** |
| | **http://www.windows95.com/** |

CHAPTER 19

# Remote Networking and Mobile Computing

**19**

This chapter describes how to use Dial-Up Networking and virtual private networking (VPN) to access a network from a remote location. It also describes how other Windows 98 mobile computing tools, such as Briefcase and Direct Cable Connection, can be used to connect to desktop computers or the network. This chapter benefits network administrators who need to install remote access service on clients and servers, implement virtual private networking, or add mobile computing features to clients on the network. It also explains to advanced users how to use Dial-Up Networking, virtual private networking, and mobile computing features.

**In This Chapter**

**See Also**

- For information about network protocols, see Chapter 15, "Network Adapters and Protocols."

- For information about setting up modems and Integrated Services Digital Network (ISDN) devices, see Chapter 21, "Modems and Communications Tools."

- For information about connecting to the Internet, see Chapter 20, "Internet Access and Tools."

# Overview of Remote Networking and Mobile Computing

Dial-Up Networking, virtual private networking (VPN), and mobile computing allow users not directly connected to the network to work as if they were. *Dial-Up Networking* allows them to make a dial-up connection to remote networks such as the Internet over a telephone or ISDN line. *Virtual private networking* allows users to connect securely to resources on a remote network by "tunneling" over an intermediary network (an existing Internet or local area network [LAN] connection) to a server on the remote network. The intermediary network is used as a substitute for a network wire, enabling you to connect to a server on a remote network even if you are not directly connected to the remote network. Finally, *mobile computing* tools allow intermittently-connected users to access network resources more easily.

Windows 98 Dial-Up Networking allows you to use a computer running Windows 98 as a dial-up client. From a remote site, you can use Dial-Up Networking to connect to a remote access server such as Windows NT version 3.1 or later Remote Access Service (RAS), a Windows 98 dial-up server, a Windows 95 dial-up server, any Point-to-Point Protocol (PPP) server, Novell NetWare Connect version 1.0 or 1.1, or Shiva NetModem or LanRover, using the IP, IPX, and NetBEUI protocols. If the client and server are running the same network protocols, the dial-up client can connect to the network to access its resources. For information about using Windows 98 Dial-Up Networking to dial in to other remote access servers, or using other remote access software to dial in to Windows 98, contact your network vendor or software supplier.

**Note** A Microsoft Windows NT Client Access License is required if the computer will be connecting to servers running Windows NT Server. For information, see Chapter 16, "Windows 98 on Microsoft Networks," or contact your Microsoft reseller.

Dial-Up Networking also allows you to designate a computer running Windows 98 as a single-connection dial-up server. A remote user can dial in to the dial-up server and access resources on the dial-up server.

For clients running the IPX or the NetBEUI protocol, the dial-up server can be used to provide access to the network. However, if you need a dial-up server that provides access to the network using Transmission Control Protocol/Internet Protocol (TCP/IP), you should use a Windows NT Server. For more information about the capabilities of the Windows 98 dial-up server, see "Configuring and Using the Windows 98 Dial-Up Server" later in this chapter.

Windows 98 provides the following tools to help users stay as functional as possible with the limited resources of a mobile site:

- Briefcase allows users to update documents on a portable computer with source documents on a desktop computer or network.

- Direct Cable Connection allows users to connect a portable computer to a desktop computer to synchronize files and share other resources.

- Microsoft Outlook Express provides remote access to electronic mail.

- Deferred printing allows users to generate print jobs when no physical printer is available.

# Overview of Dial-Up and Virtual Private Networking

Windows 98 includes the following enhancements to Dial-Up Networking:

- Client support for a single virtual private networking connection.

- Support for ISDN modems and adapters.

- Multilink capabilities.

- Connection-time scripting to automate nonstandard logons.

- Improved performance and stability.

This section provides an overview explanation of how you can use these enhancements and other Dial-Up Networking features for remote access. For information about ISDN, see Chapter 21, "Modems and Communications Tools."

With Dial-Up Networking and virtual private networking, you can connect from a remote site to a computer that has been configured as a remote access server, or connect to a network through the remote access server. For example, as Figure 19.1 shows, if you connect to a Windows NT Remote Access Server, you can access its shared resources (if the Microsoft File and Printer Sharing service has been enabled), or you can use it as a gateway to a network that is running the TCP/IP, IPX/SPX, and NetBEUI network protocols.

**Figure 19.1    Connecting to a remote access server**

Figure 19.1 illustrates two types of connections: a dial-up connection and a virtual private network connection through the Internet. You would use either the dial-up connection or the virtual private network connection to access those resources.

---

**Note**  You can also access shared resources by connecting to a Windows 98 dial-up server. For a description of the capabilities and limitations of the Windows 98 dial-up server, see "Configuring and Using the Windows 98 Dial-Up Server" later in this chapter.

---

As Figure 19.2 shows, a Windows 98 dial-up client can connect to a wide variety of networks, because Windows 98 supports a variety of connection and network protocols.

**Figure 19.2    Connecting to remote networks**

With virtual private networking, you can connect to remote servers not only over telephone lines, but also over Internet connections and the corporate intranet. This provides the following benefits:

**Inexpensive remote access**  With virtual private networking, remote users can connect to your company's network from the Internet instead of over a telephone line, so you do not need to maintain modem pools or pay long-distance charges. Your network must have a Windows NT Remote Access Server (RAS) virtual private networking server  and a dedicated connection to the Internet, such as a 56Mbits, fractional T-1, T-1 connection. Users simply dial in to their local Internet Service Providers (ISPs) and then connect to the RAS VPN server over the Internet.

**Secure access to private data**  In Windows, 98, virtual private networking is implemented using Point-to-Point Tunneling Protocol (PPTP). Because PPTP is a secure protocol, only authenticated users can gain access to your dial-up server. Also, you can encrypt data transfer to prevent Internet intruders from listening in.

**Private addressing schemes** Using certain types of routers and gateway servers, it is possible to connect your network to the Internet so that all your computers and their IP addresses are visible on the Internet. However, this configuration presents two drawbacks. First, your computers are vulnerable to attack by intruders on the Internet. Second, you must obtain IP addresses that conform to the Internet addressing scheme. Using virtual private networking, on the other hand, you can configure all the computers on your private intranet by using a private addressing scheme that does not need to conform to the Internet addressing scheme. The VPN server then shields the internal addresses from the rest of the Internet. The IP addresses of the computers on your private intranet remain hidden, providing additional security for those computers.

Different remote access servers provide different security systems to protect access to a network. The Windows 98 dial-up server uses pass-through (user-level) or share-level security as described in "Configuring Security Options for a Windows 98 Dial-Up Server" later in this chapter.

Dial-Up Networking uses the Windows 98 communications architecture to communicate through a modem to a network. It initializes the modem, determines device status, and dials the telephone number by using the telephony application program interface (TAPI) and the Unimodem driver. For more information about the communications architecture and the Dial-Up Networking architecture, see Chapter 29, "Windows 98 Network Architecture."

A Windows 98 Dial-Up Networking configuration includes the components described in the following sections

## Dial-Up Client

With Dial-Up Networking, you can configure a remote computer running Windows 98 as a dial-up client to dial in to a remote access server. A dial-up client, running the appropriate connection protocol, can connect to many types of remote access servers, including the following:

- Windows NT 3.51 or later Server computer.
- Windows NT 3.51 or later Workstation computer.
- Windows 98 dial-up server.
- Windows 95 dial-up server.
- Windows for Workgroups version 3.11.
- NetWare Connect 1.0 or 1.1.
- Any network access server that supports PPP (including NetWare Connect 2.0).
- Any UNIX server that runs Serial Line Internet Protocol (SLIP) or PPP.

# Connection Protocols

Connection protocols control the transmission of data over the wide-area network (WAN). A Windows 98 dial-up client can use the following connection protocols to connect to a remote access server:

- PPP.
- Novell NetWare Connect 1.0 and 1.1.
- Windows NT 3.1 or Windows for Workgroups RAS (Asynchronous NetBEUI).
- SLIP.

The type of connection protocol you choose depends on the server you are connecting to. Some connection protocols support a subset of the common network protocols. For example, PPP allows you to connect to a network server or a computer running Windows 98 with TCP/IP, IPX/SPX-compatible, or NetBEUI network protocols.

This section describes the connection protocols.

**Point-to-Point Protocol**  Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. It has become the standard for remote access because of its flexibility, password encryption security, and compatibility with future client and server hardware and software. A dial-up client running PPP can connect to a network running IPX, TCP/IP, or NetBEUI protocols. Windows 98 dial-up clients can use PPP to connect to any remote access server running PPP, including Windows NT Server version 3.51 or later. PPP is the default protocol for the Microsoft Dial-Up adapter.

**Novell NetWare Connect**  NetWare Connect 1.0 and 1.1 is a proprietary connection protocol. It allows a computer running Windows 98 to connect directly to a NetWare Connect 1.0 or 1.1 server and, if running a NetWare-compatible network client, connect to NetWare servers.

Windows 98 can connect to NetWare Connect 2.0 using PPP. For information about PPP, see "Technical Notes for PPP-Compatible Servers" later in this chapter.

---

**Note**  Windows 98 can act only as a client for connecting to a NetWare Connect 1.0 or 1.1 server. NetWare Connect 1.0 or 1.1 clients themselves cannot directly connect to a Windows 98 dial-up server through a dial-up connection.

---

### RAS for Windows NT 3.1 or Windows for Workgroups 3.11 (Asynchronous NetBEUI)

Asynchronous NetBEUI is used to connect computers running Windows 98 to remote access servers running Windows NT Server 3.1 LAN Manager, or Windows for Workgroups 3.11. It is also supported by Windows NT Server 3.5 and later. The remote access server must also be running NetBEUI.

**Serial Line Internet Protocol**  SLIP is an older remote access standard that is typically used by UNIX remote access servers. Use SLIP only if your site has a UNIX system configured as a SLIP server for Internet connections. The remote access server must be running TCP/IP.

Windows 98 does not provide SLIP server capabilities; SLIP is used for client dial-out only.

## Local Area Network Protocols

Windows 98 makes it easy to configure dial-up clients to access a network. When you install Dial-Up Networking, any protocols already installed on the computer are automatically enabled for Dial-Up Networking. Windows 98 includes support for TCP/IP, IPX/SPX, and NetBEUI network protocols.

---

**Note**  In Properties for your Dial-Up Networking connection, all network protocols show up as automatically enabled. However, remember that you cannot use them unless they have actually been installed on your computer. For information about how to install network protocols, see Chapter 15, "Network Adapters and Protocols."

---

The following list presents the combinations of protocols you can use to run either Windows Sockets or NetBIOS applications on a network.

| Connection protocol | Network protocols (APIs) |
| --- | --- |
| NetWare Connect 1.0 or 1.1 | IPX/SPX (Windows Sockets/NetBIOS) |
| PPP | TCP/IP (Windows Sockets/NetBIOS) <br> IPX/SPX (Windows Sockets/NetBIOS) <br> NetBEUI (NetBIOS) |
| RAS for Windows NT 3.1 or Windows for Workgroups 3.11 | NetBEUI (NetBIOS) |
| SLIP | TCP/IP (Windows Sockets/NetBIOS) |

Figure 19.3 shows the protocols Dial-Up Networking clients can use to connect to host servers and to remote networks.



**Figure 19.3   Connection protocols**

# Dial-Up Server

You can designate a computer running Windows 98 a single-connection dial-up server. If both the server and the client are running IP, IPX, or NetBEUI, the dial-up server can provide access to its shared resources. If both the server and the client are running IPX or NetBEUI, the dial-up server can act as a gateway to a network running the same protocol. For more information about the capabilities of the Windows 98 dial-up server, see "Configuring and Using the Windows 98 Dial-Up Server" later in this chapter.

## Using Software and Hardware Compression to Transfer Data

To improve the throughput and transfer times when you use Dial-Up Networking, Windows 98 supports dynamic compression of information when you are connected to another computer that also supports compression—for example, a computer running Windows 98 or Windows NT.

You do not need to perform any special configuration to enable hardware and software compression. Software compression on the client is enabled by default and is available for PPP connections. You should leave it enabled. Hardware compression is also enabled by default and is performed by the modem. You should leave it enabled. For more information about hardware compression, see Chapter 21, "Modems and Communications Tools."

## Using Data Encryption for Dial-Up Clients

You do not need to perform any special configuration to enable data encryption on dial-up clients. This option can be required by either the server or the client. For instructions on how to configure a Dial-Up connection so that the dial-up client will refuse to connect to a server that does not support data encryption. For instructions, see "Configuring a Dial-Up Connection," later in this chapter.

Data encryption requires that the client and server share a common key, which is generated at connection time using Microsoft Challenge Handshake Authentication (MS-CHAP).

## Security Options for Dial-Up Clients and Servers

Dial-Up Networking servers can be configured with either user-level or share-level security. Additionally, a Dial-Up Networking client can be configured to use encrypted passwords if the server it is connecting to supports that feature. For more information, see "Configuring Security Options for a Windows 98 Dial-Up Server" later in this chapter.

# Planning for Dial-Up and Virtual Private Networking

To use Dial-Up Networking to connect to the Internet or a remote network, you need the following hardware:

- One or more compatible modems or ISDN devices, as described in Chapter 21, "Modems and Communications Tools."
- Enough available hard disk space to install Dial-Up Networking. Currently, about 2 to 3 MB of free disk space are required to install the client and server portions of Dial-Up Networking.

In most cases, you will need the same hardware to use virtual private networking to connect to a remote network through the Internet. If you will be connecting to a remote network through a VPN server on your corporate network and you will never make a dial-up connection, you will not need a modem or ISDN device, but you will need a network adapter that is physically connected to the LAN.

To use a Dial-Up Networking client to connect to the network, you need to decide the following:

- The kind of remote access server remote users will connect to. For example, a Windows 98 dial-up server allows only 1 remote connection at a time, whereas a Windows NT Server 3.5 or later remote access server allows 256 connections. Depending on the size and needs of your network, you might configure a Windows 98 dial-up client to connect to a Windows NT Server 3.5 or later remote access server or another remote access server. For a list of the types of remote access servers that a Windows 98 dial-up client can be configured to connect to, see "Dial-Up Client" earlier in this chapter.

- The type of connection protocol your dial-up client will use to connect to the remote access server. Windows 98 provides support for PPP, RAS for Windows for Workgroups 3.11 and Windows NT 3.1, NetWare Connect 1.0 and 1.1, and SLIP. The dial-up client and the remote access server must both be running the same connection protocol. For a complete list of protocol types, see "Connection Protocols" earlier in this chapter.

- The kind of network protocol to install on the dial-up client to connect the client to the network. Windows 98 dial-up clients support IPX/SPX, TCP/IP, and Microsoft NetBEUI protocols. For more information about network protocols and Dial-Up Networking, see "Local Area Network Protocols" earlier in this chapter.

If you want to add a Windows 98 dial-up server to your network, you need to decide the following:

- Which computers on the network will function as Windows 98 dial-up servers.

- Whether you want to connect the client to the network and what kind of network protocol you need to install on the dial-up server. Windows 98 dial-up servers support only the IPX/SPX and Microsoft NetBEUI protocols; to use TCP/IP to connect the client to the network, you must use a Windows NT Server instead of a Windows 98 dial-up server.

- The level of security you need for dial-up servers. You can enable either user-level or share-level security on a Windows 98 dial-up server. For more information, see "Configuring Security Options for a Windows 98 Dial-Up Server" later in this chapter.

