

Novell NetWare

Each NeXT computer includes client software for Novell NetWare. This software allows NeXT computers to access files and printers on the NetWare network. If you're not the administrator of the Novell network, you'll need to involve the NetWare administrator in the configuration procedures.

Configuring the NetWare Network

To access Novell NetWare servers from a NeXT computer, you first need to do some setup on the NetWare servers. Then you'll be able to use network files and printers from your NeXT computers.

To take advantage of the Novell client software, you need a network running NetWare 286 version 2.15c or later, or NetWare 386 version 3.1 or later.

1. Connect your NeXT computer(s) and Novell servers to the same network. If necessary, connect Ethernet segments with bridges and/or routers.
2. On each of the NetWare servers, create a user account for each of the NeXT users that will be accessing those servers. Make sure the NetWare users belong to the group EVERYONE; if you don't, the NetWare file and directory permissions won't map correctly to the UNIX permissions.

Configuring the NeXT Computers

To have a NeXT computer take advantage of the NetWare services is simply a matter of enabling NetWare.

1. Log into the NeXT computer using any valid account.
2. Start up NetWareManager, located in **/NextAdmin**.
3. A panel appears telling you that NetWare isn't enabled and asking if you want to enable it. Click Enable.

F77.tiff ,

4. Another panel appears informing you that the NetWare service will be turned on after you reboot your computer. Click OK.

F78.tiff ,

5. Reboot the NeXT computer.

Accessing Files

Once the NeXT computer has been configured as a NetWare client, the files on a NetWare server appear in the File Viewer.

1. Log into the NeXT computer that's been configured as a NetWare client.
2. Select **/Net** in the File Viewer, then click **NetWare**. The subdirectories listed under **NetWare** are the names of the available NetWare servers.

F1.tiff ,

3. Click the name of the NetWare server you want to access. The Authentication panel appears.

F2.tiff ,

4. Enter the name of an account that's been set up on the NetWare server, then enter the password. Click OK.
Note: The password is limited to 16 characters, regardless of the length of the password on the NetWare server.
5. The files on the NetWare server now appear in the File Viewer, and can be accessed just as you would a local file.

F3.tiff ,

Restricting Visible Servers

If your Novell network has a large number of servers, performance on your NeXT computer can be seriously degraded when it displays all the servers in the file viewer. You can help improve performance by defining a list of servers to be displayed in the File Viewer. Servers not included in this list won't show up in the File Viewer.

Create the list of visible servers with NetInfoManager:

1. Start up NetInfomanager.
2. Click **//locations** in the local domain. If you want to restrict visible servers for more than the local computer, open the root domain (or a midlevel domain, if appropriate), then click **//locations**.

F88.tiff ,

3. Choose New Subdirectory from the Domain window.
4. Double-click **newValue** to open the Directory window.

F89.tiff ,

5. Click **newValue** in the Values column, enter **NetWare** into the text field, and press Return.

F90.tiff ,

6. Click **name** in the Properties column, then choose Append Property from the Directory menu.

7. Enter **VisibleServers** into the text field and press Return.

8. Choose New Value from the Directory menu.

F91.tiff ,

9. Enter the name of one of the NetWare servers you want to be visible in the File Viewer and press Return.

10. For each additional server you want to make visible in the File Viewer, choose Append Value from the Directory menu, enter the server name in the text field and press Return.

F92.tiff ,

11. Choose Save from the Domain menu.

From now on, only those NetWare servers listed in the **VisibleServers** property will appear in the File Viewer.

Authentication

When you log into a NetWare file server, you stay logged in until you reboot your NeXT computer. If you want to access the file server as some other NetWare user, perhaps to perform activities that require supervisor access, you use NetWare Manager.

1. Start up NetWareManager. The viewer displays a list of NetWare servers and the name of the NetWare user that's logged into that server, if any.
2. To change which user is logged into a particular server, click the name of the server in the list.

F4.tiff ,

3. Choose Reauthenticate from the Server menu. The Authenticate panel appears.

F39.tiff ,

4. Enter the name of the NetWare user account and the associated password. Click Login.

The list reflects the new NetWare user, and any further access to the NetWare file server will be with that NetWare user's permissions.

