CHAPTER 8

BPX SNMP Agent

This chapter introduces the functions of the Simple Network Management Protocol (SNMP) agent that is embedded in each BPX node. To benefit from this chapter, readers should have a general knowledge of SNMP, IP protocols, and MIBs.

Introduction

An SNMP agent is embedded in each BPX node. (This feature is an addition to and functionally different from the SNMP Proxy Agent that can be used by a non-SV+ workstation to provide access to a MIB on the SV+ workstation which contains data extracted from the SV+ Informix database) The SNMP agent permits an SNMP manager to view and set certain network objects in Management Information Bases (MIBs) that are maintained in each BPX node within a managed network. The embedded SNMP agent supports the standard Internet MIB II, the ATM 3.1 UNI MIB, and a StrataCom proprietary MIB. The StrataCom proprietary MIB contains information necessary to control ports and connections on the switches in the network. The standard Internet MIB II contains MIB modules defined by the IESG (Internet Engineering Steering Group). SNMP support is available on both IPX and BPX switches.

The proprietary MIB is supplied on a tape for compilation into the user's SNMP manager.

SNMP Overview

An SNMP manager manages the SNMP agents in each BPX node in a single domain. To gain access to network nodes, the SNMP manager is connected to one of the BPX nodes through its Ethernet port, which acts as a gateway for the SNMP manager to communicate with all the other BPX nodes in the domain.

In multiple networks, a separate SNMP manager must exist for each network that is being managed. Furthermore, nodes within a multi-network can be managed by multiple SNMP managers. Also, ATM connections that span multiple networks are supported in the SNMP MIB.

Figure 8-1 shows an SNMP manager and the nodes within a domain.

Figure 8-1 SNMP Manager and Agents in a BPX Domain

Communication between the agents and the SNMP manager uses the standard UDP protocol encapsulated within IP protocol. The communication link between the SNMP manager and the directly attached BPX node uses the Ethernet interface of an BCC processor card. The SNMP manager can be either local or remote to the BPX node.

Figure 8-1 illustrates the SNMP manager's communication with the agents in the network. Each node in the domain must have a network IP address assigned by the **cnfnwip** command (see Command Reference Manual for details). The manager uses the network IP address to address an agent in the domain. The directly attached node (Node 4 in Figure 8-1) directs the SNMP message to the addressed BPX node. Responses from the agent go to the directly attached node then pass over the Ethernet link to the SNMP manager.

Note The LAN IP address of the directly attached node must be configured with the **cnflan** command.

SNMP Functions

The SNMP protocol provides a basic query-response model for network management. The network manager has access to Get (Get-Next) and Set functions.

A Get request lets the manager read variables in the BPX. The request consists of a single variable or a list of variables. The BPX database subsequently returns the requested values.

The Get-Next request lets the manager obtain the successor to the given variable's object identifier. The returned object identifier can serve as input to another Get-Next request so the manager can lexicographically walk through the MIB.

A Set request lets the manager modify variables in the BPX. The request consists of either a single variable or a list of variables. The values supplied in the request modify the BPX database. The variables and their associated values in the request message are put into a response message and returned to the requesting management workstation. The format of the Set response message is the same as that of the Get response message.

SNMP requests from the manager have the same access level as non-privileged users. Non-privileged access can be read-only, read-write, or no access. To maintain access control, each Get and Set request is checked for the correct community string. The community string determines the access privileges that a management workstation has. A separate community string exists for Get requests and Set requests.

The node initializes the community strings to no access, so the user must set the strings to the appropriate values. The community strings can be set and displayed by the **cnfsnmp** and **dspsnmp** super-user commands, respectively (see the Super-User Command Reference Manual for details).

Responses to Get, Get-Next, and Set requests are returned in a response packet along with a status field. The status field can be one of the following:

- noError (0) Successful operation.
- tooBig (1) The agent could not fit the results of an operation into a single SNMP message.
- noSuchName (2) The requested operation identified an unknown variable when attempting to modify a variable.
- badValue (3) Requested operation specified an incorrect syntax or value when attempting to modify a variable.
- readOnly (4) Requested operation attempted to modify a variable that, according to the community profile, may not be written. (no longer supported by Standards)
- genErr (5) All other failure responses.

If an error occurs, the appropriate error code is encoded in ASN.1 format and inserted into the response packet.

Note In the sections that follow, user-specified command names are in lower case.

Responses to Get (Get-Next) Requests

When an SNMP manager workstation sends an SNMP Get request packet to a BPX agent, it utilizes the IP protocol for addressing. The request packet can use either a LAN interface for a locally attached management workstation or a network interface for remote access. Each packet is in ASN.1 format, which is suitable for transmission via the UDP protocol. Once it arrives, the packet is decoded to a Protocol Data Unit (PDU). This PDU is the SNMP internal packet structure.

A PDU consists of one or more variables requested by the manager. The PDU's community string is validated for correct access permissions, then the requested variables are collected within an SNMP varbind list for processing.

For each variable in the request message, the agent calls a user-defined test function that makes sure the requested variable exists. If the test confirms the existence of the variable, the agent calls a user-defined get function to gain access to the BPX database for the specified variable. The get function is appropriate for the type of request (Get or Get-Next).

A get function can read either a single scalar value or a single column entry from the database row. The user-defined get-next function provides a way to read a table of unknown elements. The get-next function returns the lexicographically next variable in the table with respect to the next variable. This mechanism lets the manager sequentially retrieve the entire table.