# Installing Dial-Up Networking

By default, Windows 98 Setup automatically installs Dial-Up Networking, other communications tools, and most of the components you need to connect to a network. Table 19.1 shows the communications tools that appear in the **Add/Remove Programs** option in Control Panel. For information about which of these tools are installed by default under the Typical, Portable, Compact, or Custom installations, see Chapter 2, "Setting Up Windows 98."

**Table 19.1    Communications tools available in Windows 98**

| Tool | Purpose |
| --- | --- |
| Dial-Up Networking | Allows a Windows 98 computer to access a network or the Internet from a remote location. |
| Dial-Up Server | Gives a Windows 98 computer the ability to provide remote access to a single dial-up client. |
| Direct Cable Connection | Allows you to establish a direct serial or parallel cable connection between two computers. |
| HyperTerminal | Provides file transfer and terminal emulation capabilities. |
| Infrared | Allows a Windows 98 computer to communicate with other computers or the network using infrared. |
| Microsoft Chat 2.0 | Allows you to chat with people on a chat server. |
| Microsoft NetMeeting | Allows you to call people on the Internet or a corporate intranet and talk, share applications, draw on a shared whiteboard, or share files and messages. |
| Phone Dialer | Allows a Windows 98 computer to make voice calls. |
| Virtual private networking | Allows a Windows 98 computer to connect securely to a remote server over telephone lines, the Internet, or a corporate intranet. |

If you want to add an additional component, you must install it after running Windows 98 Setup.

▶  **To add an additional component**

1. In Control Panel, double-click **Add/Remove Programs,** and then click the **Windows Setup** tab.

2. Double-click **Communications** in the list of components.

3. Select the component.

4. Click **OK,** and then click **Apply.**

Windows 98 Setup also installs most of the components you need to connect to a network. For example, Windows 98 installs the Microsoft Dial-Up adapter, connection protocols, and the Microsoft TCP/IP network protocol if TCP/IP has not already been installed on the computer.

**Note** If you are upgrading from Windows 3.1 or Windows for Workgroups, Setup does not upgrade your phonebook entries (your connection information). You must reenter all connection information. However, if you are upgrading from Windows 95, Setup does upgrade your connection information.

However, Windows 98 Setup does not automatically install network protocols such as IPX/SPX and NetBEUI. If you need to use those protocols but they are not already installed on your computer, you must install them.

To verify that the correct protocols are installed, in Control Panel, double-click Network, and then check the list of installed components.

For information about adding protocols, see Chapter 15, "Network Adapters and Protocols."

# Configuring and Using Dial-Up Networking Clients

Configuring computers as Dial-Up Networking clients consists of four tasks:

- Running the Install New Modem Wizard to install a modem.
- Configuring Telephony Dialing Properties.
- Running the Make New Connection Wizard in Dial-Up Networking to set up a connection to a remote access server for the dial-up client.
- Optionally, configuring the connection by selecting the remote access server type it will connect to, and by choosing whether to log on to the network after connecting to the remote access server. Selecting the server type automatically enables the correct connection protocol, such as PPP or SLIP.

This section explains how to perform these four tasks.

## Installing a Modem

If you have not already installed a modem, the Install New Modem wizard appears when you start Dial-Up Networking. It guides you through the process of installing a modem. For more information about modems, see Chapter 21, "Modems and Communications Tools."

# Configuring Telephony Dialing Properties

After the Install New Modem wizard installs your modem, a **Location Information** dialog box appears. This dialog box asks for such information as what country you are in and what area code you are in. Windows 98 uses this information to establish a dialing rule (called a *dialing location*). Whenever you dial a call, Windows 98 uses this dialing rule to automatically adjust your dialing string. For example, if you enter "425" as your area code in the **Location Information** dialog box, then later try to dial the number "425-555-1212," Windows 98 adjusts the dialing string to "555-1212."

If you have a portable computer and frequently dial from different places, you might also want to use the Dialing Properties utility to create different dialing locations for each place. You can also define calling card rules that you can use with one or more of your dialing locations.

---

**Note**  The information you entered in the **Location Information** dialog box also appears in the Dialing Properties utility, as your default dialing location.

---

The remainder of this section describes how to establish and use different calling locations using the Dialing Properties Utility. For more information about the Dialing Properties utility, including how to define calling card rules, see "Using Dialing Properties" in Chapter 21, "Modems and Communications Tools."

The Dialing Properties utility allows you to define different locations from which you dial. For each location, enter your country code, area code, and other information about the place you are dialing from. You can then dial a number using Dial-Up Networking, and Windows 98 automatically adjusts your dialing string based on the location from which you are calling.

For example, suppose you commonly dial from two different places:

- **Your home** in the 206 area code region. You do not need to dial an outside line, but you dial **\*70** for each call to disable call waiting.
- **Your office** in the 801 area code region. To reach an outside line, you must dial **9**.

You can create two different locations (home and office) and enter area code and other information for each location. Then, whenever you make a dialing location, Dialing Properties automatically adjusts the telephone number based on the place you are calling from.

For example, suppose you have defined a Dial-Up Networking Connection to your ISP at 206-555-5555.

If you are dialing from home, Dialing Properties adjusts the telephone number to *70,555-5555. But if you are dialing from your office, Dialing Properties changes the telephone number to 9,1-206-555-5555.

You can access Dialing Properties from several different places, including the Modems icon in Control Panel, the Telephony icon in Control Panel, and the connection you are dialing.

▶ **To define a new dialing location**

- In Dialing Properties, enter the name of your new dialing location, the area code you are dialing from, and other information about your location. Optionally, enter information about your calling card. This information will then be available to any Dial-Up Networking connection that you create.

▶ **To use the dialing location**

1. When you configure the General properties for a Dial-Up Networking connect (described in "Configuring General Properties" later in this chapter), make sure that the check box "**Use area code and Dialing Properties**" is selected.

2. When you dial the connection (described in "Making a Dial-Up Networking Connection" later in this chapter), make sure that you have selected the correct dialing location.

## Defining a Dial-Up Networking Connection

When you first start Dial-Up Networking, the Make New Connection Wizard appears. You can define two different types of remote connections:

- A dial-up connection allows you to use modems or ISDN devices to connect to the Internet or your intranet.

- A VPN connection uses two connections. With the first connection, you use a network adapter, modem, or ISDN device to connect to a remote access server on the Internet or your intranet. With the second connection, you can "tunnel through" the first connection to a VPN tunnel server, in order to gain access to any server that the VPN tunnel server allows you to access.

Before creating a new dial-up connection, you should install a modem, ISDN device, or network adapter. If you have not yet installed a modem and did not install a modem when Dial-Up Networking started, you can install one by using the Install New Modem Wizard in the Modems option in Control Panel. For information about modems and ISDN devices, see Chapter 21, "Modems and Communications Tools."

Additionally, if you are configuring a VPN connection, you must first install virtual private networking. To do so, follow the procedure "To add an additional component" described in "Installing Dial-Up Networking" earlier in this chapter.

▶ **To create a Dial-Up Networking connection using the Make New Connection Wizard**

1. From My Computer, double-click the Dial-Up Networking folder.

2. In the **Dial-Up Networking** window, double-click the Make New Connection icon.

3. In the **Type a name for the computer you are dialing** dialog box, enter a name for your connection.

4. If you are creating a dial-up networking connection, in the **Select a device** box select a modem or ISDN device.

   –Or–

   If you are creating a VPN connection, in the **Select a device:** box select **Microsoft VPN Adapter**.

5. If you are creating a dial-up networking connection, the Make New Connection Wizard prompts you for information about your connection, such as a name for the computer you are dialing, modem type, area code, telephone number, and country code.

   –Or–

   If you are creating a VPN connection, the Make New Connection Wizard prompts you for the host name or address of the VPN server.

6. The new icon for your connection appears in the **Dial-Up Networking** window. You need to provide this information only once for each connection you define.

   Once a connection has been established, remote network access becomes transparent to the user.

## Configuring a Dial-Up Connection

The Dial-Up Networking defaults for the dial-up connection are designed for Internet connections and for most other types of connections. You can change these defaults, but you should do so only if you want to change the default behavior.

There is one exception. By default, Dial-Up Networking uses the PPP protocol to connect to servers. This default will work for most Internet connections and many other types of connections. But if you are connecting to a server that does not use PPP, you must change the server type by following the procedure in "Configuring Options for the Server to Which You Are Connecting" later in this chapter.

You can configure the following options:

- General properties
- Server properties
- Scripting
- Multilink

You can predefine Dial-Up Networking connections for users by including them as part of system policies. If you enable user profiles, different users sharing the same computer can use separate dialing configurations. For more information, see Chapter 7, "User Profiles," and Chapter 8, "System Policies."

## Configuring General Properties

This section describes how to configure basic options for a dial-up connection.

▶ **To configure general properties for the connection**

1. In Dial-Up Networking, right-click a connection icon, and then select **Properties** from the **File** menu.

2. Review the information on the **General** tab to ensure that the telephone number is correct and that the correct modem or ISDN device is selected. Ensure that **Use area code and Dialing Properties** is selected if you have defined one or more dialing locations as described in "Configuring Telephony Dialing Properties" earlier in this chapter. Make any necessary changes.

3. Click **Configure**, and then click the **Options** tab.

4. Optionally, click **Bring up terminal window before dialing** or **Bring up terminal window after dialing**. For modem connections, these options allow you to use a terminal window for an interactive logon session with the server.

## Configuring Options for the Server to Which You Are Connecting

Dial-Up Networking allows you to configure options for the server to which you are connecting. You do not need to change any values in this section if you are connecting to an ISP and your ISP's remote access server supports PPP.

▶ **To configure options for the server to which you are connecting**

1. In Dial-Up Networking, right-click a connection icon, and then click **Properties**.

2. Click the **Server Types** tab.

3. In the **Type of Dial-Up Server** box, ensure that the correct remote access server type is selected. If it is not selected, you will not be able to connect to the server. The possible connections are as follows:

| This server type | Connects to |
| --- | --- |
| PPP: Internet, Windows NT Server, Windows 98 | The default; selecting it allows Windows 98 to automatically detect and connect to other remote access servers that are running TCP/IP, NetBEUI, or IPX/SPX over PPP. Select this option for connections to your ISP. |
| NRN: NetWare Connect version 1.0 and 1.1 | Novell NetWare Connect 1.0 or 1.1 running IPX/SPX over NetWare Connect 1.0 or 1.1. |
| SLIP: UNIX Connection | Any SLIP server over TCP/IP. |
| Windows for Workgroups and Windows NT 3.1 | Windows 98 dial-up server; Windows NT 3.1 or 3.5; Windows for Workgroups version 3.11 running NetBEUI over RAS. |
| CSLIP: UNIX Connection with IP Header Compression | Any SLIP server over TCP/IP that supports IP header compression. |

4. Optionally, if you are making a connection to an ISP, deselect **Log on to network** to speed connection time. This option is selected by default, but it is unnecessary for Internet connections.

5. Optionally, select **Require encrypted password**. If this option is selected, the client will use only Challenge Handshake Authentication Protocol (CHAP) and MS-CHAP encryption when generating a password. If this option is not selected, the client can also perform Password Authentication Protocol (PAP) if the server requests it. However, PAP encryption is less secure. For more information about encryption, see "PPP Dial-Up Sequence" later in this chapter.

6. Optionally, select **Require data encryption**. If this option is selected, the client will refuse to connect with any server that does not use data encryption. However, most ISPs do not support data encryption. For more information, see "Using Data Encryption for Dial-Up Clients," earlier in this chapter.

7. Optionally, select **Record a log file for this connection**. If this option is selected, Dial-Up Networking will create a PPP log file that shows information about your connection. For information about PPP log files, see "PPP Log File" later in this chapter.

8. In the **Allowed network protocols** box, ensure that the network protocols used on the target network are selected. For example, if you are configuring a connection to the Internet, ensure that TCP/IP is selected.

---

**Note**  By default, all network protocols (TCP/IP, IPX/SPX, and NetBEUI) are selected in the **Allowed network protocols** box. However, for you to use those protocols, they must also be installed on the client workstation you are configuring. For information about how to install protocols, see Chapter 15, "Network Adapters and Protocols."

---

9. Optionally, if you are configuring a connection to your ISP and your ISP requires you to enter information such as a static IP address for your computer or a DNS server to which you must connect, click **TCP/IP Settings**. However, in most cases you do not need to do so. For more information, see Chapter 20, "Internet Access and Tools."

## Configuring Scripting for Modem Connections

Windows 98 supports scripting on modem connections (not on ISDN or VPN connections.) In most cases, you do not need to create a script. Many ISPs do not require a manual logon, and ISPs that do require a manual logon almost always provide a script file you can use. Contact your ISP for more information.

However, if you need and do not have a logon script, you can create one. Windows 98 provides four sample scripts you can use as starting points. The sample scripts are located in your **\Program Files\Accessories** directory. Windows 98 also includes a document that explains how to write and modify logon scripts. The file is called Script.doc and located in your Windows directory.

After you have created a script, save it in your **\Program Files\Accessories** directory, using the file extension SCP.

---

**Important**  Microsoft does not support logon scripts you create. Also, Microsoft does not support modifications to the four sample scripts.

---

After you have created the script, you must configure scripting for each connection that will use the script. Make sure your connection is working properly before you configure scripting.

▶ **To configure scripting for the Windows 98 dial-up client**

1. In Dial-Up Networking, right-click a connection icon, and then click **Properties**.

2. Click the **Scripting** tab, and then click **Browse** .

3. Locate the script, and then click **Open**.

4. Optionally, select the **Step through script** box.

   Selecting the **Step through script** box enables you to step through the script to verify that each line is working correctly, or to troubleshoot the script if the connection fails.

5. Click **OK**.

## Configuring Multilink

The PPP Multilink protocol allows you to use two or more devices (such as modems or ISDN devices) for a single dial-up link. With Multilink, you combine the bandwidth capabilities of both devices, thus inexpensively increasing the bandwidth on your dial-up connections. This section describes how to use Multilink. For additional information about Multilink, and for information about ISDN, see Chapter 21, "Modems and Communications Tools."

The Windows 98 PPP Multilink implementation complies with the Internet Engineering Task Force (IETF) PPP Multilink standard defined by Request for Comments (RFC) 1717.

Before using Multilink, consider the following issues:

- Multilink is available only for Windows 98 dial-up clients, not for the Windows 98 dial-up server.

- The server or ISP you connect to must also support PPP Multilink. Otherwise, Multilink will not function correctly.

- You can use Multilink only when your computer is configured with multiple devices that can be combined to form the logical PPP pipe over the communication link.

- For best performance, the devices you use should be the same speed.

- When you combine both B channels under ISDN, you cannot use your second channel for other applications, such as fax or voice calls.

▶ **To configure Multilink for the Windows 98 dial-up client**

1. In Dial-Up Networking, right-click your connection icon, and then click **Properties**.

2. Click the **Multilink** tab.

3. Select **Use additional devices**.

4. Click **Add.**

5. Specify the additional device you wish to use.

6. If you need to edit an entry, click **Edit.**

▶ **To use Multilink**

- After you have configured Multilink, click the connection icon and click **Connect**. Dial-Up Networking connects using the primary device, then the secondary device.

