HITACHI
DATA SYSTEMS

Hitachi TagmaStore®
Adaptable Modular Storage
and Workgroup Modular Storage

SNMP Agent Support Function User's Guide

MK-95DF705-08

Trademarks

Notice of Export Controls

Document Revision Level

Revision	Date	Description
MK-95DF705-00	June 2005	Initial Release
MK-95DF705-01	August 2005	Revision 1, supersedes and replaces MK-95DF705-00
MK-95DF705-02	October 2005	Revision 2, supersedes and replaces MK-95DF705-01
MK-95DF705-03	December 2005	Revision 3, supersedes and replaces MK-95DF705-02
MK-95DF705-04	February 2006	Revision 4, supersedes and replaces MK-95DF705-03
MK-95DF705-05	May 2006	Revision 5, supersedes and replaces MK-95DF705-04
MK-95DF705-06	June 2006	Revision 6, supersedes and replaces MK-95DF705-05
MK-95DF705-07	January 2007	Revision 7, supersedes and replaces MK-95DF705-06
MK-95DF705-08	May 2007	Revision 8, supersedes and replaces MK-95DF705-07

Source Documents for this Revision

- *SNMP Agent Support Function User's Guide (DF700)*, (K6603142-0) Pre-Final (Hitachi Ltd. source document)
- *SNMP Agent Support Function User's Guide (DF700)*, (K6603142-0) (Final) (Hitachi Ltd. source document)
- *Hitachi Freedom Storage™ Thunder 9500™ V Series SNMP Agent Support Function User's Guide* (MK-92DF614)
- RSD-95DF705-P1, RSD-95DF705-P1, RSD-95DF705-01 (RSD review of this document)
- *SNMP Agent Support Function User's Guide (DF700)*, (K6603142-0) Pre-Final (Hitachi Ltd. source document)
- RSD-95df705-02, RSD-95df705-03a, RSD-95df705-04a (Pre Final), RSD-95df705-04a (Final), RSD-95DF705-05a, RSD-95DF705, RSD-95DF706A

Changes for this Revision

- The graphical user interface was updated to reflect changes in the code. New user interface screen shots are included in Chapter 4
- Added information about TrueCopy Extended Distance (TCE) to entire document
- Removed the error code information in section 2.2 and placed it in the new *Hitachi TagmaStore® AMS/WMS Storage Navigator Modular DF Error Codes* (MK-96DF788) document
- Updated information about supported traps and trap issuing opportunities (section 6.4)

Preface

This document describes and provides instructions for installing and using the SNMP agent support function for the Hitachi TagmaStore AMS subsystem. Before using the TagmaStore AMS SNMP Agent Support Function, please read the operating procedures and notices included in this document.

This document assumes the following:

- The user has a background in data processing and understands direct-access storage device (DASD) subsystems and their basic functions, and
- The user is familiar with the Hitachi TagmaStore AMS subsystem.
- The user is familiar with the *Hitachi TagmaStore Adaptable Modular Storage, Storage Navigator Modular for Web User's Guide* (MK-95DF719).

Note: The use of SNMP Agent and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Software Version

This document revision applies to TagmaStore Adaptable Modular Storage and Workgroup Modular Storage versions 7.1 and higher.

Convention for Storage Capacity Values

Storage capacity values for logical devices (LDEVs) are calculated based on the following values:

1 KB (kilobyte) = 1,024 bytes
1 MB (megabyte) = $1,024^2$ bytes
1 GB (gigabyte) = $1,024^3$ bytes
1 TB (terabyte) = $1,024^4$ bytes

Referenced Documents

- *Hitachi TagmaStore Adaptable Modular Storage, Storage Navigator Modular for Web User's Guide* (MK-95DF719)
- *Storage Navigator Modular (for GUI) User's Guide* (MK-95DF711)
- *Hitachi TagmaStore Adaptable Modular Storage, Storage Navigator Modular for Web User's Guide* (MK-95DF719)
- *Hitachi TagmaStore Adaptable Modular Storage 500 User's Guide* (MK-95DF714)
- *Structure and Identification of Management Information for TCP/IP-based Internets,* RFC1155 *A Simple Network Management Protocol*, RFC1157
- *Concise MIB Definitions*, RFC1212
- *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*, RFC1213
- *A Convention for Defining Traps for use with the SNMP*, RFC1215
- *Hitachi TagmaStore Adaptable Modular Storage and Workgroup Modular Storage, Storage Navigator Modular DF Error Codes,* MK-96DF788

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
  Technical Writing, M/S 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

Contents

Chapter 1 Overview of the SNMP Agent Support Function 1

1.1 Notes on Using SNMP 2
1.2 System Configuration - Network Connecting Functions 5
1.3 System Configuration - LAN Connections 5
1.4 SNMP Functions 6
1.4.1 Trap Reporting 6
1.4.2 Request Processing 7

Chapter 2 SNMP Specifications 9

2.1 Supported Operations 10

Chapter 3 SNMP Operations 11

3.1 Trap-Issuing Processing 11
3.2 Request Processing 12

Chapter 4 Installing and Uninstalling SNMP 15

4.1 Installing SNMP 16
4.2 Uninstalling SNMP 23

Chapter 5 Operating Procedures 27

5.1 Setup 28
5.1.1 Setting Up SNMP on the Subsystem 28
5.1.2 Setting Up the SNMP Host Manager Side 28
5.1.3 Checking Connections 28
5.2 Setting Enable/Disable 29
5.3 Creating an Environmental Information File 31
5.3.1 Operation Environment Setting File (Config.txt) 31
5.3.1.1 How to Create Files 32
5.3.2 Configuring the Unit Name Setting File (name.txt) 35
5.3.2.1 How to Create the File 35
5.4 Registering SNMP Environmental Information 36
5.5 Referencing the SNMP Environment Information File 39
5.6 How to Verify the SNMP Connection 40
5.7 How to Detect Failure 41

Chapter 6 Management Information Bases 43

6.1 Supported MIBs 44
6.2 MIB Access Mode 44
6.3 Object Identifier Assignment System 45
6.4 Types of Supported Traps and Trap Issuing Opportunities 48

Chapter 7 MIB Installation Specifications 51

7.1 MIB II 52
7.1.1 system Group 52
7.1.2 interfaces Group 53
7.1.3 at Group 55
7.1.4 ip Group 55
7.1.5 icmp Group 59

7.1.6 tcp Group 59
7.1.7 udp Group 59
7.1.8 egp Group 59
7.1.9 snmp Group 60
7.2 Extended MIBs 62
7.2.1 dfSystemParameter Group 62
7.2.2 dfWarningCondition Group 63
7.2.3 dfCommandExecutionCondition Group 66
7.2.4 dfPort Group 68
7.2.5 dfCommandExecutionInternalCondition Group 72

Chapter 8 Troubleshooting 73

Appendix A Operations Using CLI 75

A.1 Installing 76
A.2 Uninstalling 78
A.3 Enabling or Disabling 80
A.4 Registering or Referencing SNMP Environment Information 82

Acronyms and Abbreviations 85

Glossary 87

Index 89

List of Figures

Figure 1.1 Example of Divided SNMP Managers 4
Figure 1.2 Local LAN Connection 5
Figure 1.3 Public LAN Connection 5

Figure 2.1 Communication for SNMP Operation 10

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 Window (Logical Status Tab) 17
Figure 4.2 Install/Unlock Options Dialog 17
Figure 4.3 Options Selection Dialog 18
Figure 4.4 SNMP Install/Unlock Confirmation Message 18
Figure 4.5 Result Dialog 19
Figure 4.6 Restart After Unlock 21
Figure 4.7 Array System Viewer Window (Logical Status Tab: Option Enable) 22
Figure 4.8 Reboot Dialog 22
Figure 4.9 Subsystem Restart Successful Message 22
Figure 4.10 De-install/Lock Options Dialog Box 23
Figure 4.11 Option De-install/Lock Confirmation 24
Figure 4.12 Option Lock Confirmation 24

Figure 5.1 Disable Option Message Dialog Box 29
Figure 5.2 SNMP Agent Confirmation Window 30
Figure 5.3 Array System Viewer Window (Logical Status Tab: Option Disable) 30
Figure 5.4 Setting Address to Send a Trap 34
Figure 5.5 Operation Environment Setting File 34
Figure 5.6 Configuration Settings Dialog Box (SNMP Tab) 36
Figure 5.7 Edit SNMP Setting Files 37
Figure 5.8 Confirmation Message 37
Figure 5.9 Settings/Environment Complete Dialog Box 38
Figure 5.10 Output Confirmation Dialog Box 39
Figure 5.11 SNMP Manager TRAP Response Failure Detection 41

Figure 6.1 The Object Identifier Assignment System (Frame 1 of 3) 45

Figure 7.1 Relationship between Traps and dfWarningCondition Groups 65
Figure 7.2 Accumulated Values Over Time 67

List of Tables

Table 1.1 GET/TRAP Specifications 3
Table 1.2 Network Connecting Functions 5

Table 2.1 SNMP Operations Supported 10

Table 3.1 Header/Data Length Table 13

Table 5.1 Operation Environment Settings 31
Table 5.2 Item of Unit Name Setting 35

Table 6.1 Supported MIBs 44
Table 6.2 Supported Standard Traps 48
Table 6.3 Supported Extended Traps 49

Table 7.1 system Group 52
Table 7.2 interfaces Group 53
Table 7.3 ip Group 55
Table 7.4 snmp Group 60
Table 7.5 dfSystemParameter Group 62
Table 7.6 dfWarningCondition Group 63
Table 7.7 dfRegressionStatus Format 63
Table 7.8 dfRegressionStatus Value for Each Failure 64
Table 7.9 dfCommandExecutionCondition Group 66
Table 7.10 dfPort Group 68
Table 7.11 Port Display Numbers 69
Table 7.12 Port Addresses and Associated Values 70
Table 7.13 Topology Information for Fibre-Oriented Ports 71
Table 7.14 Topology Information for Ports other than Fibre-Oriented 71
Table 7.15 Port Display Names 71
Table 7.16 dfCommandExecutionInternalCondition Group 72

Chapter 1 Overview of the SNMP Agent Support Function

The SNMP Agent support function reports failure occurrences to the workstation for network monitoring using the Simple Network Management Protocol (SNMP) of an open platform. Command operating status (e.g., the number of commands received, the number of cache hits, etc.) of the subsystem is reported. This reported information can be used for performance tuning. To use SNMP, you need a LAN facility and a workstation in which the SNMP manager program (hereinafter referred to as "SNMP manager") is installed.

This chapter contains the following:

- Notes on Using SNMP (section 1.1)
- System Configuration - Network Connecting Functions (section 1.2)
- System Configuration - LAN Connections (section 1.3)
- SNMP Functions (section 1.4)

1.1 Notes on Using SNMP

When using SNMP, note the following:

- Since the User Datagram Protocol (UDP) is used for the SNMP Agent support function, correct reporting of error traps to the SNMP manager cannot be assured. **It is recommended that the SNMP manager acquire MIB information periodically.**
- If the interval to collect MIB information is set too short, the command processing performance of the subsystem is negatively affected.
- If the SNMP manager is started after failures occur in a subsystem, those failures are not reported with a trap. To have these failures reported, acquire the MIB objects "dfRegressionStatus" after starting the SNMP manager to see if failures occurred.
- SNMP stops if the controller is blockaded. If this is the case, the SNMP managers receive no response.
- If a subsystem is configured from a dual system and failures in hardware components (such as fans, batteries, power supplies, or cache failures) occur during power-on before the subsystem is "Ready" (including failures that occurred at the last power off), these failures are reported with a trap from both controllers. Failures in disk drives and failures that occur while a subsystem is "Ready" are reported with a trap from only the controller side that detects the failures. Table 1.1 contains the GET/TRAP Specifications.
- When a subsystem is configured from a dual system, the SNMP manager must monitor both controllers. 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 is reported for controller down of controller 1.
    ("Controller down" is reported as a systemDown trap by the faulty controller.)
  - If 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 controllers	① Both controllers are normal	GET	○	GET	○	Master controller : 0
		TRAP	○	TRAP	Δ	
	② Controller 1 is blockaded	GET	○	GET	×	Master controller : 0
		TRAP	○	TRAP	×	If controller 1 is recovered, the system goes to①.
	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
		TRAP	Δ	TRAP	○	The system goes to ① when restarted (P/S ON).
Controller 0 only	⑤ Both 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
		TRAP	Δ	TRAP	×	The system goes to ⑤ when restarted (P/S ON).

○: 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 is 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.

In a dual system configuration, SNMP managers should not be divided as shown in Figure 1.1. 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 for the above-mentioned failures, each a resource shared between both controllers, are not reported to the SNMP manager that manages the slave controller side. Use the same SNMP Manager to control both controllers of a storage array.

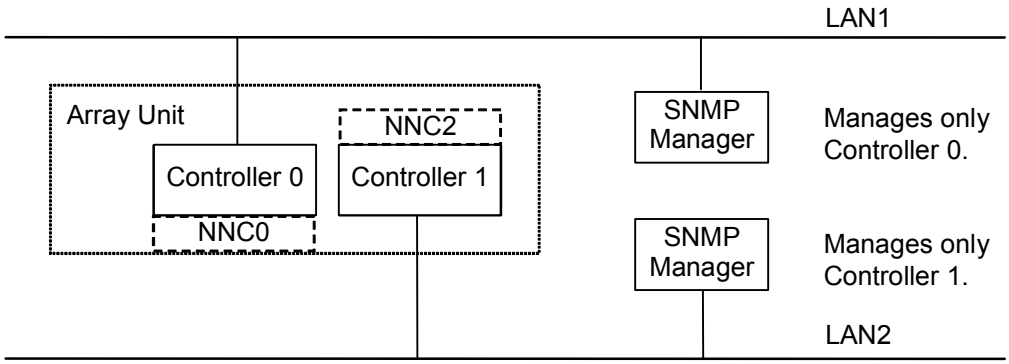


Figure 1.1 Example of Divided SNMP Managers

- Do not connect a broadcast device to the subsystem LAN. The incoming broadcast requests deteriorates the capacity to process host commands.

The subsystem must be connected to a LAN that conforms to “Ethernet Version 2”. Only “Ethernet Version 2” frames (IEEE802.3 frames, etc.) are supported at this time.

Note: Fix the IP address of the SNMP manager when using the SNMP support function in a system that 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.

Note: If the IP Address of the subsystem is changed during a Power ON sequence after getting the IP address automatically with the DHCP client function, the SNMP manager will not be able to find the subsystem, and the trap cannot be reported to the SNMP manager. If the IP address of the subsystem is changed, restart the subsystem.

1.2 System Configuration - Network Connecting Functions

Network connecting functions supported by the subsystem 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.