The test and get functions result in a Get response packet. If an error occurs, the appropriate error code is encoded in ASN.1 format and placed in the packet. If no errors occur, the returned values are encoded and placed in the response packet. The response packet goes to the workstation that originated the Get request.

ATM Set Requests

SNMP Set requests support the ATM functions in the following list. Refer to the *Command Reference* for command descriptions.

- Add ATM connection (**addcon**)
- Delete ATM connection (**delcon**)
- Up ATM connection (**upcon**)
- Down ATM connection (**dncon**)
- Modify ATM connection (**cnfrcon**, **cnfcos**, **cnfpref**, **cnfrcon**)
- Test ATM connections (**tstcon**, **tstdelay**)

SNMP Set requests can implement the following BPX commands on ATM ports:

- Up ATM port (**upfrport**)
- Down ATM port (**dnfrport**)
- Modify ATM port (**cnffrport**)

Responses to Set Requests

When an SNMP manager workstation sends an SNMP Set request packet to a BPX agent, it utilizes the IP protocol for addressing. The request packet can use either a LAN interface for a locally attached management workstation or a network interface for remote access. Each packet has the ASN.1 format, which is suitable for transmission via the UDP protocol. Once it arrives, the packet is decoded to a Protocol Data Unit (PDU). This PDU is the SNMP internal packet structure.

Each variable in the varbind list is located, checked for visibility in the current MIB view, checked for write-access, and type-matched against the set request. A user-defined function is then called to validate the Set PDU. This validation mainly determines if the Set request packet follows the guidelines defined for the BPX. This function returns either good status or an error. The error indicates the PDU is bad and should be rejected. Processing continues with tests for accessibility and acceptability.

Each variable in the varbind list is tested for accessibility and acceptability. User-defined test functions associated with each variable are called to implement the tests. A failed test returns a specifier for the variable and a reason code. Any failed test results in a failed Set request. Upon successfully passing the test functions, the set request can proceed to set the requested variables on the specified switch. The SNMP agent calls a user-specified set function to implement the modifications.

Upon either a successful completion or an error, the Set request PDU is modified to become the response PDU. The response PDU also contains the values of the variables in the original Set request. This PDU is encoded into ASN.1 format and inserted into the response packet. The Set response packet goes to the workstation that generated the request.

MIB II Support

The BPX SNMP agent supports the following groups in the Internet SNMP MIB II:

- ARP
- ICMP
- Interfaces
- IP
- SNMP
- System
- TCP
- UDP

StrataCom Proprietary MIB Structure

This section is an overview of the StrataCom proprietary MIB. The proprietary MIB resides under the enterprises branch of the SNMP tree structure (1.3.6.1.4.1.StrataCom (351)). For detailed information on the structure and contents of the MIB, refer to the actual MIB that is included on the release tape. The MIB is in ASN.1 format.

Note Release 8.2 of the MIB is backward compatible with the 8.1 and 8.0 MIB.

The MIB provides network managers with BPX information on a per switch basis. This information in the MIB relates to ATM service. The SNMP agent MIB has two major branches of information. These are the Switch Service Objects and Switch Connections.

Each variable in the MIB also includes the following:

- An access level (read-only, read-write, or no access)
- A defined MIB view, which allows appropriate agents to have access to platform-specific information

Switch Service Objects

The higher level Switch Services branch shows the available ATM services. This service information exists in a configuration table and a statistics table for each logical port on the switch. The configuration parameters for a logical port allow the manager to view and modify a specified available port. The statistics table gives the manager access to real-time counter statistics associated with a specified available port.

Switch Connections

The Switch Connections branch supports per switch management of ATM connections. In this branch, the MIB defines the following:

- Connections—a general view of all available ATM connections on a switch
- Endpoints
- Bandwidth class
- Endpoint Statistics
- Endpoint mapping

The following is a list of the categories of connection information:

- Local description (e.g., domain.node.slot.port.vpi.vci, group id) (read-only)
- Remote description (e.g., domain.node.slot.port.vpi.vci) (read-only)
- Status of the connection (read-only)
- Failure reasons (read-only)

- Current route information (read-only)
- Preferred route information (read-write)
- Access to open space information (read-only)
- Pointer to endpoint-specific information (read-only)

The ATM endpoint-specific information (last item in the previous list) provides the mechanism for the manager to provision and configure ATM connections. The available endpoint-specific information is:

- Local description (e.g., domain.node.slot.port.vpi.vci) (read-write)
- Remote description (e.g., domain.node.slot.port.vpi.vci) (read-write)
- ATM applicable bandwidth parameters (read-write)
- Foresight enable status (read-write)
- Trunk avoid types (read-write)
- Connection priority (read-only)
- Foresight round-trip delay (read-only)

Bandwidth Class

The bandwidth class information gives the manager a view of the available bandwidth classes that are configured on the switch. The manager can use a selected class as a template to create a ATM endpoint.

Endpoint Statistics

The endpoint statistics are real-time counter statistics about a specific endpoint.

Endpoint Mapping

The endpoint mapping information lets the manager have access to connection and endpoint-specific indices. The indices are associated with physical attributes of a connection (for example, *slot.port.vpi.vci*). The manager can use the indices returned to it to gain access to connection and/or endpoint-specific information.