Sometimes you may want to log into a NetWare file server with a second NeXT user account. For example, if you're logged in as **george** but want to run a process as **root** that will access the NetWare files, you'll need to log **root** into the file server as well.

1. Start up NetWareManager.
2. Choose New User from the Viewer menu.

F66.tiff ,

3. Log into this panel as another NeXT user. A second viewer appears for this user.

F80.tiff ,

4. Log into the NetWare file servers for the second NeXT user by clicking the name of the file server and

choosing Authenticate from the Server menu, or by double-clicking the server name.

F81.tiff ,

5. Enter the NetWare user account and password, then click OK.

F82.tiff ,

Whenever a process that's run as this second user accesses the Novell file server, the files will be accessed as the NetWare user you chose.

Printing

You also use NetWareManager to manage access to NetWare printers. The procedures are described in the *User's Guide*.

File Names and Permissions

When you access NetWare files from a NeXT computer, file names and permissions are handled quite differently than for UNIX files. How names and permissions are handled depends on whether the NetWare servers are using the DOS namespace or the UNIX namespace. Servers running NetWare 386 version 3.11 or later can be set up to use the UNIX namespace (see ^aUNIX Namespace^o later in this section). Servers running NetWare 286, or servers running NetWare 386 that haven't been configured to use the UNIX namespace, will use the DOS namespace.

DOS Namespace

This section describes how file names and permission are handled for NetWare servers using the DOS namespace.

File Names

DOS file names are restricted to 8 characters with a 3-character extension (like *filename.dos*). If you create a file on a NeXT computer and save it to a NetWare server, the file name must be within the DOS file name restrictions.

Permissions

When a NeXT user accesses files on a NetWare server using the DOS namespace, the files appear to be owned by the NeXT user (similar to files on a removable disk). The only permissions that apply in this situation are the owner permissions (group and other permissions are ignored). There isn't a direct relationship between UNIX file permissions and the permissions used on NetWare servers. The following table describes the relationship between NetWare file permission in the DOS namespace and UNIX file permissions.

NetWare File Permissions

Read (R) and File Scan (F)
Write (W)
Doesn't apply
Access Control (A)
All others

UNIX File Permissions

Read
Write
Execute
Assigned to file owner
Don't apply

The next table compares the DOS namespace directory permissions with equivalent UNIX directory permissions.

NetWare Directory Permissions

Read (R) and File Scan (F)

Create (C)
Erase (E)
Modify (M)

UNIX Directory Permissions

Read and Execute

Write

Access Control (A)	Assigned to directory owner
Supervisory (S) and Write (W)	Don't apply

UNIX Namespace

Your NetWare administrator can configure servers running NetWare 386 version 3.11 or later to support UNIX file names and permissions.

Configuring the NetWare Servers

Follow these steps to configure a NetWare server to use the UNIX namespace:

Note: The following procedure will work for a PC-based NetWare 3.11 server. You may need to modify the procedure to suit your specific needs.

1. Copy **nfs.nam** to the DOS partition on the server.
2. Add the command **load nfs** to the end of the script **STARTUP.NCF**.
3. Copy **nuc.nlm** to **SYS:\SYSTEM**.
4. Add the command **load nuc** to the script **AUTOEXEC.NCF**.
5. Reboot the server.

Important: Watch the server boot to make sure that **nfs.nam** and **nuc.nlm** are loaded successfully. Fix any problems before proceeding. If you don't, your server may not boot.

6. At the server console, enter the following command, replacing *volume_name* with the name of the volume where you want to add the UNIX namespace:

```
ADD NAME SPACE NFS TO VOLUME volume_name
```

This command adds NFS (UNIX) file name support to the volume *volume_name*.

Warning: Plan carefully which volumes you want to configure with the NFS namespace. Once you have added the NFS namespace to a volume, it can only be removed by using VREPAIR.