1.3 System Configuration - LAN Connections

LAN connections are shown in the following illustrations:

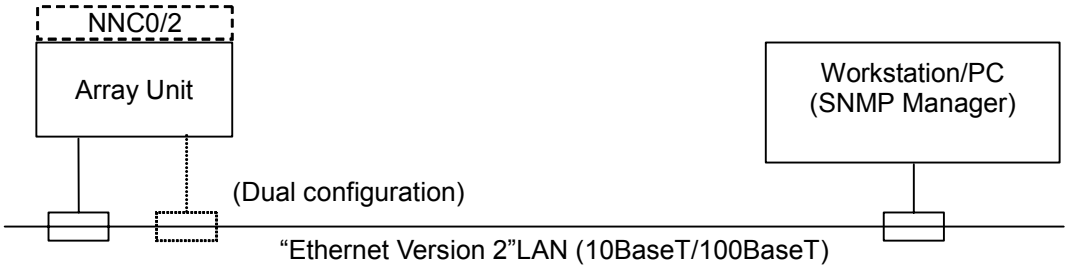


Figure 1.2 Local LAN Connection

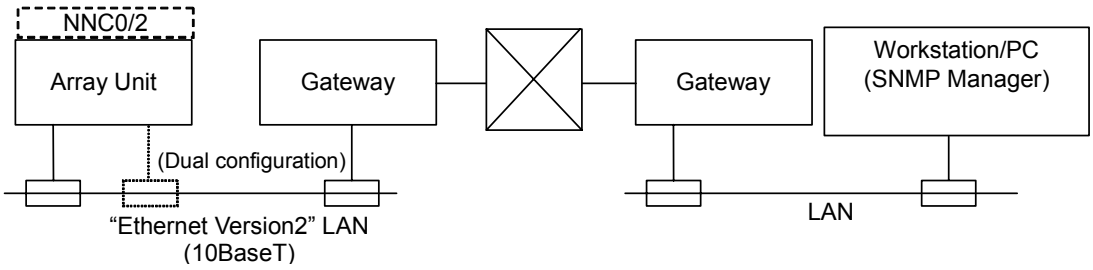


Figure 1.3 Public LAN Connection

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

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

1.4 SNMP Functions

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

- Trap Reporting
- Request Processing

1.4.1 Trap Reporting

The user can be informed of failures that occur in the subsystem in real time even when the user is away from the subsystem. This function issues a 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*** and ***Note 3***)
  - Drive blockade (data drive)
  - Fan failure
  - DC power failure
  - Battery failure
  - Cache partial blockade
  - UPS failure
  - Battery charging circuit failure
  - Blockade of the mate controller (See ***Note 3***)
  - Warned subsystem (See ***Note 4***)
  - Drive (spare drive) blockade
  - Online microprogram replacement executed
  - ENC failure
  - Loop failure
  - Path blockade (See ***Note 2***)
  - SATA Drive (data drive) blockade
  - SATA Drive (spare drive) blockade
  - SENC failure
  - Host connector
  - NNC (NAS Node Controller)

Note 1: Depending upon the contents of the failure, there may be an instance that cannot be reported.

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

Note 3: When a controller blockade occurs, the disk subsystem issues TRAPs that show the blockade. The controller blockade may recover automatically depending on the cause of the failure.

Note 4: The TRAP that shows the warning status of the subsystem may be issued through preventive maintenance, periodic part replacement, or a fieldwork of the service personnel.

1.4.2 Request Processing

This function enables the SNMP manager to refer to MIB objects supported by the subsystem. (The function to set MIB objects is not available at this time.) The information supported is:

- Device specific information (product name and microprogram revision)
- Command execution condition information
- Warning information that can be acquired by the subsystem:
  - Drive blockade (data drive or spare drive)
  - Fan failure
  - DC power failure
  - Battery failure
  - Cache partial blockade
  - UPS failure
  - Battery charging circuit failure
  - Blockade of the mate controller (See ***Note 1***)
  - Warned subsystem (See ***Note 2***)
  - Drive (data drive) blockade
  - Drive (spare drive) blockade
  - ENC failure
  - Loop failure
  - Path blockade
  - SATA Drive (data drive) blockade
  - SATA Drive (spare drive) blockade
  - SENC failure
  - Host connector
  - NNC (NAS Node Controller)

Note 1: When the other controller is blocked, the blockade will set off a warning indication. However, the controller blockade may recover automatically depending on the cause of the failure.

Note 2: The warning status of the subsystem can be automatically set in the warning information by preventive maintenance, periodic part replacement or a fieldwork of the service personnel.

Chapter 2 SNMP Specifications

The subsystem supports SNMP agent functions that conform to RFC1157, the simple network management protocol, and supports SNMP Version 1 protocol. Although the subsystem cannot issue all of the traps described in RFC1157 at this time, it does support MIB-II, which conforms to RFC1213.

For information regarding error codes, please refer to the *Hitachi TagmaStore AMS/WMS Storage Navigator Modular DF Error Codes*, MK-96DF788

This chapter contains the following:

- Supported Operations (section 2.1)

2.1 Supported Operations

Figure 2.1 illustrates SNMP communication operations. Table 2.1 lists the SNMP operations supported by the subsystem and shows communication between the SNMP manager and the SNMP agent for a supported SNMP operation.

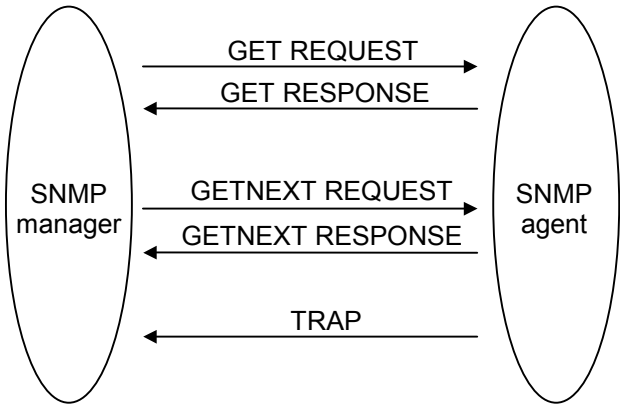


Figure 2.1 Communication for SNMP Operation

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 status change) to the SNMP manager. When an event occurs, the agent sends a TRAP to the manager, regardless of SNMP manager's request.

Chapter 3 SNMP Operations

This chapter contains the following:

- Trap-Issuing Processing (section 3.1)
- Request Processing (section 3.2)

3.1 Trap-Issuing Processing

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

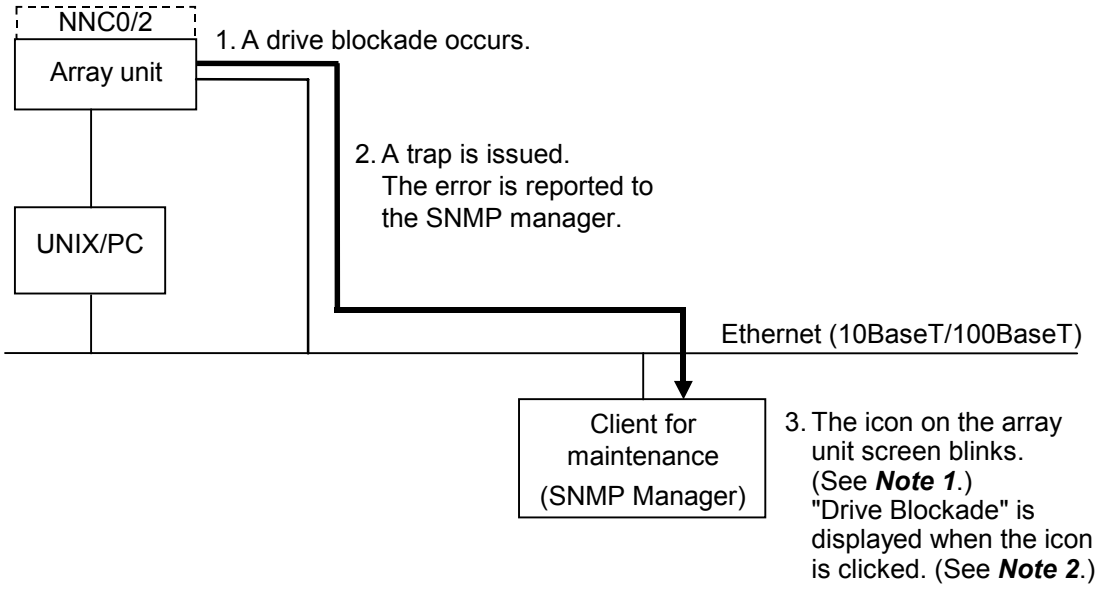


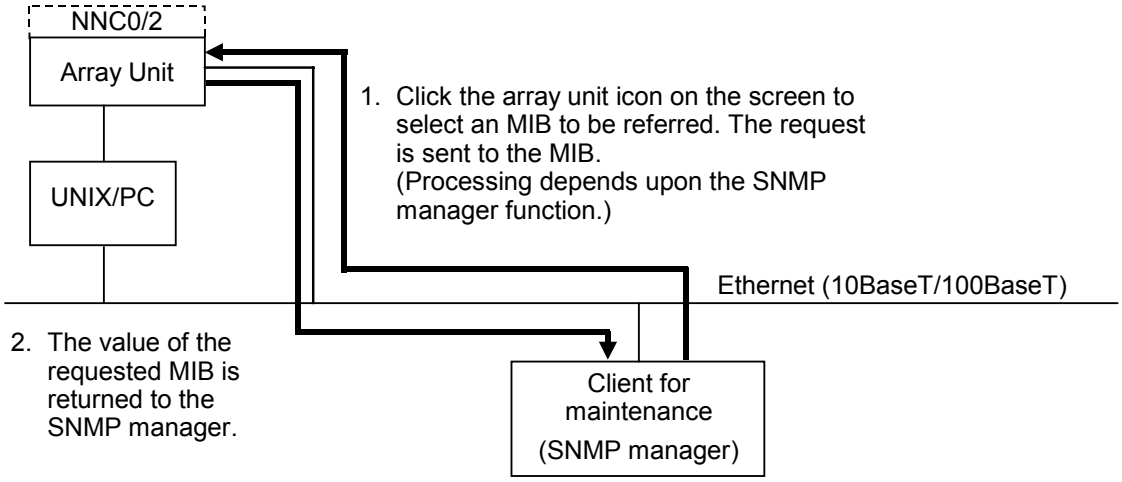
Figure 3.1 Example of a Drive Blockade and Trap Issue

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

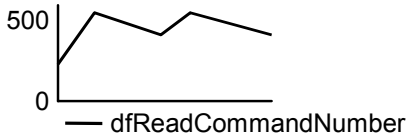
Note 2: The display operation and the display specification of the trap codes depend upon the specification of the SNMP manager used.

3.2 Request Processing

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



3. The value of the requested MIB is displayed on the screen. (***Note 1***)
   Example 1: Information specific to the device is displayed as follows:
   dfSystemProductName = HITACHI DF600F
   dfSystemMicroRevision = 07510
   Example 2: Information on the regressed portion is displayed (no error detected) as follows:
   dfRegressionStatus = 0
   Example 3: Number of read command reception is graphically displayed as shown below. (Displays can be requested, two or more times, at regular intervals.)



Note 1: The display specification of MIB depends upon 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 may be affected negatively.

The subsystem cannot send or receive SNMP messages longer than 484 bytes. If a message longer than 484 bytes is sent, the subsystem returns the message “tooBig”. To avoid this situation, the SNMP manager should not send a message exceeding 484 bytes (Figure 3.3).

SNMP Message (484 bytes max.)			
About 35 bytes (Community Name: public)	6 (Header) + Object ID length + Data length (***Note***)	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: The action when receiving a trap depends upon the specifications of the SNMP manager being used. MIB information 1 becomes 6+8+10 = 24 bytes long. The header length varies with the data length (Table 3.1).

Table 3.1 Header/Data Length Table

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

Chapter 4 Installing and Uninstalling SNMP

SNMP is an optional subsystem feature. To enable the SNMP function (in an unlocked state), installation of the software is required. Uninstallation is required to remove the software. Use the Storage Navigator Modular to perform installation and uninstallation.

Warning: If you are installing or uninstalling SNMP where the disk array subsystem is used on a TrueCopy remote site and the microcode level is earlier than 3.1A, the following occurs when the disk array subsystem is restarted:

- Both paths of TrueCopy are blocked.
- The pair status of TrueCopy is PAIR or COPY changes to PSUE.

Notes:

- **When you restart the disk array subsystem, install or uninstall SNMP after changing the pair status of TrueCopy to PSUS.**
- The installing, uninstalling, enabling, and disabling of the SNMP functions are set individually for each subsystem.
- Before installing and uninstalling SNMP, make sure that the subsystem is in normal operating order. If a failure such as a controller blockade has occurred, installing and uninstalling operations cannot be performed.
- If you install, uninstall, enable, or disable the SNMP on a subsystem connected to a NAS and the microcode level is earlier than 3.1A, you must also stop the clusters between NAS units. When restarting the subsystem, you must also restart the clusters.

This chapter contains the following:

- Installing SNMP (section 4.1)
- Uninstalling SNMP (section 4.2)

4.1 Installing SNMP

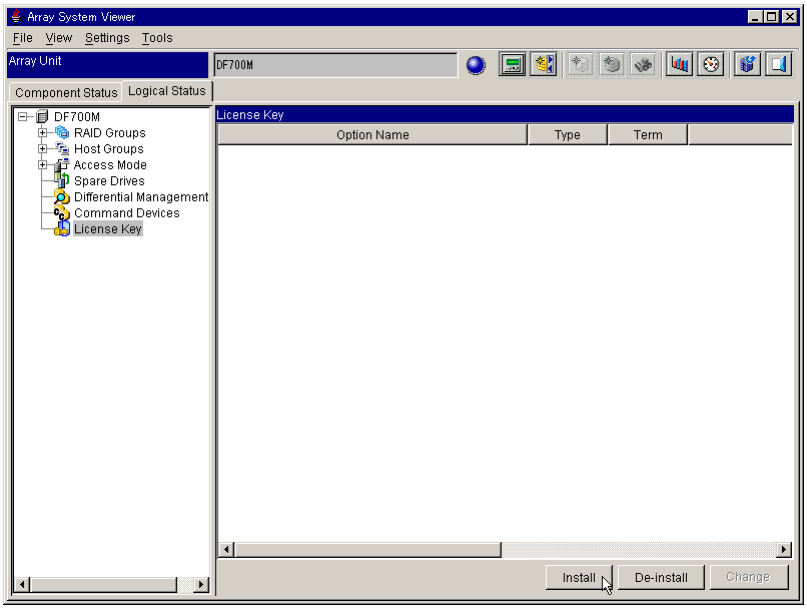
The key code or key file provided with SNMP is required to install SNMP. Install SNMP by completing the following steps:

The following describes GUI installation procedures performed by using the Navigator when the microcode level is 3.1A:

1. Register the SNMP environment file (see section 5.3)
2. Start the Navigator and switch to **Management Mode**.
3. Register the subsystem in which you will install SNMP. Connect to this subsystem.