▶ **To view information about your link**

1. Click the Dial-Up Networking icon displayed on your taskbar.

2. In the dialog box, click **Details**.

# Configuring a Connection to the Internet

To configure a Windows 98 Dial-Up Connection to dial the Internet, follow the procedures outlined in "Configuring and Using Dial-Up Networking Clients" earlier in this chapter. Keep in mind the following issues:

- Before you begin, check to make sure TCP/IP is correctly installed on your computer.

- If you want to use a terminal window for an interactive logon session with the server, in the modem's Properties, click **Bring up terminal window before dialing** or **bring up terminal window after dialing**.

- If you are using SLIP instead of PPP to connect to the Internet, in the **Server Types** dialog box, select **SLIP: UNIX Connection**.

- If you want to speed your connection time, in the **Server Types** dialog box, deselect **Log on to network**. This option is not necessary for Internet connections.

- If your ISP requires you to enter information such as an IP address for your computer or the IP address of a DNS server, enter this information in the **Server types** dialog box. In most cases, you will not need to enter information here. For more information, see Chapter 20, "Internet Access and Tools."

# Making a Dial-Up Networking Connection

After you have defined a remote connection by using the Make New Connection Wizard, you can make a connection.

---

**Note**  If you selected **Use area code and Dialing Properties** in the General Properties for your connection, Dial-Up Networking automatically adjusts the dialing string (telephone number) according to your dialing location (the place you're dialing from). For more information about your dialing location, see "Configuring Telephony Dialing Properties" earlier in this chapter.

---

▶ **To make a Dial-Up Networking Connection**

1. Double-click its connection icon in the Dial-Up Networking folder.

2. Optionally, enter a user name and password.

3. If you selected **Use area code and Dialing Properties** in the General Properties for your connection, in the **Dialing from** area, ensure that you have selected the correct dialing location (the place you are dialing from). If necessary, select another dialing location or click **Dial properties** to define a new dialing location.

After a connection has been made, a connection icon appears in the system tray. You can double-click this icon to see information about the connection, such as the server type it is using, the protocols it is using, and whether it is using authentication and compression.

---

**Note**  If you are using PPP to connect to the remote server and you are dialing in to an IPX network, you will lose IPX connectivity to your local network. Thus, after you make a dial-up networking connection, NetWare servers on the local network will no longer be visible.

You might also lose IP connectivity to your local network if you are dialing in to an IP network. For specific details and for ways to restore IP connectivity, see "Technical Notes on Dial-Up and Virtual Private Networking" later in this chapter.

---

Dial-Up Networking starts automatically in certain circumstances, through an autodial feature included in Dial-Up Networking and an autodial feature included in the Internet Explorer 4 browsing software. The following sections describe the two features.

## Using the Dial-Up Networking Autodial Feature

Dial-Up Networking provides an autodial feature. If autodial is enabled, Windows 98 starts Dial-Up Networking when you try to perform one of the following tasks:

- You try to access a network resource when your computer is not connected to any network.

- You try to access a network resource that you have accessed before using Dial-Up Networking.

- Your application specifies a UNC name (which uses the form \\servername\ sharename) that cannot be accessed by using the network.

**Note**  The Dial-Up Networking autodial feature is separate from the Internet Explorer browsing software autodial feature, described below.

When you choose a remote connection, Windows 98 retrieves the server information from the addresses stored in the registry. If the information is not available, you are asked to select a server from the connection icons in Dial-Up Networking, or to type a new server name.

If Dial-Up Networking cannot find the network resource, it displays a network error message. If the connection is successful, Windows 98 remembers the connection for future use.

You can disable the prompt that asks if you want to use Dial-Up Networking when you are attempting to connect to a network resource.

▶  **To disable the Dial-Up Networking prompt**

1. In Dial-Up Networking, click the **Connections** menu, and then click **Settings**.

2. Click **Don't prompt to use Dial-Up Networking**.

## Using the Internet Explorer Browsing Software Autodial Feature

The Internet Explorer browsing software includes an autodial feature that can automatically start Dial-Up Networking while you are browsing. When you start the Internet Explorer browsing software or try to access a URL that is not locally available, and you have not already established a Dial-Up Networking connection, a dialog box appears and asks you if you want to use Dial-Up Networking.

> **Note** The Internet Explorer autodial feature is separate from the Dial-up Networking autodial feature, described above.

The Internet Explorer browsing software starts Dial-Up Networking only if you have a modem and you have configured the Internet Explorer browsing software to automatically start Dial-Up Networking.

The following procedure shows how to do so.

▶ **To configure the Internet Explorer browsing software to automatically start Dial-Up Networking**

1. In Control Panel, double-click Internet, and then click the **Connection** tab.

2. In the **Connection** box, select **Connect to the Internet using a modem**.

3. Optionally, click the **Settings** box to specify a particular Dial-Up Networking connection and to enter information about that connection.

The following procedure shows how to configure the Internet Explorer browsing software to not start Dial-Up Networking.

▶ **To configure the Internet Explorer browsing software to not start Dial-Up Networking**

1. In Control Panel, double-click Internet, and then click the **Connection** tab.

2. In the **Connection** box, select **Connect to the Internet using a local area network**.

# Configuring and Using the Windows 98 Dial-Up Server

With Dial-Up Networking, you can configure a computer running Windows 98 to be a remote access server for dial-up clients running Windows 98, Windows 95, Windows for Workgroups, or Windows 3.1, or any other client running PPP. The Windows 98 dial-up server can act as a server to the client, sharing its file and printer resources with one dial-up client at a time. Both the dial-up server and the dial-up client must be running the same protocol (IP, IPX, or NetBEUI). The Windows 98 dial-up server can also act as a gateway to an IPX/SPX or NetBEUI network, as long as both the client and the server are using the same protocol that is used on the network.

The Windows 98 dial-up server supports software compression. It also works with ISDN; however it can use only one B channel.

A Windows 98 dial-up server differs from the Windows NT 3.5 and later dial up servers in the following ways:

- Windows NT Server 4.0 and later can act as a VPN server; Windows 98 cannot.

- Windows NT Server 3.5 and later can act as an IP router; Windows 98 cannot. IP router capabilities permit access to a TCP/IP network, such as the global Internet. Windows 98 provides all the protocols you need to connect to the Internet but cannot act as an IP router.

- Windows NT Server 3.5 and later support 256 remote connections, whereas Windows 98 provides one remote connection.

A Windows 98 dial-up server with the appropriate network protocols installed can act as a NetBIOS gateway, as shown in Figure 19.4.



Figure 19.4   Dial-up server as NetBIOS gateway

Configuring a computer running Windows 98 to be a dial-up server consists of the following steps:

- Installing the Dial-Up Server, as described in "Installing a Windows 98 Dial-Up Server," later in this chapter.

- Optionally, enabling file and printer sharing services for either Microsoft or NetWare networks on the dial-up server. Perform this step only if you want the dial-up server to share files with the dial-up clients. For more information, see Chapter 18, "Logon, Browsing, and Resource Sharing."

- Enabling user-level or share-level security on the dial-up server. For information, see "Configuring Security Options for a Windows 98 Dial-Up Server" later in this chapter.

- Configuring the server type for the dial-up server, as described in the section "Configuring the Server Type for the Dial-Up Server" later in this chapter.

After you perform the steps previously listed, your Dial-Up Server will be ready to answer incoming calls.

▶ **To disconnect any users who are currently connected to this computer through Dial-Up Networking**

- In the **Dial-Up Server** dialog box, click **Disconnect User**.

---

**Note**  The Dial-Up Server for Windows 98 can use only one modem at a time. You can enable caller access on multiple modems at any one time, but only one modem can be connected.

---

## Installing a Windows 98 Dial-Up Server

In Windows 98, the Dial-Up Server is not automatically installed. To install it, follow this procedure.

▶ **To install the Dial-Up Server**

1. In Control Panel, double-click **Add/Remove Programs**, and then click the **Windows Setup** tab.

2. In **Add/Remove Programs Properties**, double-click **Communications**.

3. Select the **Dial-Up Server** check box, and then click **OK**, and then click **OK** again.

## Configuring Security Options for a Windows 98 Dial-Up Server

Dial-Up Networking gives you the option of requiring a password to connect to the remote access server, depending on whether the Windows 98 dial-up server is protected with share-level or user-level security.

- Share-level security assigns a password to the Windows 98 dial-up server. When users dial in, they must provide the password before they can gain access to the server. After the connection is established, users can browse the resources on the dial-up server, subject to whatever level of security has been applied to them. Users can also log on to the network after connecting to the dial-up server if logging on to the network is enabled on the dial-up client. Because users can distribute passwords, this method is less secure than user-level security.

- User-level security restricts access to a network resource until a security provider, such as a Windows NT domain controller or a NetWare server, authenticates the request. You can require that a user's logon password to a remote access server be the same as the network and Windows 98 logon passwords.

  With user-level security, when the user accesses shared resources on the dial-up server, Windows 98 controls a user's rights to the shared resources, such as whether the user has read-only access or full access to files. Access rights are specified in the sharing properties for each resource protected by user-level security. For more information, see Chapter 9, "Security," and Chapter 18, "Logon, Browsing, and Resource Sharing."

The following procedure assumes that you have completed the installation procedure described in the previous section, "Installing a Windows 98 Dial-Up Server."

▶ **To configure the dial-up server for user-level security**

1. Make sure that your computer has file and printer sharing services installed and that user-level security is enabled. For more information, see Chapter 18, "Logon, Browsing, and Resource Sharing."

2. In Dial-Up Networking, click the **Connections** menu, and then click **Dial-Up Server**.

3. In the **Dial-Up Server** properties, click **Allow caller access**, and then click **Add**.

4. In the **Add Users** dialog box, specify the users who will have permission to access the dial-up server, and then click **OK**.

5. In the **Dial-Up Server** properties, click **Server Type**, and make sure **Require encrypted password** is checked if your Dial-Up client supports encrypted passwords.

   Clicking the **Require encrypted password** option requires the client to send an encrypted as opposed to a text password. Some clients support only text passwords; however, encrypted passwords are preferred. Clearing this option does not disable password protection.

▷   **To configure the dial-up server for share-level security**

1. Make sure that your computer has File and Printer Sharing services installed and that share-level security is enabled. For more information, see Chapter 18, "Logon, Browsing, and Resource Sharing."

---

**Note**  Share-level security is not available on NetWare networks.

---

2. In Dial-Up Networking, click the **Connections** menu, and then click **Dial-Up Server**.

3. In the **Dial-Up Server** dialog box, click **Allow caller access**, and then click **Change Password** to provide password protection for the Dial-Up Server.

4. Optionally, to require password encryption, click **Server Type**. In the **Server Type** dialog box, make sure **Require encrypted password** is checked, and then click **OK**.

## Configuring the Server Type for the Dial-Up Server

This section explains how to configure the server type for the dial-up server. It assumes that you have already followed the procedures in the sections "Installing a Windows 98 Dial-Up Server" and "Configuring Security Options for a Windows 98 Dial-Up Server," earlier in this chapter.

▷   **To configure a computer as a dial-up server**

1. From the **Connections** menu in the Dial-Up Networking folder, click **Dial-Up Server**.

2. Click **Server Type**, and then select the server type.

   Make sure that the server type is the same for both the dial-up server and the dial-up client. If the dial-up client uses PPP, you can also select the Default server type. If you select the Default server type, the dial-up server will automatically start in PPP mode for incoming calls and switch to Windows for Workgroups and Windows NT 3.1 if the PPP negotiation fails.

3. Click **OK**, and the dial-up server is ready to answer incoming calls.

Notice that changes to the server type do not apply to a currently open connection. Changes will apply to any future connections made to this computer.

## Disabling Dial-Up Server Support

You can disable dial-up server support in several different ways. You can disable it from within Dial-Up Networking, as the following procedure explains.

▶ **To disable the dial-up server on a single computer**

1. From the **Connections** menu in the Dial-Up Networking window, click **Dial-Up Server**.

2. In the **Dial-Up Server** dialog box, click **No caller access**.

You can also completely remove Dial-Up Server capabilities from a user's computer by using the Add/Remove Programs option in Control Panel.

Finally, you can disable dial-up support on each computer or on a system-wide basis by using System Policy Editor to change a single computer's registry or to define policies that can be shared by multiple computers.

To disable dial-up support by using System Policy Editor, click **Disable Dial-in**. The **Dial-Up Server** menu option still appears on the **Connections** menu after dial-up support has been disabled, but no dialog box for setting up the dial-up server will appear. For more information, see Chapter 8, "System Policies."

# Configuring and Connecting to Remote Servers

With Dial-Up Networking, you can connect to many different kinds of servers. This section discusses how to connect to and configure a Windows NT Remote Access Server and a Novell NetWare Connect 1.0 or 1.1 server. It also provides technical information about PPP-compatible servers.

## Connecting to a Windows NT Remote Access Server

Connecting to a Windows NT remote access server is the same as connecting to a Windows 98 Dial-Up Networking server. All you need is the telephone number of the Windows NT server when creating a connection. Dial-Up Networking negotiates the proper protocols and server connection type. You do not need to specify a default server type.

### Planning the Connection to a Windows NT Remote Access Server

Windows NT Server 3.5 and later remote access servers support PPP and RAS clients. PPP is the recommended protocol. Windows NT Server 3.5 and later support IPX/SPX, NetBEUI, and TCP/IP network protocols and can function simultaneously as a NetBIOS gateway, IPX router, and IP router. Windows NT Server 4.0 and later can act as a VPN server, so you can set up a VPN connection to Windows NT 4.0 RAS servers using the PPTP protocol.

**Note**  Windows NT 3.1 supports only the RAS protocol, which is a proprietary protocol that supports only NetBEUI. It is a fast connection type but does not allow for multiple protocols over the connection. RAS in Windows NT 3.1 cannot support the IPX/SPX or TCP/IP protocols.

Microsoft recommends that you upgrade from Windows NT RAS to Windows NT Server 3.5 or later, which provides many additional benefits, including PPP support.

A Windows NT 3.5 or later remote access server provides several features that a Dial-Up Networking server does not. For an explanation of these differences, see "Configuring and Using the Windows 98 Dial-Up Server" earlier in this chapter.

For more information about Windows NT remote access servers, see the *Microsoft Windows NT Server Networking Guide* in the *Microsoft Windows NT Server Resource Kit* (for Microsoft Windows NT Server version 4.0). See also the *Networking Supplement* for Windows NT Server version 4.0.

## Configuring a Windows NT Server for Windows 98 Dial-Up Clients

To configure a computer running Windows NT Server 3.5 or later so that Windows 98 dial-up clients can remotely access it, you need to install and configure RAS.

You must be logged on as a member of the Administrators group to install and configure RAS. It can be installed during Custom Setup of Windows NT or afterward. During Express Setup, if there is not a network adapter in a computer, you are given the option to install RAS.

RAS installation varies slightly depending on which network protocols are installed. If you use TCP/IP or IPX/SPX protocol with RAS, you should install the protocol before you install RAS, although selecting a protocol that is not installed causes that protocol to be installed at the conclusion of RAS Setup. For information about installing either protocol, see the *Networking Supplement* for Microsoft Windows NT Server 4.0.

For information about installing RAS, see the *Microsoft Windows NT Server Resource Kit* (for Microsoft Windows NT version 4.0).

**Note**  Microsoft does not recommend granting guest accounts dial-in permission. If you do, be sure to assign a password to the guest account.

