NetWare Server Security

Administration Guide
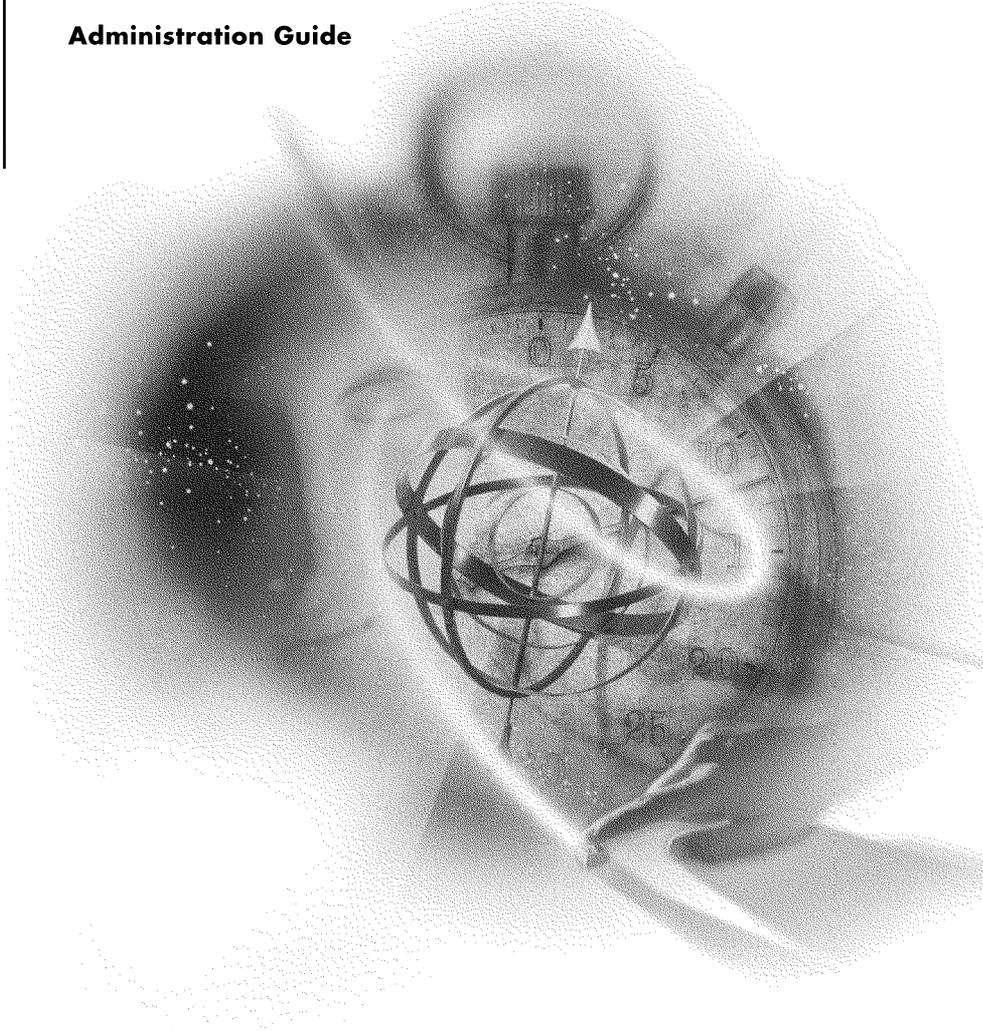
NetWare® 5.1

NETWORKING SOFTWARE

Novell®

**Legal Notices**

**Online Documentation:** To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

**Novell Trademarks**

For a list of Novell trademarks, see the final appendix of this book.

**Third-Party Trademarks**

All third-party trademarks are the property of their respective owners.

# Contents

# Server Security

NetWare® provides many features and tools for protecting your server and network. For a general discussion of NetWare security features, see "Understanding" on page 9.

Important security strategies include protecting the server console itself, protecting the network from viruses, and using an uninterruptible power supply. Specific security features of NetWare include NCP packet signature and the Transaction Tracking System™. For information about these topics, see "Managing" on page 17.

The following topics are also important to maintaining a secure server:

- *Disks and Storage Devices* > Managing > Mirroring and Duplexing Partitions in the NetWare 5.1 online documentation.

- *Disks and Storage Devices* > Managing > Managing Removable Media Devices > Locking and Unlocking a Removable Media Device in the NetWare 5.1 online documentation.

- *Auditing the Network* in the NetWare 5.1 online documentation.

# 1 **Understanding**

NetWare protects data by providing duplicate directory entry (DET) and file allocation tables (FAT), by providing features such as packet signature and the Transaction Tracking System, and by enabling the use of an uninterrupted power supply (UPS). A general discussion of these features is provided in this section.

NetWare also provides system fault tolerance by redirecting data from bad blocks to reliable blocks on the server's hard disk, and by mirroring and duplexing partitions. For information about these features, see *Disks and Storage Devices* > Understanding > Redirecting Bad Blocks and *Disks and Storage Devices* > Managing > Mirroring and Duplexing in the NetWare 5.1 online documentation.

## Duplicate File Directories

In the traditional NetWare file system, a disk's directory entry table (DET) and file allocation table (FAT) contain address information that tells the operating system where data can be stored or retrieved. If the blocks containing these tables are damaged, some or all of the data might be irretrievable.

NetWare greatly reduces the possibility of losing this information by maintaining duplicate copies of the DET and FAT on separate areas of the hard disk.