   A window for the connected subsystem is displayed.
4. Click the **Logical Status** tab (Figure 4.1).
5. Click the **License Key** icon.

   Storage Navigator, version 5.0 or later



Storage Navigator, versions earlier than 5.0

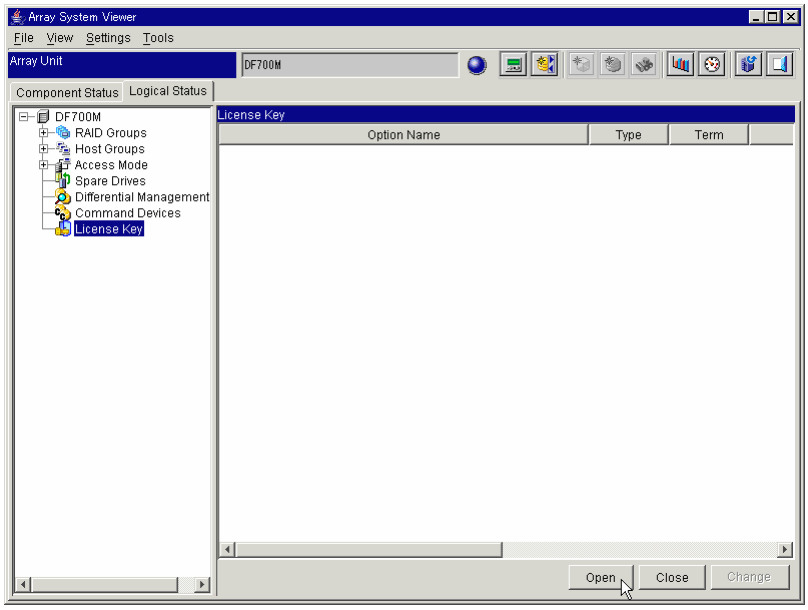


Figure 4.1 Array System Viewer Window (Logical Status Tab)

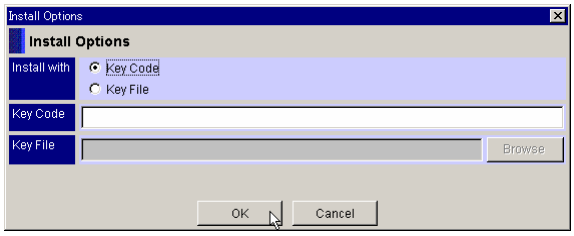
6. Click **Install**. (Storage Navigator, version 5.0 or later)

   The **Install Options** dialog is displayed (Figure 4.2).

   Click **Open**. (Storage Navigator, versions earlier than 5.0)

   The **Unlock Options** dialog is displayed (Figure 4.2).

   Storage Navigator, version 5.0 or later



Storage Navigator, versions earlier than 5.0

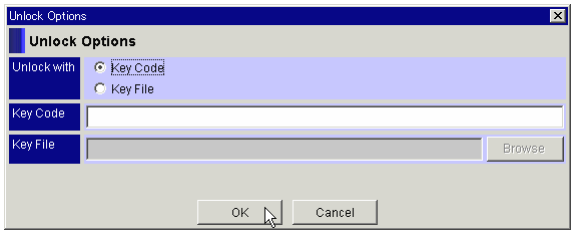


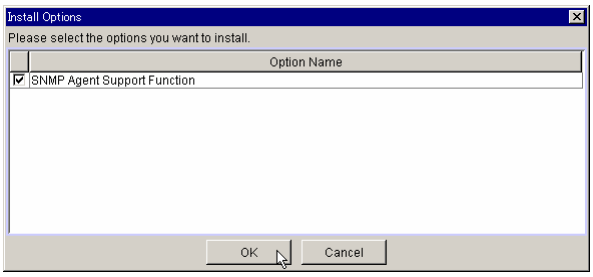
Figure 4.2 Install/Unlock Options Dialog

7. When installing the option using the key code, click the **Key Code** radio button, then set up the key code. When installing the options using the key file, click the **Key File** radio button, and set up the path for the key file. Click **OK**.

   Click **Browse** to set the path to a key file.

8. When installing the options using the key file, the options selection dialog is displayed. Verify the **Option Name** and click **OK**.

   Storage Navigator, version 5.0 or later



Storage Navigator, versions earlier than 5.0

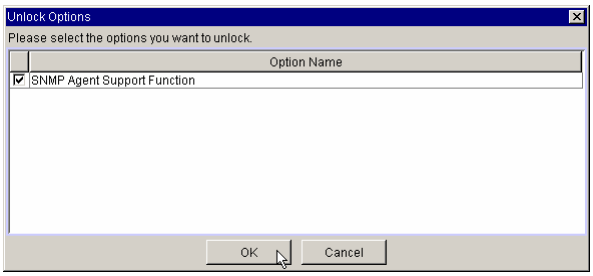
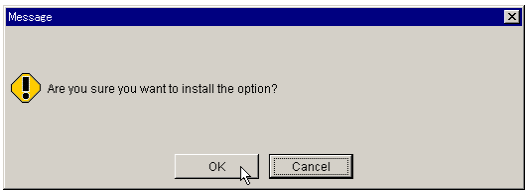


Figure 4.3 Options Selection Dialog

9. A message appears, requesting a confirmation to install the SNMP option (see Figure 4.4). Click **OK**.

   Storage Navigator, version 5.0 or later



Storage Navigator, versions earlier than 5.0

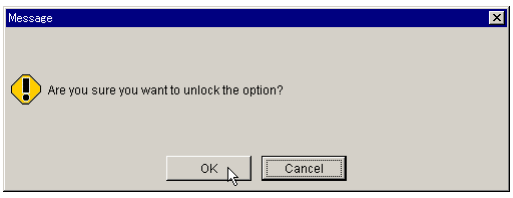
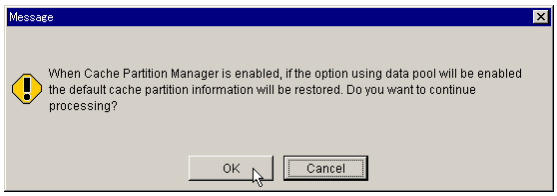


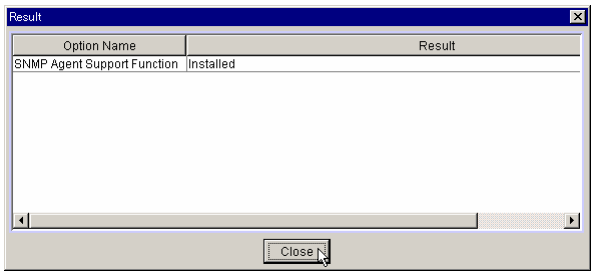
Figure 4.4 SNMP Install/Unlock Confirmation Message

10. When Storage Navigator version is 3.00 or later and Cache Partition Manager are enabled, the following message is displayed. Since SNMP does not use the data pool, click the **OK** button at this point without doing anything else.



11. When installing the options using the key file, the **Result** dialog is displayed. Click **Close**.

    Storage Navigator, version 5.0 or later



    Storage Navigator, versions earlier than 5.0

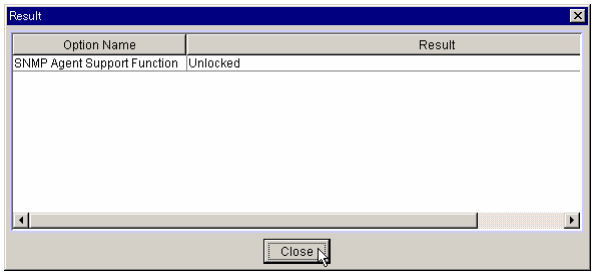
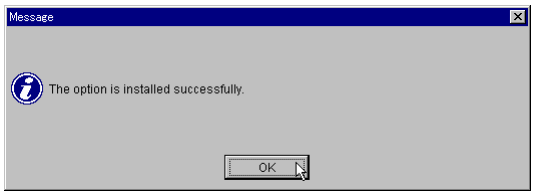


Figure 4.5 Result Dialog

12. A message appears confirming that the SNMP feature is installed. Click **OK**.

    Storage Navigator, version 5.0 or later



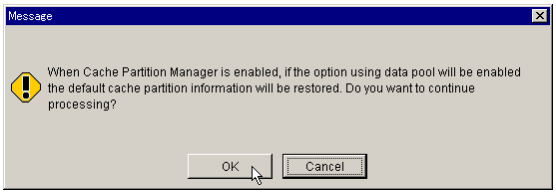
Storage Navigator, versions earlier than 5.0

If the microcode level is earlier than 3.1A:

1. Register the SNMP environment file (see section 5.3).
2. Start the Navigator and switch to **Management Mode**.
3. Register the subsystem in which you will install SNMP. Connect to this subsystem; a window for the connected subsystem is displayed.
4. Click the **Logical Status** tab.
5. Click the **License Key** icon (Figure 4.1).
6. Click **Open**.

   The **Unlock Options** dialog is displayed (Figure 4.2).
7. When installing the option using the key code, click the **Key Code** radio button, then set up the key code. When installing the options using the key file, click the **Key File** radio button, then set up the path for the key file. Click **OK**.

   Click **Browse** to set the path to a key file.
8. When installing the options using the key file, the options selection dialog is displayed, make sure the **Option Name** is selected and click **OK** (Figure 4.3).
9. A message appears, requesting a confirmation to install the SNMP option (Figure 4.4). Click **OK**.
10. When Storage Navigator version is 3.00 or later and Cache Partition Manager is enabled, the following message is displayed. Since SNMP does not use the data pool, click the **OK** button at this point without doing anything else.



11. When installing the options using the key file, the **Result** dialog box is displayed, click **Close** (Figure 4.5).
12. A message appears, confirming that the SNMP feature is installed. This message also asks you to restart the subsystem (see Figure 4.6). Click **OK**.

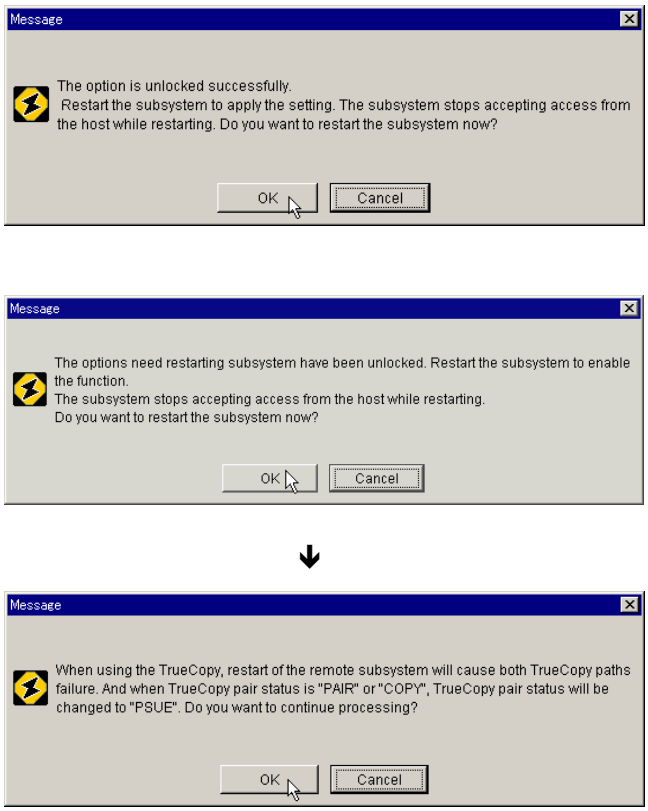


Figure 4.6 Restart After Unlock

Note: The SNMP feature is not installed until the subsystem is restarted. The subsystem cannot access the host until the restart is completed. Make sure that 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 **Cancel**. After setting information in the SNMP environment information file, restart the subsystem.

If you choose not to restart the subsystem, the **Array System Viewer** window appears displaying the installed optional feature SNMP (Figure 4.7).

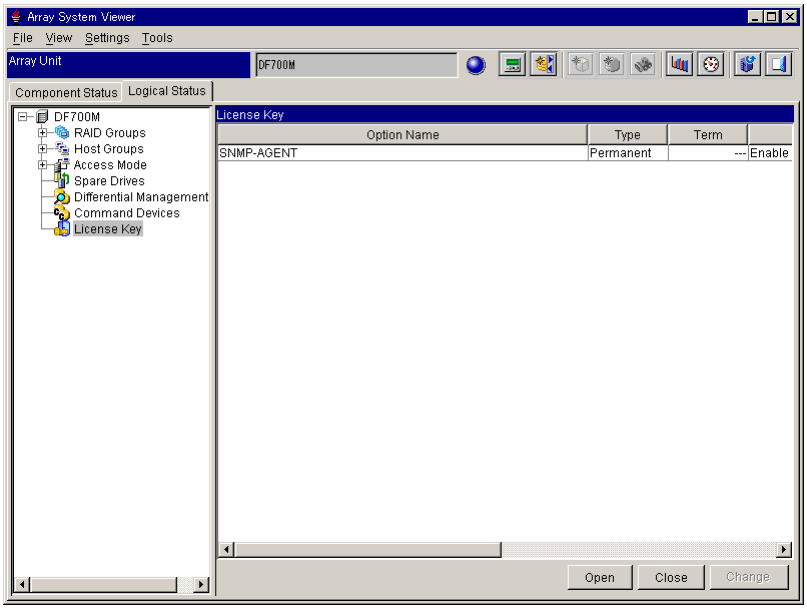


Figure 4.7 Array System Viewer Window (Logical Status Tab: Option Enable)

When choosing to restart the subsystem, the time the restart began is displayed (Figure 4.8). Restarting takes approximately 4 to 15 minutes.

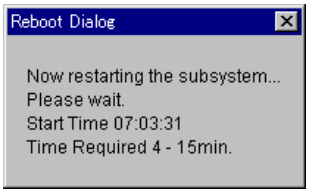


Figure 4.8 Reboot Dialog

Note: If the system does not respond after 15 minutes or more, check the system condition.

13. When the restart terminates, a message appears (Figure 4.9). Click **OK**; the Unit screen closes.

    To perform other operations on the Main window, select a subsystem from the Main window and open the selected Unit window.

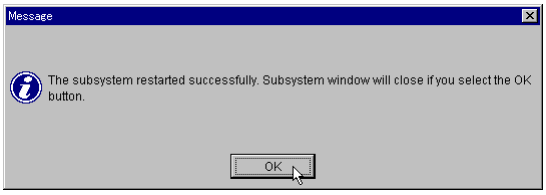


Figure 4.9 Subsystem Restart Successful Message

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 Navigator if the microcode level is 3.1A:

1. Start the Navigator and switch to **Management Mode**.
2. Register the subsystem in which you will uninstall SNMP. Connect to this subsystem.