7. Make sure each NeXT user that will be accessing the server has a corresponding NetWare user account. Then, create the file **etc/nfsusers** on the **SYS:** volume. Edit this file to contain a list of NeXT user IDs with the corresponding NetWare user names. Each line should contain one pair, similar to the following:

```
101 CARLA
```

8. Make sure that NeXT user groups have corresponding NetWare user groups. At a minimum, create a NetWare user group for the default group for each NeXT user that will access the NetWare server. Then, create the file **etc/nfsgroup** on the **SYS:** volume. This file maps a list of NeXT group IDs with the corresponding NetWare group names:

```
20 EVERYONE
```

Important: When you create a directory on the NetWare server to be accessed by NeXT users, log into a NeXT computer and use the **chgrp** command to change the group associated with the directory. By default, NetWare directories are assigned the group **nogroup**, and all files and directories created under the directory will inherit this group. By changing the group on the parent directory, you make sure that any subdirectories created from a NeXT computer inherit an appropriate group assignment. If you don't change the group associated with the directory, users may not be granted permissions to rename or delete any files they create.

File Names

With the NetWare server configured to use the UNIX namespace, the files and directories you create from a NeXT computer aren't restricted to the DOS file naming conventions.

Permissions

When a NeXT user attempts to access a file on a NetWare server that's been configured with the UNIX namespace, the UNIX permissions are checked first. If these permissions permit access, the NetWare permissions are checked. If these also permit access, access is granted. When file permissions are changed from a NeXT computer, the NetWare permissions are modified to correspond. Likewise, when the permissions

are changed from a NetWare computer, the UNIX permissions are modified to correspond.

The following table describes how NetWare permissions are translated to UNIX permission in the UNIX namespace.

NetWare File Permissions	UNIX File Permissions
Read (R)	Read
Write (W)	Write

The next table describes how UNIX namespace directory permissions are translated to UNIX directory permissions.

NetWare Directory Permissions	UNIX Directory Permissions
File Scan (F)	Read and Execute
Create (C) and Erase (E)	Write

Here's a list of some additional rules that apply for translating NetWare permissions to UNIX permissions:

- If the user ID or group ID isn't listed in NFSUSERS or NFSGROUP, the user ID or group ID is converted to -2, which corresponds to NOBODY or NOGROUP.
- If the file or directory has the NetWare attribute READ ONLY, all write permissions are removed.
- If the file or directory has the NetWare attribute TRANSACTIONAL, all write permissions are removed from the parent directory (unless the parent directory is ^{a/o}).
- For a subdirectory, the presence or absence of NetWare EF (Erase and File Scan) rights is duplicated in all files or directories contained in the subdirectory.

The next two tables describe the translation of UNIX permissions to NetWare permissions.

UNIX File Permissions	NetWare File Permissions
Read	Read (R) and File Scan (F)
Write	Write (W) and File Scan (F)

**UNIX Directory
Permissions**

Read

Write

**NetWare Directory
Permissions**

Read (R) and File Scan (F)

Write (W), Create (C), and File Scan (F)

Here's a list of some additional rules for translating UNIX permissions to NetWare permissions:

- The owner of a file or directory is granted the Netware permission Access Control (A).
- If the user ID or group ID associated with a file or directory is different from the corresponding ID on its parent directory, the NetWare Inherited Rights Mask (IRM) is set to S---E-F-.
- If permissions on a file are updated from a NeXT computer, the NetWare rights S--CEMF- are retained for the file.
- If permissions on a directory are updated from a NeXT computer, the NetWare rights SRW-EM-- are retained for the directory.
- If the parent of a file or directory isn't ^{a/o}, the NetWare rights Erase (E) and File Scan (F) are granted if they are set on the parent directory.
- If there are no write permissions for anybody (owner, group, other) on the file or directory, the NetWare attribute READ ONLY is set.

When a file or directory is created from a NeXT computer, NetWare rights are assigned based on the following rules:

- Owner of the new file is owner of parent directory
If the owner has write permission for the parent directory, the owner is granted the NetWare rights Erase (E) and Modify (M) for the new file. If the owner has read and execute permission for the parent directory, the owner is granted the NetWare right File Scan (F).
- Owner of the new file is not owner of parent directory, but is a member of the group assigned to parent directory
If the group is granted write permission for the parent directory, the group is assigned EM NetWare rights on the new file. If the group has read and execute permission for the parent directory, the group is assigned F permission on the new file.
- Parent directory of new file has write permission set for other (world)
If other (world) has write permission on

the parent directory, EM Netware rights are assigned to other (world) on the new file. If other has read and execute permissions on the parent directory, F NetWare rights are assigned to other on the new file.

