PRELIMINARY

SNMP Agent Support Function User’s Guide (DF600)

Hitachi reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi products or services can only be ordered under the terms and conditions of Hitachi's applicable agreements, including license agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

Trademarks

Hitachi is a registered trademark and service mark of Hitachi, Ltd., and the Hitachi design mark is a trademark and service mark of Hitachi, Ltd.

All other brand or product names are or may be registered trademarks, trademarks or service marks of and are used to identify products or services of their respective owners.

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
0	September 2002	Revision 0, supersedes and replaces Initial Release.

Preface

Before using SNMP Agent Support Function, read the operating procedures and notices included in this guide.

The *SNMP Agent Support Function User's Guide* assumes that:

- The user has a background in data processing and understands direct-access storage device subsystems and their basic functions.
- The user is familiar with the Hitachi Disk array subsystem.
- The user is familiar with the *Disk Array management program 2 (for GUI) User's Guide* and/or the *Disk Array management program (for CLI) User's Guide*.

Contents

Chapter 1 Overview 1

1.1 Notes on Use 2
1.2 System Configuration 5
1.2.1 Network Connecting Functions....5
1.2.2 LAN Connections....6
1.3 SNMP Functions 7
1.3.1 Trap Reporting....7
1.3.2 Request Processing....8

Chapter 2 SNMP Specifications....9

2.1 Supported Operations....9
2.2 Error Status.... 10

Chapter 3 Operations....11

3.1 Trap-Issuing Processing 11
3.2 Request Processing.... 12

Chapter 4 Installing and Uninstalling....15

4.1 Installing SNMP.... 15
4.2 Uninstalling SNMP.... 19

Chapter 5 Operation Procedures....21

5.1 Setup 21
5.1.1 Setting Up the Array Unit Side 21
5.1.2 Setting Up the SNMP Manager Side 22
5.1.3 Checking 22
5.2 Setting Enable/Disable 23
5.3 Creating an Environmental Information File 25
5.3.1 Operation Environment Setting File.... 25
5.3.1.1 File format.... 25
5.3.1.2 Settings.... 26
5.3.1.3 How to Create Files 26
5.3.2 Unit Name Setting File 29
5.3.2.1 File format.... 29
5.3.2.2 Settings.... 29
5.3.2.3 How to Create the File 29
5.4 Registering SNMP Environmental Information.... 30
5.5 Referencing the SNMP Environment Information File.... 32
5.6 How to Verify the SNMP Connection.... 33
5.7 How to Detect Failure 34

Chapter 6 Management Information....35

6.1 Supported MIBs.... 35
6.2 MIB Access Mode 35
6.3 Object Identifier Assignment System.... 36

6.4 Types of Supported Traps and Trap Issuing Opportunity 40

Chapter 7 MIB Installation Specifications 41

7.1 MIB II 41
7.1.1 system Group 41
7.1.2 interfaces Group 43
7.1.3 at Group 45
7.1.4 ip Group 46
7.1.5 icmp Group 51
7.1.6 tcp Group 51
7.1.7 udp Group 51
7.1.8 egp Group 51
7.1.9 snmp Group 52
7.2 Extended MIBs 55
7.2.1 dfSystemParameter Group 55
7.2.2 dfWarningCondition Group 56
7.2.3 dfCommandExecutionCondition Group 59
7.2.4 dfCacheLoadCondition Group 61
7.2.5 dfLUNS Group 61
7.2.5.1 Definitions and Functions 64
7.2.6 dfPort Group 65
7.2.7 dfCommandExecutionInternalCondition Group 69

Chapter 8 Relevant Specifications 71

Appendix A Operations Using CLI 73

A.1 Installing 73
A.2 Uninstallation 74
A.3 Enabling or Disabling 75
A.4 Registering or Referencing SNMP Environment Information 76

List of Figures

Figure 1.1 Example of Divided SNMP Managers 4
Figure 1.2 Local LAN Connection 6
Figure 1.3 Public LAN Connection 6
Figure 2.1 Communication for SNMP Operation 9
Figure 3.1 Example of a Drive Blockade and Trap Issue 11
Figure 3.2 Example of Request Processing 12
Figure 3.3 SNMP Message Management 13
Figure 4.1 Array System Viewer 15
Figure 4.2 Parameter Dialog Box 16
Figure 4.3 SNMP Unlock Confirmation Message 16
Figure 4.4 Restart After Unlock 17
Figure 4.5 Unlocked Optional Feature: SNMP 17
Figure 4.6 Reboot Dialogue Box: Restart Time Display 18
Figure 4.7 Subsystem Restart Successful Message 18
Figure 4.8 Option Lock Confirmation 19
Figure 4.9 Option Lock Confirmation 19
Figure 5.1 Disable Option Message Dialogue Box 23
Figure 5.2 SNMP Agent Confirmation Window 23
Figure 5.3 SNMP Agent Status Update 24
Figure 5.4 Setting Address to Send a Trap 28
Figure 5.5 Operation Environment Setting File 28
Figure 5.6 Parameter Dialogue Box (SNMP tab) 30
Figure 5.7 Settings/Environment Complete Dialogue Box 30
Figure 5.8 Output Confirmation Dialogue Box 32
Figure 6.1 The Object Identifier Assignment System 36
Figure 7.1 dfRegressionStatus Format 56
Figure 7.2 Relationship between Traps and dfWarningCondition Groups 58
Figure 7.3 Accumulated Values Over Time 60
Figure 7.4 WWN group access permission (Not supported. (Length 0)) 64

List of Tables

Table 1.1 GET/TRAP Specifications 3
Table 1.2 Network Connecting Functions 5
Table 2.1 SNMP Operations Supported 9
Table 2.2 SNMP Error Status 10
Table 5.1 Operation Environment Settings 26
Table 5.2 Item of Unit Name Setting 29
Table 6.1 Supported MIBs 35
Table 6.2 Supported Standard Traps 40
Table 6.3 Supported Extended Traps 40
Table 7.1 system Group 41
Table 7.2 interfaces Group 43
Table 7.3 ip Group 46
Table 7.4 snmp Group 52
Table 7.5 dfSystemParameter Group 55
Table 7.6 dfWarningCondition Group 56
Table 7.7 dfRegressionStatus Value for Each Failure 57

Table 7.8 dfCommandExecutionCondition Group 59
Table 7.9 dfCacheLoadCondition Group 61
Table 7.10 dfLUNS Group 61
Table 7.11 Port Table Numbers 63
Table 7.12 dfPort Group 65
Table 7.13 Port numbers 66
Table 7.14 Port Addresses and Associated Values 67
Table 7.15 Topology information for Fibre-oriented Ports 68
Table 7.16 Topology information for ports other than Fibre-oriented 68
Table 7.17 Port display names 68
Table 7.18 dfCommandExecutionInternalCondition Group 69

Chapter 1 Overview

The SNMP function reports failure occurrences to the workstation for network monitoring, using the SNMP (Simple Network Management Protocol) of an open platform. Command operating status (number of commands received, number of cache hits, etc.) of the array unit is reported. The reported information can be used for performance tuning, since the command operating status, depending on the type of access from the host, can be referred to this function. To use SNMP, a LAN facility and a workstation in which the SNMP manager program (hereinafter referred to "SNMP manager") is installed are necessary.

This document includes the following information:

- SNMP Specifications
- Operations
- Installing and Uninstalling
- Operation Procedures
- Management Information
- MIB Installation Specifications
- Relevant Specifications

1.1 Notes on Use

When using SNMP, note the following:

- Since the UDP protocol is used for the SNMP agent support function, correct reporting of error traps to the SNMP manager cannot be assured. Therefore, **it is recommended that the SNMP manager acquire MIB information periodically.**
- The command processing performance of the array unit is negatively affected if the interval to collect MIB information is set too short.
- If the SNMP manager is started after failures occur in an array unit, the failures that occur before starting the SNMP manager are not reported with a trap. Therefore, acquire the MIB objects “dfRegressionStatus” and “dfPreventiveMaintenanceInformation” after starting the SNMP manager, and check whether or not failures occur.
- SNMP also stops if the controller is blockaded. In this case SNMP managers receive no response.
- When an array unit is configured from a dual system, if failures in hardware components (such as a fan, a battery, a power supply, and a cache failure) occur during power-on until before the array unit is “Ready” (including failures that occurred at the last power off), they are reported with a trap from both controllers. Failures in disk drives and those that occur while an array unit is “Ready” are reported with a trap from only the controller side that detects the failures.
- When an array unit is configured from a dual system, both controllers must be monitored by the SNMP manager. When only one of the controllers is monitored using the SNMP manager, monitor controller 0; the following restrictions must be observed:
  - Drive blockades that are detected by the controller 1 side are not reported with a trap.
  - No trap will be reported for controller down of controller 1.
    (“Controller down” is reported as a systemDown trap by the faulty controller.)
  - After controller 0 is blockaded, the SNMP agent support function cannot be used.

Table 1.1 GET/TRAP Specifications

Connection status	Controller status	GET/TRAP specification				Remarks
		Controller 0		Controller 1		
Both controller	① Both controllers are normal	GET	○	GET	○	Master controller: 0
		TRAP	○	TRAP	Δ	
	②Controller 1 is blockaded	GET	○	GET	×	Master controller: 0 If controller 1 is recovered, the system goes to ①.
		TRAP	○	TRAP	×	
	③ Controller 0 is blockaded	GET	×	GET	○	Master controller: 1
		TRAP	×	TRAP	○	
	④ Controller 0 is recovered (the board was replaced while the power is on)	GET	○	GET	○	Master controller: 1 The system goes to ① when restarted (P/S ON).
		TRAP	Δ	TRAP	○	
Controller 0 only	⑤Both controllers are normal	GET	○	GET	×	Master controller: 0
		TRAP	○	TRAP	×	
	⑥ Controller 1 is blockaded	GET	○	GET	×	
		TRAP	○	TRAP	×	
	⑦ Controller 0 is blockaded	GET	×	GET	×	Master controller: 1
		TRAP	×	TRAP	×	
	⑧ Controller 0 is recovered (the board was replaced while the power is on)	GET	○	GET	×	Master controller: 1 The system goes to ⑤ when restarted (P/S ON).
		TRAP	Δ	TRAP	×	

○: GET and TRAP are possible. (The drive blockade and the occurrence detected by the other controller is excluded.)
×: GET and TRAP are impossible.
Δ: A trap is reported only for an own controller blockade, and a drive blockade (drive extraction is not included) detected by the own controller.

Note: A trap is reported for an error that has been detected when a controller board is replaced while the power is on or the power is turned on. Therefore, traps other than the above are also reported.

- For a dual system configuration, SNMP managers should not be divided as shown in Figure 1.1:

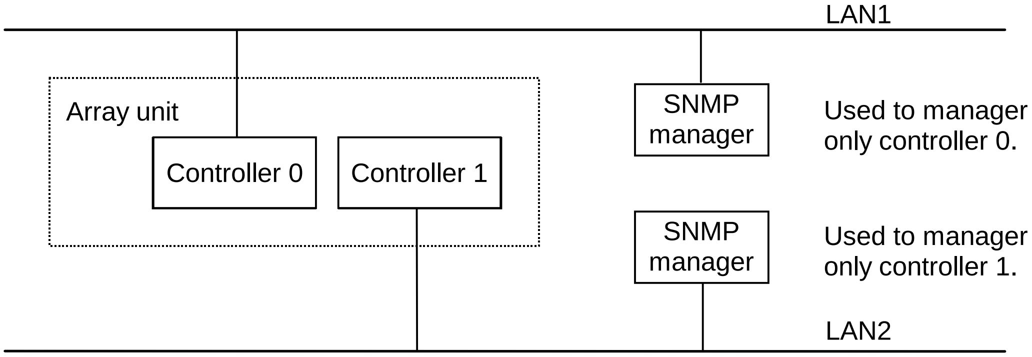

LAN1
Array unit
Controller 0
Controller 1
SNMP manager
Used to manager only controller 0.
SNMP manager
Used to manager only controller 1.
LAN2

Figure 1.1 Example of Divided SNMP Managers

Only the master side controller reports traps for fan, power supply, and battery failures. If each SNMP manager that manages individual controllers is assigned separately, the above-mentioned failures, each a resource shared between both controllers, are not reported at all to the SNMP manager that manages the slave controller side. A number of SNMP managers can be set, but each SNMP manager should be set so that it can control both controllers.

- A device which executes broadcast, etc. should not be connected to the LAN to which the array unit is connected. If broadcast, etc. comes into the array unit frequently, the capacity to process the host command deteriorates.
- The array unit must be connected to a LAN that conforms to “Ethernet Version 2”. Only “Ethernet Version 2” frames (IEEE802.3 frames, etc.) are supported; other frames are not supported.
- **Fix the IP address of the SNMP manager when using the SNMP support function in a system which uses the DHCP server.** If the IP address of the SNMP manager is changed when the DHCP function is used, the TRAP cannot be reported to the SNMP manager.
- If the IP Address of the array unit is changed during a Power ON sequence after getting the IP Address automatically with the DHCP client function, the SNMP manager cannot find the array unit, and the TRAP cannot be reported to the SNMP manager. When the IP Address of the array unit is changed, restart the array unit.
- **Contact service personnel when a failure occurs.**

1.2 System Configuration

This section includes the following:

- Network Connecting Functions
- LAN Connections

1.2.1 Network Connecting Functions

Network connecting functions supported by the array unit are shown in Table 1.2.

Table 1.2 Network Connecting Functions

No.	Item	Description of Support
1	Network interface	10BaseT, 100BaseT (RJ45 connector, Twisted pair cable)
2	Support frame type	Conforms to “Ethernet Version 2” Specifications (DIX Specifications). (See Note.)

Note: Only “Ethernet Version 2” frames (IEEE802.3 frames, etc.) are supported; other frames are not supported.

1.2.2 LAN Connections

The following LAN connections are illustrated below:

- Local LAN Connection (Figure 1.2)
- Public LAN Connection (Figure 1.3)

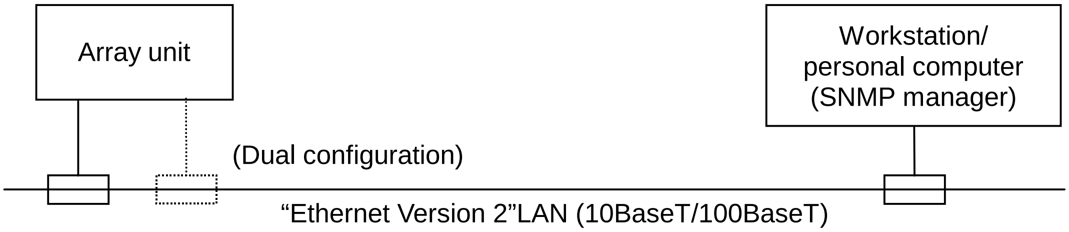


Figure 1.2 Local LAN Connection

One Gateway address (default Gateway address) can be set for each controller.