If one of the blocks in the original tables is damaged, the operating system switches to the duplicate tables to get the location data it needs. The faulty sector is then listed in the disk's bad block table, and the data it contained is stored elsewhere on the disk.

Every time the server is turned on, the operating system performs a consistency check on both sets of DETs and FATs to verify that the two copies are identical. If both sets don't match, a warning is sent, and the network administrator should run VREPAIR.

# NCP Packet Signature

NetWare includes a security feature called NCP packet signature that protects servers and clients using the NetWare Core Protocol™ (NCP) services.

NCP packet signature prevents packet forgery by requiring the server and the client to sign each NCP packet. The packet signature changes with every packet.

Without NCP packet signature installed, a user could pose as a more privileged user and send a forged NCP request to a NetWare server. By forging the proper NCP request packet, an intruder could gain the Supervisor object right and access to all network resources.

NCP packets with incorrect signatures are discarded without breaking the client's connection with the server. However, an alert message about the invalid packet is sent to the error log, the affected client, and the server console. The alert message contains the login name and the station address of the affected client.

If NCP packet signature is installed on the server and all of its workstations, it is virtually impossible to forge a valid NCP packet.

For additional information about packet signature, see:

## When to Use Packet Signature

NCP packet signature is recommended for security risks such as

- ◆ An untrustworthy user at a workstation on the network
- ◆ Easy physical access to the network cabling system
- ◆ An unattended, publicly accessible workstation

NCP packet signature is not necessary for every installation. You might choose not to use NCP packet signature if you can tolerate security risks in situations such as

- ◆ When only executable programs reside on the server
- ◆ You know and trust all network users
- ◆ Data on the NetWare server is not sensitive and loss or corruption of this data would not affect operations

## NCP Packet Signature Options

Because the packet signature process consumes CPU resources and slows performance both for the client and the NetWare server, NCP packet signature is optional.

Several signature options are available, ranging from never signing NCP packets to always signing NCP packets. NetWare servers and NetWare clients each have four settable signature levels.

The signature options for servers and clients combine to determine the level of NCP packet signature on the network.

You can choose the packet signature level that best meets both your system performance needs and network security requirements.

**NOTE:** Some combinations of server and client packet signature levels can slow performance. However, low-CPU-demand systems might not show any performance degradation.

# Effective Packet Signature

The NCP packet signature levels for the server and the client interact to create the effective packet signature for the network. Some combinations of server and client levels do not allow logging in.

The following figure shows the interactive relationship between the server packet signature levels and the client signature levels.

**Figure 1    Effective Packet Signature of Server and Client**

| If | Server = 0 | Server = 1 | Server = 2 | Server = 3 |
|----|:----------:|:----------:|:----------:|:----------:|
| **Client = 0** | ○ | ○ | ○ | ⊘ |
| **Client = 1** | ○ | ○ | ● | ● |
| **Client = 2** | ○ | ● | ● | ● |
| **Client = 3** | ⊘ | ● | ● | ● |

● Packet signature
○ No packet signature
⊘ No logging in

# Recommended Signature Levels

The default NCP packet signature level is 1 for clients and 1 for servers. In general, this setting provides the most flexibility while still offering protection from forged packets. Following are some examples of situations requiring different signature levels.

| Situation | Example | Recommendation |
|-----------|---------|----------------|
| All information on the server is sensitive. | If an intruder gains access to *any* information on the NetWare server, it could damage the company. | Set the server to level 3 and all clients to level 3 for maximum protection. |
| Sensitive and nonsensitive information reside on the same server. | The NetWare server has a directory for executable programs and a separate directory for corporate finances (such as Accounts Receivable). | Set the server to level 2 and the clients that need access to Accounts Receivable to level 3. All other clients remain at the default, level 1. |

| Situation | Example | Recommendation |
|---|---|---|
| Users often change locations and workstations. | You are uncertain which employees will be using which workstations, and the NetWare server contains some sensitive data. | Set the server to level 3. Clients remain at the default, level 1. |
| A workstation is publicly accessible. | An unattended workstation is set up for public access to nonsensitive information, but another server on the network contains sensitive information. | Set the sensitive server to level 3 and the unattended client to level 0. |

For information on implementing NCP Packet Signature, see .

# Transaction Tracking System

NetWare includes a transaction-monitoring feature called the Transaction Tracking System™ (TTS™). If you flag a file as transactional, TTS can prevent corruption of records in the file by backing out of incomplete transactions and keeping a record of backed-out data.

**NOTE:** A file flagged as transactional cannot be deleted or renamed.

TTS can also back out file truncations or extensions and multiple changes to the same data area during a single transaction. TTS can even back out interrupted backouts if the NetWare server fails in the middle of backing out transactions.

By default, NetWare uses TTS to protect the NDS$^{®}$ database from corruption. But TTS can protect against these types of failures for any type of application that issues record-locking calls and stores information in records, including traditional databases, some electronic mail applications, and some workgroup appointment schedulers.

Files that aren't organized into discrete records (such as word processing files) aren't protected by TTS.

TTS is available only for the traditional NetWare file system.

**WARNING:** By default, TTS is enabled. Do not disable TTS intentionally because this will prevent updates to the NDS replicas on the server.

Transactions on a network can be saved improperly in any of the following situations:

- Power to a server or a workstation is interrupted during a transaction.

- Server or workstation hardware fails during a transaction (for example, a parity error on a network board).

- A server or workstation hangs (a software failure) during a transaction.

- A network transmission component (such as a hub, a repeater, or a cable) fails during a transaction.

If the server fails and the file has been flagged transactional, TTS backs out the transaction when the server comes up again. If a workstation or network transmission component fails, TTS backs out the transaction immediately.

