

# Customer Tips

dc00cc0118  
July 22, 2003

... for the user

## Simple Network Management Protocol (SNMP) Primer

### Purpose

This document introduces the history, purpose, basic functionality and common uses of SNMP technology and how SNMP interacts with the Xerox multifunction devices.

### SNMP Components

By the 1980s, wide area networks (networks that span large geographical areas) had grown from a set of small, sparsely connected, independent networks, to large geographically dispersed interconnected networks. The large networks are more difficult to diagnose and require a means of remote diagnosis and repair.

SNMP answered the industry's remote diagnostic requirements for wide area networks. This protocol allows network elements to communicate information to an SNMP system through Protocol Data Units (PDU's). PDUs are communication functions that allow Network Administrators to operate on a set of data within each of the network elements.

Figure 1 illustrates the relationship between these SNMP system components.

- SNMP Manager
- SNMP Agent
- Management Information Base (MIB)

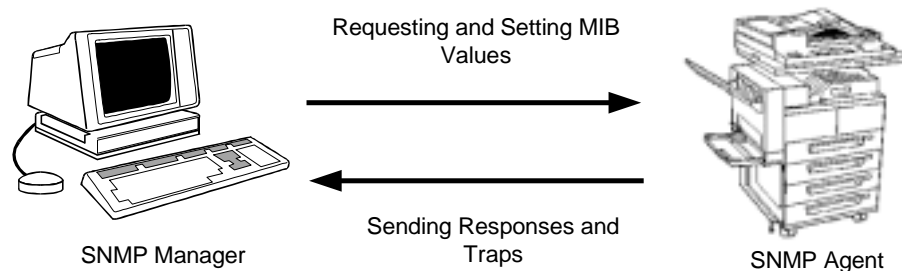


Figure 1: Relationship Between SNMP System Components

This document applies to these **Xerox** products:

x	WC Pro 32/40 Color
x	WC Pro 65/75/90
x	WC Pro 35/45/55
x	WC M35/M45/M55
x	DC 555/545/535
x	DC 490/480/470/460
x	DC 440/432/425/420
x	DC 340/332
x	DC 265/255/240
x	DC 230/220
	DCCS 50

## SNMP Manager

The SNMP Manager is software that runs on a host computer. The System Administrator uses the SNMP Manager to communicate with the Agent to manage the information stored in the network element. The SNMP Agent runs on each network element and is able to access specific items in the MIB as they are defined on that device. The Agent exchanges information with the Manager by using protocol data units (PDUs) explained in the "SNMP Protocol" section of this document. The Manager's main role is to poll Agents for specific requested information. The Manager is configured to passively listen to the network for specific traffic (Traps) and take the appropriate action.

## Agent

Typically, an Agent is a program that resides on the networked device and listens for requests from a Manager, then sends out the appropriate PDU response messages to the network.

An Agent can also send unsolicited Traps to the Manager. Traps are messages alerting the SNMP Manager to a condition on the network. Traps can indicate incorrect use of authentication, printer re-starts, link status, closing of a TCP connection, or loss of a connection to a neighbor communication server.

## Management Information Base (MIB)

An SNMP Agent uses a database of information when the SNMP Manager requests values from it. This collection of data is referred to as the Management Information Base (MIB). The information in the MIB follows the Structure of Management Information (SMI). SMI is the standard that defines the structure of a MIB so that any process that queries the receives an expected result.

You can think of the MIB as a tree. The base of the tree contains the most generic information. As you climb the tree, more detailed information about each separate aspect of an element is revealed until all information pieces about a device are exposed. Each of these pieces is known as an Object ID (OID). The lowest level of the tree is usually referred to as "Internet." The major branches are named after the more specific types of devices such as host, printer, private data, and router.