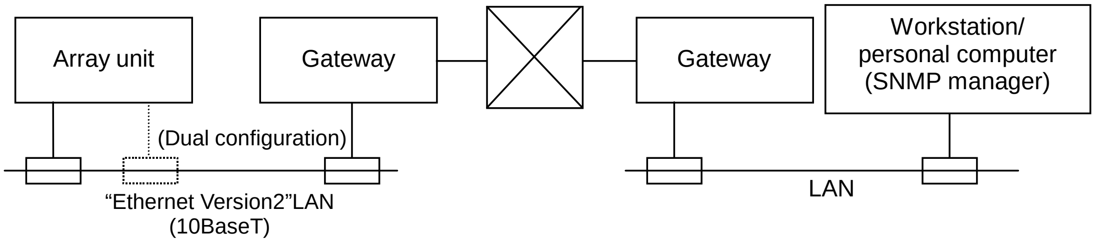


Figure 1.3 Public LAN Connection

Note: To use the SNMP function, a workstation (WS) in which SNMP manager has been installed is required on a LAN.

1.3 SNMP Functions

The following functions are provided to report the failures of the array unit to the SNMP manager:

- Trap Reporting
- Request Processing

1.3.1 Trap Reporting

The user can be informed of failures which occur in the array unit in real time even when the user is away from the array unit. This function issues an SNMP manager trap to notify the manager that any of the following events were detected:

- Standard traps
  - P/S turning on
  - SNMP access error (incorrect community name)
- Extended traps
  - Own controller blockade (See Note 1)
  - Drive blockade (data drive)
  - Fan failure
  - DC power failure
  - Battery failure
  - Cache partial blockade
  - UPS cable not connected
  - Battery charging circuit failure
  - Blockade of the mate controller
  - Warned array unit
  - Drive (spare drive) blockade
  - Online microprogram replacement executed
  - ENC failure
  - Loop failure
  - Path blockade (See Note 2.)
  - NAS Server failure
  - NAS Path failure
  - NAS UPS failure

Note 1: Depending on the contents of the failure, there may be a case that cannot be reported.

Note 2: Path blockade is reported only when the TrueCopy feature is enabled.

1.3.2 Request Processing

This function enables the SNMP manager to refer to MIB objects supported by the array unit. (The function to set MIB objects is not provided.) The specific information supported is shown below.

- Device specific information (product name and microprogram revision)
- Warning information (See Note 1.)
- Command execution condition information
- Cache load condition information (dirty segment ratio)

Note 1: Warning information that can be acquired by the array unit is shown below.

- Drive blockade (data drive or spare drive)
- Fan failure
- DC power failure
- Battery failure
- Cache partial blockade
- UPS cable not connected
- Battery charging circuit failure
- Blockade of the mate controller
- Warned array unit
- Drive (data drive) blockade
- Drive (spare drive) blockade
- ENC failure
- Loop failure
- Path blockade
- NAS Server failure
- NAS Path failure
- NAS UPS failure

Chapter 2 SNMP Specifications

The array unit supports agent functions that conform to RFC1157, the Simple Network Management Protocol. (It supports the SNMP Version 1 protocol.) The array unit cannot issue all of the traps described in RFC1157. It supports the MIB-II, which conforms to RFC1213. This section includes the following information:

- Supported Operations
- Error Status

2.1 Supported Operations

SNMP operations supported by the array unit are shown in Table 2.1.

Table 2.1 SNMP Operations Supported

No.	Operation	Meaning
1	GET	Obtains a specific MIB object value. Normal operation is assumed when both GET REQUEST (request from the SNMP manager) and GET RESPONSE (response from the agent) are completed.
2	GETNEXT	Searches MIB objects continuously. Normal operation is assumed when both GETNEXT REQUEST (request from the SNMP manager) and GET RESPONSE (response from the agent) are completed.
3	TRAP	Reports an event (error or status change) to the SNMP manager. When an event occurs, the agent sends a TRAP to the manager, regardless of SNMP manager's request.

Table 2.1 shows communications between the SNMP manager and the SNMP agent for a supported SNMP operation.

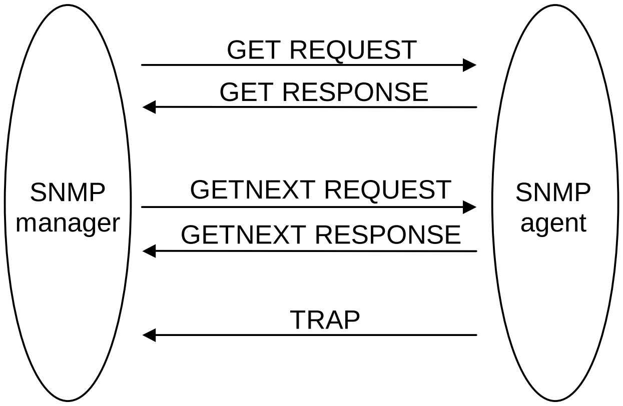


Figure 2.1 Communication for SNMP Operation

2.2 Error Status

When an error in a request from the SNMP manager is detected, the array unit sends an SNMP message (GET RESPONSE) to the manager, together with the error status, as shown below.

Table 2.2 SNMP Error Status

No.	Error status (code)	Meaning
1	noError (0)	No error detected. Normal case. In this case, the requested MIB object value is placed in the SNMP message to be sent.
2	tooBig (1)	The SNMP message is too large — more than 484 bytes — to contain the operation result.
3	noSuchName (2)	The requested MIB object could not be found. The GETNEXT REQUEST for which the identifier of an object following the last supported MIB object had been specified was received. The requested MIB object value is not set in the SNMP message. The requested process (SET REQUEST) is not executed also.
4	badValue (3)	(Does not occur.)
5	readOnly (4)	(Does not occur.)
6	genErr (5)	The requested operation cannot be executed for any reason other than the above.

Note: If any of the following errors is detected in the SNMP manager's request, the array unit does not respond.

- The community name does not match the setting:

  The array unit does not respond, however, it sends a standard trap, that is, Authentication Failure (incorrect community name), to the manager.

- The SNMP request message exceeds 484 bytes:

  Since the array unit cannot send or receive SNMP messages that are too long (more than 484 bytes), it does not respond to any SNMP messages it receives exceeding the limit.

Chapter 3 Operations

The following operations are included in this section:

- Trap-Issuing Processing
- Request Processing

3.1 Trap-Issuing Processing

A trap-issuing event in the array unit causes the array unit to issue a trap to the SNMP manager asynchronously, to report the error only once (Figure 3.1).

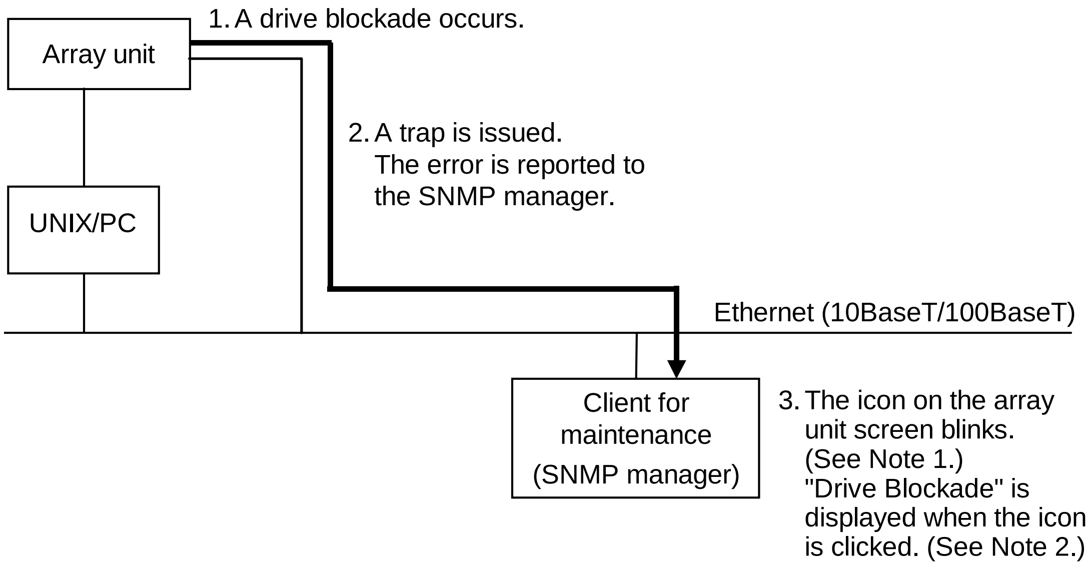


Figure 3.1 Example of a Drive Blockade and Trap Issue

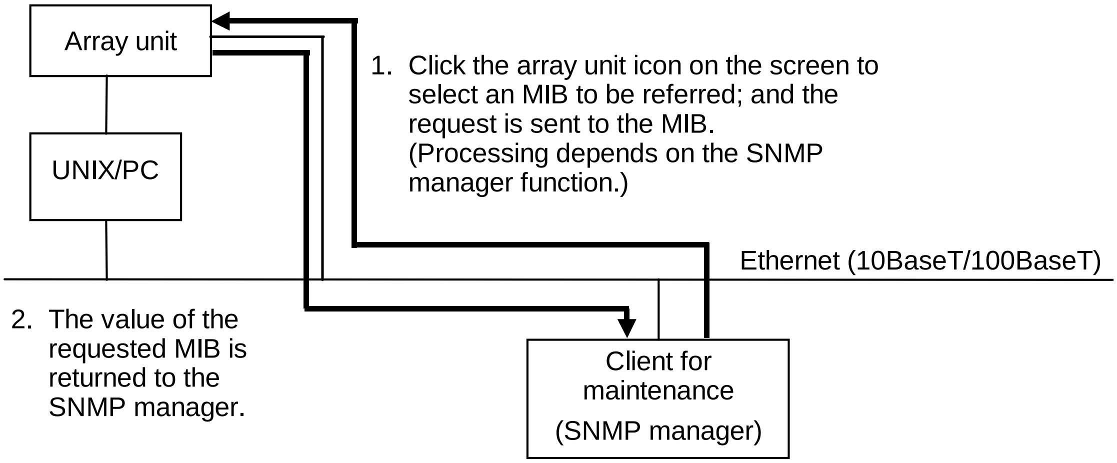
The trap indicates the occurrence of an error and the relevant regressed site only; it does not identify its exact location (e.g., drive number).

Note 1: The action taken at the time the trap is received depends on the specification of the SNMP manager used.

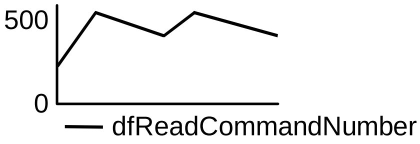
Note 2: The display operation and the display specification of the trap codes depend on the specification of the SNMP manager used.

3.2 Request Processing

This process returns the value of the MIB that the SNMP manager requested (Figure 3.2).



1. Click the array unit icon on the screen to select an MIB to be referred; and the request is sent to the MIB. (Processing depends on the SNMP manager function.)
2. The value of the requested MIB is returned to the SNMP manager.
3. The value of the requested MIB is displayed on the screen. (Note 1)
   Example 1: Information specific to the device is displayed as shown below.
   dfSystemProductName = HITACHI DF600F
   dfSystemMicroRevision = 0650
   Example 2: Information on the regressed portion is displayed (no error detected) as shown below.
   dfRegressionStatus = 0
   Example 3: Number of read command reception is graphically displayed as shown below. (Displays can be requested twice or more times at regular intervals.)



Note 1: The display specification of MIB depends on the specification of the SNMP manager used.

Figure 3.2 Example of Request Processing

Regressed portion information indicates only a regressed portion. It does not indicate the exact error location (e.g., drive number). If the interval set for obtaining the MIB information is too short, host command processing performance of the array unit may be affected negatively.

The array unit cannot send/receive SNMP messages longer than 484 bytes; the array unit does not respond to a message of that length. When sending such a message, the array unit returns the message “tooBig” (section 2.2). To avoid this problem, the SNMP manager should not send a message that will request a response exceeding 485 bytes (Figure 3.3).

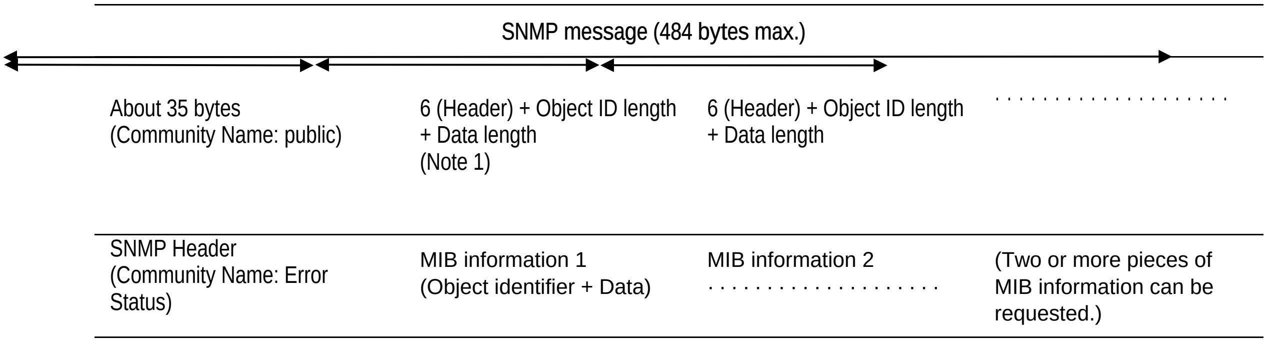

SNMP message (484 bytes max.)
About 35 bytes
(Community Name: public)
6 (Header) + Object ID length
+ Data length
(Note 1)
6 (Header) + Object ID length
+ Data length
. . . .
SNMP Header
(Community Name: Error Status)
MIB information 1
(Object identifier + Data)
MIB information 2
. . . .
(Two or more pieces of MIB information can be requested.)

Figure 3.3 SNMP Message Management

Note 1: The action when receiving a trap depends on the specifications of the SNMP manager being used. MIB information 1 becomes 6+8+10 = 24 bytes long.
However, the header length varies with the data length, as shown below:

Data length	0 to 115 bytes	: Header 6 bytes
	116 to 127 bytes	: Header 7 bytes
	128 to 242 bytes	: Header 8 bytes
	243 to 255 bytes	: Header 9 bytes
	256 bytes or more	: Header 10 bytes

Chapter 4 Installing and Uninstalling

SNMP is an optional feature of the array unit. To enable the SNMP function (in an unlocked state), install SNMP. To remove SNMP, the SNMP function must be uninstalled.
This section describes the following:

- Installing SNMP
- Uninstalling SNMP

SNMP is installed and uninstalled using the Disk Array management program 2.

Note: Before installing and uninstalling SNMP, make sure that the array unit is in normal operating order. If a failure such as a controller blockade has occurred, installing and uninstalling operations cannot be performed.

4.1 Installing SNMP

To install SNMP, the key code provided with SNMP is required. You can install SNMP using the following methods:

The following describes GUI installation procedures performed by using the Disk Array management program 2:

1. Start Disk Array management program 2 and switch to **Management Mode**.
2. Register the array unit in which you will install SNMP. Connect to this array unit; a window for the connected array unit is displayed (Figure 4.1).