NDS transactions are always backed out by TTS; you do not need to flag the NDS database in any way.

## How TTS Works

TTS guarantees that all changes to a database file are either wholly completed or not made at all. TTS follows these steps to track transactions:

1. When the application allocates a physical or logical record lock, TTS infers that the application is making a transaction. At this point, if you have flagged the file as transactional, TTS begins tracking the transaction so that the transaction can be backed out if a failure occurs.

2. TTS makes a copy of the original data so the data can be restored if the transaction fails. A copy of the data is placed in a file external to the database. This external file contains all transaction backout information; only the operating system uses it.

3. After the copy of the original data has been written to the backout file, TTS writes the changed data to the database file.

4. TTS repeats Steps 2 and 3 for additional changes (a single transaction can consist of a sequence of changes).

5. When all changed data has been written to disk, and the database application releases physical and logical record locks, TTS infers that the application has completed the transaction. TTS writes a record to the backout file, indicating that the transaction is complete, and stops tracking the transaction.

To learn how to use TTS, see .

# Uninterruptible Power Supply (UPS)

An uninterruptible power supply (UPS) is a backup power unit that supplies uninterrupted power if a commercial power outage occurs. A UPS is an indispensable part of your network. Not only does it help prevent damage to your computers from power surges and brownouts, but it also prevents data loss during power outages.

Both online and offline UPS systems are available:

- **Online UPS**. Actively modifies the power as it moves through the unit. If a power outage occurs, the unit is already active and continues to provide power.

  An online UPS is usually more expensive than an offline UPS, but provides a nearly constant source of energy during power outages.

- **Offline UPS**. Monitors the power line. When power drops, the UPS is activated.

  The drawback to this method is the slight lag before the offline UPS becomes active. However, most offline UPS systems are fast enough to offset this lag.

Because UPS systems can be expensive, most companies attach them only to the most critical devices, such as NetWare servers, routers, and hard disk subsystems.

Attaching a UPS to a server enables the server to properly close files and rewrite the system directory to disk.

Unfortunately, most programs run on the workstation and data stored in RAM is not saved during a power outage unless each station has its own UPS.

If the UPS doesn't have its own form of surge protection, install a surge protector to protect the UPS.

For instructions for using UPS with a serial port, see "Using UPS with a Serial Port" on page 25.

# 2 Managing

Two important general security strategies include protecting the server console itself and protecting the network from viruses. See "Securing the Server Console" on page 17 and "Preventing Virus Infection" on page 21.

To use specific security features of NetWare, see "Using NCP Packet Signature" on page 21, "Using UPS with a Serial Port" on page 25, and "Protecting Database Integrity with TTS" on page 28.

For information on auditing the use of the network, see *Auditing the Network* in the NetWare 5.1 online documentation.

## Securing the Server Console

The first principle of server console security is physical security. If you don't provide physical security, nothing else you do matters very much.

The processing unit should be locked in a place where no one can remove it or reboot it. Some network administrators remove both the keyboard and the monitor and manage the server remotely by using the Remote Management Facility (RCONSOLE and REMOTE). We suggest that you also consider using a power-on password whether you manage at the console or use RCONSOLE at a workstation.

Two utilities provide additional security at the console:

◆ The SECURE CONSOLE command (For more information, see *Utilities Reference* > Utilities > SECURE CONSOLE in the NetWare 5.1 online documentation.)

◆ The screen saver console-lock feature (For more information, see *Utilities Reference* > Utilities > SCRSAVER in the NetWare 5.1 online documentation.)

Procedures for using the utilities follow:

## When to Use SECURE CONSOLE

When you have provided physical security for your server, you should secure the console. The SECURE CONSOLE utility provides the following security features, while still allowing administrators to use the console:

- Prevents NetWare Loadable Module™ programs from being loaded from any directory other than SYS:SYSTEM or C:\NWSERVER. This means that no one can load an invasive NLM™ from a server's diskette drive or boot partition unless it is already in a search path.

- Prevents keyboard entry into the operating system debugger. This restricts the ability to alter the operating system.

- Prevents anyone from changing the date and time. Some security and accounting features depend on date and time for their enforcement.

Keep in mind that when you issue SECURE CONSOLE, the server must be taken down and rebooted to un-secure the console. (Now that server parameter settings are persistent in NetWare 5.1, you can down the server without losing the settings you made to optimize and tune your server.) For more information, see *Utilities Reference* > Utilities > SECURE CONSOLE in the NetWare 5.1 online documentation.

When you use SECURE CONSOLE with the Remote Management Facility, access via RCONSOLE is subject to the protections provided by SECURE CONSOLE.

SECURE CONSOLE does not lock the server console. You can lock the console by using SCRSAVER. If the console is locked using the console-locking feature, an intruder can still access the console from a remote workstation; however, the intruder must still be authenticated to NDS® through the SCRSAVER console lock.

**HINT:** For procedures on protecting the server console by encrypting the RCONSOLE password in the AUTOEXEC.NCF file, see *Remote Server Management* > Managing > Using DOS-Based Remote Console > Loading

Remote Modules on Bootup in the NetWare 5.1 online documentation. For procedures on restricting remote connections, see *Utilities Reference* > Utilities > REMOTE in the NetWare 5.1 online documentation.

## Using the SECURE CONSOLE Command

To secure the server console, enter at the server console prompt:

```
SECURE CONSOLE
```

To secure the server console whenever the server is booted, add the SECURE CONSOLE command to the server's autoexec.ncf file. If the autoexec.ncf file loads modules from any directory other than SYS:SYSTEM or C:NWSERVER, then in the .ncf file the SECURE CONSOLE command must follow the LOAD commands for these modules.