Examining the NetInfo Database

When you enable NetWare, information is stored in the NetInfo database. Follow these steps to examine the resulting change:

1. Start up NetInfoManager. Open the local domain if a domain window for the local domain isn't already open.
2. Click **/localconfig**, then **NetWare**. Double-click **NetWare** to open a Directory window.

F79.tiff ,

3. Click the property **enable**. Notice that the value is **YES**, indicating that the NetWare daemons should be started when the computer boots.

AppleTalk

NeXT computers come with client software that allows them to access files and printers on an AppleTalk network. To take advantage of these features, you must connect your NeXT computer(s) to an AppleTalk network running EtherTalk.

Enabling AppleTalk

You set up AppleTalk networking with the Preferences application:

1. Click the Apple button in the Preferences application to access the AppleTalk preferences.
2. Click the check box labeled Enable AppleTalk Networking. A message appears in the panel telling you that you must reboot the computer for the change to take effect.

F83.tiff ,

3. Reboot the computer.

Your computer now has access to AppleShare files and AppleTalk printers.

File Sharing

With AppleTalk enabled, you can now access files on an AppleShare server from a NeXT computer.

1. Click **/Net** in the File Viewer, then **AppleShare**. The directories listed here are the available AppleShare zones. Beneath each zone directory is a list of the AppleShare servers within that zone. If there aren't any zones, servers will be listed directly under **/Net/AppleShare**.

F84.tiff ,

2. Click the name of one of the AppleShare servers. A panel appears, asking you to log into the server.

F85.tiff ,

3. Log into the server, either as a guest or registered user, by clicking the appropriate button and entering a user name and password. Click OK.

F86.tiff ,

The files on the AppleShare server are now available through the File Viewer.

- 4. If you want to log out from an AppleShare server, follow these steps:
 - a. Click the Apple button in Preferences.
 - b. Click the name of the server in the AppleShare section of the panel.
 - c. Click Logout to log out the current user.

The next time you access the server in the File Viewer, you can log in as a different user.

- 5. To change the password of the AppleTalk user, follow these steps:
 - a. In Preferences, click Change Password.
 - b. In the panel that appears, enter the old password and click OK.
 - c. Enter the new password twice, as prompted.

Printing

You use PrintManager to configure an AppleTalk printer, just as you would any other printer. The procedures are described in the *User's Guide*.

Considerations

When you access AppleShare files from your NeXT computer, you're working with Apple files, not UNIX files. This has several important ramifications.

Resource Forks

Apple files are made up of a data fork, a resource fork, or both. The data fork holds the file contents, while the resource fork includes system information, such as the name of the application used to create the file. On a NeXT computer, a data fork appears with the same file name as on the AppleShare server, while resource forks appears as *.filename.rsrc*. For example, a file named **Milestones** that has both a data fork and a resource fork will appear on a NeXT computer as **Milestones** and **.Milestones.rsrc**.

Resource forks have no purpose on a NeXT computer. However, if you transfer an AppleShare file from your NeXT computer to an Apple computer, perhaps by copying it onto a floppy disk, be sure to include the resource fork.

Application Ownership

The application associated with a given file is indicated on a NeXT computer by a file name extension, such as **.frame** or **.imp**. In order to have the correct application open an AppleShare file, you'll need to change its name in the File Viewer. For example, if **Milestones** is a WriteNow file, you would use the File Viewer to change its name to **Milestones.wn**. Double-clicking its name will open the document in WriteNow. Since end-of-line translation isn't performed on the AppleShare files, you may find some unexpected formatting within a document, depending on the application.

File Permissions

File ownerships and permissions are handled quite differently on AppleShare files and UNIX files. When you access AppleShare files from a NeXT computer, the files all appear to be owned by the current user, just as files on a removable disk are treated. However, files that have been designated private on the AppleShare server remain inaccessible on a NeXT computer.

Examining the NetInfo Database

When you enable AppleTalk networking, the NetInfo database is modified to reflect this. Use NetInfoManager to examine the changes:

1. Start up NetInfoManager.
2. Click **/localconfig** in the Domain window. This directory stores information that only applies to the local computer, including information about monitors, keyboards, and AppleShare networks.