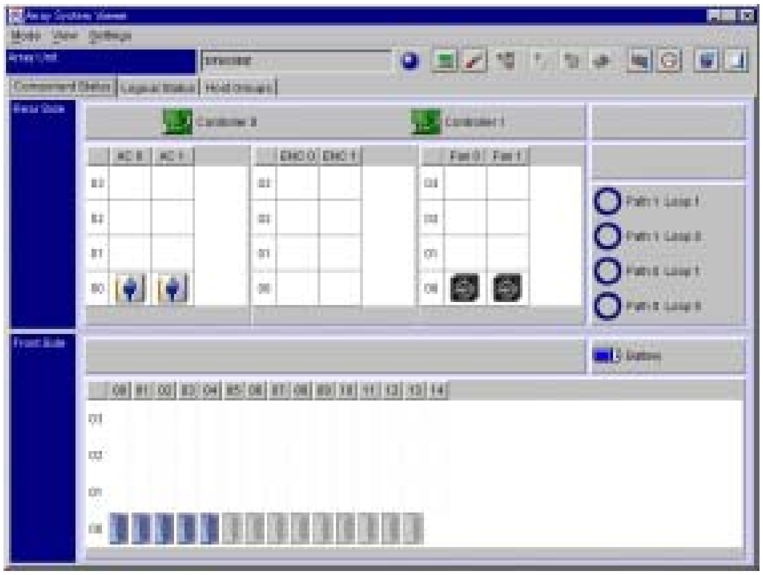
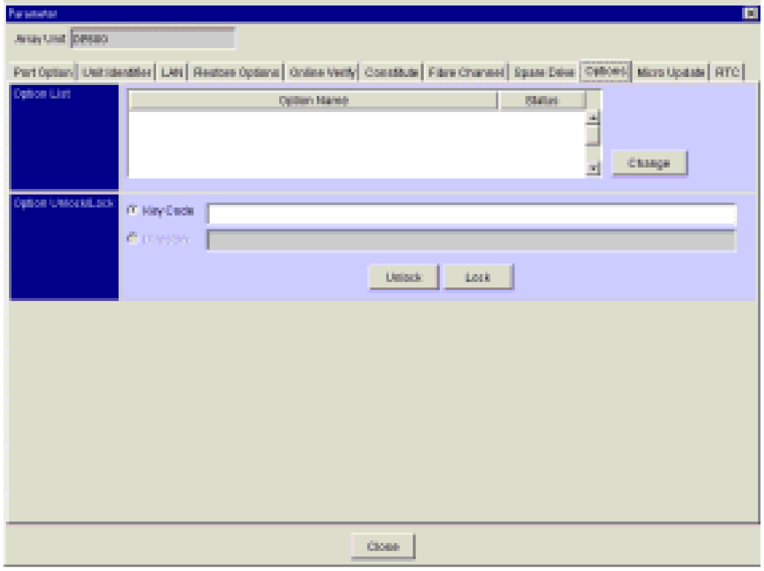


Figure 4.1 Array System Viewer

3. From the **Settings** menu, select **Configuration Settings**. Alternatively, from the tool bar, select the **Configuration Settings** button.
   The Parameter dialog box is displayed (Figure 4.2).

4. Click the **Options** tab.

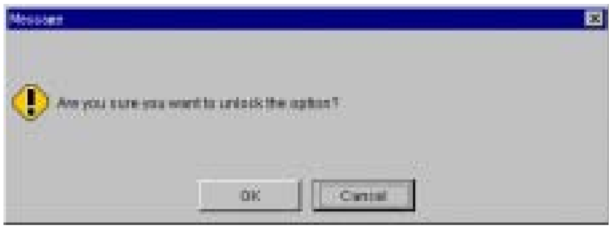


Array Unit DF680

Figure 4.2 Parameter Dialog Box

5. Enter a key code in the text box. Click the **Unlock** button.

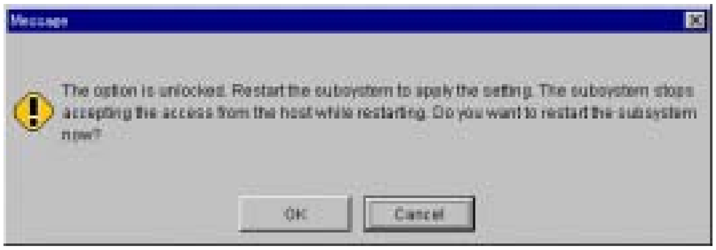
6. A screen appears, requesting a confirmation to unlock the SNMP option (Figure 4.3).
   Click the **OK** button.



Are you sure you want to unlock the option?

Figure 4.3 SNMP Unlock Confirmation Message

7. A message appears, confirming that the SNMP feature is opened. This message also asks you to restart the system (Figure 4.4). Click the **OK** button.



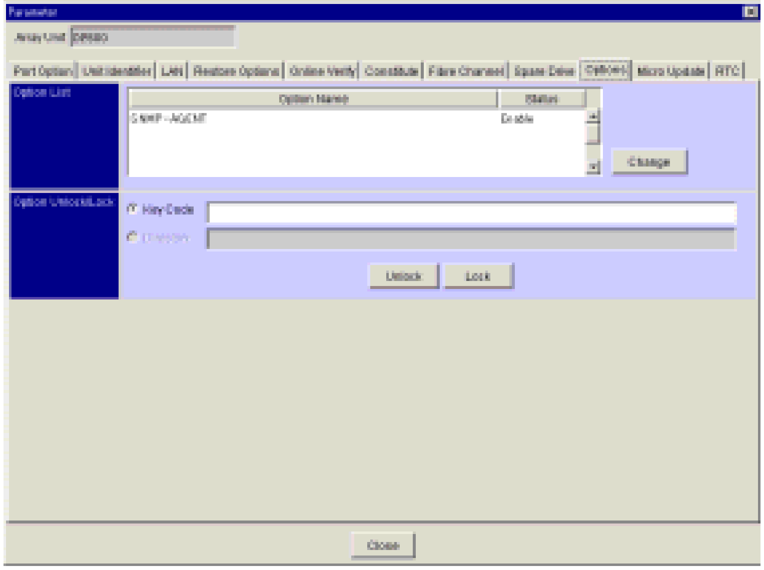
The option is unlocked. Restart the subsystem to apply the setting. The subsystem stops accepting the access from the host while restarting. Do you want to restart the subsystem now?

Figure 4.4 Restart After Unlock

Note: The SNMP feature is not opened until the system is restarted. The subsystem cannot access the host until the restart is completed. Therefore, be certain the host has stopped accessing data before beginning the restart process.

If you decide to wait to restart until you set additional information in the SNMP environment information file, click the **Cancel** button. After setting information in the SNMP environment information file, restart the disk array unit.

If you choose not to restart the array unit, a screen appears, displaying the unlocked optional feature: SNMP (Figure 4.5).

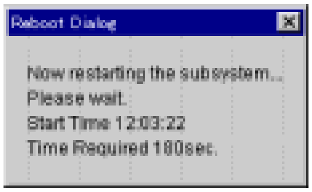


Array Unit: DF580

Option Name	Status
SNMP-AGENT	Enable

Figure 4.5 Unlocked Optional Feature: SNMP

When you choose to restart the array unit, the time the restart began is displayed. (Figure 4.6) Restarting takes approximately two to six minutes.

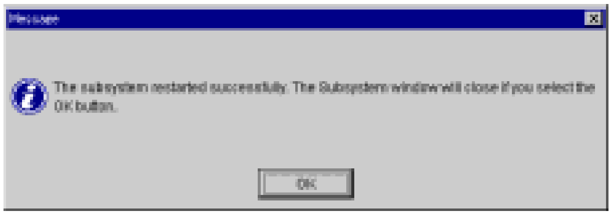


Now restarting the subsystem...
Please wait.
Start Time 12:03:22
Time Required 180sec.

Figure 4.6 Reboot Dialogue Box: Restart Time Display

Note: It may take time for an array unit to respond. However, if it does not respond after 10 minutes or more, check the condition of the array unit.

8. When the restart terminates, a message appears (Figure 4.7). Click the **OK** button; the Unit screen closes. To perform other operations on the Main screen, select an array unit from the Main screen and open the selected Unit screen.



The subsystem restarted successfully. The Subsystem window will close if you select the OK button.

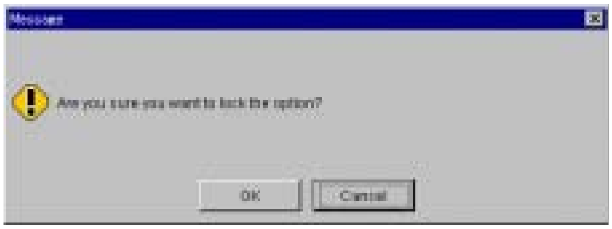
Figure 4.7 Subsystem Restart Successful Message

4.2 Uninstalling SNMP

To uninstall SNMP, the key code provided with SNMP is required.

The following describes GUI uninstallation procedures performed by using the Disk Array management program 2:

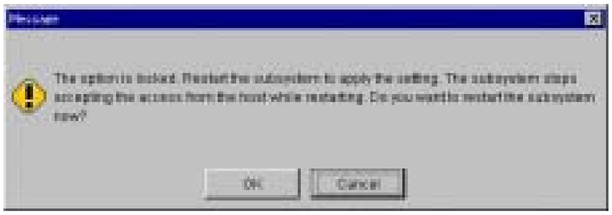
1. Start Disk Array management program 2 and switch to **Management Mode**.
2. Register the array unit in which you will uninstall SNMP. Connect to this array unit; a window for the connected array unit is displayed (Figure 4.1).
3. From the **Settings** menu, select **Configuration Settings**. Alternatively, from the tool bar, select the **Configuration Settings** button.
   The Parameter dialog box is displayed.
4. Click the **Options** tab (Figure 4.5).
5. Enter a key code in the text box. Click the **Lock** button.
6. A screen appears, requesting confirmation to lock the SNMP option (Figure 4.8) Click the **OK** button.



Are you sure you want to lock the option?

Figure 4.8 Option Lock Confirmation

7. A message appears, confirming that this optional feature is locked (Figure 4.9). This message also tells you to restart the system to apply the setting. Click the **OK** button.



The option is locked. Restart the subsystem to apply the setting. The subsystem stops accepting the access from the host while restarting. Do you want to restart the subsystem now?

Figure 4.9 Option Lock Confirmation

Note: The SNMP optional feature is not locked until the system is restarted. The subsystem cannot access the host until the restart is completed. Therefore, be certain the host has stopped accessing data before beginning the restart process.

If you choose not to restart the array unit, a screen appears, displaying the locked optional feature: SNMP.

When you choose to restart the array unit, the time the restart began is displayed (Figure 4.6). Restarting takes approximately two to six minutes.

Note: It may take time for an array unit to respond. However, if it does not respond after 10 minutes or more, check the condition of the array unit.

8. When the restart terminates, a message appears (Figure 4.7). Click the **OK** button; the Unit screen closes. To perform other operations on the Main screen, select an array unit from the Main screen and open the selected Unit screen.

Chapter 5 Operation Procedures

The SNMP operational procedures include the following:

- Setup
- Setting Enable/Disable
- Creating an Environmental Information File
- Registering SNMP Environmental Information
- Referencing the SNMP Environment Information File

5.1 Setup

Setup procedures include:

- Setting Up the Array Unit Side
- Setting Up the SNMP Manager Side
- Checking

5.1.1 Setting Up the Array Unit Side

1. Set LAN information (IP Address, Sub Net Mask, and Default Gateway Address). For operating procedures, refer to the *Hitachi DF600 User and Reference Guide.*
2. Enable the optional feature using the Disk Array management program 2. When installing the SNMP agent, it has been set in an enabled state.

   Note: For operating procedures, see section 5.2**.**
3. Create the SNMP environment information file. The SNMP environment file consists of the following two files.
   - Operating environment setting file (CONFIG.TXT)
     Sets the IP address of the SNMP manager to send traps, etc.
   - Unit name setting file (NAME.TXT)
     Sets the names of units.

   Note: For operating procedures, see section 5.3, which is created at step 3, using the Disk Array management program 2.
4. Register in an array unit the SNMP environment information file which is created in step 3, using the Disk Array management program 2.
5. *Note:* For operating procedures, see section 5.4.
6. Restart the array unit.

5.1.2 Setting Up the SNMP Manager Side

1. Transfer the provided MIB definition file into the SNMP manager.

   Note: For operating procedures, refer to manuals of individual SNMP managers.

2. Register the array unit in the SNMP manager.

   Note: For operating procedures, refer to manuals of individual SNMP managers.

5.1.3 Checking

1. Check a connection between the array unit and the SNMP manager.

   Note: For checking procedures, see section 5.6.

Completion of the operations described above enables communication between the array unit and the SNMP manager.

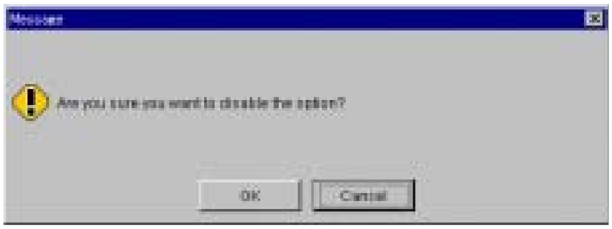
The SNMP agent is set in an “enabled/disabled” state and the SNMP environment information file is registered, using the Disk Array management program 2 or the Disk Array management program. For information on the operating procedures of the Disk Array management program 2, refer to the *Disk Array manager program 2 (for GUI) User’s Guide* and/or the *Disk Array manager program (for CLI) User’s Guide.*

5.2 Setting Enable/Disable

To use the SNMP agent, install the optional feature and set it in an enabled state. When installing the SNMP agent, it has been set in an enabled state. If the SNMP agent function is not used, set the settings invalid.

The following describes SNMP setting procedures performed by using the GUI version of the Disk Array management program 2.

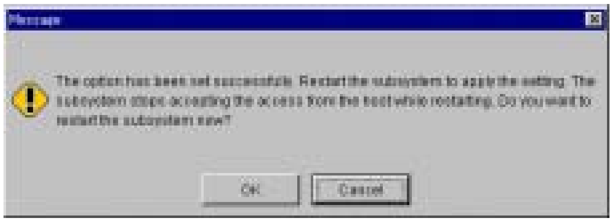
1. Start Disk Array management program 2 and switch to **Management Mode**.
2. Register the array unit in which you will set up SNMP. Connect to this array unit; a window for the connected array unit is displayed (Figure 4.1).
3. From the **Settings** menu, select **Configuration Settings**. Alternatively, from the tool bar, select the **Configuration Settings** button.
   The Parameter dialog box is displayed.
4. Click the **Options** tab (Figure 4.5).
5. Click on "SNMP-AGENT" in the **Option Name** text box. Click the **Change** button.
6. The following screen message is displayed (Figure 5.1). Click the **OK** button.



Are you sure you want to disable the option?

Figure 5.1 Disable Option Message Dialogue Box

7. A screen appears, confirming that the SNMP agent has been set up (Figure 5.2). This message also asks you to restart the system. Click the **OK** button.