**IMPORTANT:** To remove SECURE CONSOLE, you must first down the NetWare server and reboot it. If the SECURE CONSOLE command is in the autoexec.ncf file, use EDIT or any text editor to remove it before you down the server and reboot.

## Using SCRSAVER to Lock the Server Console

The console-locking feature has been removed from MONITOR and included with the screen saver in its own module, scrsaver.nlm.

When the screen saver is activated, it displays a moving snake for each processor on the server. Each snake is a different color: the first one is red; the second is blue, etc. The speed of each snake and the length of its tail are directly proportional to the processor's utilization.

The console-locking feature allows you to require a password before gaining access to the server console prompt. If a key is pressed when the console lock is enabled, a dialog box appears. You must then supply an NDS username and password. In addition, the User object must have Write rights to the access control list (ACL) of the Server object to gain access to the server console prompt.

If the console is unlocked, press any key to activate the console. The snake screen will disappear.

1 To display command options for SCRSAVER, enter at the server console prompt

```
SCRSAVER HELP
```

Command options allow you to enable and disable locking, check the status of the lock options, and change the length of time the console is allowed to be inactive before the screen saver is activated. The default is 600 seconds (10 minutes).

**2** For more information about a command option, enter at the console prompt

`SCRSAVER HELP command_option`

**3** To load the SCRSAVER module, enter at the server console prompt

`SCRSAVER [option; option...]`

When you load the screen saver, the default is to enable the console-locking feature and to require a password for access. The corresponding NDS user must have Write rights to the Access Control List (ACL) of the Server object.

For more information, see *Utilities Reference* > Utilities > SCRSAVER in the NetWare 5.1 online documentation.

## Unlocking the Server Console

The console-locking feature has been removed from MONITOR and included with the screen saver in its own module, scrsaver.nlm.

**1** From the screen saver snake display, press any key.

**2** At the login box, press Enter to highlight the username field.

The login box appears only if the console is locked.

**3** Enter the username.

The User object must have Write rights to the ACL for the Server object.

If the username field is blank or if you want to change the username, type in an NDS™ username and context. Again the User object must have the required rights.

**4** Press Enter again to highlight the password field.

**5** Type the password for the username and press Enter twice.

The screen saver disappears and the server console screen appears.

# Preventing Virus Infection

Keep viruses off the network by educating users about virus dangers and by enforcing procedures that reduce virus risks, such as the following:

- Back up data frequently.

- Maintain layers of archived backups so you can retrieve a backup from a preinfected file.

- Keep a write-protected, bootable diskette with the latest virus scan and removal software for all servers and workstations.

- Keep a backup of executable files and flag them Execute Only.

- Educate yourself about the infection techniques of the latest viruses.

- Educate network users about how to detect viruses.

- Warn users of the dangers of viruses. Discourage them from using diskettes and files that have been in computers away from work.

- Teach users to power down their workstations immediately upon encountering a virus.

- Restrict access to a server's diskette drives by locking the server in a secure room. Put tape over the drive openings to remind you not to use them unnecessarily.

- Avoid using the Admin account when possible. The fewer privileges your login account has, the less power a virus has to destroy data and to spread.

# Using NCP Packet Signature

NetWare includes a security feature called NCP Packet Signature that protects servers and clients using the NetWare Core Protocol™ (NCP) services. For general information about NCP Packet Signature, see "NCP Packet Signature" on page 10.

Instructions for using NCP Packet Signature follow:

## Server Signature Levels

◆ To determine the server's current signature level, enter

**SET NCP Packet Signature Option**

◆ To set a server's packet signature level, enter

**SET NCP Packet Signature Option = *number***

Replace *number* with 0, 1, 2, or 3. The default is 1

| Number | Explanation |
|--------|-------------|
| 0 | Server does not sign packets (regardless of the client level). |
| 1 | Server signs packets *only* if the client requests it (client level is 2 or higher). |
| 2 | Server signs packets if the client is capable of signing (client level is 1 or higher). |
| 3 | Server signs packets and requires all clients to sign packets or logging in will fail. |

You can use the SET console command to change the signature level from a lower to a higher level.

You cannot change from a higher to a lower level unless you first reboot the server. For example, if the current signature level is 2, you can't set the signature level to 1 by using the SET command at the console. To change the signature level from 2 to 1, you must add the SET command to the startup.ncf file and then restart the server:

**SET NCP Packet Signature Option = 1**

You can add this SET command to your startup.ncf file to set the signature level each time the server is brought up.

## Client Signature Levels

Set client signature levels to 0, 1, 2, or 3. The default is 1. Increasing the value increases security, but decreases performance.

| Number | Explanation |
|--------|-------------|
| 0 | Disabled. Client does not sign packets. |
| 1 | Enabled, but not preferred. Client signs packets *only* if the server requests it (server level is 2 or higher). |

| Number | Explanation |
| --- | --- |
| 2 | Preferred. Client signs packets if the server is capable of signing (server level is 1 or higher). |
| 3 | Required. Client signs packets and requires the server to sign packets or logging in will fail. |

◆ To set DOS or MS Windows client signature levels, add the parameter to the workstation net.cfg file, as follows:

**signature level = *number***

◆ To set the Windows 95 or Windows NT client signature level for an individual workstation, change the parameter setting with the Advanced Settings tab of Novell NetWare Client Properties, as follows:

From the system tray, right-click N

Click Novell Client Properties

Click Advanced Settings, then select Signature Level from the scrollable list

You can set the signature level for multiple clients at once by adding the signature level to the configuration file when you install the clients.

