16 Using SNMP for Terminal Management

This chapter describes using SNMP (Simple Network Management Protocol) to manage NCD terminals over the network. The following topics are covered in this chapter:

SNMP Overview

SNMP is an industry-standard set of protocols for network management in TCP/IP network environments. It provides mechanisms for monitoring and controlling terminals from a central location.

Using SNMP from a network host, you can:

- ❑ Display or modify the values of all terminal configuration parameters
- ❑ Obtain additional information, including network traffic levels, network error levels, basic system and network configuration data, and the state of the font cache
- ❑ Configure network-oriented timers
- ❑ Remotely reset NCD terminals

SNMP Components

SNMP consists of four interrelated parts:

- ❑ An SNMP agent in the X server
- ❑ SNMP manager software, located on a host computer and available from a number of vendors. Most management software includes utilities for

collecting information from agents. Some management software also includes utilities for generating reports and setting variables.

- MIB (Management Information Base), information defined by standard variables mandated in RFC 1212, plus variables added by NCD. The NCDware distribution includes two versions of the MIB:
  - The combined NCDware MIB and MIB II file, with the following name and default location: **/usr/lib/X11/ncd/snmp/mib.txt**
  - The new, updated NCDware-only MIB file that includes SNMP variables for all NCD remote configuration parameters, with the following name and default location: **/usr/lib/X11/ncd/snmp/mib.my**
- The protocol that connects the manager with agents

The NCDware distribution also includes two utilities: ***ncdreset***(1) for remotely resetting terminals and ***ncdquery***(1) for displaying the values of certain NCD-specific variables.

How SNMP Works

NCD terminals respond to queries from hosts running SNMP management software. Manager hosts have read / write access; monitor hosts have read-only access; and trap monitors receive information about significant events.

The SNMP manager initiates information gathering by sending a request for information to the SNMP agent in the terminal. When the request is received, the agent collects data as specified in the MIB and sends it to the manager. Using SNMP utilities, the system administrator can read or write variables.

NCDware provides an access control mechanism that you can use to prevent read / write or read-only access to the SNMP agent from outside the terminal or restrict access to a specified list of hosts. Both levels of access are further controlled by passwords called community names.

MIB Contents

All of the mandatory variables are included in NCD's SNMP agent except for the **ifAdminStatus** variable. Read-only access is provided for this variable, but write access can cause security problems and is not necessary on NCD terminals, which have only one network interface.

The NCDware MIB file contains SNMP variables for all NCD configuration parameters. Each configuration parameter has a unique SNMP variable name

and path; for example, the SNMP variable name and path for the **boot-desired-source** parameter are: **ncdBootDesiredSource** and **ncdBoot 5**.

The SNMP variable name and path for each parameter are listed in the *Remote Configuration Parameter Quick Reference*.

SNMP Host Requirements

Hosts that access the terminal's SNMP information or need to access the terminal for reset purposes must have both SNMP management software and the NCD MIB installed. The MIB is installed during the NCDware installation process.

If you are not using the default MIB file (**/etc/mib.txt**), you should set the MIBFILE environment variable to the pathname of the MIB file or specify the pathname of the MIB in the command line for SNMP utilities.

Controlling Access to Terminals through SNMP

By default, any host on the network can read and write an NCD terminal's SNMP variables. You can restrict this access using the procedures in this section.

This section also provides a procedure for configuring terminals to send notification of traps to specified hosts. Traps are responses to significant events and are generated by the terminal.

SNMP passwords (community names) are saved into a limited area in the terminal's NVRAM. To save space, you can define a global password that provides read / write access to SNMP variables as well as access to other terminal functions (Setup ⇒ Change Setup Parameters ⇒ Access Control ⇒ Unit Global Password). For more information about setting a global password, see the *System Administrator's Guide*. For information about the special area in NVRAM for saving passwords and certain other strings, see Chapter 11, Boot Monitor and NVRAM.

Except for the community names, the parameters described in the following procedures are not saved in NVRAM.

Configuring Read/Write Access

A host with read / write access to a terminal's MIB variables is called a manager. You can establish a list of hosts allowed to access the terminal or prevent access from all hosts. Access control is disabled by default.