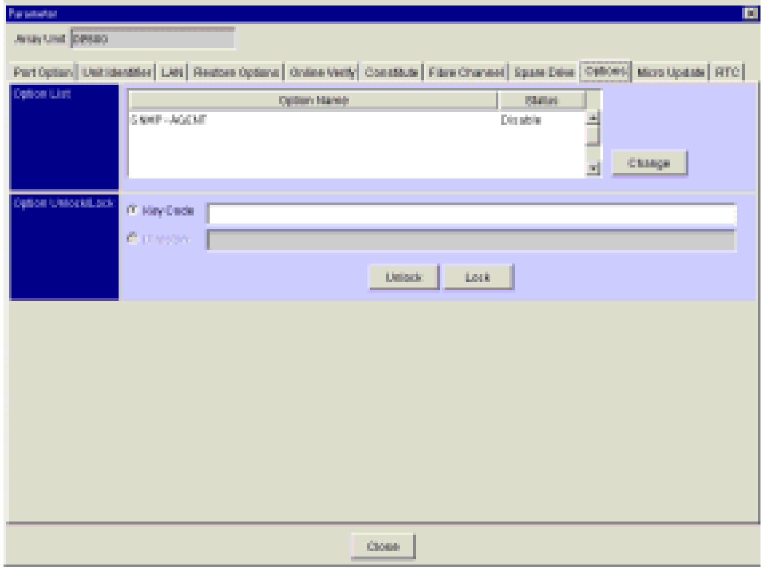


The option has been set successfully. Restart the subsystem to apply the setting. The subsystem stops accepting the access from the host while restarting. Do you want to restart the subsystem now?

Figure 5.2 SNMP Agent Confirmation Window

Note: The SNMP setup is not effective until the system is restarted. The subsystem cannot access the host until the restart is completed. Therefore, be certain the host has stopped accessing data before beginning the restart process.

If an array unit fails to restart, a screen is displayed with the set-up SNMP agent status being updated (Figure 5.3).



Option Name	Status
SNMP-AGENT	Disable

Figure 5.3 SNMP Agent Status Update

When you choose to restart the array unit, the time the restart began is displayed (Figure 4.6). Restarting takes approximately two to six minutes.

Note: It may take time for an array unit to respond, depending on the configuration of the array unit. However, if it does not respond after 10 minutes or more, check the condition of the array unit.

8. When the restart terminates, a message appears (Figure 4.7). Click the **OK** button; the Unit screen closes. To perform other operations on the Main screen, select an array unit from the Main screen and open the selected Unit screen.

5.3 Creating an Environmental Information File

To use the SNMP agent, the SNMP environment information file is created and is registered in the array unit. The following two files are created as the SNMP environment information file.

- Operation environment setting file (CONFIG.TXT)
- Unit name setting file (NAME.TXT)

The SNMP environment information file is created and registered in both cases, at the SNMP initial setting and when an operating environment is changed. The SNMP environment information file is created with an editor on a PC, etc.; some items in a provided sample file are modified to suit your environment.

In a dual controller configuration, only one set (two files) has to be created per one unit of array unit. Therefore, it is not possible to set different information for each controller.

5.3.1 Operation Environment Setting File

This section contains the following:

- File Format
- Settings
- How to Create Files

5.3.1.1 File format

This file is in text form and is on a DOS-formatted 1.44 MB disk. The file name is “CONFIG.TXT”.

5.3.1.2 Settings

Setting items are shown in Table 5.1.

Table 5.1 Operation Environment Settings

No.	Item	Description	Remarks
1	sysContact (MIB information)	Manager information for contact (name, department, extension No., etc.)	Internal object value of MIB-II system group in ASCII form, not exceeding 255 characters (Omissible item)
2	sysLocation (MIB information)	Place where the device is installed	
3	Community information setting (MIB information)	Name of the community permitted access.	A number of names of the community can be set. (Omissible item)
4	Trap sending (Trap report)	Setting of information for sending a trap • Destination manager IP address • Destination port number • Community name given to a trap	Several combinations of information can be set. (Essential item)

5.3.1.3 How to Create Files

Use the following procedure to set each item shown in Table 5.1.

1. Setting sysContact (manager’s name/items for contact):
   - Add a line beginning with “INITIAL” to the file to set the sysContact value:

     ```
     INITIAL sysContact user set information
     ```

   - User set information cannot exceed 255 alphanumeric characters.
   - For any characters (space, tab, “-”, “‘“, etc.) other than the letters a to z (uppercase and lowercase) and the numerals are used by the user to set information, the characters must be enclosed with double quotation marks (“).
   - There should be no line-feed codes in this information.

2. Setting sysLocation (installation place):
   - Add a line beginning with “INITIAL” to the file to set the sysLocation value:

     ```
     INITIAL sysLocation user set information
     ```

   - User set information cannot exceed 255 alphanumeric characters.
   - In any characters (space, tab, “-”, “‘“, etc.) other than the letters a to z (uppercase and lowercase) and the numerals are used by the user to set information, the characters must be enclosed with double quotation marks (“).
   - There should be no line-feed codes in this information.
3. Setting community information:

   Add a line beginning with “COMMUNITY” to the file to specify the community name with which the array unit allows receiving of requests:

   ```
   COMMUNITY community name
   ALLOW ALL OPERATIONS
   ```

   - Unless this is specified, the array unit accepts all community names.
   - The community name must be described in alphanumeric characters only.
     If any characters (space, tab, “-”, “‘“, etc.) other than the letters a to z (uppercase and lowercase) and the numerals are used in the community name, the characters must be enclosed with double quotation marks (“). The community name cannot contain line-feed codes.
   - To enable the array unit to accept all community names, delete the above 2 lines including the line starting with “COMMUNITY”.

4. Setting address(es) to send a trap (Multiple addresses can be set.):

   Add a line beginning with “MANAGER” (Figure 5.4) to the file to specify the SNMP manager to which the array unit issues traps.

```
MANAGER SNMP manager IP address
SEND ALL TRAPS TO PORT Port No.
WITH COMMUNITY Community name
```

Figure 5.4 Setting Address to Send a Trap

- Enter the IP address to select the object SNMP manager. Do not specify a host name.
- Enter IP addresses with the leading 0s in each dotted quad suppressed (for example, specify 111.22.3.55 for 111.022.003.055).
- Enter the UDP destination port number to be set when sending a trap to the SNMP manager for the Port No. Number 162 is the usual port number used by the SNMP manager to receive traps.
- For the Community name, a community name, which is set in an SNMP message when sending a trap, is specified with alphanumerics. If any characters (space, tab, “-”, “‘“, etc.) other than the letters a to z (uppercase and lowercase) and the numerals are used in the community name, enclose them with double quotation marks (“).
- This information cannot contain line-feed codes. If the community name does not contain a close (line beginning with WITH COMMUNITY), add “public” to the Community name.

Note 1: This file cannot exceed 1,140 bytes.

Note 2: The total length of “sysContact”, “sysLocation”, and “sysName” (to be explained later) should not exceed 280 characters (when the name of the community with right to access does not exceed 10 characters) so that all the objects in the MIB-II system group can be obtained with the one GET request (Figure 5.5). This will to prevent a “tooBig” error message.

```
INITIAL sysContact “Taro Hitachi”

INITIAL sysLocation “Computer Room A on Hitachi STR HSP 10F north”

COMMUNITY public
ALLOW ALL OPERATIONS

MANAGER 123.45.67.89
SEND ALL TRAPS TO PORT 162
WITH COMMUNITY “HITACHI DF600”

MANAGER 123.45.67.90
SEND ALL TRAPS TO PORT 162
WITH COMMUNITY “HITACHI DF600”
```

Figure 5.5 Operation Environment Setting File

5.3.2 Unit Name Setting File

This section contains the following:

- File Format
- Settings
- How to Create the File

5.3.2.1 File format

This file should be in text format on a DOS-formatted 1.44 Mbyte disk. The file name is "NAME.TXT".

5.3.2.2 Settings

Setting items are shown in Table 5.2.

Table 5.2 Item of Unit Name Setting

No.	Item	Description	Remarks
1	sysName	Unit name for management	Internal object value of MIB-II system group in ASCII character string not exceeding 255 characters

5.3.2.3 How to Create the File

To set the value of sysName, register the information continuously. Since the entire contents of this file are regarded as the sysName value, the file should not exceed 255 characters.

Do not use line-feed codes in this file. (No line-feed is necessary at the end of sentence.) Use only alphanumeric characters:

```
DF600-01 Hitachi Disk Array
```

Note: The total length of "sysContact", "sysLocation", and "sysName should not exceed 280 characters, when the name of the community with right to access does not exceed 10 characters. This allows for all the objects in the MIB-II system group to be obtained with one GET request. This will prevent a "tooBig" error message.

5.4 Registering SNMP Environmental Information

To work the SNMP agent, the SNMP environment information file in the provided FD is registered in the array unit.

1. Start Disk Array management program 2 and switch to **Management Mode**.
2. Register the array unit in which you will set up SNMP. Connect to this array unit; a window for the connected array unit is displayed (Figure 4.1).
3. From the **Settings** menu, select **Configuration Settings**. Alternatively, from the tool bar, select the **Configuration Settings** 🖥 button.
   The Parameter dialog box is displayed.
4. Click the **SNMP** tab.

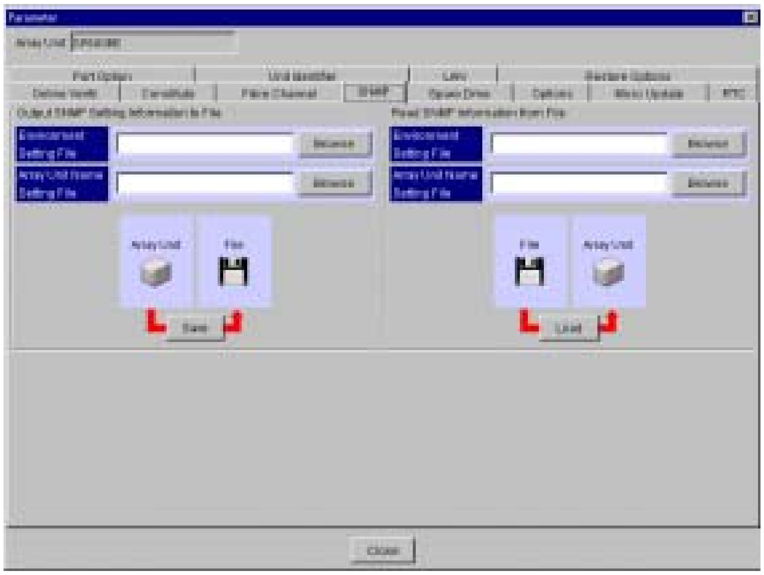
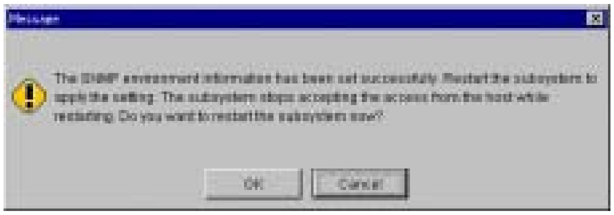


Figure 5.6 Parameter Dialogue Box (SNMP tab)

5. Set a path to the SNMP environment information file (config.txt, name.txt), and click the **Load** button. If only one file is set, specify only a path to a file to set.
6. A message appears, confirming that the settings are complete (Figure 5.7). This message also asks you to restart the system. Click the **OK** button.



Message

The SNMP environment information has been set successfully. Restart the subsystem to apply the setting. The subsystem stops accepting the access from the host while restarting. Do you want to restart the subsystem now?

Figure 5.7 Settings/Environment Complete Dialogue Box

Note: The SNMP environment information settings are not valid until the system is restarted. The subsystem cannot access the host until the restart is completed. Therefore, be certain the host has stopped accessing data before beginning the restart process.

When you choose to restart the array unit, the time the restart began is displayed (Figure 4.6). Restarting takes approximately two to six minutes.

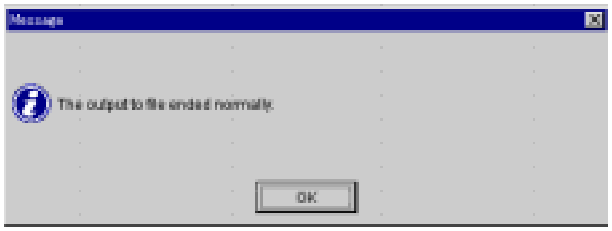
Note: It may take time for an array unit to respond. However, if it does not respond after 10 minutes or more, check the condition of the array unit.

7. When the restart terminates, a message appears (Figure 4.7). Click the **OK** button; the Unit screen closes. To perform other operations on the Main screen, select an array unit from the Main screen and open the selected Unit screen.

5.5 Referencing the SNMP Environment Information File

Output the SNMP environment information file already registered in the array unit to a text file for the SNMP agent and reference environment information. The following paragraphs describe procedures for reference.

1. Start Disk Array management program 2 and switch to **Management Mode**.
2. Register the array unit in which you will set up SNMP. Connect to this array unit; a window for the connected array unit is displayed (Figure 4.1).
3. From the **Settings** menu, select **Configuration Settings**. Alternatively, from the tool bar, select the **Configuration Settings** button.
   The Parameter dialog box is displayed.
4. Click the **SNMP** tab (Figure 5.6).
5. Set a path to the directory in which the SNMP environment information file (config.txt, name.txt) has been stored. Click the **Save** button. If only one file is output, specify only a path to a file to output.
6. A message appears, confirming that output to the file is complete (Figure 5.8). Click the **OK** button.



The output to file ended normally.

Figure 5.8 Output Confirmation Dialogue Box

The SNMP environment information file set currently in a file specified at step 5 has been output.

5.6 How to Verify the SNMP Connection

Use the following the procedure to confirm the SNMP connection between the array unit and the SNMP manager.

1. Trap connection check

   Power the array unit off and on again. Check that a standard trap, “coldStart,” has been received at all SNMP managers which have been set as a trap receiver in the SNMP environment information file (Config.txt).

2. REQUEST connection check

   Send an array unit supported MIB GET request to the array unit from all the SNMP managers to be connected to the array unit through an SNMP while the array unit is ready. Verify that the array unit responds.

If the results of operations 1 and 2 above are normal, communication, based on the SNMP between the array unit and each SNMP manager, is possible.

5.7 How to Detect Failure

The method to detect failures of the array unit by using the SNMP agent support function is described below.

1. Obtain MIB information (dfRegressionStatus and dfPreventiveMaintenanceInformation) periodically. (Recommended)

   This MIB value is set to “0” when there are no failures.