For information about configuring Novell Clients, see *Novell Clients > Setting Client Properties (http://www.novell.com/documentation/lg/noclienu/noclienu/data/hbqx7szx.html)* in the NetWare 5.1 online documentation.

You can also refer to the Novell Client Install Manager (NCIMAN) online help for more information. You will find NCIMAN for Windows 95 on the NetWare client CD at Products \ibm_enu\admin. You will find NCIMAN for Windows NT on the NetWare client CD at Products \winnt\i386\nls\english\admin.

## Changing the Signature Level for an NLM

NLM programs that use the Novell Runtime Libraries are assigned a default NCP Packet Signature level that corresponds to the current signature level of the server.

To change the packet signature level for a single NLM, use the following command syntax when you load the NLM:

**[LOAD] *NLM* [CLIB_OPT]/L *number***

Replace *number* with 0, 1, 2, or 3.

# Packet Signature and Job Servers

A job server is a server that performs a task and then returns the completed task. Most job servers are third-party products.

You should be aware that some job servers do not support NCP Packet Signature. A job server might produce unsigned sessions if

- It does not operate on top of DOS
- It does not use standard Novell clients
- It is not an NLM
- It uses its own implementation of the NCP engine (such as embedded print servers in printers)

## Minimizing Risks

To minimize security risks associated with job servers:

- Install queues only on servers with signature level 3.
- Do not allow privileged users to put jobs in queues on servers with signature levels below 3.
- Make sure the job server's account is unprivileged.
- Disable the job server's ability to change to client rights.

## Disabling Change to Client Rights

To prevent a job server from assuming the rights of a client, add the following SET command to the server's startup.ncf file:

`SET Allow Change to Client Rights = OFF`

The default is ON, because certain job servers and third-party applications cannot function without changing to client rights. Refer to the documentation that comes with the job server to determine whether the job server can function without client rights.

# Using UPS with a Serial Port

For general information about Uninterruptible Power Supplies, see "Uninterruptible Power Supply (UPS)" on page 15.

Use ups_aio.nlm when you use a serial port to monitor an uninterruptible power supply.

The UPS_AIO module for the serial port does not allow you to change parameter settings after loading the module. You must specify the parameter settings you need when you load the module. If you want to change the settings, reload the module with the new parameter values.

To display a help screen that explains the parameters, enter the following command:

**UPS_AIO ?**

The UPS_AIO command with the ? parameter displays a help screen, but does *not* load the UPS_AIO module.

You do not need to enter any parameters if the default values are acceptable. Before loading UPS_AIO, review the following table to determine the parameters you might want to enter.

Table 1      Parameter values for UPS_AIO

| Parameter | Use to |
| --- | --- |
| *path* | Specify the path to UPS_AIO only if you moved it from the default directory (SYS:SYSTEM) and if there is no server search path to the directory where the file is located. |
| DOWNTIME=*number* | Specify the amount of time to run on battery before system shutdown. If power is restored before this time elapses, no shutdown will occur. If a low battery condition occurs before this time elapses, an immediate shutdown will occur.<br><br>**Supported values:** 30 seconds minimum, no practical maximum limit<br>*Default:* 300 seconds |

| Parameter | Use to |
|---|---|
| MSGDELAY=*number* | Specify the elapsed time before a broadcast message is sent to all clients logged into the server.<br><br>**Supported values:** 0 seconds minimum, no practical maximum limit<br>*Default:* 5 seconds<br><br>The broadcast message states the time remaining until shutdown. |
| MSGINTERVAL=*number* | Specify the time interval between broadcast messages sent to users. The message is repeated at this interval.<br><br>**Supported values:** 20 seconds minimum, no practical maximum limit<br>*Default:* 30 seconds<br><br>The broadcast message states the time remaining until shutdown. |
| DRIVERTYPE=*number* | Specify the AIO device driver type.<br><br>**Supported values:** 1, 2, 3<br>*Default:* 1<br><br>The default value of 1 represents the AIOCOMX driver, which is included with NetWare. Other drivers might be represented by other numbers. Refer to the documentation that came with the driver. |
| BOARD=*number* | Specify the AIO board number.<br><br>**Supported values:** Determined by the driver manufacturer<br>*Default:* 0<br><br>To determine the board number, read the driver information when the AIOCOMX driver is loaded. The information includes both the board and port numbers.<br><br>If you do not use the AIOCOMX driver, refer to the driver documentation to determine the board number. |

| Parameter | Use to |
|---|---|
| PORT=*number* | Specify the port number.<br><br>**Supported values:** Determined by the driver manufacturer<br>*Default:* 0<br><br>To determine the port number, read the driver information when the AIOCOMX driver is loaded. The information includes both the port and board numbers.<br><br>If you do not use the AIOCOMX driver, refer to the driver documentation to determine the port number. |
| SIGNAL_HIGH | Set the normal RS-232 signaling state to high.<br><br>**Supported values:** SIGNAL_HIGH or no value<br>*Default:* none<br><br>Use this parameter only if your UPS system uses high values, instead of low values, to determine if power is off or the battery is low. Most UPS systems use low values. Refer to your UPS hardware documentation to determine whether you need to use the parameter. |
| ? | Display a help screen that explains the other parameters. When you use this parameter, the UPS_AIO module is not loaded. To load the module, execute LOAD UPS_AIO without the ? parameter. |

## Prerequisites

❑ A serial port must be available.