# Connecting to a Novell NetWare Connect 1.0 or 1.1 Server

Windows 98 Dial-Up Networking supports connecting to Novell NetWare resources in three ways:

- Connecting directly to a Novell NetWare Connect 1.0 or 1.1 server.
- Connecting directly to a Novell NetWare Connect 2.0 server. NetWare Connect 2.0 uses the PPP protocol, so you can connect to a NetWare Connect 2.0 server as you would to any other PPP server.
- Using a computer running Windows 98 or Windows NT 3.5 or later as a gateway into a network where NetWare servers are connected.

NetWare Connect 1.0 or 1.1 allows a Windows 98 client to dial in to a NetWare server running NetWare Connect 1.0 or 1.1

---

**Note** Windows 98 can act only as a client for connecting to a NetWare Connect 1.0 or 1.1 server. NetWare Connect 1.0 or 1.1 clients themselves cannot dial up a Windows 98 dial-up server.

---

The NetWare Connect 1.0 or 1.1 connection type allows a Windows 98 client to connect directly to a NetWare Connect 1.0 or 1.1 server and to connect to NetWare servers on the connected network.

To use Dial-Up Networking to connect to a NetWare Connect 1.0 server, you must specify NetWare Connect 1.0 as the server type in the properties for a Dial-Up Networking connection. You also need to use the Network option in Control Panel to make sure the following are enabled on a Windows 98 dial-up client or server:

- Microsoft Client for NetWare Networks.
- The IPX/SPX-compatible protocol bound to the Microsoft Dial-Up adapter driver.

If you use Dial-Up Networking to access NetWare Connect 1.0 or 1.1 servers, you can access data remotely, but you cannot control a computer remotely as you can with the NetWare Connect 1.0 or 1.1 client software supplied by Novell.
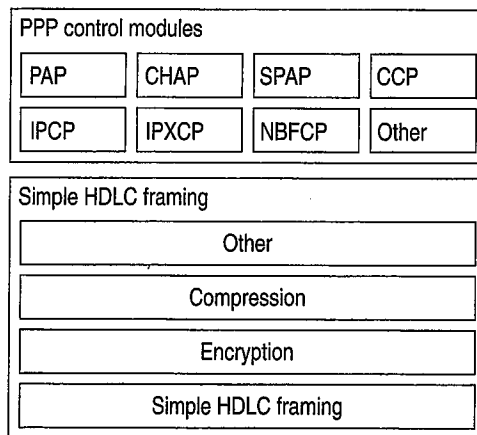
# Technical Notes for PPP-Compatible Servers

This section provides technical information about connecting to PPP-compatible servers. It covers the following topics:

- PPP architecture
- PPP dial-up sequence
- PPP log file

## PPP Architecture

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP does so by establishing and configuring different link and network-layer protocols to carry traffic from point to point. Control and data flow modules make up the PPP control protocols as illustrated in Figure 19.5.

```
┌─────────────────────────────────────────────────┐
│ PPP control modules                             │
│  ┌──────┐  ┌──────┐  ┌──────┐  ┌──────┐        │
│  │ PAP  │  │ CHAP │  │ SPAP │  │ CCP  │        │
│  └──────┘  └──────┘  └──────┘  └──────┘        │
│  ┌──────┐  ┌──────┐  ┌──────┐  ┌──────┐        │
│  │ IPCP │  │ IPXCP│  │ NBFCP│  │ Other│        │
│  └──────┘  └──────┘  └──────┘  └──────┘        │
└─────────────────────────────────────────────────┘

┌─────────────────────────────────────────────────┐
│ Simple HDLC framing                             │
│  ┌───────────────────────────────────────────┐ │
│  │                  Other                    │ │
│  └───────────────────────────────────────────┘ │
│  ┌───────────────────────────────────────────┐ │
│  │               Compression                 │ │
│  └───────────────────────────────────────────┘ │
│  ┌───────────────────────────────────────────┐ │
│  │               Encryption                  │ │
│  └───────────────────────────────────────────┘ │
│  ┌───────────────────────────────────────────┐ │
│  │           Simple HDLC framing             │ │
│  └───────────────────────────────────────────┘ │
└─────────────────────────────────────────────────┘
```

**Figure 19.5    Microsoft PPP control modules**

Figure 19.5 shows Password Authentication Protocol (PAP), Challenge Handshake Authentication (CHAP), and Shiva Password Authentication Protocol (SPAP), which perform password authentication of PPP clients. Compression Control Protocol (CCP) is used to negotiate encryption with PPP clients. IPCP, IPXCP, NBFCP, and Other are the Internet Protocol (IP), NetWare IPX, NetBIOS Extended User Interface (NetBEUI), and Other protocol modules, respectively, which control PPP client sessions. *HDLC* is the High-level Data Link Control protocol.

## PPP Dial-Up Sequence

When a user dials in to a PPP-compatible server, four things happen:

1. The Data Link Control Layer (HDLC) defines how data is encapsulated before transmission on the WAN. By providing a standard framing format, PPP ensures that various vendors' remote access solutions can communicate and distinguish data packets from each other. PPP uses HDLC framing for serial, ISDN, and X.25 data transfer.

   The PPP Data Link Control layer is a slightly modified version of the HDLC layer. The HDLC format, extensively used by IBM and others for synchronous data transfer, was modified by adding a 16-bit protocol field that allows PPP to multiplex traffic for several Network Control Protocol (NCP) layers. This encapsulation frame has a 16-bit checksum, but the size of the protocol field and address can be compressed.

2. Link Control Protocol (LCP) establishes, configures, and tests the integrity of the data-link connection. LCP also negotiates which authentication protocol (listed in step 3) will be used. When LCP negotiates authentication of protocols, it determines what level of security validation the remote access server can perform and what the server requires. LCP also determines whether Multilink will be used.

3. The authentication protocol negotiated by LCP is used. Any of the following authentication protocols can be used.

   - PAP uses a two-way handshake for the peer to establish its identity. This handshake occurs only when the link is initially established. With PAP, passwords are sent over the circuit in text format, which offers no protection from playback.

   - SPAP offers encryption of PAP passwords and Novell NetWare bindery access for user account information. When Windows 98 is set up for user-level security using a NetWare server account list, this is the security type used for remote access clients.

   - CHAP periodically verifies the identity of the peer, using a three-way handshake. The authenticator sends a challenge message to the peer. The peer returns the user name and an MD5 hash of the challenge, session ID, and client's password. The authenticator then checks this response and, if the values match, the authentication is acknowledged; otherwise, the connection is ended. CHAP provides protection against playback attack, because the challenge value changes with every message. Because the password is never sent unencrypted over the link, it is virtually impossible to learn it.

- MS-CHAP is an encrypted authentication mechanism similar to but more secure than CHAP. As with CHAP, the authenticator sends a challenge to the peer. The peer must return the user name and an MD4 hash of the challenge string, the session ID, and the MD4-hashed password. This design, which manipulates a hash of the MD4 hash of the password, provides an additional level of security because it allows the authenticator to store hashed passwords instead of clear-text passwords. MS-CHAP also provides additional error codes, including a password expired code, and additional encrypted client-server messages that permit users to change their passwords. In Microsoft's implementation of MS-CHAP, both the peer and the authenticator independently generate an initial key for subsequent data encryption. During phase 2 of PPP link configuration, the authenticator collects the authentication data and then validates the data against its own user database or against a central authentication database server.

4. After authentication, the client and server begin negotiating NCPs. NCPs establish and configure different network protocol parameters. The type of NCP that PPP selects depends on which protocol (NetBEUI, TCP/IP, or IPX) is being used to establish the Dial-Up Networking connection. Windows 98 supports the following:

- NetBIOS Frames Control Protocol (NBFCP) is used to configure, enable, and disable the NetBEUI protocol modules on both ends of the link. For information about NBFCP, see Request for Comments (RFC) 2097, "The PPP NetBIOS Frames Control Protocol."

- Internet Protocol Control Protocol (IPCP) is used to configure, enable, and disable IP protocol modules at both ends of the link. IPCP is defined in RFC 1332, "The PPP Internet Protocol Control Protocol (IPCP)"

- Internet Packet Exchange Control Protocol (IPXCP) is used to configure, enable, and disable IPX protocol modules on both ends of the link. IPXCP is widely implemented by PPP vendors. IPXCP is defined in RFC 1552, "The PPP Internetwork Packet Exchange Protocol (IPXCP)."

## PPP Log File

You can record how the PPP layers process a call by enabling the PPP log file. This file contains some of the basic layers and points of any Dial-Up Networking session, and is especially useful for monitoring PPP sessions. It is recorded and stored in the Windows directory.

Windows 98 improves over the PPP logging feature in Windows 95 in a few ways. It allows you to enable PPP logging per connection, rather than per adapter. Thus, you can enable PPP logging for only the connections you need, and you do not need to know which adapter is used for which connection. Also, you do not need to reboot for PPP logging to take effect. Moreover, PPP logging is more sophisticated in Windows 98 than in Windows 95. As the sample at the end of this section shows, with Windows 98, the PPP log shows the actual packets that are being passed.

▶ **To enable PPP logging for a connection**

1. In Dial-Up Networking, single-click a connection icon, and in the **File** menu, select **Properties**.

2. Click the **Server Types** tab.

3. Select the option named **Record a log file for this connection**.

The following example is sample content of a ppplog.txt file. This is only a partial log of a connection; it stops before authentication. For information about the format of PPP packets, see RFC 1662, "PPP in HDLC-like Framing."

```
03-19-1998 13:17:16.04 - Microsoft Dial Up Adapter log opened.
03-19-1998 13:17:16.04 - Server type is  PPP (Point to Point Protocol).
03-19-1998 13:17:16.04 - FSA : Adding Control Protocol 80fd (CCP) to
control protocol chain.
03-19-1998 13:17:16.04 - FSA : Protocol not bound - skipping control
protocol 803f (NBFCP).
03-19-1998 13:17:16.04 - FSA : Adding Control Protocol 8021 (IPCP) to
control protocol chain.
03-19-1998 13:17:16.04 - FSA : Protocol not bound - skipping control
protocol 802b (IPXCP).
03-19-1998 13:17:16.04 - FSA : Adding Control Protocol c029 (CallbackCP)
to control protocol chain.
03-19-1998 13:17:16.04 - FSA : Adding Control Protocol c027 (no
description) to control protocol chain.
03-19-1998 13:17:16.04 - FSA : Encrypted Password required.
03-19-1998 13:17:16.04 - FSA : Adding Control Protocol c223 (CHAP) to
control protocol chain.
03-19-1998 13:17:16.04 - FSA : Adding Control Protocol c021 (LCP) to
control protocol chain.
03-19-1998 13:17:16.04 - LCP : Callback negotiation enabled.
03-19-1998 13:17:16.04 - LCP : Layer started.
```

```
03-19-1998 13:17:16.05 - PPP : Transmitting Control Packet of length: 25
03-19-1998 13:17:16.05 - Data 0000: c0 21 01 01 00 17 02 06 | .!...•..
03-19-1998 13:17:16.05 - Data 0008: 00 0a 00 00 05 06 00 02 | ........
03-19-1998 13:17:16.05 - Data 0010: 50 17 07 02 08 02 0d 03 | P•......
03-19-1998 13:17:16.05 - Data 0018: 06 00 00 00 00 00 00 00 | ........
03-19-1998 13:17:19.05 - PPP : Transmitting Control Packet of length: 25
03-19-1998 13:17:19.05 - Data 0000: c0 21 01 02 00 17 02 06 | .!...•..
03-19-1998 13:17:19.05 - Data 0008: 00 0a 00 00 05 06 00 02 | ........
03-19-1998 13:17:19.05 - Data 0010: 50 17 07 02 08 02 0d 03 | P•......
03-19-1998 13:17:19.05 - Data 0018: 06 00 00 00 00 00 00 00 | ........
03-19-1998 13:17:22.05 - PPP : Transmitting Control Packet of length: 25
03-19-1998 13:17:22.05 - Data 0000: c0 21 01 03 00 17 02 06 | .!...•..
03-19-1998 13:17:22.05 - Data 0008: 00 0a 00 00 05 06 00 02 | ........
03-19-1998 13:17:22.05 - Data 0010: 50 17 07 02 08 02 0d 03 | P•......
03-19-1998 13:17:22.05 - Data 0018: 06 00 00 00 00 00 00 00 | ........
03-19-1998 13:17:22.11 - PPP : Received Control Packet of length: 8
03-19-1998 13:17:22.11 - Data 0000: c0 21 04 03 00 06 08 02 | .!......
03-19-1998 13:17:22.11 - LCP : Received configure reject for address
field compression option.
03-19-1998 13:17:22.11 - PPP : Transmitting Control Packet of length: 23
03-19-1998 13:17:22.11 - Data 0000: c0 21 01 04 00 15 02 06 | .!...•..
03-19-1998 13:17:22.11 - Data 0008: 00 0a 00 00 05 06 00 02 | ........
03-19-1998 13:17:22.11 - Data 0010: 50 17 07 02 0d 03 06 00 | P•......
03-19-1998 13:17:22.16 - PPP : Received Control Packet of length: 23
03-19-1998 13:17:22.16 - Data 0000: c0 21 02 04 00 15 02 06 | .!...•..
03-19-1998 13:17:22.16 - Data 0008: 00 0a 00 00 05 06 00 02 | ........
03-19-1998 13:17:22.16 - Data 0010: 50 17 07 02 0d 03 06 00 | P•......
03-19-1998 13:17:23.27 - PPP : Received Control Packet of length: 32
03-19-1998 13:17:23.27 - Data 0000: c0 21 01 00 00 1e 03 05 | .!...-..
03-19-1998 13:17:23.27 - Data 0008: c2 23 80 05 06 00 00 6e | .#.....n
03-19-1998 13:17:23.27 - Data 0010: 21 07 02 11 04 06 4e 13 | !.....N.
03-19-1998 13:17:23.27 - Data 0018: 09 03 00 80 5f e2 d8 a8 | ...._...
03-19-1998 13:17:23.27 - LCP : Received and accepted authentication
protocol c223 (CHAP).
03-19-1998 13:17:23.27 - LCP : Received and accepted magic number 6e21.
03-19-1998 13:17:23.27 - LCP : Received and accepted protocol field
compression option.
03-19-1998 13:17:23.27 - PPP : Transmitting Control Packet of length: 19
03-19-1998 13:17:23.27 - Data 0000: c0 21 04 00 00 11 11 04 | .!......
03-19-1998 13:17:23.27 - Data 0008: 06 4e 13 09 03 00 80 5f | .N....._
03-19-1998 13:17:23.27 - Data 0010: e2 d8 a8 00 00 00 00 00 | ........
03-19-1998 13:17:23.30 - PPP : Received Control Packet of length: 19
03-19-1998 13:17:23.30 - Data 0000: c0 21 01 01 00 11 03 05 | .!......
03-19-1998 13:17:23.30 - Data 0008: c2 23 80 05 06 00 00 6e | .#.....n
03-19-1998 13:17:23.30 - Data 0010: 21 07 02 00 00 00 00 00 | !.......
03-19-1998 13:17:23.30 - LCP : Received and accepted authentication
protocol c223 (CHAP).
03-19-1998 13:17:23.30 - LCP : Received and accepted magic number 6e21.
03-19-1998 13:17:23.30 - LCP : Received and accepted protocol field
compression option.
```

```
03-19-1998 13:17:23.30 - PPP : Transmitting Control Packet of length: 19
03-19-1998 13:17:23.30 - Data 0000: c0 21 02 01 00 11 03 05 | .!......
03-19-1998 13:17:23.30 - Data 0008: c2 23 80 05 06 00 00 6e | .#.....n
03-19-1998 13:17:23.30 - Data 0010: 21 07 02 00 00 00 00 00 | !.......
03-19-1998 13:17:23.30 - LCP : Layer up.
```

# Implementing Virtual Private Networking

Networking provides a way to connect a client computer to a server by means of a transmission medium such as a network wire or a dial-up connection. It contains three key elements: the client, the transmission media, and the server.