2. If an error occurs that results in a trap, the array unit reports the error to the SNMP manager.

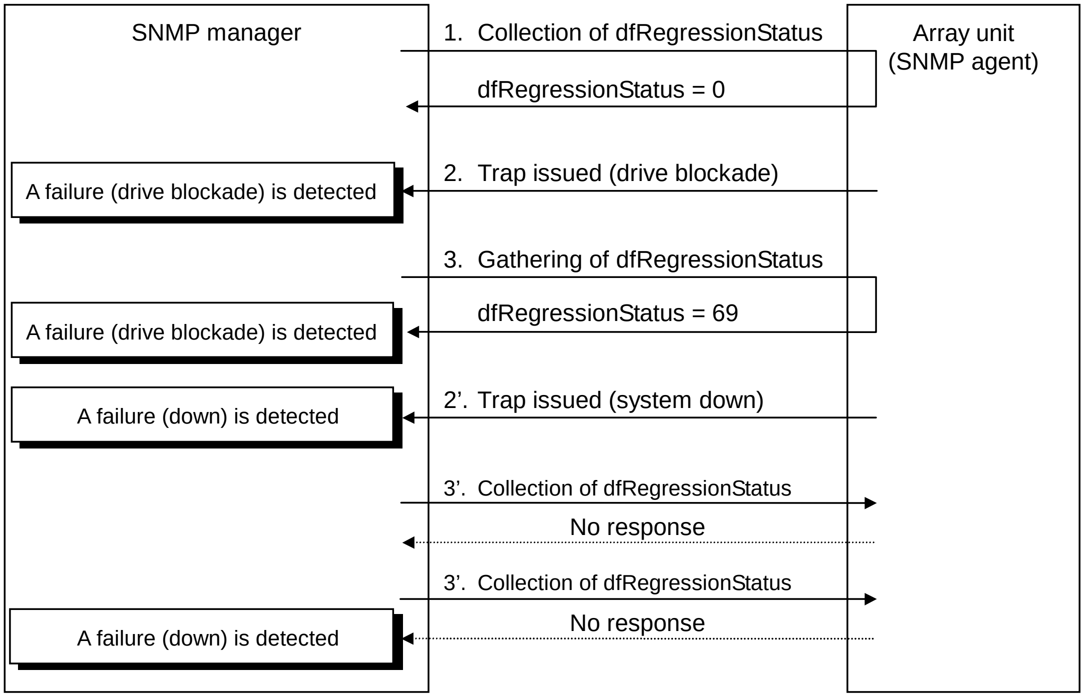
   This trap normally allows the user to detect array unit failures immediately when they occur; the UDP protocol used, however cannot assure that the trap is correctly reported to the SNMP manager. If a controller goes down, the systemDown trap may not be issued.

3. Errors are detected with MIB information obtained periodically as in item 1 above. The user will know that a failure has occurred and/or a part has failed even when a trap described in item 2 above is not reported because the MIB value (dfRegressionStatus and dfPreventiveMaintenanceInformation) in the event of failure is not 0.

   Example: When a drive is blocked;
   dfRegressionStatus = 69

A request from the SNMP manager may receive no response if a controller blockade exists. The user can detect a controller blockade even if no systemDown trap was reported. However, because the UDP protocol is used, it is possible that requests from the SNMP manager may be ignored, even when operation is normal.

When continuous requests receive no response, a controller blockade exists.


SNMP manager
Array unit
(SNMP agent)
1. Collection of dfRegressionStatus
dfRegressionStatus = 0
2. Trap issued (drive blockade)
A failure (drive blockade) is detected
3. Gathering of dfRegressionStatus
dfRegressionStatus = 69
A failure (drive blockade) is detected
2’. Trap issued (system down)
A failure (down) is detected
3’. Collection of dfRegressionStatus
No response
3’. Collection of dfRegressionStatus
No response
A failure (down) is detected

Chapter 6 Management Information

This section includes the following:

- Supported MIBs
- MIB Access Mode
- Object Identifier Assignment System
- Types of Supported Traps and Trap Issuing Opportunity

6.1 Supported MIBs

The array unit supports only the MIBs shown in Table 6.1.

GET RESPONSE of noSuchName is returned in response to the GET or SET request issued to an unsupported object.

Table 6.1 Supported MIBs

No.	MIB		Support	Relevant document	Remarks
1	MIB II			RFC1213	—
		system group	○		See 7.1.1.
		interface group	Δ		See 7.1.2.
		at group	×		See 7.1.3.
		ip group	Δ		See 7.1.4.
		icmp group	×		See 7.1.5.
		tcp group	×		See 7.1.6.
		udp group	×		See 7.1.7.
		egp group	×		See 7.1.8.
		snmp group	○		See 7.1.9.
2	Extended MIB		○	—	See 7.2.

○: Supported Δ: Supported partially ×: Not supported

6.2 MIB Access Mode

The access mode for all community MIBs should be read-only.

GET RESPONSE of noSuchName is returned in response to each SNMP manager’s SET request.

6.3 Object Identifier Assignment System

Figure 6.1 illustrates the Object Identifier Assignment System.

```
root
   |---ccitt(0)
   |---iso(1)
   |      |---org(3)
   |             |---dod(6)
   |                     |---internet(1)
   |                                 |---mgmt(2)
   |                                 |          |---mib-2(1)
   |                                 |                    |---system(1)
   |                                 |                    |---interface(2)
   |                                 |                    |---at(3)
   |                                 |                    |---ip(4)
   |                                 |                    |---icmp(5)          MIB-II
   |                                 |                    |---tcp(6)           (Standard MIB)
   |                                 |                    |---udp(7)
   |                                 |                    |---egp(8)
   |                                 |                    |---snmp(11)
   |                                 |
   |                                 |---private(4)
   |                                            |---enterprises(1)      Vendor unique MIB
   |---joint_iso_ccitt(2)

enterprises(1)
      |---hitachi(116)
               |---system(3)
               |          |---storage(11)
               |                    |---dfraid(1)
               |                               |---df300agt(1)          Array unit PC utility identifier
               |                               |
               |                               |---dfraidLan(2)         Array unit product identifier
               |                                                        (dfraid series common identifier)
               |
               |
               +---systemExMib(5)
                          |---storageExMib(11)
                                    |---dfraidExMib(1)
                                               |---df300ExMib(1)             Array unit PC utility extension MIB
                                               |
                                               |---dfraidLanExMib(2)         Array unit built-in extension MIB
                                                                             (common to dfraid series)
```

Figure 6.1 The Object Identifier Assignment System

```
dfraidLanExMib(2)
     |—-dfSystemParameter(1)
     |         |—-df0SystemProductName(1)                   Product name
     |         |—-dfSystemMicroRevision(2)                  Microprogram Rev. No.
     |         |—-dfSystemSerialNumber(3)                   DFxxx Serial No.
     |
     |—-dfWarningCondition(2)
     |         |—-dfRegressionStatus(1)                Warning failure information
     |         |—-dfPreventiveMaintenanceInformation(2)     Preventive maintenance information
     |         |—-dfWarningReserve1(3)                 Not used
     |         |—-dfWarningReserve2(4)                 Not used
     |
     |—-dfCommandExecutionCondition(3)
     |         |—-dfCommandTable(1)
     |                   |—-dfCommandEntry(1)
     |                             |—-dfLun(1)                  Logical unit No.
     |                             |—-dfReadCommandNumber(2)    Number of read command receptions
     |                             |—-dfReadHitNumber(3)        Number of cache read hits
     |                             |—-dfReadHitRate(4)          Cache read hit rate
     |                             |—-dfWriteCommandNumber(5)   Number of write command receptions
     |                             |—-dfWriteHitNumber(6)       Number of cache write hits
     |                             |—-dfWriteHitRate(7)         Cache write hit rate
     |
     |—-dfCacheLoadCondition(4)
     |         |—-dfWriteDataRate(1)                   Darty segment rate
     |
     |
  Continue to the next page (1)
```

Figure 6.1 The Object Identifier Assignment System (Continued)

Continued from the previous page (1)

```
     |
     |
     |—-dfLUNS(5)                                    LUN security information
     |       |—-dfLUNSSwitch(1)                      Security switch
     |       |       |—-dfLUNSSwitchEntry(1)
     |       |               |—-dfSwitchSerialNumber(1)      DFxxx serial number
     |       |               |—-dfSwitchPortID(2)            Port number
     |       |               |—-dfSwitchOnOff(3)             Valid/invalid status
     |       |               |—-dfSwitchControlSratus(4)     Control flag
     |       |—-dfLUNSWWN(2)                         WWN information
     |       |       |—-dfLUNSWWNEntry(1)
     |       |               |—-dfWWNSerialNumber(1)         DFxxx serial number
     |       |               |—-dfWWNPortID(2)               Port number
     |       |               |—-dfWWNControlIndex(3)         Control index
     |       |               |—-dfWWNWWN(4)                  WWN (Port Name)
     |       |               |—-dfWWNID(5)                   WWN number
     |       |               |—-dfWWNNickname(6)             Nickname
     |       |               |—-dfWWNUseNickname(7)          Use/no use of nickname
     |       |               |—-dfWWNControlStatus(8)        Control flag
     |       |—-dfLUNSWWNGroup(3)                    Not supported

     |       |—-dfLUNSLUN(4)                         LUN information

     |       |       |—-dfLUNSLUNEntry(1)
     |       |               |—-dfLUNSerialNumber(1)         DFxxx Serial number
     |       |               |—-dfLUNPortID(2)               Port number
     |       |               |—-dfLUNLUN(3)                  LUN
     |       |               |—dfLUNWWNSecurity(4)           WWN access permission
     |       |               |—dfLUNWWNGroupSecurity(5)      WWN group access permission
     |       |               |—dfLUNControlStatus(6)         Control flag
     |       |—-dfLUNSLUNGroup(5)                    Not supported
     |
     |—-dfPort(6)                                    Port information
     |       |—-dfPortInf(1)                         Port information
     |               |—dfPortinfEntry(1)
     |                       |—dfPortSerialNumber(1)         Serial number
     |                       |—dfPortID(2)                   Port number
     |                       |—dfPortkind(3)                 Kind of port
     |                       |—dfPortHostMode(4)             Host mode
     |                       |—dfPortFibreAddress(5)         N_Port ID
     |                       |—dfPortFibreTopology(6)        Topology type
     |                       |—dfPortControlStatus(7)        Control flag
     |                       |—dfPortDisplayName(8)          Port name
     |                       |—dfPortWWN(9)                  Port WWN of the port
```

Continue to the next page (2)

Figure 6.1 The Object Identifier Assignment System (Continued)

```
Continued from the previous page (2)
    |
    |
    |—-dfCommandExecutionInternalCondition(7)       Internal information for command execution conditions
           |—-dfCommandInternalTable(1)              Internal information for command execution conditions
                  |—-dfCommandInternalEntry(1)
                         |—-dfInternalLun(1)                     Logical unit No.
                         |—-dfInternalReadCommandNumber(2)  Number of read command receptions
                         |—-dfInternalReadHitNumber(3)          Number of cache read hits
                         |—-dfInternalReadHitRate(4)              Cache read hit rate
                         |—-dfInternalWriteCommandNumber(5)  Number of write command receptions
                         |—-dfInternalWriteHitNumber(6)          Number of cache write hits
                         |—-dfInternalWriteHitRate(7)              Cache write hit rate
```

Figure 6.1   The Object Identifier Assignment System (Continued)

6.4 Types of Supported Traps and Trap Issuing Opportunity

Of traps that the SNMP agent supports, Table 6.2 lists standard traps, and Table 6.3 lists extended traps.

Table 6.2 Supported Standard Traps

No.	Generic trap code	Trap	Meaning	Support
1	0	coldStart	Reset from power-off. (P/S on)	○
2	1	warmStart	Management module restarted	×
3	2	linkDown	Link goes down	×
4	3	linkUp	Link goes up	×
5	4	authenticationFailure	Illegal SNMP accessed	○
6	5	egpNeiborLoss	EGP error is detected	×
7	6	enterpriseSpecific	Enterprise extended trap	○

○: Supported ×: Not supported

Table 6.3 Supported Extended Traps

No.	Specific Trap Code	Title	Meaning
1	1	systemDown	Own controller down
2	2	driveFailure	Drive blockade (data drive)
3	3	fanFailure	Fan alarm
4	4	powerSupplyFailure	Power failure
5	5	batteryFailure	Battery alarm
6	6	cacheFailure	Partial cache blockade
7	7	UPS Failure	UPS alarm
9	9	Backup Circuit Failure	Battery charging circuit alarm
10	10	Other Controller Failure	Blockade of the mate controller
11	11	warning	Warned array unit
12	12	spareDriveFailure	Drive (spare drive) blockade
13	13	Microprogram Replacement executed	Online microprogram replacement executed
14	14	ENC Failure	ENC failure
15	15	Loop Failure	Loop failure
16	16	Path Failure	Path blockade
17	200	NAS Server Failure	NAS Server Failure
18	201	NAS Path Failure	NAS Path Failure
19	202	NAS UPS Failure	NAS UPS Failure

Chapter 7 MIB Installation Specifications

This chapter provides installation specifications for MIBs supported by the array unit. The following conventions are used to define these specifications:

- **Standard:** Indicates the standard shown on the subject standard document.
- **Content:** Indicates the content of the subject extended MIB.
- **Installation:** Indicates the specifications for mounting the subject MIB in the array unit.

Supporting status: ○: Supported △: Supported partially ×: Not supported

7.1 MIB II

mgmt OBJECT IDENTIFIER :: = {iso(1) org(3) dod(6) internet(1) 2}
mib-2 OBJECT IDENTIFIER :: = {mgmt 1}

7.1.1 system Group

system OBJECT IDENTIFIER :: = {mib-2 1}

Table 7.1 system Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	sysDescr {system 1}	R	[Standard] Name or version No. of hardware, OS, network OS [Installation] Fixed character string (Fibre connection for DF600) : HITACHI DF600F Verxxxxxx (Same as inquiry information)	○	
2	sysObjectID {system 2}	R	[Standard] Object ID indicating the agent vendor product identification No. [Installation] Value is fixed. Hitachi, Ltd..system. storage. dfraid. dfraidLan	○	
3	sysUpTime {system 3}	R	[Standard] Accumulated time since the SNMP agent software was started in units of 10 ms. [Installation] Value is fixed as 0.	○	
4	sysContact {system 4}	R	[Standard] agent manager's name and items for contact (manager, managing department, and extension number) [Installation] User specified ASCII character string (within 255 characters). No default value (NULL).	○	Should be Read_ Only in the array unit. Data should be entered from the operation environment setting file.