❑ The UPS_AIO module requires an AIO device driver, such as AIOCOMX, which is included with NetWare.

❑ You should know which parameters, if any, you want to specify when you load the UPS_AIO module. See

## Procedure

1 To load the AIOCOMX driver, enter

`[LOAD] [*path*]\AIOCOMX`

You can use another AIO driver, if specified by your hardware manufacturer.

When you load AIOCOMX, the screen displays the board and port numbers. If either the board or port number is not 0, note the number. You will enter the number as a parameter in the next step.

**2** To load the UPS_AIO module, enter

`[LOAD] [`*`path`*`]UPS_AIO [`*`parameter= value...`*`]`

If you do not enter a parameter, the default value for that parameter takes effect. For a description of parameters and their values, see Table 1 on page 25.

For example:

`[LOAD] UPS_AIO DOWNTIME=60`

Once UPS_AIO is loaded, the UPS screen displays the current status and activity of the module. These messages are also logged to the system error log, sys$log.err, in the SYS:SYSTEM directory.

**3** (Optional) To toggle from the status screen to other screens, press Alt + Esc.

To load the driver and the UPS_AIO module automatically whenever you start the server, enter the commands into the autoexec.ncf file. You can use NWCONFIG or EDIT to add the commands to the file.

# Protecting Database Integrity with TTS

The Transaction Tracking System (TTS) can prevent data corruption by backing out of incomplete transactions and keeping a record of backed-out data. TTS is available only for the traditional NetWare file system.

**WARNING:** By default, TTS is enabled. Do not disable TTS intentionally because this will prevent updates to the NDS replicas on the server.

The NetWare server automatically disables TTS if one of the following happens:

 The volume SYS: becomes full. (The SYS: volume is the TTS backout volume.)

 The NetWare server has insufficient memory to operate TTS.

If TTS has been disabled and you have solved the problems that led to its disabling, use the ENABLE TTS command to enable TTS again. Enter the following at the server console prompt:

**ENABLE TTS**

To enable and manage transaction tracking for individual files, use the commands and parameters in the following table.

| To . . . | Do the following . . . |
|---|---|
| Enable transaction tracking for a file. | Use NWADMIN to flag the file as transactional. |
| | (Note that files flagged as transactional cannot be deleted or renamed.) |
| | See *Utilities Reference* > Utilities > NetWare Administrator in the NetWare 5.1 online documentation. |
| Enable TTS to backout transactions without displaying confirmation prompts. | Place the following command into the startup.ncf file and restart the server: |
| | SET AUTO TTS BACKOUT FLAG = ON |
| | If this parameter is set to On, the backouts happen automatically. The parameter is set to ON by default. |
| | If this parameter is set to Off, you will be prompted to confirm file backouts. |
| | You can also set the parameter using MONITOR. From MONITOR, in the Available Options field, select Server Parameters > Transaction Tracking. |

| To . . . | Do the following . . . |
| --- | --- |
| Log backed out data to the sys:tts$log.err file. | Execute the following command at the server console prompt:<br><br>SET TTS ABORT DUMP FLAG = ON<br><br>If this parameter is set to ON, the transactions are stored in sys:tts$log.err.<br><br>If this parameter is set to Off, the transactions are backed out, but the server does not provide you with a record of the backouts.<br><br>You can also set the parameter using MONITOR. From MONITOR, in the Available Options field, select Server Parameters > Transaction Tracking. |
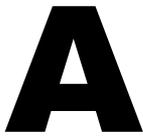
# A Novell Trademarks

Access Manager is a registered trademark of Novell, Inc. in the United States and other countries.

Advanced NetWare is a trademark of Novell, Inc.

AlarmPro is a registered trademark of Novell, Inc. in the United States and other countries.

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppTester is a registered service mark of Novell, Inc. in the United States and other countries.

BrainShare is a registered service mark of Novell, Inc. in the United States and other countries.

C-Worthy is a trademark of Novell, Inc.

C3PO is a trademark of Novell, Inc.

CBASIC is a registered trademark of Novell, Inc. in the United States and other countries.

Certified NetWare Administrator in Japanese and CNA-J are service marks of Novell, Inc.

Certified NetWare Engineer in Japanese and CNE-J are service marks of Novell, Inc.

Certified NetWare Instructor in Japanese and CNI-J are service marks of Novell, Inc.

Certified Novell Administrator and CNA are service marks of Novell, Inc.

Certified Novell Engineer is a trademark and CNE is a registered service mark of Novell, Inc. in the United States and other countries.

Certified Novell Salesperson is a trademark of Novell, Inc.

Client 32 is a trademark of Novell, Inc.

ConnectView is a registered trademark of Novell, Inc. in the United States and other countries.

Connectware is a registered trademark of Novell, Inc. in the United States and other countries.

Corsair is a registered trademark of Novell, Inc. in the United States and other countries.

CP/Net is a registered trademark of Novell, Inc. in the United States and other countries.

Custom 3rd-Party Object and C3PO are trademarks of Novell, Inc.

DeveloperNet is a registered trademark of Novell, Inc. in the United States and other countries.

Documenter's Workbench is a registered trademark of Novell, Inc. in the United States and other countries.

ElectroText is a trademark of Novell, Inc.

Enterprise Certified Novell Engineer and ECNE are service marks of Novell, Inc.

Envoy is a registered trademark of Novell, Inc. in the United States and other countries.

EtherPort is a registered trademark of Novell, Inc. in the United States and other countries.

EXOS is a trademark of Novell, Inc.