F68.tiff ,

3. Click **AppleTalk**, then double-click it to open a Directory window.

F69.tiff ,

4. Click **Enabled**. The value **YES** indicates that the AppleTalk protocols and daemon should be started at boot time.
5. Click **AppleTalkPhase**. The value of this property indicates whether you're connecting to a network running AppleTalk Phase 1 or 2 (2 is the default).
6. Click **NetID**.

F70.tiff ,

The value of this property is the first network ID to be tried when the NeXT computer boots and connects to the AppleTalk network. If the value is invalid or the specified network ID is unavailable at boot time, the NeXT computer will connect using the first available network ID.

7. Click **NodeID**. The value of this property is the first node ID to be tried when the NeXT computer boots and connects to the AppleTalk network. If the specified node ID is unavailable, the NeXT computer will connect

using the first available ID.

8. Click **ZoneName**. If this property has a value, it indicates the name of the zone to use when connecting to the AppleTalk network. If this property has no value, or the indicated zone isn't available, the NeXT computer will use the default zone.
9. Click **AppleShare** in the domain window, then double-click it to open a Directory window.

F71.tiff ,

10. Click **Enabled**. The value **YES** indicates that the AppleShare protocols and daemon should be started at boot time.
11. Click **CharacterEncoding**.

F72.tiff ,

The value of this property indicates the keyboard mapping to be used to display AppleShare file names in the File Viewer. The only valid values are **MAC-ROMAN** and **SHIFT-JIS** (only used with the Japanese version of NeXTSTEP).

12. Click **ResourceForks**. This property is reserved for future use.
13. Close the Directory windows.

ISDN Networking

Generally, a network is thought of as being made up of computers in the same room, building, or campus. However, you might have individual computers at remote sites that need access to the network. There are many ways to provide such access, frequently involving a modem. An excellent solution is to set up ISDN (Integrated

Services Digital Network) connections. With ISDN, you can connect a remote computer to your network. Users logging in from the remote computer interact with the NeXTSTEP graphical interface as if they were directly connected.

Setting Up the ISDN Equipment

Your first step in configuring ISDN is to obtain and set up the appropriate equipment. You'll need to work closely with your phone company to obtain equipment and service. On each side of an ISDN connection, you need three things:

- ISDN phone line
- Network termination unit (such as the NT1U-200), with power supply
- A Hayes ISDN Extender or equivalent device

Contact the business office of your phone company to ask about ISDN (sometimes referred to as Centrex-IS) phone lines. Assuming ISDN lines are available in your area, you need to specify how the lines should be configured. If possible, have both channels configured with circuit-switched voice and circuit-switched data. If this isn't possible, have voice configured on one channel and data on the other.

Have your phone company install the phone lines and network termination units. Depending on the type of switch your phone company uses, you may need a Service Profile ID. Be sure to ask if you need one and, if so, what yours is. The Hayes ISDN Extender attaches to the DSP port of each NeXT computer, then to the network termination unit.

Configuring the Network Side

With the hardware requirements met, you can begin configuring the software by setting up the network side of the connection:

1. Log into the computer on the network that will accept incoming ISDN connections from remote computers.

2. Start up PhoneManager, located in **/NextAdmin**.
3. Click the Network button. The main window changes to show network configuration information.

F10.tiff ,

4. Modify the host name in the Hostname field under Remote. This is the host name that will identify the remote computer when it connects to the network.
5. Enter an Internet address for the remote computer in the Address field under Remote. If you're using automatic host addition, this field will already be filled in for you. Make sure the address is unique and conforms to the other addresses used on your network.
6. Modify or enter a host name and Internet address in the Hostname and Address fields under Interface. These are used to identify the ISDN device, not a computer.
7. Choose a domain that will be the parent of the local domain for the remote computer. If the default domain listed isn't what you want, click Set Domain, then choose a domain from the Select NetInfo Domain panel that appears.

F11.tiff ,

Consider carefully which domain should be the parent for the remote computer. The remote computer will be linked into the domain hierarchy of the network with access to the information in the parent domain's file system mounting information, user accounts, mail aliases, and so on.

8. If you want an extra level of security, enter a name in the Dial In Name field and a password in the Dial In Password field. With these set, a user will have to enter the name and password before they get to the regular login window when making a remote connection. These are used solely for ISDN connections, and aren't part of a user account.
9. Make sure the check box labeled Accept Connections is checked.