Table 7.1 system Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
5	sysName {system 5}	R	[Standard] A name given to the agent for management, namely, domain name. [Installation] User specified ASCII character string (within 255 characters). No default value (NULL).	○	Should be Read_Only in the array unit. Data should be entered from the operation environment setting file.
6	sysLocation {system 6}	R	[Standard] Installation place of the agent [Installation] User specified ASCII character string (within 255 characters). No default value (NULL).	○	Should be Read_Only in the array unit. Data should be entered from the operation environment setting file.
7	sysServices {system 7}	R	[Standard] Service value [Installation] Value is fixed as 8.	○	

7.1.2 interfaces Group

interfaces OBJECT IDENTIFIER : : = {mib-2 2}

Table 7.2 interfaces Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	ifNumber {interface 1}	R	[Standard] Number of network interfaces provided by this system. [Installation] Value is fixed as 1.	○	
2	ifTable {interface 2}	Impossible	[Standard] Information on each interface is presented in tabular form. The number of entries depends on the ifNumber value. [Installation] Same as the standard. (Refer to the lower hierarchical level.)	Δ	
2.1	ifEntry {ifTable 1}	Impossible	[Standard] Each interface information comprising the entries shown below. [Installation] Same as the standard. (Refer to the lower hierarchical level.)	Δ	
2.1.1	ifIndex {ifEntry 1}	R	[Standard] Interface identification number. [Installation] Value is fixed as 1.	○	(index)
2.1.2	ifDescr {ifEntry 2}	R	[Standard] Interface information [Installation] Fixed character string for each interface type. Ethernet 100BaseT	○	
2.1.3	ifType {ifEntry 3}	R	[Standard] Interface type ID number [Installation] Fixed value. ethernetCsmacd	○	
2.1.4	ifMtu {ifEntry 4}	R	[Standard] Maximum sendable/receivable frame length in bytes. MTU (Max Transfer Unit) value [Installation] — (Not installed)	×	
2.1.5	ifSpeed {ifEntry 5}	R	[Standard] Transfer rate in units of bit/s. [Installation] 100000000	○	
2.1.6	ifPhysAddress {ifEntry 6}	R	[Standard] Interface physical address [Installation] Mac Address	○	

Table 7.2 interfaces Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
2.1.7	ifAdminStatus {ifEntry 7}	RW	[Standard] Interface set status 1 : Operation 2 : Stop 3 : Test [Installation] — (Not installed)	×	
2.1.8	ifOperStatus {ifEntry 8}	R	[Standard] Current interface status 1 : Operating 2 : Stopped 3 : Testing [Installation] — (Not installed)	×	
2.1.9	ifLastChange {ifEntry 9}	R	[Standard] sysUpTime assumed when the subject interface ifOperStatus is changed last [Installation] — (Not installed)	×	
2.1.10	ifInOctets {ifEntry 10}	R	[Standard] Total number of bytes (including synchronous bytes) in the frame received by the subject interface [Installation] — (Not installed)	×	
2.1.11	ifInUcastPkts {ifEntry 11}	R	[Standard] Number of subnetwork unicast packets reported to the host protocol [Installation] — (Not installed)	×	
2.1.12	ifInNUcastPkts {ifEntry 12}	R	[Standard] Number of broadcast or multicast packets reported to the host protocol [Installation] — (Not installed)	×	
2.1.13	ifInDiscards {ifEntry 13}	R	[Standard] Number of received packets discarded due to insufficient buffer space, even if normal [Installation] — (Not installed)	×	
2.1.14	ifInErrors {ifEntry 14}	R	[Standard] Number of received erred packets [Installation] — (Not installed)	×	
2.1.15	ifInUnknownProtos {ifEntry 15}	R	[Standard] Number of received packets discarded due to incorrect or unsupported protocol [Installation] — (Not installed)	×	
2.1.16	ifOutOctets {ifEntry 16}	R	[Standard] Total number of bytes (including synchronizing characters) in transmitted frames [Installation] — (Not installed)	×	
2.1.17	ifOutUcastPkts {ifEntry 17}	R	[Standard] Number of packets (including those not sent) requested unicast from the upper layer. [Installation] — (Not installed)	×	

Table 7.2 interfaces Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
2.1.18	ifOutNUcastPkts {ifEntry 18}	R	[Standard] Number of packets (including those discarded and not sent) requested broadcast or multicast from the upper layer. [Installation] — (Not installed)	×	
2.1.19	ifOutDiscards {ifEntry 19}	R	[Standard] Number of packets discarded due to insufficient transmit buffer space, etc. [Installation] — (Not installed)	×	
2.1.20	ifOutErrors {ifEntry 20}	R	[Standard] Number of packets not sent due to errors. [Installation] — (Not installed)	×	
2.1.21	ifOutQLen {ifEntry 21}	R	[Standard] Sent frame queue length (indicated in number of packets) [Installation] — (Not installed)	×	
2.1.22	ifSpecific {ifEntry 22}	R	[Standard] Object identifier number for defining the MIB specific to interface media [Installation] Value is fixed as 0.0.	○	

7.1.3 at Group

at OBJECT IDENTIFIER :: = {mib-2 3}

This group is not supported.

7.1.4 ip Group

ip OBJECT IDENTIFIER :: = {mib-2 4}

Table 7.3 ip Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	ipForwarding {ip 1}	R	[Standard] Specifies whether received IP packets are transferred as IP gateways. 1 : Transfer 2 : No transfer [Installation] — (Not installed)	×	
2	ipDefaultTTL {ip 2}	R	[Standard] Default value to be set in TTL (Time to live: packet life) in IP header. [Installation] — (Not installed)	×	
3	ipInReceives {ip 3}	R	[Standard] Total number of received IP packets, including erred ones [Installation] — (Not installed)	×	
4	ipInHdrErrors {ip 4}	R	[Standard] Number of packets discarded due to IP header errors. Errors : Check sum error, version mismatch, or other format error, TTL value out of limits, IP header option error, etc. [Installation] — (Not installed)	×	
5	ipInAddrErrors {ip 5}	R	[Standard] Number of packets discarded, since the address in IP header is illegal. [Installation] — (Not installed)	×	
6	ipForwDatagrams {ip 6}	R	[Standard] Number of packets transferred to the last address. If not operated as an IP gateway, indicates the number of packets transferred successfully by source routing. [Installation] — (Not installed)	×	
7	ipInUnknownProtos {ip 7}	R	[Standard] Number of discarded packets of received IP packets due to unknown or unsupported protocol. [Installation] — (Not installed)	×	
8	ipInDiscards {ip 8}	R	[Standard] Number of IP packets discarded due to internal trouble such as insufficient buffer space. (Does not include packets discarded while waiting for Re_assembly.) [Installation] — (Not installed)	×	

Table 7.3 ip Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
9	ipInDelivers {ip 9}	R	[Standard] Number of packets transferred to an IP user protocol (host protocol including ICMP) [Installation] — (Not installed)	×	
10	ipOutRequests {ip 10}	R	[Standard] Number of IP packets requested by a local IP user protocol (including ICMP). (ipForwDatagrams is not included.) [Installation] — (Not installed)	×	
11	ipOutDiscards {ip 11}	R	[Standard] Number of IP packets discarded due to insufficient buffer space, etc.; IP packets have no error. (IP packets discarded by ipForwDatagrams according to a send request are included.) [Installation] — (Not installed)	×	
12	ipOutNoRoutes {ip 12}	R	[Standard] Number of packets discarded due to no route to destination. This is the number of packets that could not be transferred because the default gateway was down (including discarded IP packets that intended to be transferred with ipForwDatagrams because the router was unknown). [Installation] — (Not installed)	×	
13	ipReasmTimeout {ip 13}	R	[Standard] Maximum time waiting for all IP packets to be assembled when receiving fragmented IP packets. [Installation] — (Not installed)	×	
14	ipReasmReqds {ip 14}	R	[Standard] Number of received fragmented IP packets to be assembled with an entity. [Installation] — (Not installed)	×	
15	ipReasmOKs {ip 15}	R	[Standard] Number of fragmented IP packets received and assembled successfully [Installation] — (Not installed)	×	
16	ipReasmFails {ip 16}	R	[Standard] Number of fragmented IP packets received but failed to be assembled due to time-out, etc. [Installation] — (Not installed)	×	
17	ipFragOKs {ip 17}	R	[Standard] Number of packets fragmented successfully with this entity [Installation] — (Not installed)	×	
18	ipFragFails {ip 18}	R	[Standard] Number of IP packets discarded without fragmenting because the “No Fragment” flag was set — or some other reason — although they must be fragmented with this entity. [Installation] — (Not installed)	×	

Table 7.3 ip Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
19	ipFragCreates {ip 19}	R	[Standard] Number of fragmented IP packets created by the fragment with this entity. [Installation] — (Not installed)	×	
20	ipAddrTable {ip 20}	Impossible	[Standard] Address information table for each IP address of this entity [Installation] Same as standard. (Refer to the lower hierarchical level.)	○	
20.1	ipAddrEnry {ipAddrTable 1}	Impossible	[Standard] IP address information [Installation] Same as standard. (Refer to the lower hierarchical level.)	○	
20.1.1	ipAdEntAddr {ipAddrEntry 1}	R	[Standard] IP address of this entity [Installation] Same as standard. A system parameter set by users.	○	(index)
20.1.2	ipAdEntIfIndex {ipAddrEntry 2}	R	[Standard] Interface identification number corresponding to this IP address. Same as ifIndex. [Installation] Same as standard. Value is fixed as 1.	○	
20.1.3	ipAdEntNetMask {ipAddrEntry 3}	R	[Standard] Subnetwork mask value related to this IP address. [Installation] Same as standard.	○	
20.1.4	ipAdEntBcastAddr {ipAddrEntry 4}	R	[Standard] LSB value of IP broadcast address when IP broadcast sending. [Installation] Value is fixed as 1.	○	
20.1.5	ipAdEntReasm Max-Size {ipAddrEntry 5}	R	[Standard] Maximum size of IP packets that can be assembled with this entity from fragmented IP packets received by this interface. [Installation] Value is fixed as 65535.	○	
21	ipRouteTable {ip 21}	Impossible	[Standard] IP routing table of this entity [Installation] — (Not installed)	×	
21.1	ipRouteEntry {ipRouteTable 1}	Impossible	[Standard] Route to a specific destination [Installation] — (Not installed)	×	
21.1.1	ipRouteDest {ipRouteEntry 1}	RW	[Standard] Destination IP address of this route table [Installation] — (Not installed)	×	(index)
21.1.2	ipRouteIfIndex {ipRouteEntry 2}	RW	[Standard] Interface identification number to send to the host next to this route. Same as ifIndex. [Installation] — (Not installed)	×	

Table 7.3 ip Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
21.1.3	ipRouteMetric1 {ipRouteEntry 3}	RW	[Standard] Primary routing metric of this route [Installation] — (Not installed)	×	
21.1.4	ipRouteMetric2 {ipRouteEntry 4}	RW	[Standard] Alternate routing metric [Installation] — (Not installed)	×	
21.1.5	ipRouteMetric3 {ipRouteEntry 5}	RW	[Standard] Alternate routing metric [Installation] — (Not installed)	×	
21.1.6	ipRouteMetric4 {ipRouteEntry 6}	RW	[Standard] Alternate routing metric [Installation] — (Not installed)	×	
21.1.7	ipRouteNextHop {ipRouteEntry 7}	RW	[Standard] Next hop IP address of this route [Installation] — (Not installed)	×	
21.1.8	ipRouteType {ipRouteEntry 8}	RW	[Standard] Routing type other = 1, invalid (invalid route) = 2, direct (direct connection) = 3, indirect (indirect connection) = 4 [Installation] — (Not installed)	×	
21.1.9	ipRouteProto {ipRouteEntry 9}	R	[Standard] Learned routing mechanism other = 1, local = 2, netmgmt = 3, icmp = 4, epg = 5, ggp = 6, hello = 7, rip = 8, is-is = 9, es-is = 10, ciscoIgrp = 11, bbnSpfIgp = 12, ospf = 13, bgp = 14 [Installation] — (Not installed)	×	
21.1.10	ipRouteAge {ipRouteEntry 10}	RW	[Standard] Elapsed time (in seconds) since the route was recognized last as the normal one. [Installation] — (Not installed)	×	
21.1.11	ipRouteMask {ipRouteEntry 11}	RW	[Standard] Subnet mask value [Installation] — (Not installed)	×	
21.1.12	ipRouteMetric5 {ipRouteEntry 12}	RW	[Standard] Alternate routing metric [Installation] — (Not installed)	×	
21.1.13	ipRouteInfo {ipRouteEntry 13}	R	[Standard] Defined number of the MIB for the routing protocol used for this route. [Installation] — (Not installed)	×	
22	ipNetToMediaTable {ip 22}	Impossible	[Standard] IP address conversion table used to convert IP addresses to physical addresses. [Installation] — (Not installed)	×	

Table 7.3 ip Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
22.1	ipNetToMediaEntry {ipNetToMedia-Table 1}	Impossible	[Standard] Entry including an IP address corresponding to a physical address. [Installation] — (Not installed)	×	
22.1.1	ipNetToMediaIf-Index {ipNetToMedia-Entry 1}	RW	[Standard] Interface identification number of this entry. The ifIndex value is used. [Installation] — (Not installed)	×	(index)
22.1.2	ipNetToMedia-PhysAddress {ipNetToMedia-Entry 2}	RW	[Standard] Physical address depending on medium [Installation] — (Not installed)	×	
22.1.3	ipNetToMedia-NetAddress {ipNetToMedia-Entry 3}	RW	[Standard] P address corresponding to the physical address of this entry. [Installation] — (Not installed)	×	(index)
22.1.4	ipNetToMediaType {ipNetToMedia-Entry 4}	RW	[Standard] Address conversion method other = 1, invalid = 2, dynamic (conversion) = 3, static (conversion) = 4 [Installation] — (Not installed)	×	
23	ipRoutingDiscards {ip 23}	R	[Standard] Total of valid routing information items discarded due to insufficient memory space, etc. [Installation] — (Not installed)	×	

7.1.5 icmp Group

icmp OBJECT IDENTIFIER :: = {mib-2 5}

This group is not supported.

7.1.6 tcp Group

tcp OBJECT IDENTIFIER :: = {mib-2 6}

This group is not supported.

7.1.7 udp Group

udp OBJECT IDENTIFIER :: {mib-2 7}

This group is not supported.

7.1.8 egp Group

egp OBJECT IDENTIFIER :: = {mib-2 8}

This group is not supported.

7.1.9 snmp Group

snmpOBJECT IDENTIFIER :: = {mib-2 11}

Table 7.4 snmp Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	snmpInPkts {snmp 1}	R	[Standard] Total of SNMP messages received from a transport service [Installation] Same as standard.	○	
2	snmpOutPkts {snmp 2}	R	[Standard] Total of SNMP messages requested to be transferred to the transport layer. [Installation] Same as standard.	○	
3	snmpInBad-Versions {snmp 3}	R	[Standard] Total of received messages of an unsupported version. [Installation] Same as standard.	○	
4	snmpInBad-CommunityNames {snmp 4}	R	[Standard] Total of received SNMP messages of an unused community. [Installation] Same as standard.	○	
5	snmpInBad-CommunityUses {snmp 5}	R	[Standard] Total of received messages indicating operation disabled for the community. [Installation] Same as standard.	○	
6	snmpInASNParse-Errs {snmp 6}	R	[Standard] Total of received messages of ASN.1 error [Installation] Same as standard.	○	
8	snmpInTooBigs {snmp 8}	R	[Standard] Total of received PDUs of tooBig error status. [Installation] Same as standard.	○	
9	snmpInNoSuchNames {snmp 9}	R	[Standard] Total of received PDUs of noSuchName error status. [Installation] Same as standard.	○	
10	snmpInBadValues {snmp 10}	R	[Standard] Total of received PDUs of badValue error status. [Installation] Same as standard.	○	
11	snmpInReadOnlys {snmp 11}	R	[Standard] Total of received PDUs with readOnly error status. [Installation] Same as standard.	○	

Table 7.4 snmp Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
12	snmpInGenErrs {snmp 12}	R	[Standard] Total of received PDUs with genErr error status. [Installation] Same as standard.	○	
13	snmpInTotalReq-Vars {snmp 13}	R	[Standard] Total of MIB objects for which MIB was gathered successfully. [Installation] Same as standard.	○	
14	snmpInTotalSet-Vars {snmp 14}	R	[Standard] Total of MIB objects for which MIB was set successfully. [Installation] Same as standard.	○	
15	snmpInGetRequests {snmp 15}	R	[Standard] Total of received GetRequest PDUs. [Installation] Same as standard.	○	
16	snmpInGetNexts {snmp 16}	R	[Standard] Total of received GetNext Request PDUs. [Installation] Same as standard.	○	
17	snmpInSetRequests {snmp 17}	R	[Standard] Total of received SetRequest PDUs. [Installation] Same as standard.	○	
18	snmpInGet-Responses {snmp 18}	R	[Standard] Total of received GetResponse PDUs. [Installation] Same as standard.	○	
19	snmpInTraps {snmp 19}	R	[Standard] Total of received TrapPDUs. [Installation] Same as standard.	○	
20	snmpOutTooBigs {snmp 20}	R	[Standard] Total of transferred PDUs of tooBig error status. [Installation] Same as standard.	○	
21	snmpOutNoSuch-Names {snmp 21}	R	[Standard] Total of transferred PDUs of noSuchName error status. [Installation] Same as standard.	○	
22	snmpOutBadValues {snmp 22}	R	[Standard] Total of transferred PDUs of badValue error status. [Installation] Same as standard.	○	
24	snmpOutGenErrs {snmp 24}	R	[Standard] Total of received PDUs of genErr error status. [Installation] Same as standard.	○	
25	snmpOutGet-Requests {snmp 25}	R	[Standard] Total of transferred GetRequest PDUs. [Installation] Same as standard.	○	

Table 7.4 snmp Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
26	snmpOutGetNexts {snmp 26}	R	[Standard] Total of transferred GetNextRequest PDUs. [Installation] Same as standard.	○	
27	snmpOutSet-Requests {snmp 27}	R	[Standard] Total of transferred SetRequest PDUs. [Installation] Same as standard.	○	
28	snmpOutGet-Responses {snmp 28}	R	[Standard] Total of transferred GetResponse PDUs. [Installation] Same as standard.	○	
29	snmpOutTraps {snmp 29}	R	[Standard] Total of transferred Trap PDUs. [Installation] Same as standard.	○	
30	snmpEnable-AuthenTraps {snmp 30}	R	[Standard] This indicates whether an authentication-failure trap can be issued. enabled = 1, disabled = 2 [Installation] Fixed value 1 (enabled)	○	Should be Read-Only in array unit.