The MIB uses the Abstract Syntax Notation 1, (ASN.1) naming convention to name all the variables. ASN.1 guarantees a unique and absolute name space to access MIB variables. For example, the naming convention for the MIB variable that counts incoming IP datagrams, `ipInReceives`, is:

```
iso.org.dod.internet.mgmt.mib.ip.ipInReceives -
```

MIBs provide variables that can be stored (set) or read (get), to change parameters or provide information on network devices and interfaces. The SNMP Agent contains MIB variables with values that the SNMP Manager can request or change. A Manager can **get** a value from an Agent or **set** a value in that Agent. The Agent gathers data from the MIB in response to the Manager's request to get or set data.

## Types of MIBs

There are three types of MIBs:

- **Public:** Public MIBs follow the standard MIBs and can be accessed by any vendor that uses SNMP as the vehicle of communication.
- **Private:** MIB implementation can be extended to accommodate the addition of new objects. This flexibility allows different vendors to create objects to manage the specific and unique entities of their products. Private MIBs can be published and made available to the public if desired. Private MIBs follow standard SMI conventions. Thus, when appropriate access is granted, it is possible for different vendors to manage other vendor's private MIBs.

- **Public/Experimental:** The Public/Experimental MIB is used by vendors to develop MIBs.

SNMP is a **simple** means of communicating between network managers and network elements. The architectures of the PDU and MIB structures are very simple. It is this simplicity that gives SNMP its flexibility and scalability.

## SNMP Protocol

Protocol Data Units (PDUs) represent the basic vocabulary through which SNMP Managers and agents communicate information. PDU's are asynchronous in nature. This means communication between the Manager and Agent is broken into two messages, **request** and **response**.

SNMP Version 1 defines five types of PDUs.

- `getRequest`
- `getNextRequest`
- `getResponse`
- `setRequest`
- `Trap`

The `getRequest` and `getNextRequest` PDU operations retrieve data from network elements (see Figure 2 and 3). The `setRequest` operation allows for the modification of data on the network element (see Figure 4). The response to these PDUs is returned with the `getResponse` command. The last PDU, `Trap`, allows the network element to broadcast data under certain conditions (Figure 5).

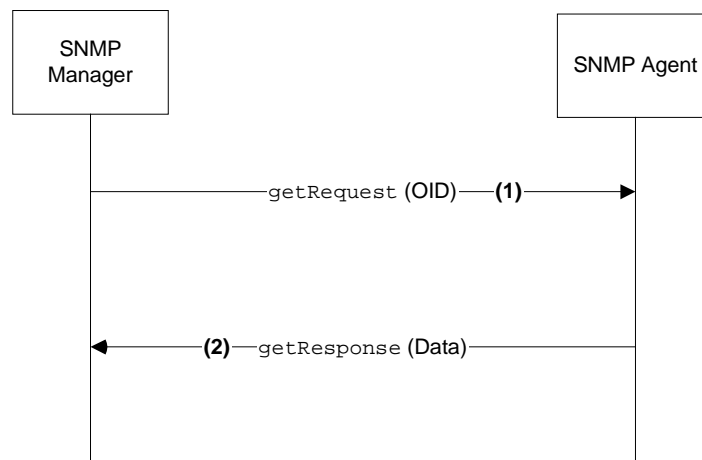
These five operations accomplish three primary tasks for the client software:

- A client PC can **read** a piece of information.
- A client can **change** a piece of information.
- A device initiates the communication of information to the client when it uses the **Trap** PDU.

## SNMP Operations

Each of these PDUs operate on a set of data contained within the MIB. The name of a value in a MIB is an Object Identifier (OID).