F12.tiff ,

10. Click the Set button. A panel appears containing all the configuration information.

F13.tiff ,

11. Review the values and, if they're acceptable, click OK. A panel appears asking for the **root** password of the local domain.

F14.tiff ,

12. Enter the password and click Login. Another panel appears, asking for the **root** password of the parent domain.

F15.tiff ,

13. Enter the password and click Login.

The network computer is now ready to accept ISDN connections.

Configuring the Remote Side

Now you're ready to configure the remote computer to initiate ISDN connections.

- 1.** Log into the remote computer and start up PhoneManager.
- 2.** Click the Phone Button to display the ISDN configuration information.

F16.tiff ,

3. Select the appropriate switch type. If your phone company uses an AT&T switch, do nothing. If it uses a Northern Telecom switch, drag the pop-up list under Switch Type to Northern Telecom and enter the service profile ID obtained from your phone company into the Service Profile ID text field.

F17.tiff ,

4. Click Set.

This computer is now ready to initiate ISDN connections.

Making a Connection

Now everything's configured and you're ready to make a connection.

1. Reboot the remote computer. When the login window appears, it shows a picture of a telephone in the lower right corner.

F18.tiff ,

2. Click the phone. The connect panel appears.

F63.tiff ,

3. Adjust the Timeout slider, if you want. If no activity occurs for longer than the time set here, the connection will be broken.
4. Enter the phone number of the computer set up to accept ISDN connections and click Connect. A short time later the ISDN Dialin Authentication panel appears if the network computer was configured with a dial-in name

and password.

F64.tiff ,

5. Enter the dial-in name and password into the fields, then click OK. The remote login window appears.

F65.tiff ,

6. Log into the network using any valid user account.

You can now work as if you were logged into a computer directly connected to the network with Ethernet.

Working While Connected

Although using an ISDN connection is considerably faster than a regular modem, performance is still slower than if you were directly connected with Ethernet. Starting up applications can take as long as 3 or 4 minutes, and opening and closing documents takes longer than if you were working with local files. To help speed up performance, consider storing applications on the local hard disk. You can also improve performance by copying remote files to the local disk, then copying them back when you're done working with them.

Disconnecting

When you're done working on the network, follow these steps to break the ISDN connection:

1. Choose Log Out from the Workspace Manager main menu. You're returned to the remote login window.

F51.tiff ,

2. Click the phone on the login window. The connect panel appears.

F53.tiff ,

3. Click Disconnect. The ISDN connection is broken, and you're returned to the login window on your local computer.

Using PhoneConnector

In most cases, you make an ISDN connection as described in the earlier section ^aMaking a Connection.^o However, you might find it useful to log into the local computer and then make an ISDN connection. With this situation, your work is on the local computer, but you can mount remote file systems and use UNIX commands to access other computers on the remote network.

Making a Connection with PhoneConnector

Use PhoneConnector to initiate a connection:

1. Log into the computer that's already been configured to initiate ISDN connections.
2. Start up PhoneConnector, located in **/NextAdmin**.
3. Choose New from the Connection menu. A connection panel appears.

F19.tiff ,

4. Enter the phone number of the remote computer in the Phone # text field.
5. Adjust the Timeout slider, if you want. You will be disconnected from the remote network when no access has been made for the amount of time set with the Timeout slider (the default is 30 minutes).

6. Click Connect. A short time later the ISDN Dialin Authentication panel appears if the network computer was configured with a dial-in name and password.

F67.tiff ,

7. Enter the dial-in name and password into the text fields, then click OK. A short time later, the connection will be made. You can now access the remote network from your local computer (see the next section).
8. When you're done working with the remote network, click Disconnect in the PhoneConnector panel. You're automatically disconnected if you log out or if you don't access the remote network within the timeout period.

Accessing Remote Directories

You continue to work on the local computer, but you now have access to the remote network. For example, you can mount a remote directory, assuming it's been exported with access granted to the remote host you set up with PhoneManager for ISDN connections.

If the parent domain of the ISDN connection contains mount information for remote directories under **/Net**, they'll automatically appear in your File Viewer.