To establish read / write access control to a terminal's SNMP variables:

1. To establish access control, set the **snmp-read-write-access-control-enabled** parameter to "true" (Setup ⇒ Change Setup Parameters ⇒ Access Control ⇒ Enable SNMP Read-Write Access Control).

Table 16-1 snmp-read-write-access-control-enabled Parameter

Possible Values	Results
default	false
false	Requests for connections to the SNMP daemon from outside the terminal are not checked against the read / write access list.
true	Requests for connections to the SNMP daemon from outside the terminal are checked against the read / write access list.

2. The **snmp-read-write-access-control-list** table contains the names of all hosts with read / write access to SNMP variables (Setup ⇒ Change Setup Parameters ⇒ Access Control ⇒ SNMP Read-Write Access Control List). If read / write access control is enabled, only hosts in the table have read / write access to the terminal.

Table 16-2 snmp-read-write-access-control-list Parameter

Table Entries	Possible Values	Results
host	default	(empty list)
	hostname or ***IP address***	The network name or address of a host granted read / write access to the terminal's SNMP daemon.

Note To disallow read / write access by all hosts, leave the table empty and make sure **snmp-read-write-access-control-enabled** is set to "true."

3. A community name must be specified in SNMP requests to obtain read / write access to the terminal's configuration information when access control is enabled. You can specify up to two community names. A community string is a string of alphanumeric characters of arbitrary length.
   — Set the first community name in Setup ⇒ Change Setup Parameters ⇒ Access Control ⇒ SNMP Read-Write Community.
   — Set the second community name in Setup ⇒ Change Setup Parameters ⇒ Access Control ⇒ SNMP Read-Write Alternative Community.

Configuring Read-Only Access

A host with read-only access to a terminal's MIB variables is called a monitor. The default is to allow any host read-only access to the terminal through SNMP. You can establish a list of hosts allowed to access the terminal or prevent access from all hosts. Access control is disabled by default.

You can use the default read-only password, called a community name, or specify a different one.

Complete the following steps to configure read-only access to a terminal's SNMP variables:

1. To establish access control, set the **snmp-read-only-access-control-enabled** parameter to "true" (Setup ⇒ Change Setup Parameters ⇒ Access Control [SNMP section] ⇒ Enable SNMP Read-Only Access).

Table 16-3 snmp-read-only-access-control-enabled Parameter

Possible Values	Results
default	false
false	Requests for connections to the SNMP daemon from outside the terminal are not checked against the read-only access list.
true	Requests for connections to the SNMP daemon from outside the terminal are checked against the read-only access list.

2. The **snmp-read-only-access-control-list** table contains the names of all hosts with read-only access to SNMP variables (Setup ⇒ Change Setup

Parameters ⇒ Access Control [SNMP section] ⇒ SNMP Read-Only Access Control List). If read-only access control is enabled, only hosts in the table have read-only access to the terminal.

Table 16-4 snmp-read-only-access-control-list Parameter

Table Entries	Possible Values	Results
host	default	(empty list)
	hostname or ***IP address***	The network name or address of a host granted read-only access to the terminal's SNMP daemon.

Note To disallow read-only access by all hosts, leave the table empty and make sure **snmp-read-only-access-control-enabled** is set to "true."

3. The community name must be specified in SNMP requests to obtain read-only access to the terminal's configuration information. You can specify up to two community names. A community name is a string of alphanumeric characters of any length.
   - — If you do not wish to use the default community name for read-only access, set the community name in Setup ⇒ Change Setup Parameters ⇒ Access Control ⇒ SNMP Read-Only Community.
   - — Set the second community name in Setup ⇒ Change Setup Parameters ⇒ Access Control ⇒ SNMP Read-Only Alternative Community.

Configuring Terminals to Allow Trap Monitoring

The two trap events defined for NCD terminals are:

- ❑ The cold start trap, sent when the terminal is powered on
- ❑ The authentication failure trap, sent when an attempt to access the terminal using SNMP fails

To designate a host as a trap monitor, list its hostname or IP address and a community name (password) in Setup ⇒ Change Setup Parameters ⇒ Access Control ⇒ SNMP Trap Monitors. A community name is an alphanumeric string of arbitrary length.