Similarly, virtual private networking (VPN) provides a way to connect a client computer to a server by means of a tunnel through an intermediary network. That is, it uses a network as a transmission medium. The virtual private network consists of the two computers (one at each end of the connection) and a route, or *tunnel*, over the public or private network.

For example, suppose you want to access the resources on your corporate LAN, but you have only an Internet connection. With virtual private networking, you can "tunnel through" the Internet to access resources on your corporate LAN.

In another example, suppose you are connected to your corporate LAN (LAN A), but you want to access the resources on a server on another LAN (LAN B). LAN A and LAN B are connected by means of a private TCP/IP network. With virtual private networking, you can tunnel through the private network to access the resources on the server on LAN A just as if you were directly connected to it.

In Windows 98, virtual private networking is implemented using the *Point-to-Point Tunneling Protocol* (PPTP). PPTP allows you to tunnel through TCP/IP-based data networks to securely access resources on remote servers. PPTP supports multiple network protocols (IP, IPX, and NetBEUI) and can be used for virtual private networking over public and private networks. You can use PPTP to provide secure, on-demand, virtual networks by using dial-up lines, LANs, WANs, or the Internet and other public, TCP/IP-based networks.

The networking technology of PPTP is an extension of the remote access PPP protocol defined in the IETF document "The Point-to-Point Protocol" (RFC 1661). PPTP is a network protocol that encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. PPTP can also be used in private LAN-to-LAN networking.

For more information about virtual private networking, visit Microsoft's Web site at **http://www.microsoft.com/communications/**. You can also download the IETF Internet draft "Point-to-Point Tunneling Protocol—PPTP" from **http://www.ietf.org/**.

# Planning for Virtual Private Networking

There are two common virtual private networking scenarios:

- You can connect your workstation to a remote network by making a Dial-Up Networking connection to a network access server at an ISP facility, and then tunneling through the Internet to a VPN server that is attached to both the Internet and the remote network. Once you are connected to the VPN server, you can transparently gain access to any public or private network that is connected to it.

- If you have a permanent IP connection to a VPN tunnel server (such as a LAN connection), you can use that VPN server to tunnel to any public or private network that is connected to it.

Some less common virtual private networking scenarios require a server provided by a third party. For instance, some VPN tunnel servers, called front end processors (FEPs), can be used for modem pooling. If your PC is on a network with a FEP that has modems available for dialing out, users can simply connect to that tunnel server, dial out, and establish a connection to a PPP access server on another network.

The following section describes the first scenario, in which you use the Internet as the network through which the client tunnels. However, keep in mind that you could use any TCP/IP network in place of the Internet. If so, you must have a permanent TCP/IP connection to a VPN server, and you do not need a dial-up connection to a network access server.

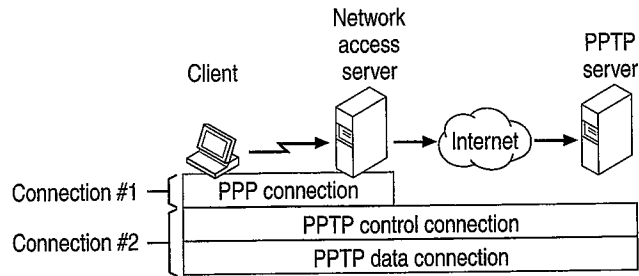## Typical Virtual Private Networking Deployment

A typical deployment of virtual private networking starts with a remote or mobile Windows 98 client that uses a local ISP to access the Internet. The client then tunnels through the Internet to a private enterprise LAN.

A Windows 98 client must make two connections to establish a VPN tunnel: one physical connection and one logical connection. Figure 19.6 shows these connections. The client first uses Dial-Up Networking and the remote access protocol, PPP, to connect to a network access server at an ISP's facility. Once connected, the client can send and receive packets over the Internet. The network access server uses the TCP/IP protocol for all traffic to the Internet.

**Note**  Network access servers are also referred to as dial-in servers, or point-of-presence (POP) servers.

**Figure 19.6   Creating a VPN tunnel**

The client then uses Dial-Up Networking to make a second logical connection over the existing PPP connection. Data sent using this second connection is in the form of IP datagrams that contain PPP packets, referred to as encapsulated PPP packets.
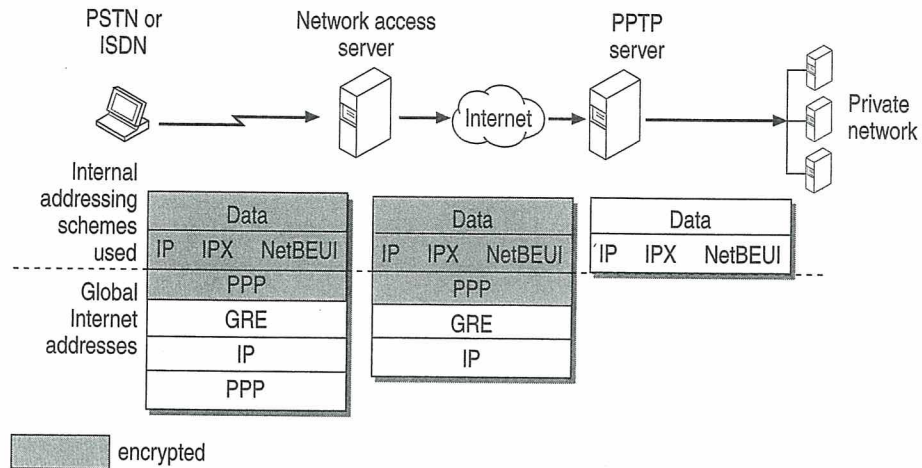
The second connection creates the VPN connection to a VPN server on the private enterprise LAN (a computer running Windows NT Server 4.0 and configured as a VPN server). This connection is referred to as a *tunnel*.

*Tunneling* is the process of sending packets to a computer on a private network by routing them over some other network, such as the Internet. The other network's routers cannot access computers on the private network. However, tunneling enables the routing network to transmit the packet to an intermediary computer, a VPN server that is connected to the both the routing network and the private network. Both the VPN client and the VPN server use tunneling to route packets securely to a computer on the private network by using routers that know only the address of the private network intermediary server.

When the VPN server receives the packet from the routing network, it sends it across the private network to the destination computer. The VPN server does this by processing the PPTP packet to obtain the private network computer name or address information in the encapsulated PPP packet. Note that the encapsulated PPP packet can contain multi-protocol data such as IP, IPX, or NetBEUI protocols. Because the VPN server is configured to communicate across the private network by using private network protocols, it is able to read multi-protocol packets.

Figure 19.7 illustrates the multi-protocol support built into virtual private networking. A packet sent from the VPN client to the VPN server passes through the VPN tunnel to a destination computer on the private network.

**Figure 19.7    Connecting a Dial-Up Networking VPN client to the private network**

PPTP encapsulates the encrypted and compressed PPP packets into IP datagrams for transmission over the Internet. The IP datagrams are created using a modified version of the Internet Generic Routing Encapsulation (GRE) protocol. (defined in RFCs 1701 and 1702).These IP datagrams are routed over the Internet until they reach the VPN server that is connected to both the Internet and the private network. The VPN server disassembles the IP datagram into a PPP packet and then decrypts the PPP packet. It then sends the de-encapsulated IP, IPX, or NetBEUI packet on the private network.

## Using Network Protocols with Virtual Private Networking

Virtual private networking allows you to create a tunnel over a public TCP/IP network but retain existing network protocols, network node addresses, and naming schemes on the private enterprise network. Thus, no changes to existing network configurations or network-based applications are required when using virtual private networking to tunnel across the Internet or other TCP/IP-based public networks. For example, IPX or NetBEUI clients can continue to run applications on the private network that require these protocols.

Name resolution methods used on the private network—such as Windows Internet Naming Service (WINS) for NetBIOS computers, Domain Name System (DNS) for TCP/IP host names, and Service Advertisement Protocol (SAP) for IPX networking—do not need to be changed.

---

**Note** The address and name resolution schemes on the private enterprise network must be correctly configured. If they are not, VPN clients are unable to communicate with computers on the private network.

---

## Virtual Private Networking Issues

Consider the following issues when using virtual private networking:

- A VPN server can be placed behind a firewall on the private enterprise network to ensure that traffic in and out of the private network over the VPN server is secured by the firewall computer. (For more information, visit **http://www.microsoft.com/communications/** and download "Understanding PPTP.")

- Using the Internet to establish a connection between a VPN client and a VPN server means that the VPN server must have a globally unique IP address that is valid for the global Internet. However, the encapsulated IPX, NetBEUI, or TCP/IP packets sent between the VPN client and the VPN server can be addressed to computers on the private enterprise network using private network addressing or naming schemes. The VPN server disassembles the PPTP packet from the VPN client and forwards the packet to the correct computer on the private network. For more information about private network addressing, see Chapter 15, "Network Adapters and Protocols."

# Configuring Virtual Private Networking

Depending on how you will be using virtual private networking, you will need to configure different types of connections.

If you have a permanent TCP/IP connection (such as a LAN connection) to a VPN tunnel server, and you want to connect to a remote network that is connected to your VPN server, you need only configure the connection to that VPN tunnel server.

If you want to connect your workstation to a remote server by tunneling through the Internet, you must configure two connections: a connection to the Internet through your ISP and a tunnel connection to the VPN server on the target network.

To configure the connection to your ISP or your VPN tunnel server, follow the procedures outlined in "Defining a Dial-Up Networking Connection" and "Configuring and Using Dial-Up Networking Clients" earlier in this chapter.

# Using Virtual Private Networking

This section describes how to use the two common VPN configurations.

**Note** If you are using PPP or PPTP to connect to another IPX network, you will lose IPX connectivity to your local network. Thus, after you make a dial-up or virtual private networking connection, you will no longer be able to see NetWare servers on the local network.

## Using Virtual Private Networking over the LAN to Connect to a Tunnel Server

VPN clients with a permanent IP connection to a VPN tunnel server can use VPN tunneling over that IP connection. For example, suppose that you are in a networked office environment and your network has a VPN tunnel server. You can then use that VPN server to tunnel to any private network that is connected to that VPN server, such as the personnel department's private network. Thus, you can create a virtual private network by using your direct LAN connection. Data sent from your VPN client to another computer on the LAN is encrypted and secure because you are using a VPN server to connect to the remote computer.

In the following scenario, the VPN client uses Dial-Up Networking over a LAN connection instead of a telephone line. Only one connection to the VPN server is required.

▶ **To connect to a VPN server over a LAN connection**

1. Double-click My Computer, and then double-click Dial-up Networking.
2. Click the icon that you have created for your VPN server.
3. Enter the user name and password required for the target network.
4. Click **Connect**.
5. You now have a connection to your VPN server.

---

**Note** The connection speed displayed is only an estimate. If you see a connection speed that seems too high or too low it will not impact performance and should not be cause for concern.
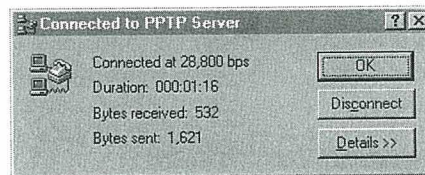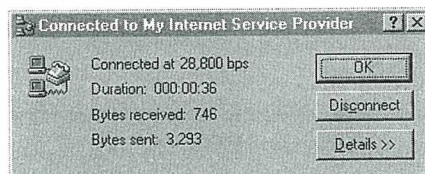
---

After you successfully connect to a VPN server, all traffic from your computer is first routed to your VPN server, which then forwards your data across the LAN to the remote computer. Your computer behaves as if it were physically connected to the remote network. While the tunnel is open, you continue to see computers and servers on your immediate LAN subnet. However, you might not be able to see hosts and servers on other subnets on your LAN. Contact your network administrator for more information.

## Dialing an ISP to Connect to a Virtual Private Networking Server

With virtual private networking, you can connect your workstation to a remote network by tunneling through the Internet to a VPN server on that network. To do so, you must make two connections. First, you must connect to the Internet through an ISP. Next, you must create a tunnel to the target network. This section explains how to make these connections.

▶ **To connect to the Internet**

1. In My Computer, double-click Dial-Up Networking.

2. Double-click the connection icon that was created for your ISP.

3. In the **Connect To** dialog box that appears, enter the user name and password required by your ISP, and then click **Connect**.

▶ **To connect to the target network using a tunnel to the VPN server**

1. After connecting to your ISP, click the icon that was created for your VPN server.

2. Enter the user name and password required for the target network.

3. In the **Connect To** window, click **Connect**.

You now have two connections, as seen in the two following similar boxes.

**Connected to My Internet Service Provider**   [?][X]

Connected at 28,800 bps        [ OK ]
Duration: 000:00:36
Bytes received: 746            [Disconnect]
Bytes sent: 3,293
                               [Details >>]

**Connected to PPTP Server**   [?][X]

Connected at 28,800 bps        [ OK ]
Duration: 000:01:16
Bytes received: 532            [Disconnect]
Bytes sent: 1,621
                               [Details >>]

After you connect successfully to the VPN server on the remote network, the ISP routes all traffic sent from your workstation over the Internet to the VPN server. The VPN server then routes the traffic to the correct computer on the remote network. Consequently, you see only computers and servers on the remote network. You no longer see the Internet unless the remote network itself provides access to the Internet.

# Virtual Private Networking Security

This section describes VPN security and discusses how to use virtual private networking with firewalls.

## Authentication

When you dial an ISP network access server (NAS), the NAS requires require initial dial-in authentication. This authentication is required only to log on to the NAS; it is not related to Windows NT-based authentication. Check with your ISP for their authentication requirements.

When you dial a VPN tunnel server to connect to a private network, the VPN server requires a standard Windows NT-based logon. Therefore, remote access logon using a computer running Windows 98 is as secure as logging on from a Windows-based computer connected to the local LAN.

Authentication of remote VPN clients is performed using the same PPP authentication methods used for any Dial-up Networking client dialing directly to a RAS server. Microsoft's implementation of Dial-up Networking supports the CHAP, MS-CHAP, and PAP authentication schemes.

## Access Control

After authentication, all access to a private LAN continues to use the Windows NT-based security model. Access to resources on NTFS drives or to other network resources requires the proper permissions.

For more information about using security on NTFS drives or other network resources, see your product documentation or the *Microsoft Windows NT Server Resource Kit* (for Microsoft Windows NT version 4.0).

## Data Encryption

For data encryption, virtual private networking uses the RAS "shared-secret" encryption process. Both the client and the server share a secret, the user's password. Both the client and the server uses the secret to generate an initial 40-bit encryption key, then uses the key to encrypt and decrypt all data that it passes over the Internet. When you are connecting to a Windows NT 4 RAS Server with Service Pack 4 or later, the key changes on every packet. For earlier versions of Windows NT 4, the key changes every 256 packets.

