A Preview of Use of the Simple Network Management Protocol in Broadcast Monitoring and Control Systems Course

About the Author

This course was written for SBE by Tony Peterle, CSRE. Peterle grew up in Central Ohio and began taking things apart at an early age to find out how they worked. Fortunately for his parents' sanity, he quickly learned how to put things back together, and graduated from the College of Wooster in 1981. He has been involved in radio broadcasting continuously since high school, working in Ohio, Kansas, Hawaii and Washington State, both on air and engineering. Peterle has held Chief Engineer positions in Honolulu, Kansas City, and Wichita. After attaining his commercial pilot's license, Peterle spent several years as a traffic reporter in Kansas City, Honolulu and Seattle before receiving CSRE certification from the SBE in 2005. Shortly thereafter, he came to work for Audemat, and enjoys helping customers solve problems, traveling, contributing to the design of new products, and seeing familiar faces at NAB and SBE events.

Introduction

The purpose of this course is to give students an introduction and overview of the Simple Network Management Protocol, or SNMP. With IP networking becoming an ever-increasing part of a broadcast engineer's environment, there is an opportunity to exploit this legacy IT protocol for our benefit. SNMP is a way to monitor data points and control different functions in remote equipment, using an existing IP network. Much of the latest generation broadcast equipment supports this protocol, and facility control devices are appearing on the market that can incorporate data and control functions obtained via SNMP alongside information and controls that use traditional hardwired inputs and outputs.

This course will offer a basic description of how SNMP works – the structure and types of SNMP messages, how they are transported over the network, and how they can be used to monitor and control remote equipment. We will then explore the data that the distant equipment might return, and how best to integrate that into an overall facility control plan. And finally we will discuss the types of equipment that support SNMP communications, and also cover the topic of using the protocol for site-to-site communications.

Chapter Breakdown

1. Overview
2. SNMP Transport and Packet Structure
3. SNMP Versions and Messages
4. Object Identifiers and MIB Files
5. Understanding an OID
6. OID Index Values
7. Using SNMP Commands and Understanding Data
8. Advantages of Using SNMP

Enrollment Information

SBE Member Price: $85
Non-Member Price: $120

SNMP Versions and Messages

Like many technology related standards, the SNMP protocol has seen several changes and additions over the years. As uses of the system expanded and changed, the protocol added more message types and standards, particularly in the areas of security and bulk commands. Bulk commands are valuable when retrieving many data points from an SNMP Agent, to reduce the network traffic and minimize potential syntax errors and time spent writing individual commands.

The list of SNMP message types is still very small, however, and can be broken into three basic categories:

The GET family - these are the commands used by an SNMP Manager device to query and retrieve information from the target Agent device(s) across the network. This family also includes the GETNEXT and GETBULK commands, and the GETRESPONSE messages returned to the Manager by the Agent.

The SET message - this is the message used by an SNMP Manager to change the value of a specific data object in the Agent. The SET command (as with every SNMP message) contains the OID and community string and the desired value to be set for the object. The Agent software will respond with a message that indicates whether the application of the new value for the object was or was not successful.

Alarm messages - these are the only messages generated by the Agent that are not in response to a GET or SET message from the Manager. These SNMP messages could be in the forms of a TRAP type message. This is the alarm message format introduced with SNMP V1, and in the MIB file a definition of a TRAP type message might look something like this:

```
TRAP-TEST-MIB DEFINITIONS ::= BEGIN
        IMPORTS ucdExperimental FROM UCD-SNMP-MIB;

demotraps OBJECT IDENTIFIER ::= { ucdExperimental 990 }

demo-trap TRAP-TYPE
        STATUS current
        ENTERPRISE demotraps
        VARIABLES { sysLocation }
        DESCRIPTION "This is just a demo"
        ::= 17

END
```

This would be an example of an" Enterprise specific" trap, in that the trap ID (in this case, 17), will follow the Enterprise ID in the MIB.

A second type of alarm trap, called a NOTIFICATION, was introduced in SNMP V2. It has the advantage that the data structure of the PDU is much more similar to the PDUs of GET and SET messages, which can make trap handling and analysis easier. The MIB definition of a V2 NOTIFICATION message might look like this:

```
NOTIFICATION-TEST-MIB DEFINITIONS ::= BEGIN
        IMPORTS ucdavis FROM UCD-SNMP-MIB;

demonotifs OBJECT IDENTIFIER ::= { ucdavis 991 }

demo-notif NOTIFICATION-TYPE
        STATUS current
        OBJECTS { sysLocation }
        DESCRIPTION "Just a test notification"
        ::= { demonotifs 17 }

END
```

This trap is created in another, lower branch of the MIB file (in demonotifs) rather than "right up top" as with the enterprise specific traps. An additional enhancement for traps is the INFORM type, also introduced in SNMP V2c. While other TRAP and NOTIFY message are unidirectional, the INFORM V2C type requires an acknowledgement from the Manager when

the trap is received. If no acknowledgement is received, the Agent software can re-send the trap until it gets a response, greatly enhancing the surety of the alarm message being received.

In all cases, a trap can be an alarm message to indicate some sort of error or problem detected in the Agent device or it can be simply informational.

There is a fourth category of SNMP messages called REPORT, used to send a performance summary from one Manager Device to another.

The first version of SNMP (V1) is still widely used, and supports the main and most useful types of SNMP messages. Some new commands were added when SNMP V2c was introduced, as seen in the table below, and V2c was probably the most widely used version at the time this course was written. SNMP V3 adds a separate login and password structure to the SNMP messages, and also encrypts the data being sent between Manager and Agent. V3 is more widely used in critical network structures that still have a strong possibility of unauthorized access, such as public web servers, etc. Below is a table that describes the various commands and structures supported by the 3 versions of SNMP.

SNMP Version	Commands used
SNMP V1	GET, GETNEXT, GETRESPONSE, SET, TRAP
SNMP V2c	As above plus GETBULK, INFORM, NOTIFICATION, REPORT
SNMP V3	As above but adds encryption and password protection

Command definitions:
GET - Manager requests the value of a single object from the Agent.

GETNEXT - Manager requests the value of the next object in the MIB tree. Multiple GETNEXT commands will step the Agent through the entire MIB, returning the value of all objects in the Agent device. This technique is called "walking" the MIB, and is an excellent method to establish the number and types of objects available from the Agent, particularly if the MIB file is absent or inaccurate.

GETRESPONSE (or just RESPONSE) - message returned by the Agent containing the data on the objects as requested in the GET command from the Manager.

GETBULK - a request from a Manager for data of a large number of objects from a single Agent. This is a way to get information on many objects with a single request, eliminating the need to create and send a separate GET for each OID.

SET - used by a Manager to change the value for a specific object in the Agent device.

TRAP / NOTIFY - a message generated by an Agent and sent autonomously to the Manager, usually to report an error or out-of-tolerance condition of some type.

INFORM - also generated and sent independently by the Agent for alarms and other functions, but with the additional capability for the Agent to repeatedly send the message until an acknowledgement is received from the Manager.

REPORT - used to send status and summaries from one Manager to another.

Which of the following message does SNMP V1 NOT support?

- TRAP
- GET
- GETBULK
- V1 supports all of the above

Which SNMP message can be used to 'walk' through all of the objects in an Agent?

- GET
- GETNEXT
- INFORM
- REPORT

In order to support encrypted communications and password protection on SNMP messages, which version should be used?

- V1
- V2c
- V3
- Any of the above

Which SNMP messages are generated independently by the Agent?

- TRAP, NOTIFY, INFORM
- SET, RESPONSE, TRAP
- GET, NOTIFY, TRAP
- All of the above