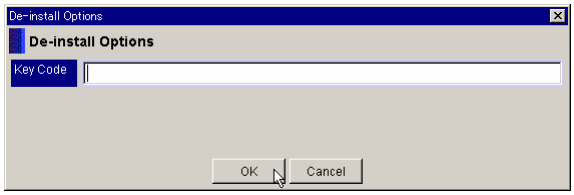
   A window for the connected subsystem is displayed.
3. Click the **Logical Status** tab (Figure 4.1).
4. Click the **License Key** icon (Figure 4.7).
5. Click **De-install**. (Storage Navigator, version 5.0 or later)

   The **De-install Options** dialog box is displayed.

   Click **Close**. (Storage Navigator, versions earlier than 5.0)

   The **Lock Options** dialog box is displayed.

   Storage Navigator, version 5.0 or later



Storage Navigator, versions earlier than 5.0

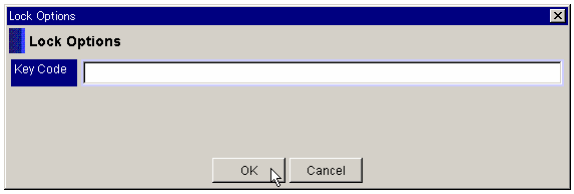
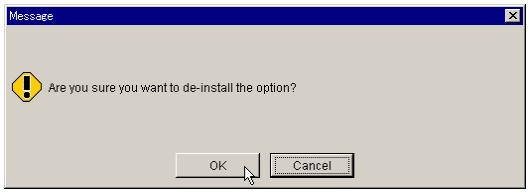


Figure 4.10 De-install/Lock Options Dialog Box

6. Enter a **key code** in the text box and click **OK**.
7. A message appears, requesting confirmation to uninstall the SNMP option (see Figure 4.11). Click **OK**.

   Storage Navigator, version 5.0 or later



Storage Navigator, versions earlier than 5.0

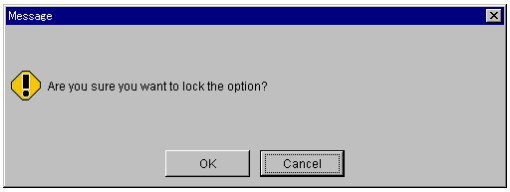


Figure 4.11 Option De-install/Lock Confirmation

If the microcode level is earlier than 3.1A:

1. Start the Navigator and switch to **Management Mode**.
2. Register the subsystem in which you will uninstall SNMP. Connect to this subsystem.

   A window for the connected subsystem is displayed.
3. Click the **Logical Status** tab (Figure 4.1).
4. Click the **License Key** icon (Figure 4.7).
5. Click **Close**.

   The **Lock Options** dialog box is displayed.
6. Enter a **key code** in the text box and click **OK**.
7. A message appears, requesting confirmation to uninstall the SNMP option (see Figure 4.11). Click **OK**.
8. A message appears confirming that this optional feature is uninstalled (see Figure 4.12). Click **OK**.

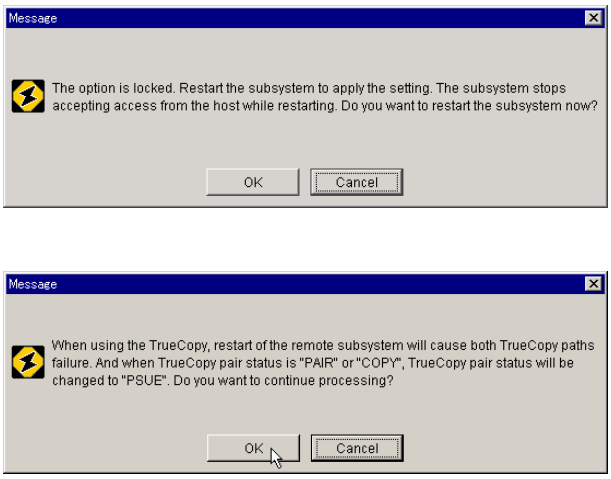


Figure 4.12 Option Lock Confirmation

Note: The SNMP optional feature is not uninstalled until the system is restarted. The subsystem cannot access the host until the restart is completed. Make sure the host has stopped accessing data before beginning the restart process.

If you choose not to restart the subsystem, the **Array System Viewer** window appears, displaying the uninstalled optional feature SNMP.

When restarting the subsystem, the time the restart began is displayed (refer to Figure 4.8). Restarting takes approximately four to fifteen minutes.

Note: If the system does not respond after 15 minutes or more, check the condition of system.

9. When the restart is complete, a message appears (see Figure 4.9). Click **OK**; the Unit window closes.

   To perform other operations on the Main window, select a subsystem from the Main window and open the selected Unit window.

Chapter 5 Operating Procedures

This chapter includes the following sections:

- Setup (section 5.1)
- Setting Enable/Disable (section 5.2)
- Creating an Environmental Information File (section 5.3)
- Registering the SNMP Environment Information File (section 5.4)
- Referencing the SNMP environment information file (section 5.5)
- How to Verify the SNMP Connection (section 5.6)
- How to Detect Failure (section 5.7)

Note: When performing the setting enable/disable or registering of SNMP environmental information on a subsystem used with TrueCopy, the following occurs with the restart of the disk array subsystem, if the microcode level is earlier than 3.1A and the Storage Navigator version is not 3.10 or later:

- Both paths of TrueCopy are blocked.
- When the pair status of TrueCopy is PAIR or COPY, it is changed to PSUE.

When restarting the disk array subsystem necessarily, perform the setting enable/disable or registering SNMP environmental information after changing the pair status of TrueCopy to PSUS.

Note: If the microcode level is earlier than 3.1A and the Storage Navigator version is 3.10 or earlier, and you install, uninstall, enable, or disable the SNMP on a subsystem connected to a NAS, you must also stop the clusters between NAS units. When restarting the subsystem, you must restart the clusters.

5.1 Setup

Completing the following setup procedures enables communication between the subsystem and the SNMP manager.

5.1.1 Setting Up SNMP on the Subsystem

1. Set all appropriate LAN information, (e.g., IP Address, Sub Net Mask, and Default Gateway Address). For detailed procedures, refer to the *Hitachi TagmaStore Adaptable Modular Storage 500 User's Guide™*, MK-95DF714.
2. Enable the optional Side feature using the Navigator and install the SNMP agent by setting it to **enable**.
3. Create the SNMP environment information file.

   The SNMP environment file consists of the following:

   - Operating environment setting file (Config.txt)

     Sets the IP address and community of the SNMP manager to send traps. The Community name is described in the config.txt file with the provided CD-ROM.

   - Unit name setting file (Name.txt)

     Sets unit names.

4. Register the SNMP environment information file in a subsystem. Refer to section 5.4 for details.
5. Restart the subsystem.

5.1.2 Setting Up the SNMP Host Manager Side

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

   For more detail, refer to the appropriate documentation for your SNMP manager.
2. Register the subsystem in the SNMP manager. ***Note:*** For more detail, refer to the appropriate documentation for your SNMP manager.

5.1.3 Checking Connections

Check the connection between the subsystem and the SNMP manager. By completing the procedure described previously, communication between the subsystem and the SNMP manager is enabled. The SNMP agent is set in an "enabled/disabled" state and the SNMP environment information file is registered using the Navigator. For information on the operating procedures of the Navigator, refer to the *Storage Navigator Modular (for GUI) User's Guide*, (MK-95DF711).

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 as invalid.

The following describes SNMP setting procedures performed by using the GUI version of the Navigator if the microcode level is 3.1A or later, and the Storage Navigator version is 3.10 or later.

1. Start the Navigator and switch to **Management Mode**.
2. Register the subsystem in which you will set up SNMP. Connect to this subsystem; a window for the connected subsystem is displayed.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon (Figure 4.7).
5. Click on **"SNMP-AGENT"** in the **Option Name** text box and then click **Change**.
6. The following message is displayed (see Figure 5.1). Click **OK**.

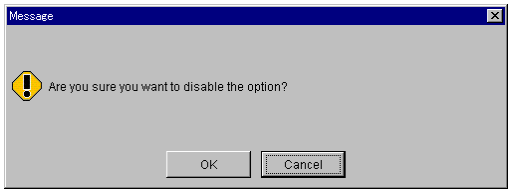
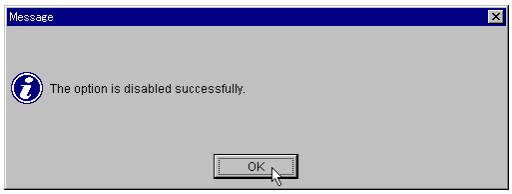


Figure 5.1 Disable Option Message Dialog Box

7. A message appears, confirming that the SNMP agent has been set up (see Figure 5.2). Click **OK**.



- When the Microprogram revision of the subsystem is less than 3.1A, or the Storage Navigator version is earlier than 3.10:

1. Start the Navigator and switch to **Management Mode**.
2. Register the subsystem in which you will set up SNMP. Connect to this subsystem; a window for the connected subsystem is displayed.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon (Figure 4.7).
5. Click on **"SNMP-AGENT"** in the **Option Name** text box and click **Change**.
6. A message is displayed (see Figure 5.1). Click **OK**.

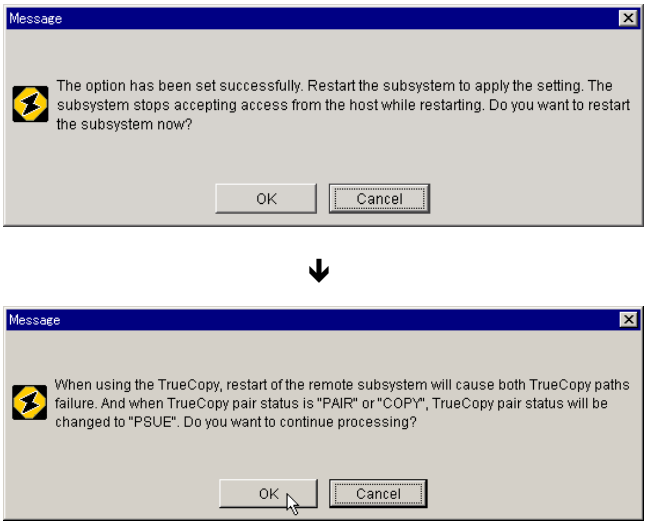


Figure 5.2 SNMP Agent Confirmation Window

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

If a subsystem fails to restart, the **Array System Viewer** window is displayed with the set-up SNMP agent status being updated (Figure 5.3).

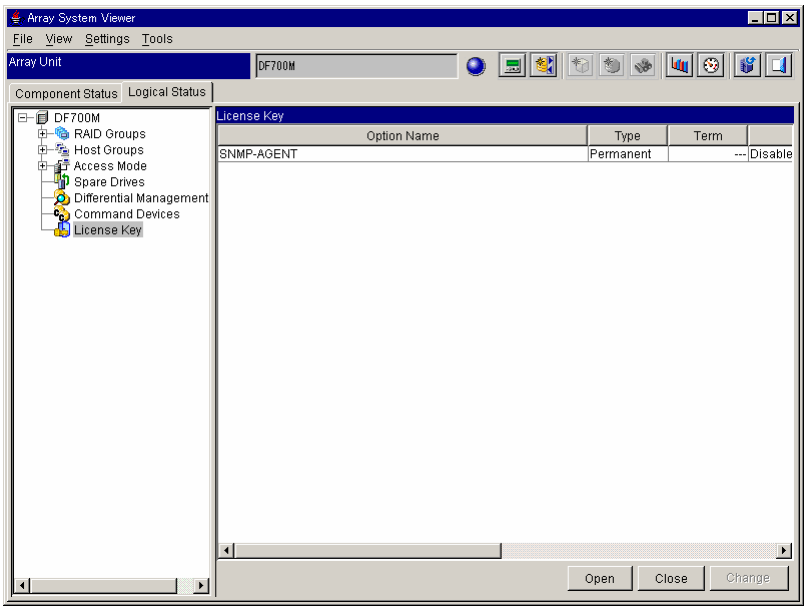


Figure 5.3 Array System Viewer Window (Logical Status Tab: Option Disable)

When restarting the subsystem, the time the restart began is displayed (refer to Figure 4.8). Restarting takes approximately 4 to 15 minutes.

If the subsystem does not respond after 15 minutes or more, check the condition of it.

7. When the restart terminates, a message appears (refer to Figure 4.9). Click **OK**; the Unit window closes.

   To perform other operations on the Main window, select a subsystem from the Main window and open the selected Unit window.

5.3 Creating an Environmental Information File

To use the SNMP agent, the SNMP environment information file is created and is registered in the subsystem. The following two files are created as the SNMP environment information file (these steps were explained in section 5.1).

- 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. The items provided in a sample file may be modified to suit your environment.

In a dual controller configuration, only one set (two files) must be created per one unit of subsystem. It is not possible to set different information for each controller.

5.3.1 Operation Environment Setting File (Config.txt)

This section contains the following:

- File Format
- Settings
- How to Create Files

File Format

This file is in text form and is on a DOS-formatted disk. The file name is “Config.txt”.

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)

5.3.1.1 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.
   - With any characters (space, tab, "-", "'", etc.) other than the letters a to z (uppercase and lowercase) and numerals used to set information, the characters must be enclosed with double quotation marks (").
   - There should be no line-feed codes in this information.
   - When not setting the sysContact value, describe as follow:

     If setting the sysContact:

     `INITIAL sysContact ""`

     If not setting the sysContact:

     Delete this setting item.

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.
   - With any characters (space, tab, "-", "'", etc.) other than the letters a to z (uppercase and lowercase) and numerals used to set information, the characters must be enclosed with double quotation marks (").
   - There should be no line-feed codes in this information.
   - When not setting the sysLocation value, describe as follow:

     When leave the sysLocation:

     `INITIAL sysLocation ""`

     When not setting the sysLocation:

     Delete this setting item.

3. Setting community information:
   - Add a line beginning with “COMMUNITY” to the file to specify the community name with which the subsystem allows receiving of requests. Unless this is specified, the subsystem accepts all community names:

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

   - The community name must be in alphanumeric characters only.

     With any characters (space, tab, “-”, “‘“, etc.) other than the letters a to z (uppercase and lowercase) and numerals used to set information, the characters must be enclosed with double quotation marks (“).
   - The community name cannot contain line-feed codes.
   - To enable the subsystem to accept all community names, delete the above 2 lines.