Other remote directories can be mounted using a command similar to the following:

```
mount server:/directory /local_mount_point
```

In this command, *server* is replaced by the host name of the file server on the remote network, */directory* is the name of the exported directory, and */local_mount_point* is the name of the mount point where you want the remote directory to appear on the local computer. If there's already mounting information for the remote directory in the NetInfo domain, you can omit */local_mount_point*; the directory will be mounted on the directory specified in the mount entry in NetInfo.

Saving Connections

If you use PhoneConnector to make repeated connections to the same remote site, you can save the connection information in a file to be reused.

1. Start up PhoneConnector.
2. Enter a phone number in the text field and adjust the Timeout slider.
3. Choose Save from the Connection menu. A Save panel appears.

F20.tiff ,

4. Choose an appropriate directory to hold your connection files, then enter a file name in the text field. Click OK.
5. To use this file in the future, choose Open from the Connection menu of PhoneConnector, or just double-click the file name in the File Viewer.

Examining the NetInfo Database

Your ISDN configuration included changes to the NetInfo databases. Use NetInfoManager to examine these changes:

1. Log into the network computer that's set up to accept ISDN connections.
2. Start up NetInfoManager.
3. In the local domain window, click **/localconfig**, then **ISDN**.

F21.tiff ,

4. Click **Networking**, then double-click it to open a Directory window.

F22.tiff ,

- 5. Click the various properties and examine the values. These reflect the configuration information you entered with PhoneManager.
- 6. Close the Directory window, then open the root domain (the domain you selected as the parent domain in PhoneManager).
- 7. Click **/machines**, then the name you gave to the remote connection. Double-click the name to open a Directory window.

F23.tiff ,

- 8. Click **isdn_dialin_host**.

F24.tiff ,

The value of this property identifies the host that's been configured to accept ISDN connections. The other properties in this directory are the standard properties for a host entry. Notice that this host serves a local domain.

- 9. Close the Directory window, then open one for the host name you gave to the local ISDN connection.

F25.tiff ,

Again, this directory has a property called **isdn_dialin_host** identifying the host configured to accept ISDN connections.

- 10. Close the Directory window.
- 11. Log into the remote computer and start up NetInfoManager.
- 12. In the local domain window, click **/localconfig/ISDN/Phone**. Double-click the name to open a Directory

window.

F26.tiff ,

The property **SwitchType** identifies the type of switch used by your phone company, as configured with PhoneManager. If the type is **dms** (Northern Telecom), there's also a property named **ServiceProfile** containing the Service Profile ID you entered in PhoneManager.

SNMP

SNMP (simple network management protocol) is a facility that allows you to collect statistics for a network of computers. You might already have a network management program running on your computers that uses SNMP to collect information. If you do, you can enable SNMP on your NeXT computers so that your management program will include the NeXT computers in its data collection. If you don't already have such a management program on your computers, there's no need to enable SNMP on your NeXT computers.

Enabling SNMP

The daemon process **/usr/etc/snmpd** is run to enable SNMP on a NeXT computer. The **snmpd** daemon is started with the **-N** flag from **/etc/rc** during system boot. When **snmpd** is executed with the **-N** flag, it checks the NetInfo databases for configuration information. If none is found, **snmpd** exits.

Follow these steps to modify the NetInfo database so that SNMP is enabled when the computer boots:

1. Start up NetInfoManager.
2. In the local domain window, click **//locations** (if you want to enable SNMP for more than one NeXT computer, open the root domain or an appropriate midlevel domain).

3. Choose New Subdirectory from the Domain menu. A directory named **newValue** is created.

F27.tiff ,

4. Double-click newValue to open a Directory window.
5. Click **newValue**, enter **snmp** in the text field and press Return.
6. Click **name**, then choose Append Property from the Directory menu.
7. Click **new_property**, then enter **enabled** in the text field and press Return.
8. Choose New Value from the Directory menu.
9. Click **new_value** in the Values column, then enter **yes** in the text field and press Return.

F29.tiff ,

10. Choose Save from the Directory menu to save the changes to the new directory. Enter the **root** password, if prompted.

When **snmpd** is started with the **-N** option, it checks for the **enabled** property in the **/locations/snmp** NetInfo directory. With the value of this property set to **yes**, **snmpd** will run the next time this computer is booted.