7.2 Extended MIBs

```
Enterprises          OBJECT IDENTIFIER :: = {iso(1) org(3) dod(6) internet(1) 4}
Hitachi              OBJECT IDENTIFIER :: = {enterprises 116}
systemExMib          OBJECT IDENTIFIER :: = {hitachi 5}
storageExMib         OBJECT IDENTIFIER :: = {systemExMib 11}
dfraidExMib          OBJECT IDENTIFIER :: = {storageExMib 1}
dfraidLanExMib       OBJECT IDENTIFIER :: = {dfraidExMib 2}
```

7.2.1 dfSystemParameter Group

```
dfSystemParameter    OBJECT IDENTIFIER :: {dfraidLanExMib 1}
```

Table 7.5 dfSystemParameter Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	dfSystemProductName {dfSystemParameter 1}	R	[Content] Product name [Installation] (DF600) : HITACHI DF600F (Same as inquiry information)	○	
2	dfSystemMicro-Revision {dfSystemParameter 2}	R	[Content] Microprogram revision number [Installation] Same as above	○	
3	dfSystemSerialNumber {dfSystemParameter 2}	R	[Content] Disk array serial number [Installation] The lower four digits of the manufacturing serial number	○	

7.2.2 dfWarningCondition Group

dfWarningCondition OBJECT IDENTIFIER :: = {dfraidLanExMib 2}

Table 7.6 dfWarningCondition Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	dfRegressionStatus {dfWarningCondition 1}	R	[Content] Warning error information [Installation] Same as above. When normal, this is assigned to 0. (See Note 1.)	○	
2	dfPreventiveMainte-nanceInformation {dfWarningCondition 2}	R	[Content] Drive preventive maintenance information [Installation] Same as above. This is assigned to 0 when normal, and to 1 when a drive preventive maintenance warning occurs.	○	
3	dfWarningReserve1 {dfWarningCondition 3}	R	[Content] Reserved area [Installation] Not used. Value is fixed as 0.	○	
4	dfWarningReserve2 {dfWarningCondition 4}	R	[Content] Reserved area [Installation] Not used. Value is fixed as 0.	○	

Note 1: The format is the same as that of the 4 bytes integer-type object.

Bit Byte	7	6	5	4	3	2	1	0
0	0	0	0	0	0	0	0	Cache
1	0	0	0	Fan	BK	0	DC PS	Battery
2	0	0	NAS UPS	NAS Path	NAS Server	Path	Loop	UPS
3	CTL	Warning	0	0	ENC	D-Drive	S-Drive	Drive

Figure 7.1 dfRegressionStatus Format

Note: Subject bits should be “on” if each part is in the regressed state. This value may be fixed as “0” depending on the array unit type and the microprogram revision.

Table 7.7 shows this object value for each failure status.

Table 7.7 dfRegressionStatus Value for Each Failure

No.	Bit position		Object value (decimal)	Failed component
	Byte	Bit		
1			0	Array unit normal status
2	3	0	1	Drive blockade
3	3	1	2	Drive (spare drive) blockade
4	3	2	4	Drive (data drive) blockade
5	3	3	8	ENC alarm
6	3	6	64	Warned array unit
7	3	7	128	Mate controller blockade
8	2	0	256	UPS alarm
9	2	1	512	Loop alarm
10	2	2	1024	Path blockade
11	2	3	2048	NAS Server failure
12	2	4	1096	NAS Path failure
13	2	5	8192	NAS UPS failure
14	1	0	65536	Battery alarm
15	1	1	131072	DC power supply failure
16	1	3	524288	Battery charging circuit alarm
17	1	4	1048576	Fan alarm
18	0	0	16777216	Cache partial blockade

Note: If the “Drive” bit is On, the “D-Drive” or “S-Drive” bit is set to On, and this distinguishes between the data drive and the spare drive type.

If there are two or more failed components, the object value is that which adds up each object value.

> ***Example:*** When failure occurs in the battery and the fan
> Object value: 1114112 (65536 + 1048576)

When a value of an object is converted into a binary number, it corresponds to the format shown in Figure 7.1.

[dfRegressionStatus]

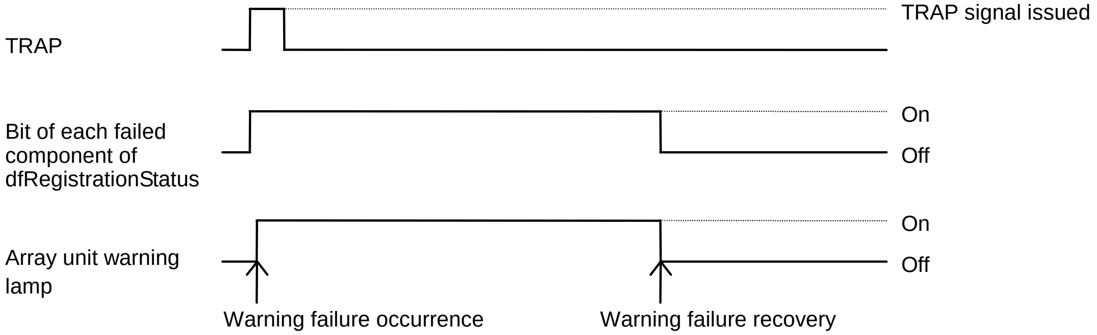


Figure 7.2 Relationship between Traps and dfWarningCondition Groups

Each of the TRAP signals (specific trap code 2 to 6) is issued each time a warning failure in related component occurs (Figure 7.2).

When a warning failure occurs, the bit of the related component of “dfRegistrationStatus” is turned on. The bit is turned off when warning failure is recovered.

7.2.3 dfCommandExecutionCondition Group

dfCommandExecutionCondition OBJECT IDENTIFIER :: = {dfraidLanExMib 3}

Table 7.8 dfCommandExecutionCondition Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	dfCommandTable {dfCommandExecutionCondition 1}	Impossible	[Content] Command execution condition table [Installation] Same as above (Refer to the lower hierarchical level)	○	
1.1	dfCommandEntry {dfCommandTable 1}	Impossible	[Content] Command execution condition entry [Installation] Same as above (Refer to the lower hierarchical level)	○	
1.1.1	dfLun {dfCommandEntry 1}	R	[Content] Logical unit number [Installation] Same as above (0 to 511)	○	(index)
1.1.2	dfReadCommandNumber {dfCommandEntry 2}	R	[Content] Number of read command receptions [Installation] Same as above	○	
1.1.3	dfReadHitNumber {dfCommandEntry 3}	R	[Content] Number of cache read hits [Installation] Number of read commands whose host request range completely hits that of the cache	○	
1.1.4	dfReadHitRate {dfCommandEntry 4}	R	[Content] Cache read hit rate (%) [Installation] (Number of cache read hits / Number of read command receptions) × 100	○	
1.1.5	dfWriteCommandNumber {dfCommandEntry 5}	R	[Content] Number of write command receptions [Installation] Same as above	○	
1.1.6	dfWriteHitNumber {dfCommandEntry 6}	R	[Content] Number of cache write hits [Installation] Number of write commands that were not restricted to write data (not made to wait for writing data) in cache by the dirty threshold value manager	○	
1.1.7	dfWriteHitRate {dfCommandEntry 7}	R	[Content] Cache write hit rate (%) [Installation] Number of cache write hits / Number of write command receptions) × 100	○	

Note 1: The information of this group is updated every 10 seconds. The value accumulated in the previous ten seconds is set (Figure 7.3).

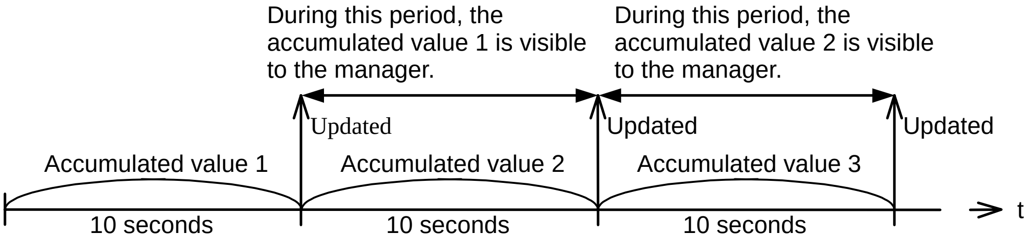

During this period, the accumulated value 1 is visible to the manager.
During this period, the accumulated value 2 is visible to the manager.
Updated
Updated
Updated
Accumulated value 1
Accumulated value 2
Accumulated value 3
10 seconds
10 seconds
10 seconds
t

Figure 7.3 Accumulated Values Over Time

Note 2: The dfCommandExecutionCondition group is updated at an interval of 10 seconds and is set to a value accumulated for individual 10 seconds. However, this interval time of 10 seconds may vary within an error span, depending on the command execution condition. In this case, the group is set to a value converted to every 10 seconds from an accumulated value.

> ***Example:*** If an elapsed time : 11 seconds, and the accumulated number of read command received for that time : 110, then the dfReadCommandNumber is set to 100.

Note 3: The number of hits (dfReadHitNumber, dfWriteHitNumber) may exceed the number of commands received (dfReadCommandNumber, dfWriteCommandNumber), depending on the timing of updating the dfCommandExecutionConditiongroup. The hit rate (dfReadHitRate, dfWriteHitRate) at this time is set to 100%.

Note 4: The dfCommandExecutionCondition group indicates the information of the logical units that can be accessed from the host. If the LUN Concatenation Feature is being used, this group indicates information of the unified LUs.

7.2.4 dfCacheLoadCondition Group

dfCommandExecutionCondition OBJECT IDENTIFIER :: = {dfraidLanExMib 3}

Table 7.9 dfCacheLoadCondition Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	dfWriteDataRate {dfCacheLoadCondition 1}	R	[Content] Dirty segment rate(%) [Installation] Same as above	○	

Note 1: The information of this group is updated every 10 seconds.

7.2.5 dfLUNS Group

dfCommandExecutionCondition OBJECT IDENTIFIER :: = {dfraidLanExMib 5}

Table 7.10 dfLUNS Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	dfLUNSSwitch {dfLUNS 1}	Impossible	[Content] Command operation status table [Installation] Ditto. (See the lower layer.)	○	
1.1	dfLUNSSwitchEntry {dfLUNSSwitch 1}	Impossible	[Content] Command operation status entry [Installation] Ditto. (See the lower layer.)	○	
1.1.1	dfSwitchSerialNumber {dfLUNSSwitch Entry 1}	R	[Content] Disk array serial number [Installation] The lower four digits of the manufacturing serial number.	○	(index)
1.1.2	dfSwitchPortID {dfLUNSSwitch Entry 2}	R	[Content] Port number [Installation] Ditto.	○	(index)
1.1.3	dfSwitchOnOff {dfLUNSSwitch Entry 3}	R	[Content] Function switch [Installation] Ditto.	○	0: off (Invalid) 1: on (Valid)
1.1.4	dfSwitchControlStatus {dfLUNSSwitch Entry 4}	R	[Content] Control flag [Installation] Fixed at 1.	○	1: Regular return value 2: Request for setting

Table 7.10 dfLUNS Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
2	dfLUNSWWN {dfLUNS 2}	Impossible	[Content] WWN table [Installation] Ditto. (See the lower layer.)	○	
2.1	dfLUNSWWNentry {dfLUNSWWN 1}	Impossible	[Content] Write command receipt count [Installation] Ditto.	○	
2.1.1	dfWWNSerialNumber {dfLUNSWWNEntry 1}	R	[Content] Disk array serial number [Installation] The lower four digits of the manufacturing serial number.	○	(index)
2.1.2	dfWWNPortID {dfLUNSWWNEntry 2}	R	[Content] Port number [Installation] Ditto. (See Note 1.)	○	(index)
2.1.3	dfWWNControlIndex {dfLUNSWWNEntry 3}	R	[Content] Control index [Installation] Ditto. (1 to 128) (See Note 2.)	○	(index)
2.1.4	dfWWNWWN {dfLUNSWWNEntry 4}	R	[Content] WWN [Installation] 8 bytes bit string (See Note 3.)	○	
2.1.5	dfSWWNID {dfLUNSWWNEntry 5}	R	[Content] WWN number [Installation] Ditto. (0 to 31) (See Note 4.)	○	
2.1.6	dfWWNNickname {dfLUNSWWNEntry 6}	R	[Content] Nickname [Installation] Ditto. (See Note 5.)	×	No Data
2.1.7	dfWWNUseNickname {dfLUNSWWNEntry 7}	R	[Content] Use/no use of nickname [Installation] Ditto. (Fixed at 0.)	○	No use of nickname
2.1.8	dfSwitchControlStatus {dfLUNSWWNEntry 8}	R	[Content] Control flag [Installation] Fixed at 1.	○	1: Regular return value 2: Request for setting
3	dfLUNSWWNGroup {dfLUNS 3}	Impossible	[Content] WWN group table [Installation] —	×	

Table 7.10 dfLUNS Group (Continued)

No.	Object identifier	Access	Specifications for installation	Support	Remarks
4	dfLUNSLUN {dfLUNS 4}	Impossible	[Content] LUN table [Installation] Ditto. (See the lower layer.)	○	
4.1	dfLUNSLUNentry {dfLUNSWWN 1}	Impossible	[Content] Write command receipt count [Installation] Ditto.	○	
4.1.1	dfLUNSerialNumber {dfLUNSWWNEntry 1}	R	[Content] Disk array serial number [Installation] The lower four digits of the manufacturing serial number.	○	(index)
4.1.2	dfLUNPortID {dfLUNSWWNEntry 2}	R	[Content] Port number [Installation] Ditto. (See Note 1.)	○	(index)
4.1.3	dfLUNLUN {dfLUNSWWNEntry 3}	R	[Content] LU number [Installation] Ditto. (0 to 511)	○	(index)
4.1.4	dfLUNWWNSecurity {dfLUNSWWNEntry 4}	R	[Content] WWN access permission [Installation] 16 bytes bit string (See Note 6.)	○	
4.1.5	dfLUNWWNGroupSecurity {dfLUNSWWNEntry 5}	R	[Content] WWN group access permission [Installation] Ditto. (See Note 7.)	×	No Data
4.1.6	dfLUNControlStatus {dfLUNSWWNEntry 6}	R	[Content] Control flag [Installation] Ditto. (Fixed at 1.)	○	1: Regular return value 2: Request for setting
5	dfLUNSLUNGroup {dfLUNS 5}	Impossible	[Content] LUN group table [Installation] Ditto.	×	

Table 7.11 Port Table Numbers

Port No.	Controller No.	Fibre
0	0	0A
1		0B
2		Not applicable
3		Not applicable
4	1	1A
5		1B
6		Not applicable
7		Not applicable

7.2.5.1 Definitions and Functions

- Control index: Field entry number (consecutive number).
- WWN: Sets the port identifier (WWN) of the host registered in the corresponding port. For ports other than Fibre-oriented ones and unregistered entry, the value is 0.
- WWN number: Sets the registration number (0 to 31) of the registered WWN. For unregistered entry, the value is 0. (Valid only for WWN registered entry)
- Nickname: Not supported. (Length 0)
- WWN access permission: Sets the bit corresponding to the WWN that has permission to access the corresponding LUN.