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

   Add a line beginning with “MANAGER” to the file to specify the SNMP manager to where the subsystem issues traps.
   - Enter the IP address to select an SNMP manager. Do not specify a host name.
   - Enter IP addresses with the leading 0s in each dotted quad suppressed (e.g., 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.
   - The 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 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. This will prevent a “tooBig” error message.

```
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

```
INITIAL sysContact "Taro Hitachi"

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

COMMUNITY tagmastore
ALLOW ALL OPERATIONS

MANAGER 123.45.67.89
SEND ALL TRAPS TO PORT 162
WITH COMMUNITY "HITACHI DF700"

MANAGER 123.45.67.90
SEND ALL TRAPS TO PORT 162
WITH COMMUNITY "HITACHI DF700"
```

Figure 5.5 Operation Environment Setting File

5.3.2 Configuring the Unit Name Setting File (name.txt)

This section contains the following:

- File Format
- Settings
- How to Create the File

File Format

This file is in text form and is on a DOS-formatted disk. The file name is “Name.txt”.

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

5.3.2.1 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:

```
DF700-01 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 register the SNMP environment information file, perform the following steps if the microcode level is 3.1A or later, and the Storage Navigator version is 3.10 or later:

1. Start the Navigator and switch to **Management Mode**.
2. Register the subsystem in which you will set up SNMP. Connect to this subsystem; a window for the connected subsystem is displayed (refer to Figure 4.1).
3. From the **Settings** menu, select **Configuration Settings**, or select the **Configuration Settings** button ( ) from the tool bar. The **Configuration Settings** dialog box is displayed (Figure 5.6).
4. Click the **SNMP** tab.

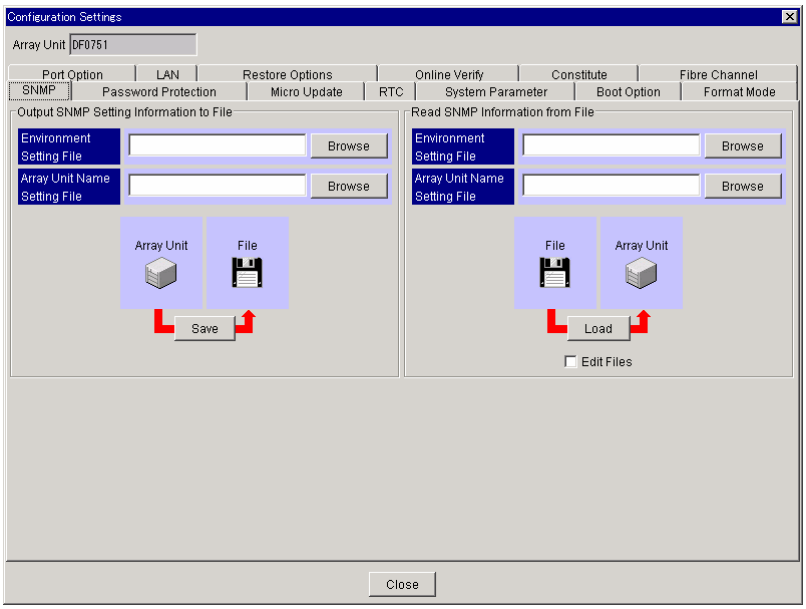


Figure 5.6 Configuration Settings Dialog Box (SNMP Tab)

5. Set a path to the SNMP environment information file (config.txt, name.txt), and click **Load**. If only one file is set, specify only a path to a file to set.

   To edit contents of a file at the time of its registration, put a check mark next to **Edit Files**.

6. Since contents of the file are displayed, edit them. When you select **Set to the Subsystem**, the file is registered with the contents that have been edited. When selecting **Save to the File**, the contents that have been edited are stored in the file.

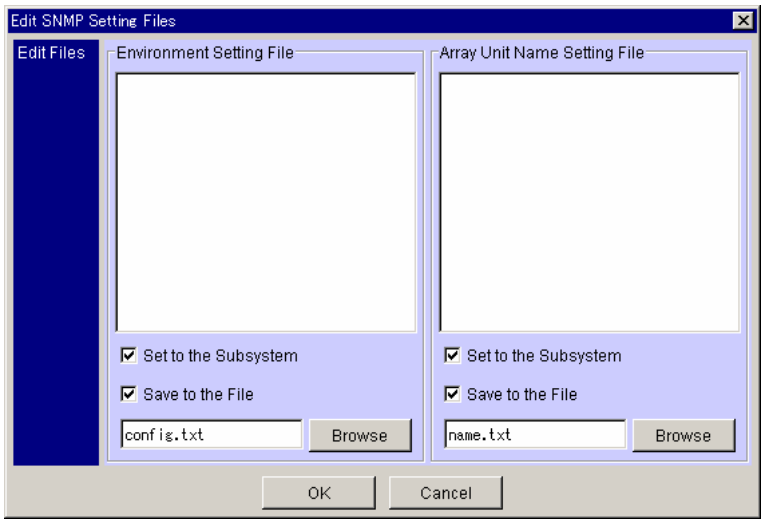


Figure 5.7 Edit SNMP Setting Files

7. Click **OK**.
8. A message appears, confirming that the settings are complete (Figure 5.8). This message also asks you to restart the system. Click **OK**.

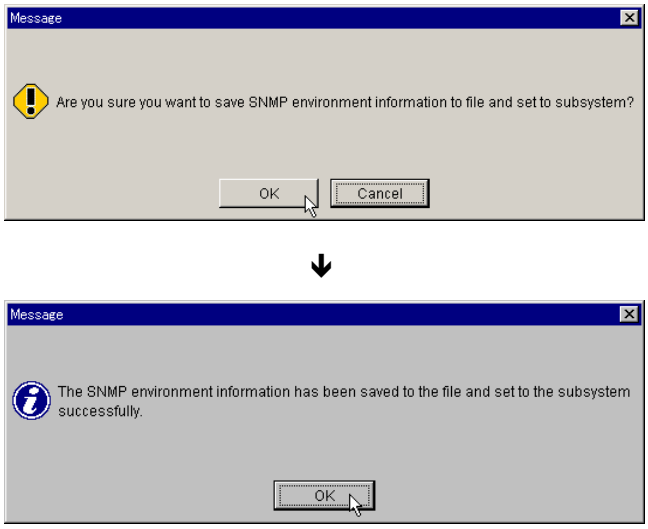


Figure 5.8 Confirmation Message

- When the Microprogram revision of the subsystem is less than 3.1A, or the Storage Navigator version is earlier than 3.10:

1. Start the Navigator and switch to **Management Mode**.
2. Register the subsystem in which you will set up SNMP. Connect to this subsystem; a window for the connected subsystem is displayed.
3. From the **Settings** menu, select **Configuration Settings**, or select the **Configuration Settings** button ( ) from the tool bar. The **Configuration Settings** dialog box is displayed.
4. Click the **SNMP** tab (Figure 5.6).
5. Set a path to the SNMP environment information file (config.txt, name.txt), and click **Load**. If only one file is set, specify only a path to a file to set.

   When you want to edit contents of a file at the time of its registration, put a check mark next to **Edit Files**.
6. Since contents of the file are displayed, edit them. When selecting **Set to the Subsystem**, the file is registered with the contents that have been edited. When selecting **Save to the File**, the contents that have been edited are stored in the file.
7. Click **OK**.
8. A message appears, confirming that the settings are complete (Figure 5.9). This message also asks you to restart the subsystem. Click **OK**.

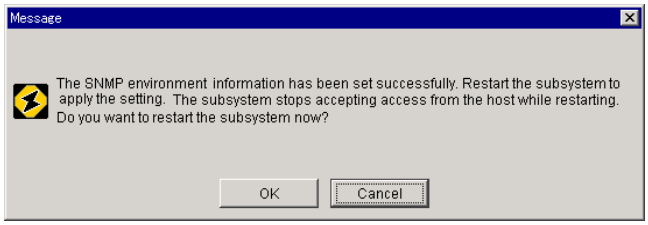


Figure 5.9 Settings/Environment Complete Dialog Box

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. Make sure that the host has stopped accessing data before beginning the restart process.

When restarting the subsystem, the time the restart began is displayed (refer to Figure 4.8). Restarting takes approximately 4 to 15 minutes.

Note: If there is no response after 15 minutes or more, check the condition of the subsystem.

When the restart is complete, a message appears (refer to Figure 4.9). Click **OK**; the Unit window closes. To perform other operations on the Main window, select a subsystem from the Main window and open the selected Unit window.

5.5 Referencing the SNMP Environment Information File

This section contains the procedures for referencing the SNMP environmental information file by outputting it to a text file for the SNMP agent.

1. Start the Navigator and switch to **Management Mode**.
2. Register the subsystem in which you will set up SNMP. Connect to this subsystem; a window for the connected subsystem is displayed (refer to Figure 4.1).
3. From the **Settings** menu, select **Configuration Settings,** or select the **Configuration Settings** button ( ) from the tool bar. The **Configuration Settings** dialog box is displayed.
4. Click the **SNMP** tab (refer to 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 **Save**.

   If only one file is output, specify only a path to the file to be output.
6. A message appears, confirming that output to the file is complete (Figure 5.10). Click **OK**.

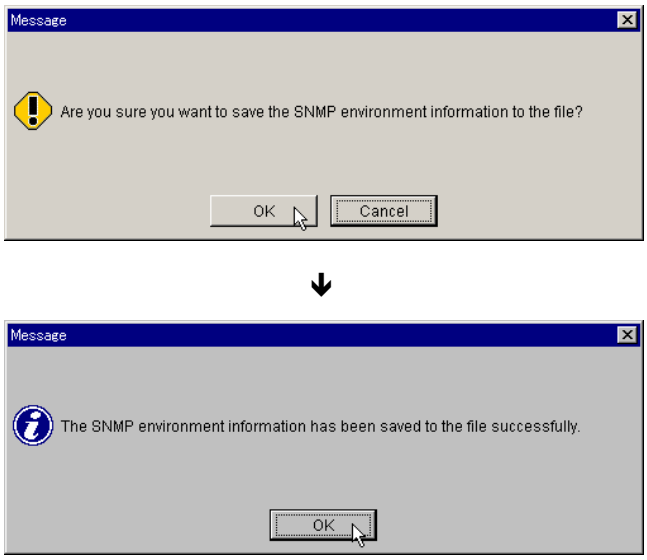


Figure 5.10 Output Confirmation Dialog Box

The SNMP environment information file set currently in a file specified during Step 5 has been output.

5.6 How to Verify the SNMP Connection

This section contains the procedures to confirm the SNMP connection between the subsystem and the SNMP manager.

1. Trap connection check:

   Set the SNMP Agent function to Invalid, and then to Valid again. Make sure that a standard trap “warmStart,” has been received by all SNMP managers that have been set as trap receivers in the SNMP environment information file (Config.txt).

2. REQUEST connection check:

   Send an array-unit-supported MIB GET request to the subsystem from all the SNMP managers to be connected. Verify that the subsystem responds.

If the results of procedures 1 and 2 above are normal, communication between the subsystem and each SNMP manager is verified as possible.

5.7 How to Detect Failure

The following procedure describes the SNMP agent support function detection.

1. Obtain MIB information (dfRegressionStatus) periodically. This MIB value is set to "0" when there are no failures.
2. If an error occurs that results in a trap, the subsystem reports the error to the SNMP manager. This trap normally allows the user to detect subsystem failures immediately when they occur; however, the UDP protocol used cannot assure that the trap is correctly reported to the SNMP manager. If a controller goes down, the systemDown trap may not be issued (Figure 5.11).
3. Errors are detected with MIB information obtained periodically as in Step 1. The user will know that a failure has occurred and/or a part has failed even when a trap described in Step 2 is not reported because the MIB value (dfRegressionStatus) is not set to 0 in the event of failure. For 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.

Note: Because the UDP protocol is used, it is possible that requests from the SNMP manager may be ignored even when operation is normal.

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

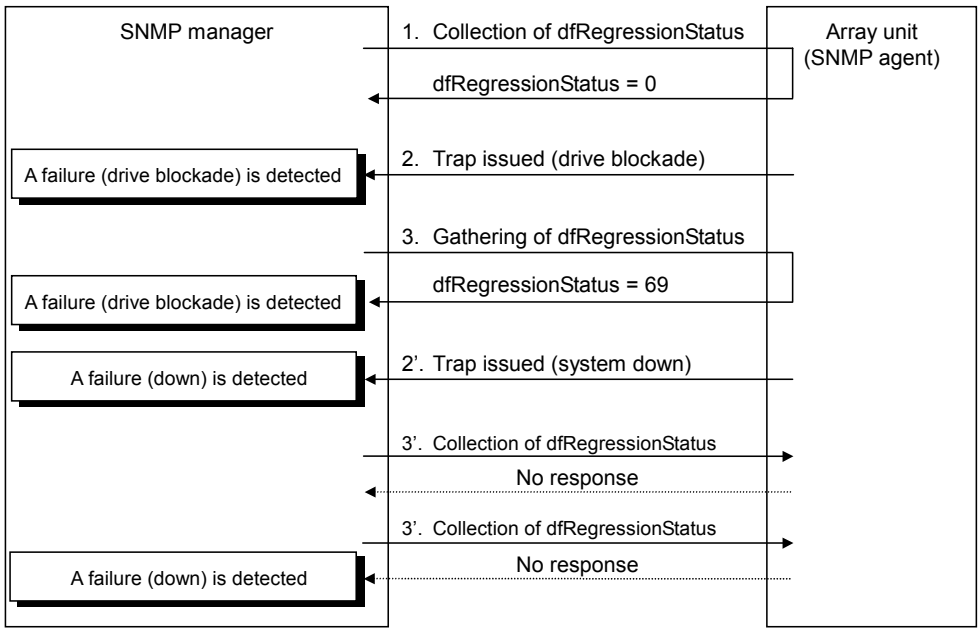


Figure 5.11 SNMP Manager TRAP Response Failure Detection

Chapter 6 Management Information Bases

This chapter includes the following:

- Supported MIBs (section 6.1)
- MIB Access Mode (section 6.2)
- Object Identifier Assignment System (section 6.3)
- Types of Supported Traps and Trap Issuing Opportunities (section 6.4)

6.1 Supported MIBs

The subsystem supports only the Management Information Bases (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		Supported?	Relevant Document	Applicable Section
1	MIB II			RFC1213	—
		system group	Yes		See section 7.1.1.
		interface group	Partially		See section 7.1.2.
		at group	No		See section 7.1.3.
		ip group	Partially		See section 7.1.4.
		icmp group	No		See section 7.1.5.
		tcp group	No		See section 7.1.6.
		udp group	No		See section 7.1.7.
		egp group	No		See section 7.1.8.
		snmp group	Yes		See section 7.1.9.
2	Extended MIB		Yes	—	See section 7.2.

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.