Defining Communities

An **snmp** community is a collection of computers or networks the members of which have access to network information about the other members. You define communities with NetInfoManager.

1. Click **/locations/snmp** in the domain window.
2. Choose New Subdirectory from the Domain menu. Double-click the new subdirectory to open a Directory

window.

3. Click **newValue** in the Values column, enter **communities** in the text field, and press Return. Choose Save from the Directory menu.

F30.tiff ,

4. Close the Directory window, then click **//locations/snmp/communities** in the domain window.

F31.tiff ,

5. Choose New Subdirectory from the Domain menu, then double-click **newValue** to open a Directory window.
6. Click **newValue** in the Values column, enter **public** in the text field, then press Return.
7. Click **name**, then choose Append Property from the Directory menu.

F32.tiff ,

This property will determine which hosts or networks will have access to the information provided by SNMP.

8. Enter either **hosts** or **networks** into the text field. Enter **hosts** if you will specify access by individual hosts, **networks** if you will specify access by networks. Press Return.
9. Choose New Value from the Directory menu. If you named the property **hosts**, enter a host name or Internet address in the text field. If you named the property **networks**, enter a network name or address, such as **192.72.142** (no trailing period). If you want to allow access to all hosts or all networks, enter **a*o** instead. Press Return.

F33.tiff ,

10. If you are specifying access by individual host names or network addresses, choose Append Value from the

Directory menu. Enter a host name or network address in the text field and press Return. Repeat for all other host names or network addresses that you're granting access to.

11. Choose Save from the Directory menu, then close the Directory window.

F34.tiff ,

12. Reboot the computer (or computers, if you put the directories in the root domain). The **snmpd** daemon will be started, granting access to those hosts or networks you specified in the **public** directory.

Tip: If you want to enable SNMP temporarily, you can enter **/usr/etc/snmpd -A** in a shell window. This starts the SNMP daemon without any access control.

SNMP Commands

Two commands are available to report information from SNMP. The commands **snmp** and **snmpnetstat** (both located in **/usr/bin**) allow you to inspect the status of a networked machine, such as a computer or gateway. For example, you can verify that SNMP communication is working properly by entering the following command in a shell window, replacing *hostname* with the host name of a computer running SNMP:

```
snmp status hostname
```

The output from this command should be something like this:

```
NeXT Mach 3.0: Wed Apr  1 17:44:27 PST 1992;  
root(kodak):mk-127.5.1/BUILD/RELEASE_M68K
```

Name	Speed	Type	Stat	Ibyte	Obyte	Ierr	Oerr	Physical Address
en0		other	up	4.3MB	6.9MB	<.1%	<.1%	00:00:0F:00:32:41
lo0		other	up	1.6MB	1.6MB	<.1%	<.1%	
en0		other	down	5.9KB	5.9KB	<.1%	<.1%	
isdn0	64Kb	basicIsd	down	0 B	0 B			
en0	10Mb	ethernet	up	4.3MB	6.9MB	<.1%	<.1%	

More information can be found in the UNIX manual pages for **snmp**, **snmpd**, and **snmpnetstat**.

Troubleshooting

Problems can arise in a mixed network due to a number of causes. If you're encountering difficulties, review the steps you took to configure the network. Double-check all configuration files and NetInfo entries. A small error can have far-reaching consequences. Here are a couple of common problem areas:

- **Permissions** If users are having problems accessing files, make sure that there is a corresponding user account for each NeXT user on the UNIX or NetWare servers. Also check that group accounts are duplicated on both sides of the network. On UNIX networks, make sure that each user name, user ID, group name, and group ID is unique and exactly matches the corresponding information on the other side of the network. On NetWare servers, make sure that the files NFSUSERS and NFSGROUP have accurate entries for the NeXT user IDs and group IDs.
- **Mounting** If you're having problems accessing NFS directories on a UNIX network, make sure that each directory is exported correctly. Check NFSManager on the NeXT computers and **/etc/exports** on the non-NeXT computers. Make sure the mounting information is accurate on both the NeXT (NFSManager) and non-NeXT (**/etc/fstab**) computers and that it's in the correct domain on the NeXT computers.