



# Technology Backgrounder

## SNMP Environment

1.	Introduction.....	1
2.	SNMP Principles.....	1
	SNMP Operations.....	1
	Management Information Base.....	2
	MIB Structure.....	2
3.	Management Domains Under SNMP.....	2
	SNMP Communities.....	3
	Access Restriction Using SNMP Communities.....	3
	Communities.....	3

---

---

## 1. Introduction

The SNMP management functions of RAD's products are provided by an internal SNMP agent.

SNMP management communication uses the User Datagram Protocol (UDP), a connectionless-mode transport protocol, part of the suite of protocols of the Internet Protocol (IP).

**Note**

---

*Telnet management uses the TCP protocol over IP for management communication. After a Telnet session is started, the management interface is similar to that used for the supervision terminal.*

---

---

---

## 2. SNMP Principles

The SNMP management protocol is an asynchronous command/response polling protocol: all the management traffic is initiated by the SNMP-based network management station (except for trap messages), which addresses the managed entities in its management domain. Only the addressed managed entity answers the polling of the management station.

The managed entities include a function called an "SNMP agent", which is responsible for interpretation and handling of the management station requests to the managed entity, and the generation of properly-formatted responses to the management station.

### SNMP Operations

The SNMP protocol includes four types of operations:

<b>getRequest</b>	Command for retrieving specific management information from the managed entity. The managed entity responds with a <b>getResponse</b> message.
<b>getNextRequest</b>	Command for retrieving sequentially specific management information from the managed entity. The managed entity responds with a <b>getResponse</b> message.
<b>setRequest</b>	Command for manipulating specific management information within the managed entity. The managed entity responds with a <b>setResponse</b> message.
<b>trap</b>	Management message carrying unsolicited information on extraordinary events (e.g., alarms) reported by the managed entity.

## Management Information Base

The management information base (MIB) includes a collection of *managed objects*. A managed object is defined as a parameter that can be managed, such as a performance statistics value.

The MIB includes the definitions of relevant managed objects. Various MIBs can be defined for various management purposes, types of equipment, etc.

An objects definition includes the range of values and the “access” rights:

<b>Read-only</b>	Object value can be read, but cannot be set.
<b>Read-write</b>	Object value can be read or set.
<b>Write-only</b>	Object value can be set, but cannot be read.
<b>Not accessible</b>	Object value cannot be read, nor set.

## MIB Structure

The MIB has an inverted tree-like structure, with each definition of a managed object forming one leaf, located at the end of a branch of that tree. Each “leaf” in the MIB is reached by a unique path, therefore by numbering the branching points, starting with the top, each leaf can be uniquely defined by a sequence of numbers. The formal description of the managed objects and the MIB structure is provided in a special standardized format, called Abstract Syntax Notation 1 (ASN.1).

Since the general collection of MIBs can also be organized in a similar structure, under the supervision of the Internet Activities Board (IAB), any parameter included in a MIB that is recognized by the IAB is uniquely defined.

To provide the flexibility necessary in a global structure, MIBs are classified in various classes (branches), one of them being the experimental branch, and another the group of private (enterprise-specific) branch. Under the private enterprise-specific branch of MIBs, each enterprise (manufacturer) can be assigned a number, which is its enterprise number. The assigned number designates the top of an enterprise-specific sub-tree of non-standard MIBs. Within this context, RAD has been assigned the enterprise number **164**. Therefore, enterprise MIBs published by RAD can be found under **1.3.6.1.4.1.164**.

MIBs of general interest are published by the IAB in the form of a Request for Comment (RFC) document. In addition, MIBs are also often assigned informal names that reflect their primary purpose. Enterprise-specific MIBs are published and distributed by their originator, which is responsible for their contents.

Enterprise-specific MIBs supported by RAD equipment are available in ASN.1 format from the RAD Technical Support Department.

---

## 3. Management Domains Under SNMP

SNMP enables, in principle, each management station that knows the MIBs supported by a device to perform all the management operations available on that

device. However, this is not desirable in practical situations, so it is necessary to provide a means to delimit management domains.

## SNMP Communities

To enable the delimitation of management domains, SNMP uses “communities”. Each community is identified by a name, which is a case-sensitive alphanumeric string defined by the user. Any SNMP entity (this term includes both managed entities and management stations) can be assigned by its user community names.

## Access Restriction Using SNMP Communities

In general, SNMP agents support two types of access rights:

- **Read-only:** the SNMP agent accepts and processes only SNMP *getRequest* and *getNextRequest* commands from management stations which have the same read-only community name.
- **Read-write:** the SNMP agent accepts and processes all the SNMP commands received from a management station with the same write community name.

For each SNMP entity it is possible to define a list of the communities which are authorized to communicate with it, and the access rights associated with each community (this is the SNMP community name table of the entity). For example, the SNMP community name table of the SNMP agent can include three community names.

In accordance with the SNMP protocol, the SNMP community of the originating entity is sent in each message.

When an SNMP message is received by the addressed entity, first it checks the originator's community: if the community name of the message originator differs from the community name specified for that type of message in the agent, the message is discarded (SNMP agents of managed entities report this event by means of an authentication failure trap).

## Communities

The SNMP agents recognize the following community types:

- |              |  |
|--------------|--|
| <b>Read</b>  | SNMP community that has read-only authorization, i.e., the SNMP agent will accept only <i>getRequest</i> and <i>getNextRequest</i> commands from management stations using that community. |
| <b>Write</b> | SNMP community that has read-write authorization, i.e., the SNMP agent will also accept <i>setRequest</i> commands from management stations using that community.                          |
| <b>Trap</b>  | SNMP community which the SNMP agent will send within trap messages.  |