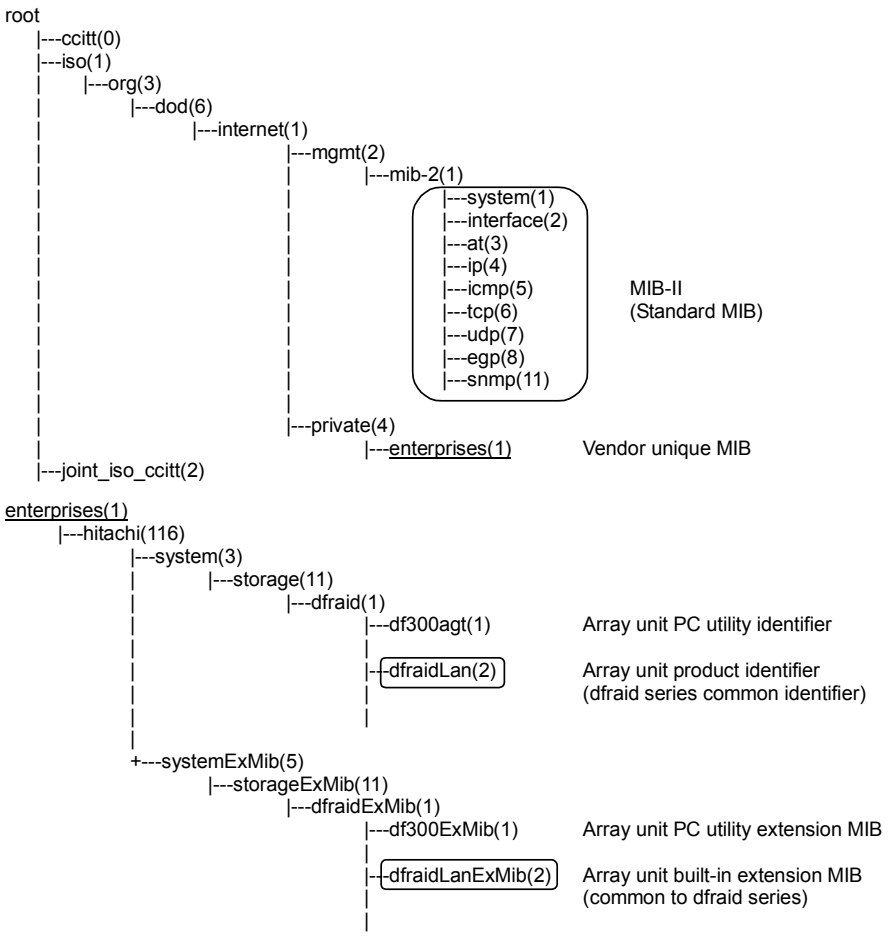


Figure 6.1 The Object Identifier Assignment System (Frame 1 of 3)

```
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
    |
    ├──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
    |
  Continue to the next page (1)
```

Note: The dfCacheLoadCondition(4) and dfLUNS(5) are set as 0 (zero).

Figure 6.1 The Object Identifier Assignment System (Frame 2 of 3)

Continued from the previous page (1)

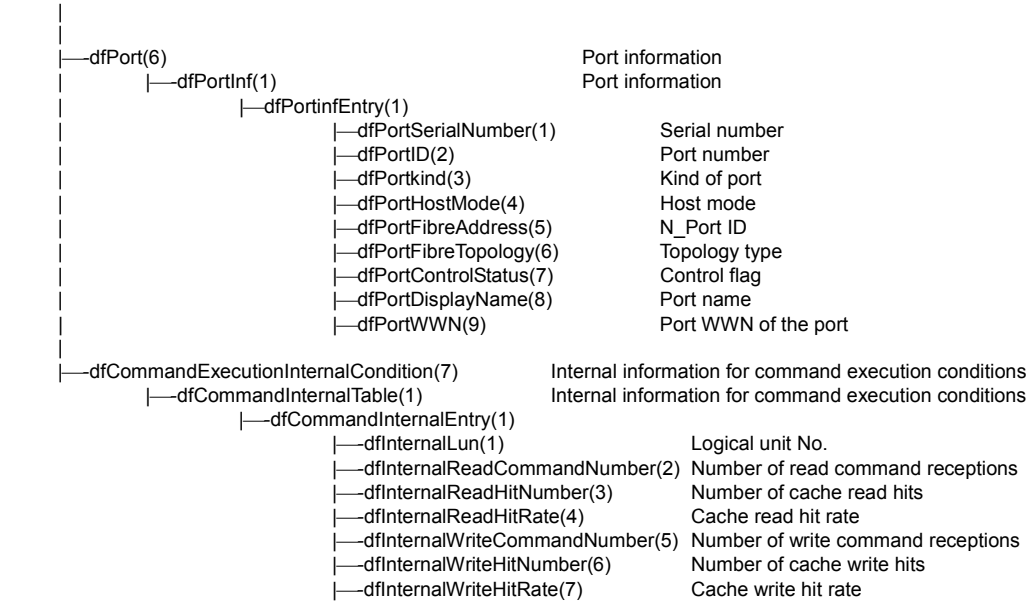


Figure 6.1 The Object Identifier Assignment System (Frame 1 of 3)

6.4 Types of Supported Traps and Trap Issuing Opportunities

Table 6.2 lists standard traps the SNMP agent supports, and Table 6.3 lists extended traps.When the disk array subsystem is used as a local subsystem of TrueCopy or TCE, both paths are blocked following a restart of the remote disk array subsystem and TRAPs are issued. If the local disk array subsystem is started or restarted before the remote disk array subsystem becomes ready, both paths are blocked and TRAPs are issued.

Table 6.2 Supported Standard Traps

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

Table 6.3 Supported Extended Traps

No.	Specific Trap Code	Meaning
1	1	System down occurred. (See ***Note 1***)
2	2	Drive blocking occurred.
3	3	Fan failure occurred.
4	4	Power supply failure occurred.
5	5	Battery failure occurred.
6	6	Cache memory failure occurred.
7	7	UPS failure occurred.
8	9	Cache backup circuit failure occurred.
9	10	Other controller failure occurred. (See ***Note 1***)
10	11	Warning occurred. (See ***Note 2***)
11	12	Spare drive failure occurred.
12	13	Microprogram replacement executed.
13	14	Enclosure controller failure occurred.
14	15	Loop failure occurred.
15	16	Path failure occurred.
16	17	SATA Drive blocking occurred.
17	18	SATA Spare drive failure occurred.
18	19	SENC failure occurred.
19	20	Host connector failure occurred.
20	203	NNC warning occurred.

Note 1: When a controller blockade occurs, the subsystem issues TRAPs that show the blockade. The controller blockade may recover automatically depending on the cause of the failure.

Note 2: The warning status of the subsystem can be automatically set in the warning information by preventive maintenance, periodic part replacement or a fieldwork of the service personnel.

Chapter 7 MIB Installation Specifications

This chapter provides installation specifications for management information bases (MIBs) supported by the subsystem. The following conventions are used in 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 subsystem.
- Supported status: Can be **Yes**, **Partial**, or **No**.

This chapter includes the following:

- MIB II (section 7.1)
- Extended MIBs (section 7.2)

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	Supported?	Remarks
1	sysDescr {system 1}	R	[Standard] Name or version No. of hardware, OS, network OS [Installation] Fixed character string (Fibre connection for DF700): HITACHI DF600F Verxxxxxxxx (Same as inquiry information)	Yes	
2	sysObjectID {system 2}	R	[Standard] Object ID indicating the agent vendor product identification number [Installation] Value is fixed. 1.3.6.4.1.116.3.11.1.2	Yes	
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.	Yes	
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).	Yes	Should be Read_Only in the subsystem. Data should be entered from the operation environment setting file.
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).	Yes	Should be Read_ Only in the subsystem. 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).	Yes	Should be Read_ Only in the subsystem. Data should be entered from the operation environment setting file.
7	sysServices {system 7}	R	[Standard] Service value [Installation] Value is fixed as 8.	Yes	

7.1.2 interfaces Group

interfaces OBJECT IDENTIFIER : = {mib-2 2}

Table 7.2 interfaces Group

No.	Object Identifier	Access	Specifications for Installation	Supported?	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.)	Partially	
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.)	Partially
2.1.1	ifIndex {ifEntry 1}	R	[Standard] Interface identification number. [Installation] Value is fixed as 1.	Yes	(index)
2.1.2	ifDescr {ifEntry 2}	R	[Standard] Interface information [Installation] Fixed character string for each interface type. Ethernet 100BaseT	Yes	
2.1.3	ifType {ifEntry 3}	R	[Standard] Interface type ID number [Installation] Fixed value.ethernetCsmacd	Yes	
2.1.4	ifMtu {ifEntry 4}	R	[Standard] Maximum sendable/receivable frame length in bytes. MTU (Max Transfer Unit) value [Installation] - (Not installed)	No	
2.1.5	ifSpeed {ifEntry 5}	R	[Standard] Transfer rate in units of bit/s. [Installation] - 100000000	Yes	
2.1.6	ifPhysAddress {ifEntry 6}	R	[Standard] Interface physical address [Installation] - Mac Address	Yes	
2.1.7	ifAdminStatus {ifEntry 7}	RW	[Standard] Interface set status 1 = Operation, 2 = Stop, 3 = Test [Installation] - (Not installed)	No	
2.1.8	ifOperStatus {ifEntry 8}	R	[Standard] Current interface status 1 = Operating, 2 = Stopped, 3 = Testing [Installation] - (Not installed)	No	
2.1.9	ifLastChange {ifEntry 9}	R	[Standard] sysUpTime assumed when the subject interface ifOperStatus is changed last [Installation] - (Not installed)	No	
2.1.10	ifInOctets {ifEntry 10}	R	[Standard] Total number of bytes (including synchronous bytes) in the frame received by the subject interface	No	

			[Installation] - (Not installed)		
2.1.11	ifInUcastPkts {ifEntry 11}	R	[Standard] Number of subnetwork unicast packets reported to the host protocol [Installation] - (Not installed)	No	
2.1.12	ifInNUcastPkts {ifEntry 12}	R	[Standard] Number of broadcast or multicast packets reported to the host protocol [Installation] - (Not installed)	No	
2.1.13	ifInDiscards {ifEntry 13}	R	[Standard] Number of received packets discarded due to insufficient buffer space, even if normal [Installation] - (Not installed)	No	
2.1.14	ifInErrors {ifEntry 14}	R	[Standard] Number of received erred packets [Installation] (Not installed)	No	
2.1.15	ifInUnknownProtos {ifEntry 15}	R	[Standard] Number of received packets discarded due to incorrect or unsupported protocol [Installation] - (Not installed)	No	
2.1.16	ifOutOctets {ifEntry 16}	R	[Standard] Total number of bytes (including synchronizing characters) in transmitted frames [Installation] - (Not installed)	No	
2.1.17	ifOutUcastPkts {ifEntry 17}	R	[Standard] Number of packets (including those not sent) requested unicast from the upper layer [Installation] - (Not installed)	No	
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)	No	
2.1.19	ifOutDiscards {ifEntry 19}	R	[Standard] Number of packets discarded due to insufficient transmit buffer space, etc. [Installation] - (Not installed)	No	
2.1.20	ifOutErrors {ifEntry 20}	R	[Standard] Number of packets not sent due to errors. [Installation] - (Not installed)	No	
2.1.21	ifOutQLen {ifEntry 21}	R	[Standard] Sent frame queue length (indicated in number of packets) [Installation] - (Not installed)	No	
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.	Yes	

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	Supported?	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)	No	
2	ipDefaultTTL {ip 2}	R	[Standard] Default value to be set in TTL (Time to live: packet life) in IP header. [Installation] - (Not installed)	No	
3	ipInReceives {ip 3}	R	[Standard] Total number of received IP packets, including erred ones [Installation] - (Not installed)	No	
To 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)	No	
5	ipInAddrErrors {ip 5}	R	[Standard] Number of packets discarded, since the address in IP header is illegal. [Installation] - (Not installed)	No	
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)	No	
7	ipInUnknownProtos {ip 7}	R	[Standard] Number of discarded packets of received IP packets due to unknown or unsupported protocol. [Installation] - (Not installed)	No	
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)	No	
9	ipInDelivers {ip 9}	R	[Standard] Number of packets transferred to an IP user protocol (host protocol including ICMP) [Installation] - (Not installed)	No	
10	ipOutRequests	R	[Standard] Number of IP packets	No	

	{ip 10}		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)	No	
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)	No	
13	ipReasmTimeout {ip 13}	R	[Standard] Maximum time waiting for all IP packets to be assembled when receiving fragmented IP packets. [Installation] - (Not installed)	No	
14	ipReasmReqds {ip 14}	R	[Standard] Number of received fragmented IP packets to be assembled with an entity. [Installation] - (Not installed)	No	
15	ipReasmOKs {ip 15}	R	[Standard] Number of fragmented IP packets received and assembled successfully [Installation] - (Not installed)	No	
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)	No	
17	ipFragOKs {ip 17}	R	[Standard] Number of packets fragmented successfully with this entity [Installation] - (Not installed)	No	
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)	No	
19	ipFragCreates {ip 19}	R	[Standard] Number of fragmented IP packets created by the fragment with this entity. [Installation] - (Not installed)	No	
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.)	Yes	
20.1	ipAddrEnry {ipAddrTable 1}	Impossible	[Standard] IP address information [Installation] Same as standard. (Refer to the lower hierarchical level.)	Yes	

20.1.1	ipAdEntAddr {ipAddrEntry 1}	R	[Standard] IP address of this entity [Installation] Same as standard. A system parameter set by users.	Yes	(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.	Yes	
20.1.3	ipAdEntNetMask {ipAddrEntry 3}	R	[Standard] Subnetwork mask value related to this IP address. [Installation] Same as standard.	Yes	
20.1.4	ipAdEntBcastAddr {ipAddrEntry 4}	R	[Standard] LSB value of IP broadcast address when IP broadcast sending. [Installation] Value is fixed as 1.	Yes	
20.1.5	ipAdEntReasmMax-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.	Yes	
21	ipRouteTable {ip 21}	Impossible	[Standard] IP routing table of this entity [Installation] - (Not installed)	No	
21.1	ipRouteEntry {ipRouteTable 1}	Impossible	[Standard] Route to a specific destination [Installation] - (Not installed)	No	
21.1.1	ipRouteDest {ipRouteEntry 1}	RW	[Standard] Destination IP address of this route table [Installation] - (Not installed)	No	(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)	No	
21.1.3	ipRouteMetric1 {ipRouteEntry 3}	RW	[Standard] Primary routing metric of this route [Installation] - (Not installed)	No	
21.1.4	ipRouteMetric2 {ipRouteEntry 4}	RW	[Standard] Alternate routing metric [Installation] - (Not installed)	No	
21.1.5	ipRouteMetric3 {ipRouteEntry 5}	RW	[Standard] Alternate routing metric [Installation] - (Not installed)	No	
21.1.6	ipRouteMetric4 {ipRouteEntry 6}	RW	[Standard] Alternate routing metric [Installation] - (Not installed)	No	
21.1.7	ipRouteNextHop {ipRouteEntry 7}	RW	[Standard] Next hop IP address of this route [Installation] - (Not installed)	No	
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)	No	
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	No	