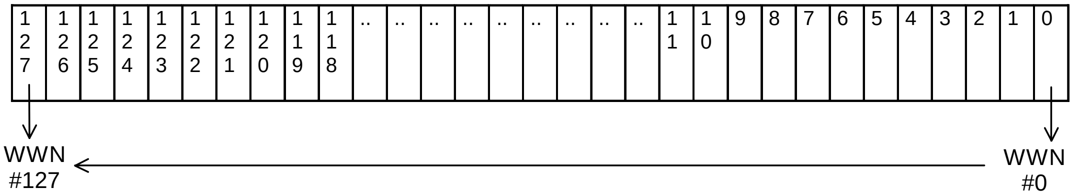


Figure 7.4 WWN group access permission (Not supported. (Length 0))

7.2.6 dfPort Group

dfPort OBJECT IDENTIFIER :: = {dfraidLanExMib 6}

Table 7.12 dfPort Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	dfPortinf {dfPort 1}	Impossible	[Content] Port information table [Installation] Ditto. (See the lower layer.)	○	
1.1	dfPortinf Entry {dfPortinf 1}	Impossible	[Content] Port information entry [Installation] Ditto. (See the lower layer.)	○	
1.1.1	dfLUNSerialNumber {dfLUNSWWNEntry 1}	R	[Content] Disk array serial number [Installation] The lower four digits of the manufacturing serial number.	○	(index)
1.1.2	dfPortID {dfPortinf Entry 2}	R	[Content] Port number [Installation] Ditto. (0 to 7) (See Note 1.)	○	(index)
1.1.3	dfPortKind {dfPortinf Entry 3}	R	[Content] Port type [Installation] Ditto. (See Note 2.)	○	
1.1.4	dfPortHostMode {dfPortinf Entry 4}	R	[Content] Host mode [Installation] Ditto.	○	No Data
1.1.5	dfPortFibreAddress {dfPortinf Entry 5}	R	[Content] N_Port_ID of the port [Installation] Ditto. (See Note 3.)	○	
1.1.6	dfPortFibreTopology {dfPortinf Entry 6}	R	[Content] Topology information [Installation] Ditto. (1 to 5) (See Note 4.)	○	
1.1.7	dfPortControlStatus {dfPortinf Entry 7}	R	[Content] Control flag [Installation] Ditto. (Fixed at 1.)	○	1: Regular return value 2: Request for setting
1.1.8	dfPortDisplayName {dfPortinf Entry 8}	R	[Content] Port name [Installation] Ditto. (0A to 0B, 1A to 1B) (See Note 5.)	○	
1.1.9	dfPortWWN {dfPortinf Entry 9}	R	[Content] WWN of the port [Installation] Ditto. (8 bytes OCTET String) (See Note 6.)	○	

Table 7.13 Port numbers

Port No.	Controller No.	Fibre
0	0	0A
1		0B
2		Not applicable
3		Not applicable
4	1	1A
5		1B
6		Not applicable
7		Not applicable

Notes: On port types:

- Sets ”Fibre”.
- For ports other than those that are not applicable, “None” is set.
- The item of the ports of a blocked controller is “None.”
- Fibre address host mode
- For Fibre-oriented ports, address translation is performed and then setting is performed. When the address is illegal, the value is 0.
- For ports other than Fibre-oriented ones, the value is 0.

Table 7.14 Port Addresses and Associated Values

Value	Address	Value	Address	Value	Address	Value	Address
1	EF	33	B2	65	72	97	3A
2	E8	34	B1	66	71	98	39
3	E4	35	AE	67	6E	99	36
4	E2	36	AD	68	6D	100	35
5	E1	37	AC	69	6C	101	34
6	E0	38	AB	70	6B	102	33
7	DC	39	AA	71	6A	103	32
8	DA	40	A9	72	69	104	31
9	D9	41	A7	73	67	105	2E
10	D6	42	A6	74	66	106	2D
11	D5	43	A5	75	65	107	2C
12	D4	44	A3	76	63	108	2B
13	D3	45	9F	77	5C	109	2A
14	D2	46	9E	78	5A	110	29
15	D1	47	9D	79	59	111	27
16	CE	48	9B	80	56	112	26
17	CD	49	98	81	55	113	25
18	CC	50	97	82	54	114	23
19	CB	51	90	83	53	115	1F
20	CA	52	8F	84	52	116	1E
21	C9	53	88	85	51	117	1D
22	C7	54	84	86	4E	118	1B
23	C6	55	82	87	4D	119	18
24	C5	56	81	88	4C	120	17
25	C3	57	80	89	4B	121	10
26	BC	58	7C	90	4A	122	0F
27	BA	59	7A	91	49	123	08
28	B9	60	79	92	47	124	04
29	B6	61	76	93	46	125	02
30	B5	62	75	94	45	126	01
31	B4	63	74	95	43	-	-
32	B3	64	73	96	3C	-	-

Table 7.15 Topology information for Fibre-oriented Ports

Value	Meaning
1	Fabric (on) & FCAL
2	Fabric (off) & FCAL
3	Fabric (on) & Point To Point
4	Fabric (off) & Point To Point

Table 7.16 Topology information for ports other than Fibre-oriented

Value	Meaning
5	Not Fibre

Table 7.17 Port display names

Port No.	Controller No.	Fibre
0	0	“0A“
1		“0B“
2		“None“
3		“None“
4	1	“1A“
5		“1B“
6		“None“
7		“None“

Note: For port WWN:

- For Fibre-oriented ports, the port identifier (WWN) is set.
- For non-Fibre-oriented ports, the value is 0.

7.2.7 dfCommandExecutionInternalCondition Group

dfCommandExecutionInternalCondition OBJECT IDENTIFIER :: = {dfraidLanExMib 7}

Table 7.18 dfCommandExecutionInternalCondition Group

No.	Object identifier	Access	Specifications for installation	Support	Remarks
1	dfCommandInternalTable {dfCommandExecutionCondition 1}	Impossible	[Content] Command execution condition table [Installation] Same as above (Refer to the lower hierarchical level)	○	
1.1	dfCommandInternalEntry {dfCommandTable 1}	Impossible	[Content] Command execution condition entry [Installation] Same as above (Refer to the lower hierarchical level)	○	
1.1.1	dfInternalLun {dfCommandEntry 1}	R	[Content] Logical unit number [Installation] Same as above (0 to 511)	○	(Index)
1.1.2	dInternalfReadCommand Number {dfCommandEntry 2}	R	[Content] Number of read command receptions [Installation] Same as above	○	
1.1.3	dfInternalReadHitNumber {dfCommandEntry 3}	R	[Content] Number of cache read hits [Installation] Number of read commands whose host request range completely hits that of the cache	○	
1.1.4	dfInternalReadHitRate {dfCommandEntry 4}	R	[Content] Cache read hit rate (%) [Installation] (Number of cache read hits / Number of read command receptions) × 100	○	
1.1.5	dfInternalWriteCommand Number {dfCommandEntry 5}	R	[Content] Number of write command receptions [Installation] Same as above	○	
1.1.6	dfInternalWriteHitNumber {dfCommandEntry 6}	R	[Content] Number of cache write hits [Installation] Number of write commands that were not restricted to write data (not made to wait for writing data) in cache by the dirty threshold value manager	○	
1.1.7	dfInternalWriteHitRate {dfCommandEntry 7}	R	[Content] Cache write hit rate (%) [Installation] Number of cache write hits / Number of write command receptions) × 100	○	

Note 1: The dfCommandExcutionInternalCondition group indicates the information of the internal logical units of the subsystem. If the LUN Concatenation Feature is being used, this group not indicates the information for the unified LU, but indicates the information of the internal logical units in the subsystem. The information of this group is updated every 10 seconds.

Note 2: For other notes, see Notes 1-3 at the end of Table 7.8.

Chapter 8 Relevant Specifications

The relevant specifications are shown below:

- RFC1155 (Structure and Identification of Management Information for TCP/IP-based Internets)
- RFC1157 (A Simple Network Management Protocol)
- RFC1212 (Concise MIB Definitions)
- RFC1213 (Management Information Base for Network Management of TCP/IP-based internets: MIB-II)
- RFC1215 (A Convention for Defining Traps for use with the SNMP)

Appendix A Operations Using CLI

This section describes the following operation procedure for SNMP Agent Support Function using the CLI of the Disk Array management program. The following sections are included:

- Installing
- Uninstalling
- Enabling or Disabling
- Registering or Referencing SNMP Environment Information

A.1 Installing

The SNMP Agent Support Function feature is usually unselectable (locked); to make it available, you must install the SNMP Agent Support Function feature and make its functions selectable (unlocked). **To install this function, the key code provided with the optional feature is required.**

Follow the instructions below to install the SNMP Agent Support Function feature. SNMP Agent Support Function is installed and uninstalled using Disk Array management program.

Note: Before installing and uninstalling, make sure that the array unit is in normal operating condition. If a failure such as a controller blockade has occurred, installation and uninstallation operations cannot be performed.

The following instructions describe how to install SNMP Agent Support Function, using the CLI version of Disk Array management program:

1. From the command prompt, register the subsystem (array unit) in which you will install the SNMP Agent Support Function feature. Connect to the subsystem.
2. Unlock the optional features by using the following:

Example 1:

```
% auopt -unit df600 -lock off -keycode Key code
Password:
Option was opened.
Restart the subsystem to apply the setting.
The subsystem stops accepting the access from the host while restarting.
Also, if you are logging in, the login status will be cancelled when restarting
begins.
Do you want to restart the subsystem now? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required nnnsec.
The subsystem restarted successfully.
%
```

Example 2:

```
% auopt -unit df600 -refer
Password:
Option name   Status
SNMP-AGENT    Enable
%
```

Note: To validate the unlocking of this optional feature, restart the array unit. The previous setting stays valid until restarting. The array unit cannot access the host until the restart is completed. Therefore, be certain the host has stopped accessing data before beginning the restart process.

Note: It may take up to six minutes for an array unit to respond, depending on the configuration of the array unit.

A.2 Uninstallation

The following instructions describe how to uninstall SNMP Agent Support Function, using the CLI version of Disk Array management program:

1. From the command prompt, register the subsystem (array unit) in which you will uninstall the SNMP Agent Support Function feature. Connect to the subsystem.
2. Lock the optional features by using the following:

Example 1:

```
% auopt -unit df600 -lock on -keycode Key code
Password:
Option was closed.
Restart the subsystem to apply the setting.
The subsystem stops accepting the access from the host while restarting.
Also, if you are logging in, the login status will be cancelled when restarting
begins.
Do you want to restart the subsystem now? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required nnnsec.
The subsystem restarted successfully.
%
```

Example 2:

```
% auopt -unit df600 -refer
Password:
DMEC002015:No information displayed.
%
```

Note: To validate the locking of this optional feature, restart the array unit. The previous setting stays valid until restarting. The array unit cannot access the host until the restart is completed. Therefore, be certain the host has stopped accessing data before beginning the restart process.

Note: It may take up to six minutes for an array unit to respond, depending on the configuration of the array unit.

A.3 Enabling or Disabling

SNMP Agent Support Function can be enabled or disabled without uninstalling this function. The following instructions describe how to enable or disable SNMP Agent Support Function without uninstalling this function, using the CLI version of Disk Array management program.

1. From the command prompt, register the subsystem (array unit) in which you will change the status of the SNMP Agent Support Function feature. Connect to the subsystem.
2. Execute the auopt command to change the status (enable or disable) of the SNMP Agent Support Function feature.

   The following is an example of how to change the status from enable to disable. To change the status from disable to enable, enter enable after the –st option.

Example 1:

```
% auopt -unit df600 -option SNMP-AGENT -st disable
Password:
The option has been set successfully.
Restart the subsystem to apply the setting.
The subsystem stops accepting the access from the host while restarting.
Also, if you are logging in, the login status will be cancelled when restarting
begins.
Do you want to restart the subsystem now? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required nnnsec.
The subsystem restarted successfully.
%
```

Example 2:

```
% auopt -unit df600 -refer
Password:
Option name   Status
SNMP-AGENT    Disable
%
```

Note: This setting is not active until the system is restarted. The subsystem cannot access the host until the restart is completed. Therefore, be certain the host has stopped accessing data before beginning the restart process.

Note: It may take up to six minutes for an array unit to respond, depending on the configuration of the array unit.

A.4 Registering or Referencing SNMP Environment Information

A.4.1 Registering

1. From the command prompt, register the subsystem (array unit) in which you want to set SNMP Agent Support Function. Connect to the subsystem.
2. Execute the ausnmp command to specify the subsystem.

Example:

```
%  ausnmp -unit df600 -set -config config.txt -name name.txt
Password:
The SNMP environment information has been set successfully.
Restart the subsystem to apply the setting.
The subsystem stops accepting the access from the host while restarting.
Also, if you are logging in, the login status will be cancelled when restarting
begins.
Do you want to restart the subsystem now? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required nnnsec.
The subsystem restarted successfully.
%
```

A.4.2 Referencing

1. From the command prompt, register the subsystem (array unit) in which you want to set SNMP Agent Support Function. Connect to the subsystem.
2. Execute the ausnmp command to specify the subsystem.

Example:

```
% ausnmp -unit df600 -get -config config.txt -name name.txt
%
```