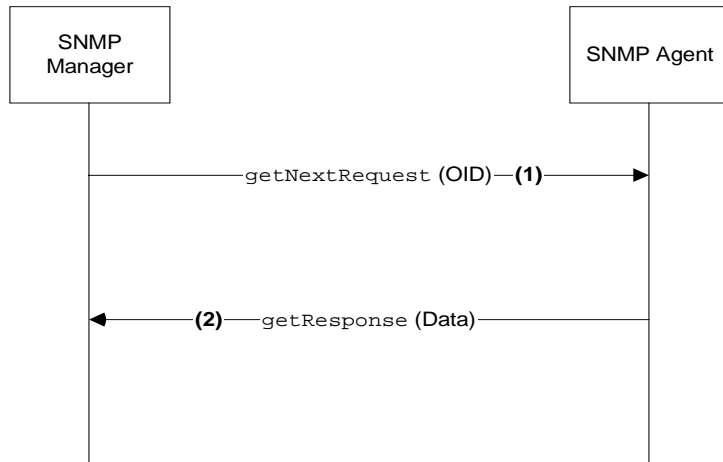
### `getRequest` Operation



**Figure 2:** *SNMP `getRequest` Operation*

1. `getRequest` informs the SNMP Agent to obtain the value of an object identifier (OID).
2. `getResponse` returns the value associated with the OID from the SNMP-Agent's MIB.

## getNextRequest Operation

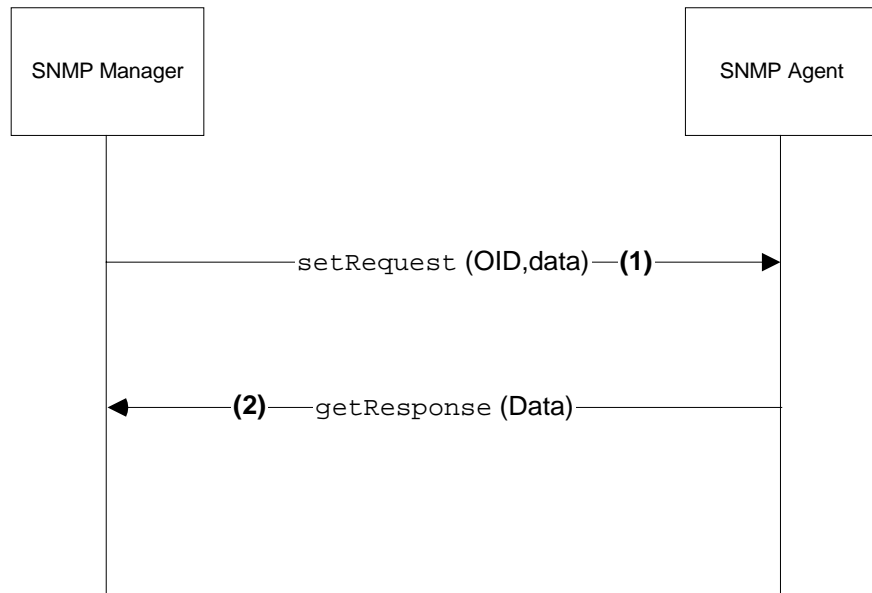


**Figure 3:** *SNMP getNextRequest Operation*

1. `getNextRequest` informs the SNMP Agent to obtain the value of the next OID following the requested OID.
2. `getResponse` returns the value associated with the next OID from the SNMP-Agent's MIB.

This technique is used to "walk" the MIB to allow a client to interrogate each value contained within the MIB. When there is no "next" OID, the SNMP Agent returns an error.

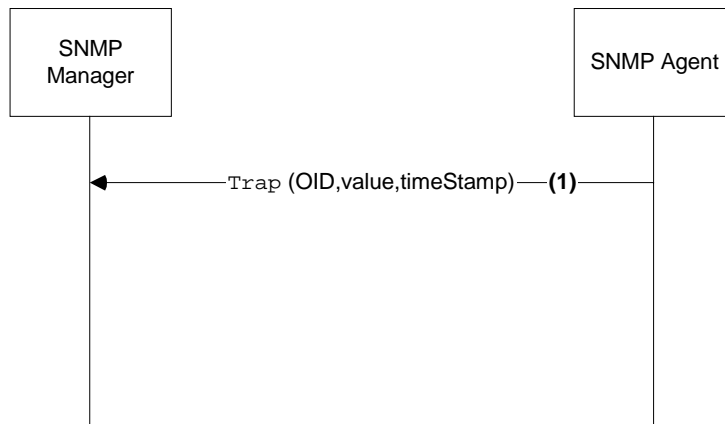
## setRequest Operation



**Figure 4:** *SNMP setRequest Operation*

1. `setRequest` tells the SNMP Agent to modify the value of an OID to a specific value.
2. `getResponse` returns the value that was set by the SNMP Agent, or an error, if the Manager has insufficient permissions, or the OID is not valid.