**Note** The process by which the client and server generate the initial key occurs only when MS-CHAP is used.

Users in the United States and Canada can obtain a 128-bit session key through a cryptography pack for use inside the US. Contact your Microsoft reseller for more information. When 128-bit encryption is used, the initial key is based on the password and a unique MS-CHAP challenge.

## PPTP Packet Filtering

To protect the VPN server from malicious attacks, you can enable PPTP filtering on the VPN server. With PPTP filtering, the VPN server on the private network accepts and routes *only* authorized, encrypted PPTP packets from authenticated users.

PPTP filtering is enabled on the VPN server. For step-by-step instruction on enabling PPTP filtering, see the white paper "Installing, Configuring, and Using PPTP with Microsoft Clients and Servers" at **http://www.microsoft.com/communications/**.

## Virtual Private Networking with Firewalls and Routers

PPTP traffic uses TCP port 1723, and IP protocol uses ID 47, as assigned by the Internet Assigned Numbers Authority (IANA). Virtual private networking can be used with most firewalls and routers by enabling traffic destined for TCP port 1723 and protocol 47 to be routed through the firewall or router.
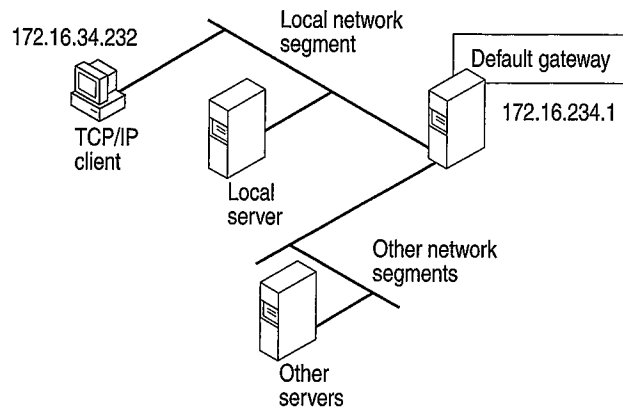
Firewalls ensure corporate network security by strictly regulating data that comes *into* the private network from the Internet. An organization can deploy a VPN server running Windows NT Server 4.0 behind its firewall. The VPN server accepts PPTP packets passed to the private network from the firewall and extracts the PPP packet from the IP datagram, decrypts the packet, and forwards the packet to the computer on the private network.

# Technical Notes on Dial-Up and Virtual Private Networking

In Windows 98, computers can be *multihomed*, or configured with multiple IP addresses. This enables them to connect to multiple networks that are physically separate, such as a corporate network and the Internet, with certain limitations. This section describes those limitations as they apply to Dial-Up Networking. For general information about multihoming, see Chapter 15, "Network Adapters and Protocols."

If you are connected to a LAN and you make a PPP dial-up connection or a VPN connection, you might lose connectivity to some of the servers on your LAN. Likewise, if you connect to the Internet, then make a VPN connection to another network, you might lose connectivity to the Internet itself.

This is because of the default routing changes that Dial-up Networking makes when setting up a connection. Clients on TCP/IP networks can send packets directly to hosts on their immediate network segment. However, to reach other network segments and other networks, they send their packets to a default gateway instead. That gateway then determines where to send the packets. Thus, clients can send packets to servers anywhere in a very large, complex network without having to know how to reach each server. Figure 19.8 shows how TCP/IP clients use default gateways.



**Figure 19.8    Default gateway for a TCP/IP client**

You can find out what your default gateway is by looking at the route table for your computer. The *route table* shows all the routes your computer uses to reach other computers on the network.

For more information about the route table and to see the complete route table for the network shown in Figure 19.8, see Chapter 15, "Network Adapters and Protocols."

▷  **To view the route table**

•  At the command prompt, type **route print**.

Table 19.2 shows a partial route table for the network shown in Figure 19.8.

**Table 19.2    Partial route table for TCP/IP client**

| Network address | Netmask | Gateway address | Interface | Metric |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 172.16.34.1 | 172.16.34.232 | 1 |
| ... | ... | ... | ... | ... |

Notice that the first line of the route table shows the address for the default gateway, and that it has a metric of 1. The *metric* indicates which gateway will be used and what the gateways that will be used if the first is removed from the route table. TCP/IP clients always use the default gateway with the smallest metric.

TCP/IP clients can be configured with several different default gateways. If one default gateway fails, the clients automatically switch to another. However, because TCP/IP clients always use the default gateway with the smallest metric, they cannot use more than one default gateway at a time.

Figure 19.9 shows what happens when you make a PPP dial-up connection to the Internet. Dial-Up Networking assigns a new default gateway, that of the PPP server. Because the client can use only one default gateway, it sends all network traffic through that gateway. You can no longer gain access to some of the servers on your LAN.
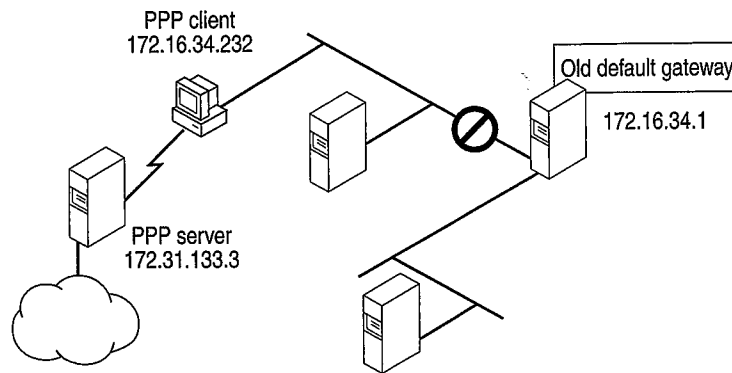


**Figure 19.9   New default gateway for PPP client**

The partial route table displayed in Table 19.3 shows what happens to the default gateway.

**Table 19.3   New partial route table for PPP client**

| Network address | Netmask | Gateway address | Interface | Metric |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 172.16.34.232 | 172.16.34.232 | 1 |
| 0.0.0.0 | 0.0.0.0 | 172.16.34.1 | 172.16.34.232 | 2 |
| ... | ... | ... | ... | ... |

The first line now shows the new default gateway for the PPP server, and the second line shows the old default gateway on your LAN. Because the old default gateway has a metric of 2, the TCP/IP stack does not use it.

If you need to reach servers on your network while connected to the Internet, you can manually add host routes to those servers. Use the **route** command to add a route manually to the gateway, IP subnet, or IP network you want to reach. For more information about adding routes, see Chapter 15, "Network Adapters and Protocols." See also the *Windows NT Server Networking Guide for Windows NT version 4.0*.

Finally, Figure 19.10 shows what happens when you make a VPN tunnel connection over the PPP connection. (For more information about PPP, see "Implementing Virtual Private Networking" earlier in this chapter.) Dial-Up Networking assigns a third default gateway to the VPN server, invalidating the first two default gateways. You lose access not only to servers on your LAN but to hosts on the Internet.



**Figure 19.10    New default gateway for PPTP client**

The partial route table displayed in Table 19.4 shows the default gateways.

**Table 19.4    New partial route table for VPN client**

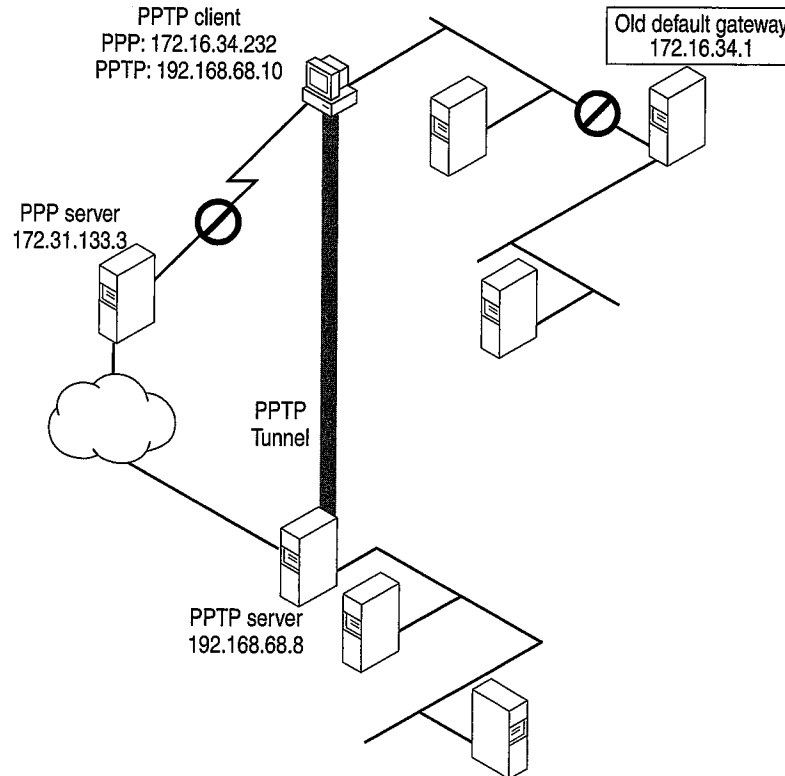| Network address | Netmask | Gateway address | Interface | Metric |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.68.10 | 192.168.68.10 | 1 |
| 0.0.0.0 | 0.0.0.0 | 172.16.34.232 | 172.16.34.232 | 2 |
| 0.0.0.0 | 0.0.0.0 | 172.20.232.1 | 172.20.234.232 | 2 |
| ... | ... | ... | ... | ... |

If you want to regain lost connectivity to servers on your local network or to the Internet, you have the following options:

- You can manually add host routes to servers on your network, as described in Chapter 15, "Network Adapters and Protocols."
- For VPN connections, you can disable the default gateway to the VPN tunnel server. You must then add routes to the virtual private network.

The following procedure describes how to disable the default gateway to the VPN tunnel server. After you disable the default gateway, you might need to configure routes to servers on the remote network. However, you do not need to configure a route to the VPN tunnel server, because Dial-Up Networking automatically assigns a host route to that server.

▶ **To disable the default gateway to the VPN tunnel server**

1. In the Dial-Up Networking folder, right-click the VPN server connection icon, and then click **Properties**.
2. Click the **Server Types** tab.
3. Click **TCP/IP Settings**.
4. Clear the **Use default gateway on remote networks** check box.

Dial-up Networking automatically creates a host route to the VPN tunnel server, so you can still reach it.

# Using Windows 98 Mobile Computing Features

You can be productive away from the office by using the following Windows 98 mobile computing tools:

**Windows 98 Briefcase**  Briefcase allows you to update documents on a portable computer with source documents on a desktop computer or network, thus minimizing the task of keeping track of the relationships between files on a portable computer and on a desktop computer. With Briefcase, you can simultaneously update related files.

**Direct Cable Connection**   Direct Cable Connection (DCC) allows you to establish a connection between two computers quickly and easily by using a parallel cable, a null-modem serial cable, or an infrared connection. After the connection is established, Direct Cable Connection facilitates the transfer of files from the host computer to the guest computer. The host can act as a gateway to an IPX/SPX or NetBEUI network for the guest.

**Infrared**   Windows 98 supports infrared devices, so you can wirelessly connect a laptop or a computer to infrared cameras, other computers, or printers. Infrared works with file sharing tools such as Direct Cable Connection, so you can quickly and easily take a laptop with you wherever you go and then update files on a standalone computer or the network.

**Deferred printing**   Windows 98 supports deferred printing, which allows you to generate print jobs when you are not connected physically to a printer. The print jobs are stored until a printer becomes available. Windows 98 detects the printer connection and automatically spools the print jobs in the background. For information, see Chapter 11, "Printing, Imaging, and Fonts."

**Internet Mail and News**   With Outlook Express, you can dial into your internet service provider and download your e-mail from an IMAP4 or POP3 server. You can also download news from your newsgroups located on an NNTP server. For information, see Chapter 22, "Electronic Mail with Outlook Express."

Other mobile computing tools, such as the following, help you manage a portable computer's limited battery power and disk space:

- With Advanced Power Management, you can use the battery indicator on the taskbar and a **Suspend** command on the **Start** menu to save power without turning off your computer. For more information, see Chapter 30, "Hardware Management."

- With DriveSpace, you can free space on their portable computer's hard disk drive and floppy disks by compressing them. For more information, see Chapter 10, "Disks and File Systems."

- With Outlook Express, you can view the headers of mail messages before deciding whether to download, preventing unnecessary messages from taking up disk space.

- With Quick View, you can view the contents of a file in Windows Explorer by right-clicking a file icon. For information, see Chapter 25, "Application Support."

# Using Direct Cable Connection

With Direct Cable Connection, you can establish a direct serial connection, parallel cable connection, or infrared connection between two computers in order to share the resources of the computer designated as the host. If the host is connected to a network, the guest computer can also access the network.

For example, if you have a portable computer, you can use a cable to connect it to your work computer and network. To establish a local connection between two computers, you must connect a compatible serial or null-modem parallel cable to both computers, or both computers must be equipped with infrared devices. For information about using Direct Cable Connection with infrared devices, see the section "Using Infrared" later in this chapter.

Before you can transfer files from the host to the guest computer, the files must be in a shared directory, and File and Printer Sharing services for either Microsoft or NetWare networks must be enabled in the Network option in Control Panel. You can also apply share-level security to the shared files. For information, see Chapter 18, "Logon, Browsing, and Resource Sharing," and Chapter 9, "Security."

Before you install and configure Direct Cable Connection, you need to decide:

- What remote access and network protocols do you need to install on the guest and host computers? They must both be running at least one common network protocol in order to connect. A broadcast protocol such as NetBEUI is simplest.
- Do you want the host computer to act as a gateway to a TCP/IP network? If so, you must install NetBEUI.
- What kind of cable or infrared device do you need?
- Do you want to assign a password to the host computer? If you assign a password on the host, all users connecting from the guest computer will be prompted for it. After connecting, the guest can access resources on the host computer according to the type of security applied to it, that is, user-level or share-level security.

---

**Note**  You cannot use Direct Cable Connection and Dial-Up Networking at the same time. Both applications use the same network interface (Pppmac.vxd). Before using Direct Cable Connection, make sure to shut down any active Dial-Up Networking connections.

---

## Installing and Configuring Direct Cable Connection

To install Direct Cable Connection during Windows 98 Setup, you must run Setup from the DOS prompt and choose Custom or Portable as the setup type. You can also install Direct Cable Connection after installing Windows 98.

▶ **To install Direct Cable Connection after Windows 98 Setup**

1. In Control Panel, click Add/Remove Programs, and then click the **Windows Setup** tab.

2. In the **Components** list, click **Communications**, and then click **Details**.

3. In the **Components** dialog box, click **Direct Cable Connection**, and then click **OK**.

Windows 98 provides a Direct Cable Connection Wizard for establishing the connection between two computers. The wizard runs when you open Direct Cable Connection the first time. It allows you to designate one computer as the guest and the other as a host. Before you run the wizard, you must install Direct Cable Connection on each computer and connect them with a null-modem serial or parallel cable, or with an infrared device.

For more information about setting up and using Direct Cable Connection, see Help, or the Networks troubleshooter section on "I am unable to connect my Windows 95 computer to my Windows 98 computer."

## Cables Compatible with Direct Cable Connection

Windows 98 supports a serial null-modem standard (RS-232) cable and the following parallel cables:

- Standard or Basic 4-bit cable, including LapLink and InterLink cables available before 1992.

- Extended Capabilities Port (ECP) cable. This type of cable works on a computer with ECP-enabled parallel ports, which must be enabled in BIOS. This kind of parallel cable allows data to be transferred more quickly than a standard cable.