Global MHS is a trademark of Novell, Inc.

Global Network Operations Center and GNOC are service marks of Novell, Inc.

Graphics Environment Manager and GEM are registered trademarks of Novell, Inc. in the United States and other countries.

GroupWise is a registered trademark of Novell, Inc. in the United States and other countries.

GroupWise XTD is a trademark of Novell, Inc.

Hardware Specific Module is a trademark of Novell, Inc.

Hot Fix is a trademark of Novell, Inc.

InForms is a trademark of Novell, Inc.

Instructional Workbench is a registered trademark of Novell, Inc. in the United States and other countries.

Internetwork Packet Exchange and IPX are trademarks of Novell, Inc.

IPX/SPX is a trademark of Novell, Inc.

IPXODI is a trademark of Novell, Inc.

IPXWAN is a trademark of Novell, Inc.

LAN WorkGroup is a trademark of Novell, Inc.

LAN WorkPlace is a registered trademark of Novell, Inc. in the United States and other countries.

LAN WorkShop is a trademark of Novell, Inc.

LANalyzer is a registered trademark of Novell, Inc. in the United States and other countries.

LANalyzer Agent is a trademark of Novell, Inc.

Link Support Layer and LSL are trademarks of Novell, Inc.

MacIPX is a registered trademark of Novell, Inc. in the United States and other countries.

ManageWise is a registered trademark of Novell, Inc. in the United States and other countries.

Media Support Module and MSM are trademarks of Novell, Inc.

Mirrored Server Link and MSL are trademarks of Novell, Inc.

Mobile IPX is a trademark of Novell, Inc.

Multiple Link Interface and MLI are trademarks of Novell, Inc.

Multiple Link Interface Driver and MLID are trademarks of Novell, Inc.

My World is a registered trademark of Novell, Inc. in the United States and other countries.

N-Design is a registered trademark of Novell, Inc. in the United States and other countries.

Natural Language Interface for Help is a trademark of Novell, Inc.

NDS Manager is a trademark of Novell, Inc.

NE/2 is a trademark of Novell, Inc.

NE/2-32 is a trademark of Novell, Inc.

NE/2T is a trademark of Novell, Inc.

NE1000 is a trademark of Novell, Inc.

NE1500T is a trademark of Novell, Inc.

NE2000 is a trademark of Novell, Inc.

NE2000T is a trademark of Novell, Inc.

NE2100 is a trademark of Novell, Inc.

NE3200 is a trademark of Novell, Inc.

NE32HUB is a trademark of Novell, Inc.

NEST Autoroute is a trademark of Novell, Inc.

NetExplorer is a trademark of Novell, Inc.

NetNotes is a registered trademark of Novell, Inc. in the United States and other countries.

NetSync is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare 3270 CUT Workstation is a trademark of Novell, Inc.

NetWare 3270 LAN Workstation is a trademark of Novell, Inc.

NetWare 386 is a trademark of Novell, Inc.

NetWare Access Server is a trademark of Novell, Inc.

NetWare Access Services is a trademark of Novell, Inc.

NetWare Application Manager is a trademark of Novell, Inc.

NetWare Application Notes is a trademark of Novell, Inc.

NetWare Asynchronous Communication Services and NACS are trademarks of Novell, Inc.

NetWare Asynchronous Services Interface and NASI are trademarks of Novell, Inc.

NetWare Aware is a trademark of Novell, Inc.

NetWare Basic MHS is a trademark of Novell, Inc.

NetWare BranchLink Router is a trademark of Novell, Inc.

NetWare Care is a trademark of Novell, Inc.

NetWare Communication Services Manager is a trademark of Novell, Inc.

NetWare Connect is a registered trademark of Novell, Inc. in the United States.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Distributed Management Services is a trademark of Novell, Inc.

NetWare Document Management Services is a trademark of Novell, Inc.

NetWare DOS Requester and NDR are trademarks of Novell, Inc.

NetWare Enterprise Router is a trademark of Novell, Inc.

NetWare Express is a registered service mark of Novell, Inc. in the United States and other countries.

NetWare Global Messaging and NGM are trademarks of Novell, Inc.

NetWare Global MHS is a trademark of Novell, Inc.

NetWare HostPrint is a registered trademark of Novell, Inc. in the United States.

NetWare IPX Router is a trademark of Novell, Inc.

NetWare LANalyzer Agent is a trademark of Novell, Inc.

NetWare Link Services Protocol and NLSP are trademarks of Novell, Inc.

NetWare Link/ATM is a trademark of Novell, Inc.

NetWare Link/Frame Relay is a trademark of Novell, Inc.

NetWare Link/PPP is a trademark of Novell, Inc.

NetWare Link/X.25 is a trademark of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

NetWare LU6.2 is trademark of Novell, Inc.

NetWare Management Agent is a trademark of Novell, Inc.

NetWare Management System and NMS are trademarks of Novell, Inc.

NetWare Message Handling Service and NetWare MHS are trademarks of Novell, Inc.

NetWare MHS Mailslots is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Mirrored Server Link and NMSL are trademarks of Novell, Inc.

NetWare Mobile is a trademark of Novell, Inc.

NetWare Mobile IPX is a trademark of Novell, Inc.

NetWare MultiProtocol Router and NetWare MPR are trademarks of Novell, Inc.

NetWare MultiProtocol Router Plus is a trademark of Novell, Inc.

NetWare Name Service is trademark of Novell, Inc.

NetWare Navigator is a trademark of Novell, Inc.

NetWare Peripheral Architecture is a trademark of Novell, Inc.