## Trap Operation



**Figure 5:** SNMP Trap Operation

The Trap allows an SNMP Agent to communicate a changed value when the value crosses a pre-specified threshold.

The SNMP Agent can be configured to send `Trap` information to the designated SNMP Manager(s).

## SNMP Community String Name

SNMP is not a very secure protocol, but it contains a minimum level of security called SNMP Community Strings. You can think of SNMP Community Strings as the passwords that SNMP uses to access the information stored in the MIB. There are three kinds of SNMP Community Strings.

- **Read-Only:** When the Community String is set to Read-Only, the information in the MIB can only be read and not modified. A client is only allowed to issue `getRequest` and `getNextRequest` commands with the Read-Only community name.
- **Read-Write:** A Read-Write setting allows the value of the MIB object to be accessed as well as modified. A client can issue the `setRequest` command as well as the `getRequest` and `getNextRequest`. If one tries to access an SNMP Agent with the wrong SNMP Community String name, the Agent refuses to provide the requested information. If for some reason the SNMP Agent is set up in a way to perform that request, an SNMP Trap called an Authentication Failure Trap may occur.
- **Trap:** The Trap Community String is not used for security, instead it allows a client to group traps received from network devices together. Since this task can be accomplished by other methods, this particular Community String is not commonly used.

## History

On the Internet, each individual Network has its own set of rules and regulations. In 1993, to enable communication between different networks, an independent committee called the Internet Activity Board (IAB) was established to standardize the Internet rules among work groups. The IAB has two task forces.

- Internet Research Task Force (IRTF): IRTF members manage the research of network protocols such as TCP/IP.
- Internet Engineering Task Force (IETF): Members of IETF meet three times a year and are responsible for keeping the Internet operational. Thus the IETF evolved and standardized the usage of the SNMP protocol to what it is today.

SNMP is an application layer protocol and it can be used by the TCP/IP protocol suit for communication and information management. Over the last 20 years, SNMP has evolved in a number of ways. The original SNMP specification had little support for secure

communication. Follow-on versions of SNMP attempted to address this shortcoming. The following is a timeline of the changes to SNMP.

## Version 1

SNMP Version 1 contained the basic MIB model, and set/get approach described earlier. It also contained a rudimentary security mechanism known as SNMP community names, also described in the *SNMP Community String Name* section of this document.

The problem with community names, however, is that the password is in plain text, and can be intercepted and used by individuals monitoring the SNMP traffic between the client and the network device.

This version of SNMP is an established Internet standard and is predominant in the industry.

## Version 2

In addition to enhanced security, SNMP Version 2 support includes a “bulk retrieval mechanism” and more detailed error message reporting to management stations. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information. This mechanism improves network performance when accessing large amounts of data.

SNMP Version 2 has improved error-handling support and includes expanded error codes that distinguish different types of error conditions. These error conditions are reported through a single error code in SNMP Version 1. In Version 2, the error code also reports the type of error. In addition, three kinds of exceptions are also reported in SNMP version 2. They are:

- No such object
- No such instance
- End of MIB

Since SNMP Version 2 is an Internet draft standard (just below a final standard) that has significant performance improvements and is a growing industry practice, support of SNMP version 2 is strongly recommended. It is important to note that there are different versions of Version 2. Please refer to the reference section of this document for a more detailed description.

## Version 3

SNMP version 3 was approved as a standard by the Internet Engineering Task Force (IETF) standards body in 2002. Implementation of SNMP version 3 is not widespread and Xerox anticipates to implement it in the future.

## Uses

### Network Management

Up to now we have described SNMP, and its origins. To what applications do network managers apply SNMP? The International Organization for Standards has defined five important objectives for SNMP in network management.