- Universal Cable Module (UCM) cable. This cable supports connecting different types of parallel ports. Using this cable between two ECP-enabled ports allows the fastest possible data transfer between two computers.

Parallel cables transmit data simultaneously over multiple lines, whereas serial cables transmit data sequentially over one pair of wires. Thus, parallel cables are faster than serial cables.

You can also use Direct Cable Connection over an infrared link. For more information, see "Using Infrared" later in this chapter.

# Using Briefcase to Synchronize Files

If you can use a portable computer and a desktop computer, or you are connected to a network, you must constantly work to keep the files synchronized. Windows 98 Briefcase minimizes this task by keeping track of the relationships between files on two or more computers.

With Briefcase, you can do the following:

- Create a Briefcase folder.
- Add files to Briefcase.
- Check the status of files in Briefcase and their related files.
- Update related files, either individually or all at once.
- Split related files to maintain them separately.

Windows 98 provides a set of OLE interfaces that allow applications to bind reconciliation handlers to it, track the contents of Briefcase, and define the outcome of any reconciliation on a class-by-class basis. For example, when both the file in Briefcase and its synchronized copy outside have changed, Windows 98 calls the appropriate reconciliation handler to merge the two files. This could be handy when several users are simultaneously updating one large document.

**Caution**  Do not place one Briefcase inside another Briefcase. You cannot drag a file into a Briefcase that is in another Briefcase.

## Creating and Configuring a Briefcase

To install Briefcase during Windows 98 Setup, you must run Setup from the DOS prompt and choose Custom or Portable as the setup type. You can also install Briefcase after installing Windows 98.

▶ **To install Briefcase after Windows 98 installation**

1. In Control Panel, double-click Add/Remove Programs.
2. Click the **Windows Setup** tab, in the **Components** list click **Accessories**, and then click **Details**.
3. In the **Accessories** dialog box, click **Briefcase**, and then click **OK**.

If you install Briefcase, it appears as an icon on your Windows 98 desktop. To run Briefcase, double-click its icon.

▶ **To uninstall Briefcase**

- Drag the Briefcase icon to the Recycle bin.

---

**Tip**  You can use Briefcase to synchronize files between a portable computer running Windows 98 and a desktop computer running Windows NT Server 3.5 or later.

---

## Updating Files with Briefcase

When you update files by using Briefcase, Windows 98 automatically replaces unmodified files with modified files. If both files have changed, Windows 98 calls the appropriate application (if available) to merge the disparate files. The host and guest can be connected in the following ways:

- You can copy files from your desktop to Briefcase and then load Briefcase onto your portable computer. If you are using a Plug and Play BIOS docking station, Briefcase automatically updates files when you later dock your portable computer.

- You can update files using Briefcase and a floppy disk. For information, see Windows 98 Help.

- You can synchronize files between a portable computer and a network if the portable computer has a network connection.

- You can use Direct Cable Connection to connect two computers running Windows 98, and then use Briefcase to synchronize their files. For more information about Direct Cable Connection, see "Using Direct Cable Connection" earlier in this chapter.

For more information about Briefcase, and for instructions for using Briefcase to update two connected computers, see Help.

---

**Tip**  To find the copy of a file that is outside Briefcase, click **Find Original** in the **Update Status** dialog box.

---

# Using Infrared

Windows 98 includes Microsoft Infrared version 3.0, which allows you to use infrared devices to connect to computers, printers, or other devices such as infrared cameras. Microsoft Infrared 3.0 supports the Infrared Data Association (IrDA) standards IrDA 1.0, for Serial Infrared Devices (SIR); and IrDA 1.1, for Fast Infrared Devices (FIR). Because of its low cost and simple implementation, infrared is the first widely used wireless transmission technology. It can be used for the following purposes:

- Exchanging files wirelessly between two computers.
- Printing wirelessly on infrared-capable printers.

- Connecting to the network wirelessly instead of using cabling, through a computer connected by Direct Cable Connect.

The Windows 98 implementation of Infrared provides the following benefits:

- Device drivers for SIR devices capable of sending and receiving at speeds up to 115.2 kbps.
- Support for FIR devices capable of sending and receiving data at 4 Mbps.

Windows 98 also includes Microsoft Infrared Transfer, an application that enables a suitably enabled computer to quickly send files using their infrared device.

## Installing an Infrared Device

This section describes how to install infrared devices.

---

**Note**  If you change the infrared adapter model that is connected to the computer, you should reinstall it.

---

The procedure for installing an infrared device varies depending on whether it is a Plug and Play device. All Fast Infrared devices are Plug and Play–compatible.

▶  **To install a Plug and Play device**

1. If it is an external device, attach it. The Infrared 3.0 software loads automatically.

2. Double-click the Infrared icon in Control Panel to activate the infrared device. If there is no Infrared icon in Control Panel, press F5 to make the icon appear.

▶  **To install a non-Plug and Play infrared device**

1. If it is an external device, attach it.

2. In Control Panel, double-click the Add New Hardware wizard. Follow the instructions on the screen, making the following choices:

   - If asked whether the device you want is in the list, click **No**.
   - When asked whether you want Windows to search for your new hardware, click **No**.
   - When the **Hardware Types** box appears, click **Infrared devices**.
   - When asked to select a device, accept the default selection **Generic Infrared Serial Port or dongle**. (The other devices listed are Plug and Play devices.)
   - When asked for such information as the communications port that the infrared device is physically connected to, if you are not sure, accept the defaults.

## Using the Infrared Monitor

You can use the Infrared Monitor to keep track of your computer's infrared activity. You can activate Infrared Monitor once your infrared device is installed by double-clicking the Infrared icon in Control Panel or by clicking the animated Infrared icon in the system tray on the Taskbar. The Infrared Monitor contains the tabs and options shown in Table 19.5.

**Table 19.5   Infrared Monitor tabs**

| Tab name | Tab option | Description |
|---|---|---|
| Status | | Tells you whether infrared is working properly and displays information about the infrared connections. |
| Options | Enable infrared communication | Enables and disables infrared services on the physical serial port. |
| | Search for and provide status for devices in range | Starts and stops the infrared device's ability to detect other devices that are in range. |
| | Enable software install for Plug and Play devices in range | Enables and disables Microsoft Infrared Support software from automatically configuring a device across the infrared communication link when the computer comes into range of a new Plug and Play device. |
| | Limit connection speed | Configures the maximum speed for the infrared. Limiting this speed may improve communication. |
| | Restore defaults | Restores settings to defaults. |
| Preferences | Display the infrared icon in the taskbar | Determines whether the infrared icon displays in the system tray. |
| | Open Infrared Monitor for interrupted communication | Specifies whether to open the Infrared Monitor when infrared communication is interrupted. |
| | Play sounds for devices in range and interrupted communication | Specifies whether sounds will be played for various infrared events. |
| Identification | Computer name | Contains the name assigned to the computer. This is the same name used to identify your computer on the network. If no name appears here, enter one. |
| | Computer description | Contains a description of the computer. This is the same description used to identify your computer on the network. If no description appears here, enter one. |

▷ **To verify your connection using Infrared Monitor**

1. On one of the computers, in the system tray on the Taskbar, double-click the animated infrared icon. Infrared Monitor appears.

2. Click the **Status** tab. It shows all devices visible to the computer.

3. Repeat steps 1 and 2 for the other computer.

## Transferring Files Using Infrared Transfer

Windows 98 includes Infrared Transfer, a new application for transferring files through an infrared connection.

When an infrared device has been installed, an icon called Infrared Recipient is added to My Computer, and a shortcut to it is added to the **\Windows\Send To** folder. This shortcut adds an item to the **Send To** menu option that appears when you right-click a file or folder.

The first time Infrared Transfer is used to send a file or folder, a folder called My Received Files is created, and all sent files or folders will be copied to this folder. If a file or folder is sent that already exists in the My Received Files folder, a copy of the file or folder is made.

You can transfer files using one of several different methods. Before attempting to transfer files, make sure the infrared communications driver is properly installed and the infrared devices are enabled by carrying out the procedures in "Installing an Infrared Device" and "Using the Infrared Monitor" earlier in this chapter.

▶ **To transfer files or folders using Infrared Recipient**

1. In My Computer, double-click Infrared Recipient.

2. Select an available infrared device.

3. Click **Send Files**.

4. Select the files to send.

5. Click **Open**.

▷ **To transfer files or folders using Send To**

1. Select the files you want to send.

2. Right-click the selected files, and then point to **Send To**.

3. Click **Infrared Recipient**.

▷ **To transfer files or folders using Drag and Drop**

1. In My Computer, open Infrared Recipient.

2. If there is more than one infrared device in range, select an available infrared device.

3. In Windows Explorer, select files you want to send.

4. If there is only a single infrared device in range, drag and drop files onto the Infrared Recipient icon in my computer.

-Or-

5. If there is more than one infrared device in range, drag and then drop files onto the computer selected in **Available** devices within range.

## Transferring Files using Direct Cable Connection and Infrared

You can use Direct Cable Connection over an infrared link to connect a host and guest computer. This section describes how to transfer files over an infrared link, using Direct Cable Connection. Before transferring files, you must install Direct Cable Connection on both computers by following the procedure outlined in "Using Direct Cable Connection" earlier in this chapter. Both computers must also use a common network protocol; a broadcast protocol such as NetBEUI is easiest to configure.

Additionally, the files must be in a shared directory, and File and Printer Sharing services for either Microsoft or NetWare networks must be enabled in the Network option in Control Panel. You can also apply share-level security to the shared files. For information about File and Printer Sharing, see Chapter 18, "Logon, Browsing, and Resource Sharing." For more information about share-level security, see Chapter 9, "Security."

▶ **To transfer files using Direct Cable Connection**

1. Make sure the infrared communications driver is properly installed and the infrared devices are enabled by carrying out the procedures in "Installing an Infrared Device" and "Using the Infrared Monitor" earlier in this chapter.

2. On one of the computers, open the Infrared Monitor and click the **Options** tab. It lists the virtual COM port the infrared device uses. Note this information.

3. On the host computer, click **Start**, point to **Accessories**, and then click **Direct Cable Connection**.

4. Follow the steps in the Direct Cable Connection Wizard to set up the host computer.

   When the wizard prompts you for it, select the Host option. When the wizard prompts you to choose a port, use the same virtual port you found in Step 2.

   The wizard also offers password protection. It is not necessary to establish password protection on the host computer for this test of the infrared link. When you have finished the wizard, click **Finish**. Direct Cable Connection starts running on the infrared link and displays the following message: "Status: Waiting to connect via Serial cable on Com$x$," where Com$x$ is the name of the virtual port the infrared link is using.

5. Repeat steps 3 and 4 for the guest computer, except select the Guest option instead of the Host option. When you have finished the wizard, click **Finish**.

The connection is automatically made over the infrared link, and all the shared folders on the host computer are displayed on the guest computer's screen.

When you run Direct Cable Connection to establish the connection between the host and guest computers, the guest computer might display the message "Direct Cable Connection was unable to display shared folders of the host computer" and prompt you to enter the computer name of the host computer. If this happens, check the **Status** tab of the Infrared Monitor interface screen.

If you are working on the guest computer, and you want to copy a shared folder from the host computer to the guest computer, select the folder's icon in the window that displays all the shared folders that are on the host computer, and drag the icon to the desktop.

To work on a shared folder on the host computer without copying it to the guest computer, double-click the folder in the display on the guest computer. Note that if the host computer is connected to a network, the guest computer can reach shared resources on the network through the connection to the host.

## Printing with Infrared Transfer

Before attempting to print, make sure the infrared communications driver is properly installed and the infrared devices are enabled by carrying out the procedures in "Installing an Infrared Device" and "Using the Infrared Monitor" earlier in this chapter.

▶   **To print to an Infrared-Capable Printer**

1. Make sure the infrared communications driver is installed on the computer.

2. Bring an infrared-enabled printer within range.

3. Your computer might automatically detect and install the printer. If not, make sure the printer driver for the infrared-capable printer is installed on the computer.

4. Try the Print option in a program.

You can make printers without built-in infrared ports infrared-capable by connecting an infrared adapter made for printers into the printer's parallel port. An example of an infrared adapter for printers is the Extended Systems JetEye Infrared Printer Port ESI-9580. If a parallel cable is also used to connect the computer to the infrared printer adapter, you can use either the infrared link or the parallel cable to print. The infrared link is used when you select the virtual parallel port; the cable is used when you select the physical parallel port.

To validate the infrared link to the printer, make sure the correct printer driver is installed for the infrared-capable printer. (Most printers with built-in infrared ports are Plug and Play devices, which are installed automatically.) Then use a program to print over the infrared link.

If the program prints on an infrared-capable printer, the infrared driver installation is validated. If there is trouble printing, see "Troubleshooting Infrared" later in this chapter for more information.

# Troubleshooting Remote Networking and Mobile Computing

This section describes problems you may encounter in using Dial-Up Networking, virtual private networking, and Mobile Computing.

## Troubleshooting Dial-Up Networking

This section describes problems that you may encounter in using Dial-Up Networking and how to resolve them. Windows 98 provides a troubleshooting aid for Dial-Up Networking in Help. Try using the troubleshooting aid before taking the troubleshooting steps included in this section.

You can monitor any Dial-Up Networking session for possible problems by enabling the Record a Log File option. This produces a Ppplog.txt file in the Windows directory, which you can reference to find out the cause of a problem. For more information, see Knowledge Base Article Q156435, "How to Interpret the Ppplog.txt File."

### Dial-Up Networking does not install properly.

If you cancel Setup while Dial-Up Networking is copying files and then restart the computer, you will see an error message stating that the following files are missing:

- Vnetsup.vxd
- Nwlink.vxd
- Nwredir.vxd
- Nscl.vxd
- Vredir.vxd
- Ndis.vxd
- Ndis2sup.vxd
- Vnetbios.vxd

If these files are missing, Dial-Up Networking will not function correctly. You must remove and reinstall Dial-Up Networking.

▶   **To remove Dial-Up Networking**

1. In Control Panel, click Add/Remove Programs.

2. Remove all Dial-Up Networking components.

3. Restart your computer.

To reinstall Dial-Up Networking, follow the procedures outlined in "Installing Dial-Up Networking" earlier in this chapter.

**Caution**  Never remove Dial-Up Networking components using Network in Control Panel.

### Dial-Up Networking cannot find modem.

If you see an error message stating that Dial-Up Networking cannot find the specified modem, check the following:

- Check that the modem is properly installed and configured.

- In Modems in Control Panel, check the **General tab** to make sure it lists your modem.

- Check the connection to make sure the modem you have specified is the modem connected to your computer.

### The remote server does not respond.

If you receive an error message that the computer you are connecting to has not responded, check the following items:

- Check your connection to make sure it is configured to use the network protocols used on the remote server.

- If you are using TCP/IP, check your connection to make sure that the network protocols are configured correctly.

- In Control Panel, check the Network option to make sure it lists all the network protocols used on the remote server.

- Check your connection to make sure it is configured to access the correct server type.

- Check that the server is configured correctly.

- If a terminal logon is required, check that you have configured the **Options** tab in your connection to bring up a terminal window before dialing.

**You cannot access the Dial-Up Networking server because a user name is not valid.**

In the properties for the Windows 95 or Windows 98 dial-up server, verify that the user name is in the list of users that are allowed access.