NetWare Print Server is a trademark of Novell, Inc.

NetWare Ready is a trademark of Novell, Inc.

NetWare Requester is a trademark of Novell, Inc.

NetWare Runtime is a trademark of Novell, Inc.

NetWare RX-Net is a trademark of Novell, Inc.

NetWare SFT is a trademark of Novell, Inc.

NetWare SFT III is a trademark of Novell, Inc.

NetWare SNA Gateway is a trademark of Novell, Inc.

NetWare SNA Links is a trademark of Novell, Inc.

NetWare SQL is a trademark of Novell, Inc.

NetWare Storage Management Services and NetWare SMS are trademarks of Novell, Inc.

NetWare Telephony Services is a trademark of Novell, Inc.

NetWare Tools is a trademark of Novell, Inc.

NetWare UAM is a trademark of Novell, Inc.

NetWare WAN Links is a trademark of Novell, Inc.

NetWare/IP is a trademark of Novell, Inc.

Novell Gold Partner is a service mark of Novell, Inc.

Novell Labs is a trademark of Novell, Inc.

Novell N-Design is a registered trademark of Novell, Inc. in the United States and other countries.

Novell NE/2 is a trademark of Novell, Inc.

Novell NE/2-32 is a trademark of Novell, Inc.

Novell NE3200 is a trademark of Novell, Inc.

Novell Network Registry is a service mark of Novell, Inc.

Novell Platinum Partner is a service mark of Novell, Inc.

Novell Press is a trademark of Novell, Inc.

Novell Press Logo (teeth logo) is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Replication Services is a trademark of Novell, Inc.

Novell Research Reports is a trademark of Novell, Inc.

Novell RX-Net/2 is a trademark of Novell, Inc.

Novell Service Partner is a trademark of Novell, Inc.

Novell Storage Services is a trademark of Novell, Inc.

Novell Support Connection is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Technical Services and NTS are service marks of Novell, Inc.

Novell Technology Institute and NTI are registered service marks of Novell, Inc. in the United States and other countries.

Novell Virtual Terminal and NVT are trademarks of Novell, Inc.

Novell Web Server is a trademark of Novell, Inc.

Novell World Wide is a trademark of Novell, Inc.

NSE Online is a service mark of Novell, Inc.

NTR2000 is a trademark of Novell, Inc.

Nutcracker is a registered trademark of Novell, Inc. in the United States and other countries.

OnLAN/LAP is a registered trademark of Novell, Inc. in the United States and other countries.

OnLAN/PC is a registered trademark of Novell, Inc. in the United States and other countries.

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

Open Look is a registered trademark of Novell, Inc. in the United States and other countries.

Open Networking Platform is a registered trademark of Novell, Inc. in the United States and other countries.

Open Socket is a registered trademark of Novell, Inc. in the United States.

Packet Burst is a trademark of Novell, Inc.

PartnerNet is a registered service mark of Novell, Inc. in the United States and other countries.

PC Navigator is a trademark of Novell, Inc.

PCOX is a registered trademark of Novell, Inc. in the United States and other countries.

Perform3 is a trademark of Novell, Inc.

Personal NetWare is a trademark of Novell, Inc.

Pervasive Computing from Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Portable NetWare is a trademark of Novell, Inc.

Presentation Master is a registered trademark of Novell, Inc. in the United States and other countries.

Print Managing Agent is a trademark of Novell, Inc.

Printer Agent is a trademark of Novell, Inc.

QuickFinder is a trademark of Novell, Inc.

Red Box is a trademark of Novell, Inc.

Reference Software is a registered trademark of Novell, Inc. in the United States and other countries.

Remote Console is a trademark of Novell, Inc.

Remote MHS is a trademark of Novell, Inc.

RX-Net is a trademark of Novell, Inc.

RX-Net/2 is a trademark of Novell, Inc.

ScanXpress is a registered trademark of Novell, Inc. in the United States and other countries.

Script Director is a registered trademark of Novell, Inc. in the United States and other countries.

Sequenced Packet Exchange and SPX are trademarks of Novell, Inc.

Service Response System is a trademark of Novell, Inc.

Serving FTP is a trademark of Novell, Inc.

SFT is a trademark of Novell, Inc.

SFT III is a trademark of Novell, Inc.

SoftSolutions is a registered trademark of SoftSolutions Technology Corporation, a wholly owned subsidiary of Novell, Inc.

Software Transformation, Inc. is a registered trademark of Software Transformation, Inc., a wholly owned subsidiary of Novell, Inc.

SPX/IPX is a trademark of Novell, Inc.

StarLink is a registered trademark of Novell, Inc. in the United States and other countries.

Storage Management Services and SMS are trademarks of Novell, Inc.

Technical Support Alliance and TSA are collective marks of Novell, Inc.

The Fastest Way to Find the Right Word is a registered trademark of Novell, Inc. in the United States and other countries.

The Novell Network Symbol is a trademark of Novell, Inc.

Topology Specific Module and TSM are trademarks of Novell, Inc.

Transaction Tracking System and TTS are trademarks of Novell, Inc.

Universal Component System is a registered trademark of Novell, Inc. in the United States and other countries.

Virtual Loadable Module and VLM are trademarks of Novell, Inc.

Writer's Workbench is a registered trademark of Novell, Inc. in the United States and other countries.

Yes, It Runs with NetWare (logo) is a trademark of Novell, Inc.

Yes, NetWare Tested and Approved (logo) is a trademark of Novell, Inc.

ZENworks is a trademark of Novell, Inc.