**Configuration Management:** Configuration Management allows the network managers to change the configuration of remote network devices. Specific values in the MIB may allow the Network Administrator to adjust the operation of the network element based on the usage of the device.

**Security Management:** Security Management ensures that the privacy of the data is reserved. Some MIB information may be sensitive. Ensuring that an unauthorized user is not allowed to view or change the data in a MIB is an objective of the later versions of SNMP.

**Performance Management:** Performance Management manages the performance of the network devices. High traffic is one of the reasons why the performance of a network can deteriorate. SNMP allows a Network Administrator to remotely acquire and combine into an integrated picture the performance of an array of network devices. This allows the Network Administrator to quickly pinpoint the source of a network bottleneck, and take corrective action.

**Fault Management:** Fault Management ensures the correction of the generated fault with minimum delay. As faults occur, the network device logs the occurrence in the MIB, allowing the remote Administrator to diagnose any problem that occurred.

**Accounting Management:** Accounting Management can be set to charge the users for resources used on the network. It also can restrict users to access some of the resources.

## Printer Management

While the original design of SNMP did not support printer products, management of printing installations gains much efficiency from the usage of SNMP. Consider the following hypothetical applications:

**Printer Administration:** An Administrator can accomplish the network management objectives listed above with SNMP compliant printers.

**Software Installation:** A Company has 30 mid-volume copier/printers that need a firmware upgrade. Due to the expense of the upgrade, the company only wants to perform the upgrade on those devices that experience a rare fault caused by a software error. Using SNMP to extract fault information from the 30 printers, identification can be made of those devices that have experienced the fault. Without SNMP, a physical inspection of each copier/printer is required.

**Supplies Management:** The Printer Administrator uses SNMP to determine the quantity of paper/toner/supplies used by the fleet of printers under his responsibility. This becomes the basis for supplies re-ordering for the site.

**Facilities Management:** A Printer Administrator tracks the AMCV (Average Monthly Copy Volume) for each of the 30 copier/printers under her responsibility. By overlaying the physical location of each unit with the volume, it becomes clear that several high-volume copiers are under-utilized, and some mid-volume copiers are over-utilized. Moving the printers can more effectively meet the demands of the organization.

**Sales Support:** A Sales district uses SNMP to track the job demographics and usage of the machines in the district. It identifies several machines that have demographics that are more suitable for a different model printer. The Account Manger initiates a call to discuss new opportunities with the customer.

Many of these applications are not immediately possible with the basic networking SNMP MIBs defined by the standards organizations. To resolve this problem, two new MIBs have been defined in recent years.

The first was an extension of the industry sponsored Public MIB to address basic printer management needs. The **Printer MIB** defined many of the basic printer attributes that most printers are likely to use.

Xerox created a second MIB to extend the unique feature sets of the Xerox Products. This MIB is called the Xerox Common Management Interface (**XCMI**) MIB. The following section describes the XCMI MIB more in detail.

## Xerox and SNMP

The industry standards currently available are not sufficient to fully support the management of Xerox products (or the products of most of Xerox competitors). To remedy the situation, Xerox defined the Xerox Common Management Interface (XCMI), based on the SNMP Private MIB.

XCMI incorporates (by reference) all industry standard MIBs that are appropriate to XCMI. The XCMI extends these standards with additional components necessary to support Xerox products as defined by Xerox.

Xerox supports both SNMP Version 2C and SNMP Version 1. SNMP Version 2 offers more robust support than SNMP Version 1. Xerox continues to support SNMP Version 1 because not all SNMP managers have migrated to SNMP Version 2.

Support of SNMP and various MIB components enables certain capabilities depending on the application being used by the end user/System Administrator. The Xerox plan includes broad compliance with all major IETF MIB components. It is important to note that each printing device on a network may provide different types of information depending upon the degree to which the device's MIB objects comply with the industry standards.