▷ **To set Dial-Up Networking Server to allow caller access options**

1. In Dial-Up Networking, click the **Connections** menu, and then click **Dial-Up Server**.

2. In the **Dial-Up Server** properties, click **Allow Caller Access**, if this is not already selected, and then view the User name list to ensure the user's name appears.

   The User name list appears only if you have chosen user-level security for the dial-up server. The type of security is selected in the Network option in Control Panel.

If the dial-up client is also running File and Printer Services for NetWare Networks, the File and Printer Sharing service automatically becomes the default server, but it cannot receive the information needed to find the remote servers.

**You cannot access remote NetWare servers when making a dial-up connection.**

Disable File and Printer Sharing Service for NetWare Networks when you make the dial-up connection.

**Software compression does not work.**

Check the settings for the dial-up server type and software compression.

▷ **To verify dial-up server and compression options in Dial-Up Networking**

1. In the **Connections** menu, click **Dial-Up Server**.

2. Click **Server Type** and verify that the correct type of dial-up server is selected.

3. Check that **Enable software compression** is selected. Compression will occur only if the dial-up client and server have enabled it.

**The modem is dialing but not connecting.**

- Check the modem configuration; change the configuration if necessary.

- Verify all parameters, such as access codes, area code, country code, and dialing properties.

- Try choosing the driver for **Generic Modem Drivers**.

- If you are using an external modem, check the cable and verify that it is connected correctly.

- Check the COM port configuration in Device Manager.

For more information, see the troubleshooting section in Chapter 21, "Modems and Communications Tools."

### Dial-Up Networking Server is not answering incoming calls.

- If you are using an external modem, check the cable and verify that it is connected correctly.

- If you are using an internal modem with a nonstandard IRQ selection, use Device Manager to check the IRQ setting for the COM port and change it if necessary.

- Disable **Allow Caller Access** and shut down the computer. Turn off the computer to reset the COM port. If the modem is external, turn off the modem. Turn the computer back on and reconfigure the Dial-Up Networking server, and then try again.

- If these steps fail, disable **Allow Caller Access** and see if any modem software can manually answer the incoming call.

- Try choosing the **Generic Modem Drivers** on the dial-up server.

The password for the Dial-Up Networking server is stored in the Rna.pwl file. However, simply deleting this file or removing and reinstalling Dial-Up Networking may not remove the password. If you set the Dial-Up Networking server to monitor for calls and then delete the Rna.pwl file, the password is not removed, because it is stored in memory. If you shut down Windows 98 at this point, the Rna.pwl file is re-created with the password in memory.

▶ **To replace a forgotten password in a Dial-Up Networking server**

1. Disable **Allow Caller Access**, and then shut down and restart Windows 98.

2. Delete the Rna.pwl file, and then restart Dial-Up Networking.

---

**Note**  When you first connect to the Dial-Up Networking server, an error message states that the password file is missing or corrupt for every modem device you have installed. If you have any null modem devices installed (for example, when you run Direct Cable Connection it installs a modem device for every COM and LPT port you have), this error message also appears.

---

### You lose connectivity to servers on your network or to the Internet.

If you are connected to a LAN and you make a PPP or VPN connection, you might lose connectivity to some of the servers on your LAN. Likewise, if you connect to the Internet, then make a VPN connection to another network, you might lose connectivity to the Internet itself. For information about the cause of this problem and its solution, see "Technical Notes on Dial-Up and Virtual Private Networking," earlier in this chapter.

**Multilink does not provide additional bandwidth.**

- Check that the server you are connecting to supports Multilink.

- Check that you have two modems or a dual-channel ISDN card. If you do not have two modems or a dual-channel ISDN card, you cannot use Multilink.

- Check that your modems are exactly the same speed. Performance degrades if the modems connect at different speeds.

- Check that your modems or ISDN card are configured correctly. For more information about the correct configuration, see Chapter 21, "Modems and Communications Tools."

**TAPI codes do not work properly.**

If you entered TAPI codes, an area code, or a country code in one connection, but Dial-Up Networking does not use those codes when you use the connection, make sure that all your connections use the TAPI codes.

▶ **To verify that all your connections use the TAPI codes**

1. Right-click each connection icon, and then select **Properties** from the context menu.

2. In the **General** tab for each connection, check that **Use area code and Dialing Properties** is selected.

# Troubleshooting Your Virtual Private Networking Connection

This section describes common virtual private networking problems and explains how to correct them.

### Two Dial-Up networking adapters appear in Network in Control Panel.

This is by design. Do not attempt to remove Dial-Up Networking components using Network in Control Panel. If you need to remove virtual private networking, do so using Add/Remove Programs in Control Panel.

### You cannot connect to a VPN server.

If you cannot connect to a VPN server, you can begin to diagnose the problem by looking at the status messages that appear when you attempt to make a connection. If the connection is successful, you will see the following messages:

- a message stating that your computer is dialing a server.

- a message that says the server is verifying your name and password.

- a message that says the client is logging on to the network.

If the connection fails before you see the "Verifying name and password" message, you might have a problem with DNS name resolution, or the VPN server might not be responding. If the connection fails before you see the "Verifying name and password" message and gives you the error message that the other computer is not responding, a computer along the way might be filtering out Generic Routing Encapsulation (GRE) packets, which are required for VPN to work.

However, if you do see the message "verifying name and password," your PPP connection succeeded and PPTP is working, and you probably have a problem with your user name and password.

You can also check the following items.

**Verify that you are properly connected to the Internet.**  Make sure that your Internet connection is working properly.

▶  **To check that your connection to the Internet is working properly:**

1. Ping a host that you can normally reach using **ping**.

   If **ping** succeeds, your Internet connection is working properly.

2. If **ping** does not reach that host, type its IP address.

   If **ping** succeeds, you are properly connected to the Internet, but you are not properly connected to your DNS server. You should be able to connect to your VPN server by typing its IP address instead of its host name.

   – Or –

   If **ping** fails, you might not be connected to the Internet. Contact your ISP.

**Ping the VPN server.**  Ping the host name or IP address of the VPN server.

If you receive a response, you are properly connected to the VPN server, and you might have entered an incorrect user name or password.

If you do not receive a response, the administrator of the VPN server might have turned on PPTP filtering. This prevents you from pinging the VPN server. Contact the administrator of that server.

**Check for a firewall.**  Firewalls sometimes filter out PPTP packets. Contact your ISP and the administrator of your corporate server and ask if they are using a firewall. If they are, request that they pass TCP port 1723 and IP protocol 47 (the GRE protocol).

Because PPTP is a secure protocol, adding TCP port 1723 and IP protocol 47 will not affect the security of the firewall.

**Make sure your ISP is not filtering out PPTP.** Contact your ISP and ask if it filters out GRE packets. If so, request that it pass GRE protocol 47.

**Check for a proxy server.** It is not possible to create a VPN tunnel that passes through a proxy server such as a computer running Microsoft Proxy Server. Therefore, if your internal network's proxy server handles all Internet traffic, including PPTP traffic, you will not be able to create a VPN tunnel to access resources on the internal network.

### You cannot log on to the target network.

If you can connect to the VPN tunnel server, but you cannot perform a domain logon to the target network, verify that you have configured the connection to your VPN server to allow you to perform a domain logon to the target network.

▶ **To verify your VPN configuration**

1. In the Dial-Up Networking folder, right-click the icon for your VPN server connection.

2. Click **Properties**.

3. Click the **Server Types** tab.

4. In the **Advanced options** dialog box, make sure the **Log on to the network** check box is selected.

### Your VPN connection is slow.

If your VPN connection is slow, follow the procedures outlined below.

- Check your ISP connection.

  You might be able to improve your performance by changing settings in your ISP connection. Specifically, you can improve performance by deselecting the option **Log on to network** and by deselecting all network protocols you are not using. To do so, follow the steps outlined in the procedure in the "Configuring Options for the Server to Which You Are Connecting" section earlier in this chapter. For information about other issues you should consider when setting up a connection to the Internet, see "Configuring a Connection to the Internet" earlier in this chapter.

- Check the connection to other Internet sites.

  To check the speed of your Internet connection, ping Internet sites you can normally ping. If **ping** shows a response time of more than five seconds, you have a slow Internet connection. Contact your ISP.

- Check the connection to your VPN server.

  If you do not have problems with your Internet connection, but the connection to your VPN server is still slow, the VPN server might be overloaded. Contact the administrator of the VPN server.

**You cannot connect after disconnecting from a LAN.**

If you have a mobile computer that has a directly attached network adapter card that you use to access resources on your corporate network, you might have trouble connecting to some of your network's hosts after disconnecting a mobile computer such as a laptop from your corporate network and then making a VPN connection to your corporate network. This happens because your computer is still forwarding all its network traffic to the network adapter instead of over the VPN connection. To force your computer to forward its network traffic over the VPN connection, disable your network adapter using the following procedure.

▶ **To disable your network adapter**

1. In Control Panel, double-click System.

2. Click the **Device Manager** tab.

3. Double-click **Network adapters**.

4. Select your network adapter.

5. Click **Properties**.

6. In the **Device usage** box, select the **Disable in this hardware profile** check box.

If this procedure does not work, but you are using DHCP to automatically assign IP addresses, you can try using **winipcfg** to release your IP address. For more information, see Chapter 15, "Network Adapters and Protocols."

▶ **To release your IP address**

1. Click **Start**, click **Run**, type **winipcfg**, and then press the ENTER key.

2. In the **IP Configuration** dialog box, click **Release All**.

# Troubleshooting Direct Cable Connection

This section presents problems that might occur when you are using Direct Cable Connection.

As general troubleshooting steps, verify the following:

- Verify that your cable is properly connected.
- Make sure that you are using a compatible cable, listed in "Using Direct Cable Connection" earlier in this chapter. Make sure that you are not using such devices as gender-benders or devices that convert 25-pin cables to 9-pin cables.
- Check Device Manager to make sure that you do not have an IRQ port conflict.

- Verify that both computers have the same network protocol installed. A broadcast protocol such as NetBEUI is simplest.

### You cannot find the host computer.

If you cannot find the host computer using Direct Cable Connection, follow the procedures in "Using Direct Cable Connection" earlier in this chapter to make sure Direct Cable Connection has been installed correctly on the host computer and is working.

If Direct Cable Connection is working properly but you still cannot find the host computer, make sure you have Client for Microsoft Networks is installed. For more information, see Chapter 16, "Windows 98 on Microsoft Networks."

### You can connect to the host computer but you cannot use it as a gateway to the network.

The host computer and guest computer can communicate using the TCP/IP protocol, which is generally installed by default. However, if you want the host computer to act as a gateway to a TCP/IP network, you should make sure that NetBEUI is installed as well. For more information, see Chapter 15, "Network Adapters and Protocols."

### You cannot use Direct Cable Connection with Dial-Up Networking.

Both Dial-Up Networking and Direct Cable Connection use the same network interface (Pppmac.vxd). You cannot have more than one instance of Pppmac.vxd running at one time, so you cannot use both Direct Cable Connection and Dial-Up Networking at the same time. You must close either Direct Cable Connection or Dial-Up Networking.

## Troubleshooting Infrared

Following are several factors to check as you begin to troubleshoot your infrared connection:

- Check distance between infrared adapters.

  Try moving the devices closer together or farther apart. The devices must be no more than three feet apart, and some devices work best if kept at least six inches apart. Make sure that there are no obstructions between the devices.

- Check alignment between infrared adapters.

  Infrared devices produce an "arc" of infrared light. This arc is usually between 15 and 30 degrees. Try realigning the devices so that they fall within this arc.

- Check for interference with infrared transmission.

  Direct sunlight contains infrared light and can cause degradation of the infrared signal between devices. If this occurs, try blocking the sunlight or moving the devices closer together.

- Experiment with connection speed.

  Use the **Limit Connection Speed To** option in the Infrared Monitor **Options** tab to limit the connection speed to 19.2 kbps. If this is successful, you can experiment with establishing a connection at a higher speed. This is especially important if an infrared adapter is attached to a COM port that is using an 8250 UART instead of a 16550 UART or if the adapter is connected to a relatively slow computer.

- Ensure that application is set to use virtual infrared port.

  Ensure that the application you are using is configured for the virtual port, not the physical port that the infrared device is attached to. Keep in mind that, as with all communications and printer ports, only one application can use the virtual port at one time.

- Verify infrared adapter settings.

  Open the Infrared Monitor and verify that all settings are correct.

- Verify the physical COM port.

  If you select the wrong physical COM port during installation of the infrared communications driver, the infrared device will be unable to discover another infrared device within range. If this happens, put an actively searching infrared device close to the computer's infrared device and reinstall infrared on a different COM port until the infrared device on the computer discovers the nearby infrared device.

- Verify that the infrared adapter has power.

  You might need to change the batteries in an infrared adapter or plug the AC power into an infrared adapter.

## Troubleshooting General Infrared Problems

This section discusses general problems that might occur when using infrared. For information about specific infrared hardware, see the next section.

### Communication over a virtual COM port link is unreliable with printer's infrared adapter in range.

Communication over a virtual COM port link between two computers might not be reliable if a printer's infrared adapter is also within range. You should move the adapter out of range.

### Zmodem fails over infrared.

You might experience problems transferring files over an infrared link. If the Zmodem protocol fails with a link speed of 115.2 kbps, use the Infrared Monitor Limit Connection Speed To tab to limit the link speed to 19.2 kbps and then retry the Zmodem file transfer.

## Troubleshooting Specific Infrared Hardware

This section discusses common problems you might experience with specific infrared hardware. For information about general problems you might encounter, see the previous section.

The Texas Instruments TravelMate 5000 might communicate over an infrared link only at very low speeds (9600 bps). The Sharp PC 3050 might communicate over an infrared link only at speeds between 9600 bps and 19.2 kbps.

For the Hewlett Packard Omnibook 4000C or the Hewlett Packard Omnibook 600CT, which have built-in infrared ports, you must install a special echo-canceling serial driver in addition to the components that make up the infrared communications driver. The echo-canceling driver, and instructions on how to install it, are available from Hewlett-Packard.

### Serial port does not provide sufficient power for Adaptec AIRport 2000.

The Adaptec AIRport 2000 infrared adapter can be powered in three ways: by the serial port, by installed AA batteries, or by an external power supply. In some cases the serial port might not provide sufficient power for the operation of the adapter. This can cause reduced operating range and/or a failure to find another infrared device that is nearby and aligned correctly. If you suspect this problem, connect an AC adapter or add four AA batteries to the battery compartment in the infrared adapter. This will assure sufficient power. In some instances, you might also need to separate the adapter by at least six inches from the other infrared device.

### Cannot print from ActiSys 220L infrared adapter.

If an ActiSys 220L infrared adapter is attached to a computer and used to print to a printer that is using an Extended Systems ESI-9580 printer infrared adapter, or a Hewlett Packard DeskJet 340, you must use the **Options** tab in the Infrared Monitor properties to limit the connection speed to 19.2 kbps in order to print successfully. If the infrared devices are allowed to negotiate the connection speed automatically without setting this limit, they will negotiate a higher connection speed, and a program will be unable to print.

### Additional Resources

| For more information about | See this resource |
|---|---|
| Internet drafts and RFCs | **http://www.ietf.org/.** |
| Virtual private networking | **http://www.microsoft.com/communications/.** |
| Windows NT remote access servers | *Windows NT Server Networking Guide for Windows NT Server version 4.0* and the *Networking Supplement* for the Windows NT Server 4.0. |