Note If any of the trap monitor hosts are also manager or monitor hosts, use the community names already specified for those hosts. For information about manager and monitor hosts, see "Configuring Read / Write Access" on page 16-4 and "Configuring Read-Only Access" on page 16-5.

Using SNMP to Read and Write Variables

You can read and write SNMP variables using the SNMP utilities provided with your SNMP host software. In addition, you can read a few variables using the ***ncdquery***(1) utility provided on the NCDware distribution.

Reading a Terminal's SNMP Variables

The following sections describe how to use SNMP management software or the ***ncdquery*** utility to read a terminal's SNMP variables.

Using SNMP Management Software

A host's SNMP management software usually includes a **get** command that allows you to read a terminal's SNMP variables. Reading variables requires read-only or read / write access to the terminal, which is allowed by default.

Using the *ncdquery* Utility

The ***ncdquery*** utility allows you to display the contents of a few MIB variables for a specified terminal. An ***ncdquery*** command must be executed from a host designated as an SNMP manager or monitor:

- When executing the command from a manager host, you must supply the read / write community string.
- When executing the command from a monitor host, you must supply the read-only community name.

For more information about community names, see "Configuring Read / Write Access" on page 16-4 and "Configuring Read-Only Access" on page 16-5.

The command syntax is:

ncdquery [**-V -v -c** ***community*** **-d** ***variable_options***] ***hostname***

where:

-V	Displays version information for ***ncdquery***
-v	Displays the hostname
-c ***community***	Is the community name. If the community name is not one of the defaults (manager for manager hosts and public for monitor hosts), you must supply the community name.
-d	Displays debugging information
variable_options	Specifies the variable(s) to display. The default is to display the X server version. The options and variables displayed by each are: **-s** X server version **-b** Boot Monitor version **-k** Keyboard controller version **-i** Amount of memory installed **-h** Memory fragments **-f** Amount of free memory **-a** All of the above
hostname	Is the hostname of the terminal.

For example, the following command displays the X server and Boot Monitor versions, assuming the default community name and MIB file:

```
% ncdquery -s -b ncdu60
server version: NCD19c server 3.1.0 03/12/91 downloaded
boot monitor version: Boot PROM V2.2.4
```

For more information about the ***ncdquery*** command and its options, see the man page.

Writing SNMP Variables—Configuring Terminals

You can modify an NCD terminal's SNMP variables using your host SNMP management software. Host SNMP software usually includes a **set** command for modifying variables. Modifying variables requires read / write access to the terminal, which is allowed by default.

Consult your SNMP management documentation for information about commands to use for modifying SNMP variables.

Each remote configuration parameter has a variable name and path assigned to it. You can obtain SNMP variable names and paths for the read / write parameters from the *Remote Configuration Parameter Quick Reference*.

Depending on the SNMP management software at your site, you may need to assign numerical values to parameters that accept choices or Boolean values. To assign numerical values to a parameter, complete the following steps:

1. Identify the values available for the desired parameter.
2. If required by your SNMP management software, assign numerical values to the available choices:
   - For Boolean values, use 1 for "false," "no," and "off." Use 2 for "true," "yes," and "on."
   - For choice values, assign 1 to the first choice, 2 to the second choice, and so on, unless otherwise specified. Use the order of choices listed in the *Remote Configuration Parameter Quick Reference*.

     For example, the following numerical values correspond to the choices for **boot-desired-source**:

     1 = tcpip

     2 = tftp

     3 = nfs

     4 = ncdnet

     5 = local

     6 = prom

   For more information about assigning values to parameters, refer to the documentation for your SNMP management software.