Various applications take advantage of the MIB objects. These include, but are not limited to:

- Third-party network management applications (HP OpenView, CA Unicenter, Novell ManageWise, etc.)
- PrinterMap (from the Xerox Channels Group)
- CentreWare Internet Services
- CentreWare Conductor, Device Administration Wizard, Printer Admin Wizard, Device Discovery Wizard

Each one of these applications provides different levels of information about the configuration, capability and general condition of the product. The first two applications are generally considered System Administrator applications, and in many cases, the third-party network management applications are Network Administrator tools only. The third, CentreWare Internet Services, is both a System Administrator and an end user tool.

## References

### RFCs

An RFC (Request For Comment) lists specific information about a protocol or application. The information is written in as much detail as is necessary for the Internet community to implement the functionality. There are RFCs covering almost every non-proprietary protocol and communications standard. These RFCs cover host name conventions, printing, addressing, TCP/IP and more. These RFCs are available at <http://www.faqs.org/rfcs/>.

RFCs that apply to SNMP include:

### SNMP Version 1

- RFC1089 - SNMP over Ethernet
- RFC1157 - SNMP : Simple Network Management Protocol
- RFC1187 - Bulk table retrieval with the SNMP
- RFC1212 - Concise MIB definitions.
- RFC1213 - MIB-II : Management Information Base for network management of TCP/IP based internets
- RFC1215 - Convention for defining traps for use with SNMP
- RFC1228 - SNMP-DPI : Simple Network Management Protocol Distributed Program Interface
- RFC1270 - SNMP communications services
- RFC1303 - A Convention for Describing SNMP-based Agents
- RFC1351 - SNMP Administrative Model
- RFC1352 - SNMP Security Protocols
- RFC1353 - Definitions of Managed Objects for Administration of SNMP Parties

## SNMP Version 2

- RFC1442 - Structure of Management Information for SNMP version 2
- RFC1443 - Textual Conventions for SNMP version 2
- RFC1444 - Conformance Statements for SNMP version 2
- RFC1445 - Administrative Model for SNMP version 2
- RFC1446 - Security Protocols for SNMP version 2
- RFC1447 - Party MIB for SNMP version 2
- RFC1448 - Protocol Operations for SNMP version 2
- RFC1449 - Transport Mappings for SNMP version 2
- RFC1450 - Management Information Base for SNMP version 2
- RFC1503 - Algorithms for Automating Administration in SNMP version 2 Managers
- RFC1901 - Introduction to Community-based SNMPv2

## SNMP Version 3

- RFC 2272 -- SNMP Version 3u (SNMP Version 3 – User), defined in January 1998
- RFC 2274 -- User-based security defined in January, 1998
- RFC 2273 -- Trap registration in SNMP version 3u and notification MIB using targets in SNMP version 3u defined in January, 1998

## Printer MIB

- RFC 1759 -- describes the printer MIB. The printer MIB describes the information a printer can set or provide about the printer sub-systems to the manager or to the network.

## Web Sites

### **SNMP Overview:**

[http://webopedia.internet.com/Networks/Network\\_Management/SNMP.html](http://webopedia.internet.com/Networks/Network_Management/SNMP.html)

### **SNMP (Simple Network Management Protocol):**

<http://www.rad.com/networks/1995/snmp/snmp.htm>

### **Abstract Syntax notation One – ASN.1:**

<http://www.rad.com/networks/1995/snmp/asn1.htm>

## Additional Information

Xerox Customer Service welcomes feedback on all documentation - send feedback via e-mail to: [USA.DSSC.Doc.Feedback@mc.usa.xerox.com](mailto:USA.DSSC.Doc.Feedback@mc.usa.xerox.com).

You can reach Xerox Customer Support at 1-800-821-2797 (USA), TTY 1-800-855-2880 or at <http://www.xerox.com>.

Other Tips about Xerox multifunction devices are available at the following URL: <http://www.xerox.com/DocumentCentreFamily/Tips>.

XEROX®, The Document Company®, the digital X®, and all Xerox product names are trademarks of XEROX CORPORATION. Other trademarks belong to their respective owners.

Copyright © XEROX CORPORATION 2003. All Rights Reserved.