			[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)	No	
21.1.11	ipRouteMask {ipRouteEntry 11}	RW	[Standard] Subnet mask value [Installation] - (Not installed)	No	
21.1.12	ipRouteMetric5 {ipRouteEntry 12}	RW	[Standard] Alternate routing metric [Installation] - (Not installed)	No	
21.1.13	ipRouteInfo {ipRouteEntry 13}	R	[Standard] Defined number of the MIB for the routing protocol used for this route. [Installation] - (Not installed)	No	
22	ipNetToMediaTable {ip 22}	Impossible	[Standard] IP address conversion table used to convert IP addresses to physical addresses. [Installation] - (Not installed)	No	
22.1	ipNetToMediaEntry {ipNetToMedia-Table 1}	Impossible	[Standard] Entry including an IP address corresponding to a physical address. [Installation] - (Not installed)	No	
22.1.1	ipNetToMediaIf-Index {ipNetToMedia-Entry 1}	RW	[Standard] Interface identification number of this entry. The ifIndex value is used. [Installation] - (Not installed)	No	(index)
22.1.2	ipNetToMedia-PhysAddress {ipNetToMedia-Entry 2}	RW	[Standard] Physical address depending on medium [Installation] - (Not installed)	No	
22.1.3	ipNetToMedia-NetAddress {ipNetToMedia-Entry 3}	RW	[Standard] P address corresponding to the physical address of this entry. [Installation] - (Not installed)	No	(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)	No	
23	ipRoutingDiscards {ip 23}	R	[Standard] Total of valid routing information items discarded due to insufficient memory space, etc. [Installation] - (Not installed)	No	

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	Supported?	Remarks
1	snmpInPkts {snmp 1}	R	[Standard] Total of SNMP messages received from a transport service. [Installation] Same as standard.	Yes	
2	snmpOutPkts {snmp 2}	R	[Standard] Total of SNMP messages requested to be transferred to the transport layer. [Installation] Same as standard.	Yes	
3	snmpInBad-Versions{snmp 3}	R	[Standard] Total of received messages of an unsupported version. [Installation] Same as standard.	Yes	
4	snmpInBad-CommunityNames {snmp 4}	R	[Standard] Total of received SNMP messages of an unused community. [Installation] Same as standard.	Yes	
5	snmpInBad-CommunityUses {snmp 5}	R	[Standard] Total of received messages indicating operation disabled for the community. [Installation] Same as standard.	Yes	
6	snmpInASNParse-Errs {snmp 6}	R	[Standard] Total of received messages of ASN.1 error [Installation] Same as standard.	Yes	
8	snmpInTooBigs {snmp 8}	R	[Standard] Total of received PDUs of tooBig error status. [Installation] Same as standard.	Yes	
9	snmpInNoSuchNames {snmp 9}	R	[Standard] Total of received PDUs of noSuchName error status. [Installation] Same as standard.	Yes	
10	snmpInBadValues {snmp 10}	R	[Standard] Total of received PDUs of badValue error status. [Installation] Same as standard.	Yes	
11	snmpInReadOnlys {snmp 11}	R	[Standard] Total of received PDUs with readOnly error status. [Installation] Same as standard.	Yes	
12	snmpInGenErrs {snmp 12}	R	[Standard] Total of received PDUs with genErr error status. [Installation] Same as standard.	Yes	
13	snmpInTotalReq-Vars {snmp 13}	R	[Standard] Total of MIB objects for which MIB was gathered successfully. [Installation] Same as standard.	Yes	
14	snmpInTotalSet-Vars {snmp 14}	R	[Standard] Total of MIB objects for which MIB was set successfully. [Installation] Same as standard.	Yes	
15	snmpInGetRequests {snmp 15}	R	[Standard] Total of received GetRequest PDUs. [Installation] Same as standard.	Yes	
16	snmpInGetNexts {snmp 16}	R	[Standard] Total of received GetNext Request PDUs. [Installation] Same as standard.	Yes	

17	snmpInSetRequests {snmp 17}	R	[Standard] Total of received SetRequest PDUs. [Installation] Same as standard.	Yes	
18	snmpInGet-Responses {snmp 18}	R	[Standard] Total of received GetResponse PDUs. [Installation] Same as standard.	Yes	
19	snmpInTraps {snmp 19}	R	[Standard] Total of received TrapPDUs. [Installation] Same as standard.	Yes	
20	snmpOutTooBigs {snmp 20}	R	[Standard] Total of transferred PDUs of tooBig error status. [Installation] Same as standard.	Yes	
21	snmpOutNoSuch-Names {snmp 21}	R	[Standard] Total of transferred PDUs of noSuchName error status. [Installation] Same as standard.	Yes	
22	snmpOutBadValues {snmp 22}	R	[Standard] Total of transferred PDUs of badValue error status. [Installation] Same as standard.	Yes	
24	snmpOutGenErrs {snmp 24}	R	[Standard] Total of received PDUs of genErr error status. [Installation] Same as standard.	Yes	
25	snmpOutGet-Requests {snmp 25}	R	[Standard] Total of transferred GetRequest PDUs. [Installation] Same as standard.	Yes	
26	snmpOutGetNexts {snmp 26}	R	[Standard] Total of transferred GetNextRequest PDUs. [Installation] Same as standard.	Yes	
27	snmpOutSet-Requests {snmp 27}	R	[Standard] Total of transferred SetRequest PDUs. [Installation] Same as standard.	Yes	
28	snmpOutGet-Responses {snmp 28}	R	[Standard] Total of transferred GetResponse PDUs. [Installation] Same as standard.	Yes	
29	snmpOutTraps {snmp 29}	R	[Standard] Total of transferred Trap PDUs. [Installation] Same as standard.	Yes	
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)	Yes	Should be Read-Only in subsystem.

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	Supported?	Remarks
1	dfSystemProductName {dfSystemParameter 1}	R	[Content] Product name [Installation] (DF700): HITACHI DF600F (Same as inquiry information)	Yes	
2	dfSystemMicro-Revision {dfSystemParameter 2}	R	[Content] Microprogram revision number [Installation] Same as above	Yes	
3	dfSystemSerialNumber {dfSystemParameter 2}	R	[Content] Disk array serial number [Installation] Eight digits of the manufacturing serial number	Yes	

7.2.2 dfWarningCondition Group

dfWarningCondition OBJECT IDENTIFIER : = {dfraidLanExMib 2}

Table 7.6 dfWarningCondition Group

Object identifier	Access	Specifications for installation
dfRegressionStatus {dfWarningCondition 1}	R	[Content] Warning error information [Installation] Same as above. When normal, this is assigned to 0 (see ***Note 1***).
dfPreventiveMainte-nanceInformation {dfWarningCondition 2}	R	[Content] Drive preventive maintenance information [Installation] Same as above. Value is fixed as 0.
dfWarningReserve1 {dfWarningCondition 3}	R	[Content] Reserved area [Installation] Not used. Value is fixed as 0.
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.

Table 7.7 dfRegressionStatus Format

Bit/Byte	7	6	5	4	3	2	1	0
0	0	0	NNC Warning	Host Connector	SENC	SATA D-Drive	SATA S-Drive	Cache
1	0	0	0	Fan	BK	0	DC PS	Battery
2	0	0	0	0	0	Path	Loop	UPS
Home 3	CTL	Warning	0	0	ENC	D-Drive	S-Drive	Drive

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

Table 7.8 shows this object value for each failure status.

Table 7.8 dfRegressionStatus Value for Each Failure

Bit Position		Object Value (Decimal)	Failed Component
Byte	Bit		
		0	Array unit normal status
3	0	1	Drive blockade
3	1	2	Drive (spare drive) blockade
3	2	4	Drive (data drive) blockade
3	3	8	ENC alarm
3	6	64	Warned array unit
3	7	128	Mate controller blockade
2	0	256	UPS alarm
2	1	512	Loop alarm
2	2	1024	Path blockade
1	0	65536	Battery alarm
1	1	131072	DC power supply failure
1	3	524288	Battery charging circuit alarm
1	4	1048576	Fan alarm
0	0	16777216	Cache partial blockade
0	1	33554432	SATA drive (spare drive) blockade
0	2	67108864	SATA drive (data drive) blockade
0	3	134217718	SENC alarm
0	4	268435456	Host connector alarm
0	5	536870912	NNC warning

Note: If the “Drive” bit is On, the “D-Drive”, “S-Drive”, “SATA D-Drive”, or “SATA 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 Table 7.7.

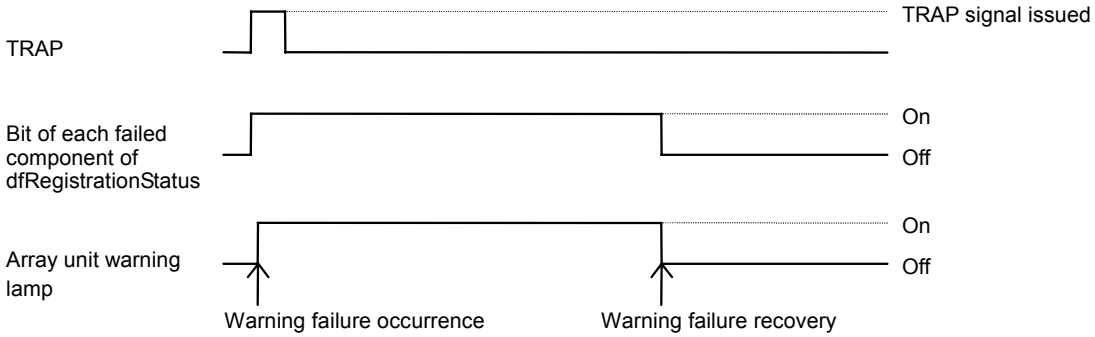


Figure 7.1 Relationship between Traps and dfWarningCondition Groups

Each of the TRAP signals (specific trap code 2 to 6) is issued each time a warning failure in related component occurs (Figure 7.1).

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 7.9 dfCommandExecutionCondition Group

No.	Object identifier	Access	Specifications for installation	Supported	Remarks
1	dfCommandTable {dfCommandExecutionCondition 1}	Impossible	[Content] Command execution condition table [Installation] Same as above (Refer to the lower hierarchical level)	Yes	
1.1	dfCommandEntry {dfCommandTable 1}	Impossible	[Content] Command execution condition entry [Installation] Same as above (Refer to the lower hierarchical level)	Yes	
1.1.1	dfLun {dfCommandEntry 1}	R	[Content] Logical unit number [Installation] Same as above (AMS200/WMS100: 0 to 511, AMS500: 0 to 2,047, AMS1000: 0 to 4,095)	Yes	(index)
1.1.2	dfReadCommandNumber {dfCommandEntry 2}	R	[Content] Number of read command receptions [Installation] Same as above	Yes	
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	Yes	
1.1.4	dfReadHitRate {dfCommandEntry 4}	R	[Content] Cache read hit rate (%) [Installation] (Number of cache read hits / Number of read command receptions) x 100	Yes	
1.1.5	dfWriteCommandNumber {dfCommandEntry 5}	R	[Content] Number of write command receptions [Installation] Same as above	Yes	
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	Yes	
1.1.7	dfWriteHitRate {dfCommandEntry 7}	R	[Content] Cache write hit rate (%) [Installation] Number of cache write hits / Number of write command receptions) x 100	Yes	

Note 1: The information of this group is updated every 10 seconds. The value accumulated in the previous ten seconds is set (Figure 7.2).

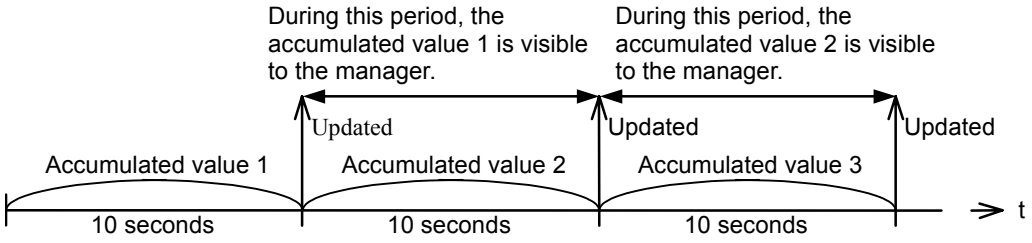


Figure 7.2 Accumulated Values Over Time

Note 2: The dfCommandExecutionCondition group is updated every 10 seconds and is set to a value accumulated for individual 10 seconds. This interval time of 10 seconds may vary within an error span, depending upon 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 is 11 seconds, and the accumulated number of read command received for that time is 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 Size Expansion (LUSE) is being used, this group indicates information of the unified LUs.

7.2.4 dfPort Group

dfPort OBJECT IDENTIFIER : = {dfraidLanExMib 4}

Table 7.10 dfPort Group

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

Note 1: Port Numbers

Table 7.11 Port Display Numbers

Port No.	Controller No.	Fibre	Notes
0	0	0A	
1		0B	AMS200/WMS100 is not applicable (The 4 G bps fibre I/F board is not installed).
2		0C	AMS200/WMS100/AMS500 is not applicable.
3		0D	AMS200/WMS100/AMS500 is not applicable.
4	1	1A	
5		1B	AMS200/WMS100 is not applicable. (The 4 G bps fibre I/F board is not installed)
6		1C	AMS200/WMS100/AMS500 is not applicable.
7		1D	AMS200/WMS100/AMS500 is not applicable.

Note 2: On port types:

- Sets “Fibre” “NAS”, or “iSCSI”.
- For ports other than those that are not applicable, “None” is set.
- The item of the ports of a blocked controller is “None.”

Note 3: 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.

Note 4: The item of the ports of a blocked controller is “None.”