3. Enter the command, using the appropriate value. For example, a command using host-based SNMP management software to change the **boot-desired-source** parameter to "local" is:

```
% xsnmpi -a 191.42.153.147 -c manager set ncdBootDesiredSource.0=5
```

where:

191.42.153.147	Is the IP address of the terminal
-c manager	Is the community name for read/write permission
ncdBootDesiredSource	Is the SNMP variable name for the **boot-desired-source** parameter
5	Is the choice "local"

Using SNMP Remote Reset/Reboot

On a TCP/IP network, terminals can be reset remotely using SNMP and the ***ncdreset***(1) command. The host from which terminals are reset must be an SNMP manager host. ***ncdreset*** (1) provides the following choices:

- ❏ Establishing an SNMP connection without restarting the session
- ❏ Restarting the X session
- ❏ Rebooting the terminal after all clients exit
- ❏ Rebooting the terminal immediately

The following sections describe the host and terminal configuration required before you can reset a terminal remotely.

Configuring a Host for SNMP Remote Reset

Complete the following steps to set up the host from which the remote reset command is issued:

1. Install the ***ncdreset*** executable and the NCD MIB from the NCDware distribution, if necessary. They are installed when you install NCDware with the ***ncdinstall*** script.
2. Make sure the host has SNMP management software.

Configuring a Terminal for SNMP Remote Reset

Complete the following steps to configure a terminal for remote reset:

1. Set the **snmp-allow-reset** parameter to "true" (Setup ⇒ Change Setup Parameters ⇒ Access Control [SNMP section] ⇒ Allow SNMP Reset). Reset is disabled by default.
2. The default is to allow reset from any host and by any user. To restrict access to the reset function, do the following:
   - — To restrict access to certain hosts, make sure the hosts are included in the **snmp-read-write-access-control-list** table if SNMP write access is enabled. Write access is enabled if **snmp-read-write-access-control-enabled** is set to "true."
   - — To prevent other users from resetting the terminal, set a password, in the **snmp-read-write-community** parameter.

   These parameters are described in "Controlling Access to Terminals through SNMP" on page 16-3.

Resetting Session and Rebooting Terminals

You can use the ***ncdreset*** utility or the **unit-administrative-status** remote configuration parameter to reset terminals remotely.

Using the *ncdreset* Utility for Remote Reset

To use ***ncdreset*** to remotely reset a terminal or restart the X session, enter an ***ncdreset*** command from a host designated as an SNMP manager. The default action of this command is to reset the terminal after the last client closes.

Note The reset process is irreversible. You cannot change to another reset level after resetting the terminal.

The syntax of ***ncdreset*** is:

`ncdreset` [**`-V -v -c`** ***community*** **`-r`** ***reset_level***] ***hostname***

where:

-V Prints version information for the program on the standard output.

-v Prints a message on the standard output when the terminal is actually reset.

-c *community* Is the community name. If the community name is not the default (manager), you must supply the community name.

hostname Is the hostname of the terminal being reset.

-r *reset_level* Is the reset level. The values are:

1 Establishes an SNMP connection without resetting the terminal.

2 Restarts the X session.

3 Reboots the terminal when the last client closes. This is the default reset level.

4 Reboots the terminal immediately.

For example, the following command reboots the terminal when the last client closes and prints a message on the standard output when the terminal resets:

```
# ncdreset -v -r3 ncdu203
```

Using unit-administrative-status for SNMP Remote Reset

The **unit-administrative-status** remote configuration parameter (Setup ⇒ Change Setup Parameters ⇒ Unit ⇒ Administrative Status) both displays the SNMP administrative status of terminals and provides for immediate or delayed resetting of terminals from a remote location.

Use of **unit-administrative-status** for remote reset requires that the **snmp-allow-reset** parameter be set to "true." The possible values for this parameter are described in Table 16-5. The parameter is not saved in NVRAM.

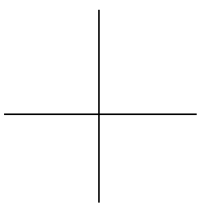

Table 16-5 unit-administrative-status Parameter Values

Possible Values	Results
default	running
running	The terminal is running; no reset commands are pending.
session-reset	The terminal restarts the session. This option is the same as logging out of the current session (in the Console, select Login ⇒ Logout).
last-client-close-reset	The terminal reboots when the last client closes.
unit-reset	The terminal reboots immediately. This option is the same as rebooting the terminal (in the Console, select Console ⇒ Reboot).