Note 5: 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 7.12 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	—	—

Note 6: Topology information:

Table 7.13 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

Note 7: Port Display Names:

Table 7.14 Topology Information for Ports other than Fibre-Oriented

Value	Meaning
5	Not Fibre

Table 7.15 Port Display Names

Port No.	Controller No.	Fibre	Notes
0	0	"0A"	
1		"0B"	AMS200/WMS100 is "None"(the 4 G bps fibre I/F board is not installed)
2		"0C"	AMS200/WMS100/AMS500 is "None"
3		"0D"	AMS200/WMS100/AMS500 is "None"
4	1	"1A"	
5		"1B"	AMS200/WMS100 is "None" (the 4 G bps fibre I/F board is not installed)
6		"1C"	AMS200/WMS100/AMS500 is "None"
7		"1D"	AMS200/WMS100/AMS500 is "None"

Note 8: For port WWN:

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

7.2.5 dfCommandExecutionInternalCondition Group

dfCommandExecutionInternalCondition OBJECT IDENTIFIER : = {dfraidLanExMib 5}

Table 7.16 dfCommandExecutionInternalCondition Group

No.	Object identifier	Access	Specifications for installation	Supported?	Remarks
1	dfCommandInternalTable {dfCommandExecutionCondition 1}	Impossible	[Content] Command execution condition table [Installation] Same as above (Refer to the lower hierarchical level)	Yes	
1.1	dfCommandInternalEntry {dfCommandTable 1}	Impossible	[Content] Command execution condition entry [Installation] Same as above (Refer to the lower hierarchical level)	Yes	
1.1.1	dfInternalLun {dfCommandEntry 1}	R	[Content] Logical unit number [Installation] Same as above (AMS200/WMS100: 0 to 511, AMS500: 0 to 2,047, AMS1000: 0 to 4,095)	Yes	(Index)
1.1.2	dInternalfReadCommandNumber {dfCommandEntry 2}	R	[Content] Number of read command receptions [Installation] Same as above	Yes	
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	Yes	
1.1.4	dfInternalReadHitRate {dfCommandEntry 4}	R	[Content] Cache read hit rate (%) [Installation] (Number of cache read hits / Number of read command receptions) x 100	Yes	
1.1.5	dfInternalWriteCommandNumber {dfCommandEntry 5}	R	[Content] Number of write command receptions [Installation] Same as above	Yes	
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	Yes	
1.1.7	dfInternalWriteHitRate {dfCommandEntry 7}	R	[Content] Cache write hit rate (%) [Installation] Number of cache write hits / Number of write command receptions) x 100	Yes	

Note 1: The dfCommandExcutionInternalCondition group indicates the information of the internal logical units of the subsystem. If the LUN Size Expansion (LUSE) 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 through 3 at the end of Table 7.8.

Chapter 8 Troubleshooting

If you need to call the Hitachi Data Systems Technical Support Center, be sure to provide as much information about the problem as possible. Include the circumstances surrounding the error failure and the exact content of any error codes and/or messages displayed. The worldwide Hitachi Data Systems Technical Support Centers are:

- Hitachi Data Systems North America/Latin America
  San Diego, California, USA
  1-800-446-0744
- Hitachi Data Systems Europe
  Contact Hitachi Data Systems Local Support
- Hitachi Data Systems Asia Pacific
  North Ryde, Australia
  61-2-9325-3300

Appendix A Operations Using CLI

This appendix describes the following operation procedure for SNMP Agent Support Function using the CLI of the Navigator. The following sections are included:

- Installing (section A.1)
- Uninstalling (section A.2)
- Enabling or Disabling (section A.3)
- Registering or Referencing SNMP Environment Information (section A.4)

Note: When the Microprogram revision of the subsystem is less than 3.1A, or the Storage Navigator version is earlier than 3.10: Performing the setting enable/disable or registering SNMP environmental information in the case where the disk array subsystem is used on the remote side of TrueCopy, the following phenomena occur with the restart of the disk array subsystem.

- Both paths of TrueCopy are blocked.
- When the pair status of TrueCopy is PAIR or COPY, it is changed to PSUE.

When restarting the disk array subsystem necessarily, perform the setting enable/disable or registering SNMP environmental information after changing the pair status of TrueCopy to PSUS.

Note: If you install, uninstall, enable, or disable the SNMP on a subsystem connected to a NAS, you must also stop the clusters between NAS units. When restarting the subsystem, you must restart the clusters.

A.1 Installing

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

The SNMP Agent Support Function is installed and uninstalled using the Navigator.

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

- When the Microprogram revision of the subsystem is 3.1A or later:

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

Example 1:
Navigator version is 5.00 or later and Cache Partition Manager is enabled

```
% auopt -unit subsystem-name -lock off -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to install the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be e
nabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is installed successfully.
%
```

Example 2:
Navigator version is 3.10 to 4.05 and Cache Partition Manager is enabled

```
% auopt -unit subsystem-name -lock off -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to unlock the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be e
nabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is unlocked.
%
```

Example 3:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name          Type       Term     Status
SNMP-AGENT           Permanent  ---      Enable
%
```

- When the Microprogram revision of the subsystem is less than 3.1A:

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

Example 1:

Navigator version is 3.00 to 3.10 and Cache Partition Manager is enabled

```
% auopt -unit subsystem-name -lock off -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to unlock the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be e
nabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is unlocked.
Restart the subsystem to apply the setting.
The subsystem stops accepting 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
When using the TrueCopy, restart of the remote subsystem will cause both
TrueCopy paths failure. And when TrueCopy pair status is "PAIR" or "COPY",
TrueCopy pair status will be changed to "PSUE".
Do you want to continue processing? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required 4 - 15min.
The subsystem restarted successfully.
%
```

Example 2:

Navigator version is less than 3.00 and Cache Partition Manager is enabled

```
% auopt -unit subsystem-name -lock off -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to unlock the option? (y/n [n]): y
The option is unlocked.
Restart the subsystem to apply the setting.
The subsystem stops accepting 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
When using the TrueCopy, restart of the remote subsystem will cause both
TrueCopy paths failure. And when TrueCopy pair status is "PAIR" or "COPY",
TrueCopy pair status will be changed to "PSUE".
Do you want to continue processing? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required 4 - 15min.
The subsystem restarted successfully.
%
```

Example 3:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name  Type       Term     Status
SNMP-AGENT   Permanent  ---      Enable
%
```

Note: To validate the installing of this optional feature, restart the subsystem. The previous setting stays valid until restarting. The subsystem cannot access the host until the restart is completed, make sure the host has stopped accessing data before beginning the restart process.

Note: It may take up to 15 minutes for a subsystem to respond, depending upon the configuration of the subsystem.

A.2 Uninstalling

The following steps describe SNMP Agent Support Function uninstallation using the CLI version of the Navigator:

- When the Microprogram revision of the subsystem is 3.1A or later:

1. From the command prompt, register the subsystem in which you will uninstall the SNMP Agent Support Function feature. Connect to the subsystem.
2. Uninstall the optional features by using the either of the following examples:

Example 1:

Navigator: Version 5.00 or later

```
% auopt -unit subsystem-name -lock on -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to de-install the option? (y/n[n]): y
The option is de-installed successfully.
%
```

Example 2:

Navigator: Less than 5.00 version

```
% auopt -unit subsystem-name -lock on -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to lock the option? (y/n[n]): y
The option is locked.
%
```

Example 3:

```
% auopt -unit subsystem-name -lock on -keycode manual-attached-keycode
Password: manager-password
DMEC002015: No information displayed.
%
```

- When the Microprogram revision of the subsystem is less than 3.1A:

1. From the command prompt, register the subsystem in which you will uninstall the SNMP Agent Support Function feature. Connect to the subsystem.
2. Uninstall the optional features by using the either of the following examples:

Example 1:

```
% auopt -unit subsystem-name -lock on -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to lock the option? (y/n[n]): y
The option is locked.
Restart the subsystem to apply the setting.
The subsystem stops accepting 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
When using the TrueCopy, restart of the remote subsystem will cause both
TrueCopy paths failure. And when TrueCopy pair status is "PAIR" or "COPY",
TrueCopy pair status will be changed to "PSUE".
Do you want to continue processing? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required 4 - 15min.
The subsystem restarted successfully.
%
```

Example 2:

```
% auopt -unit subsystem-name -lock on -keycode manual-attached-keycode
Password: manager-password
DMEC002015: No information displayed.
%
```

Notes:

- To validate optional feature uninstalling, restart the subsystem. The previous setting will stay valid until restarting. The subsystem cannot access the host until restart is completed.
- Make sure that the host has stopped accessing data before beginning the restart process.

A.3 Enabling or Disabling

The SNMP Agent Support Function can be enabled or disabled without uninstallation. The following instructions describe how to enable or disable it without uninstallation using the CLI version of the Navigator.

- When the Microprogram revision of the subsystem is 3.1A or later, and Navigator version is 3.10 or later:

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

To change the status from **disable** to **enable**, enter "enable" after the **-st** option, and see the following examples:

Example 1:

```
% auopt -unit subsystem-name -option SNMP-AGENT -st disable
Password: manager-password
Are you sure you want to disable the option? (y/n[n]): y
The option has been set successfully.
%
```

Example 2:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name  Type       Term     Status
SNMP-AGENT   Permanent  ---      Disable
%
```

- When the Microprogram revision of the subsystem is less than 3.1A, or the Storage Navigator version is earlier than 3.10:

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

To change the status from **disable** to **enable**, enter "enable" after the **-st** option, and see the following examples:

Example 1:

```
% auopt -unit subsystem-name -option SNMP-AGENT -st disable
Password: manager-password
Are you sure you want to disable the option? (y/n[n]): y
The option has been set successfully.
Restart the subsystem to apply the setting.
The subsystem stops accepting 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
When using the TrueCopy, restart of the remote subsystem will cause both
TrueCopy paths failure. And when TrueCopy pair status is "PAIR" or "COPY",
TrueCopy pair status will be changed to "PSUE".
Do you want to continue processing? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required 4 - 15min.
The subsystem restarted successfully.
%
```

Example 2:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name  Type       Term     Status
SNMP-AGENT   Permanent  ---      Disable
%
```

This setting is not active until the system is restarted. The subsystem cannot access the host until the restart completes.

Important Note: Make sure the host has stopped accessing data before beginning the restart process. It may take up to 15 minutes for a subsystem to respond depending upon the configuration of the subsystem.

A.4 Registering or Referencing SNMP Environment Information

A.4.1 Registering

- When the Microprogram revision of the subsystem is 3.1A or later, and Navigator version is 3.10 or later:

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

```
%  ausnmp -unit subsystem-name -set -config config.txt -name name.txt
Password: manager-password
The SNMP environment information has been set successfully.
%
```

- When the Microprogram revision of the subsystem is less than 3.1A, or the Storage Navigator version is earlier than 3.10:

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

```
%  ausnmp -unit subsystem-name -set -config config.txt -name name.txt
Password: manager-password
The SNMP environment information has been set successfully.
Restart the subsystem to apply the setting.
The subsystem stops accepting 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
When using the TrueCopy, restart of the remote subsystem will cause both
TrueCopy paths failure. And when TrueCopy pair status is "PAIR" or "COPY",
TrueCopy pair status will be changed to "PSUE".
Do you want to continue processing? (y/n [n]): y
Now restarting the subsystem. Start Time HH:MM:SS Time Required 4 - 15min.
The subsystem restarted successfully.
%
```

A.4.2 Referencing

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

```
% ausnmp -unit subsystem-name -get -config config.txt -name name.txt
Password: manager-password
Are you sure you want to save the SNMP environment information to the file? (y/n
 [n]): y
The SNMP environment information has been saved to the file successfully.
%
```

Acronyms and Abbreviations

CLI	command line interface
DHCP	dynamic host configuration protocol
GUI	graphical user interface
iSCSI	Internet SCSI
LU	logical unit
LUN	logical unit number
LUSE	LUN size expansion
MIB	management information base
MIB	(alternate meaning) message information block
MIB-II	management information base (updated)
NAS	network attached storage
NNC	NAS node controller
SATA	Serial ATA
SNMP	simple network management protocol
UDP	user datagram protocol
WS	workstation

Glossary

Cache

Cache is a temporary, high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are found in computers: memory caching and disk caching. Memory caches are built into the architecture of microprocessors and often computers have external cache memory. Disk caching works like memory caching; however, it uses slower, conventional main memory that on some devices is called a memory buffer.

Configuration

Configuration for hardware involves setting various switches and jumpers. For software it means defining the values of parameters. For hardware and software respectively, configuration is the arrangement of the components that make up the system or the set up and set values of the software.

Logical

Logical is used to describe a user's view of the way data or systems are organized. The opposite of logical is physical, which refers to the real organization of a system. A logical description of a file is that it is a quantity of data collected together in one place. The file appears this way to users. Physically, the elements of the file could live in segments across a disk.

Microcode

Microcode is the lowest-level instructions directly controlling a microprocessor. Microcode is generally hardwired and cannot be modified.

Storage Navigator

The TagmaStore Storage Navigator consists of a group of Java™ applet programs that enable users to manage the TagmaStore subsystem. Storage Navigator Java™ applet programs run on a web browser to provide a user-friendly interface for TagmaStore web client functions.

Trap

A program interrupt usually caused by some exceptional situation in a user program. In most cases, the OS performs some action and then returns control to the program.

TrueCopy

The TrueCopy™ feature enables you to create and maintain duplicate copies of all user data stored on a Hitachi TagmaStore™ subsystem for data duplication, backup, and disaster recovery purposes.

Volume

A volume is the basic unit of storage that includes recovery logs and storage pools. A volume can be a logical volume management (LVM) logical volume, a standard file system file, a tape cartridge, or an optical cartridge. The various types of defined volumes include: external, internal, copy source, copy destination, reserve, data, journal, virtual, pool, system, LUSE, copy pair, and USP.

Index

A
at group, 49

C
CONFIG.TXT settings, 28
connections, checking, 24
controller specifications, 2

D
dfCommandExecutionCondition group, 60
dfCommandExecutionInternalCondition group, 66
dfPort group, 62
dfSystemParameter group, 56
dfWarningCondition group, 57
dual systems, using, 2

E
egp group, 53
enable/disable, setting, 25
environmenal setting files, creating, 29
environmental information file, 28
environmental information, referencing, 36
extended MIBs, 56

F
failure, detecting, 38
file format, CONFIG.TXT, 28

I
icmp group, 53
installation, 15
interfaces group, 47
ip group, 49
iSCSI, 63

L
LAN connections, 5

M
MIB access mode, 40
MIB installation, 45
MIB-II, 46
MIBS, supported, 40

N
NAME.TXT file, 32
network connecting functions, 5

O
object identifier assignment system, 41
operation environment setting, 28

P
procedures, operating, 23
processing specifications, 2

R
reporting, hardware failure, 2
request processing, 7, 12

S
SATA, 6, 7
setup procedures, 24
SNMP
  communication, 10
  installing, 16
  uninstalling, 21
SNMP Agent
  overview, 1
SNMP environmental information, registering, 33
SNMP functions, 6
snmp group, 54
SNMP Manager setup, 24
system group, 46

T
tcp group, 53
technical support, 67
trap reporting, 6
trap-issuing, 11
traps, supported, 43
troubleshooting, 67

U
udp group, 53
unit name setting, 32
unit name setting, creating, 32

V
verifying connection, 37