

SNMP Notes

Introduction

The Simple Network Management Protocol (SNMP) is an application level protocol used for network management. To avoid confusion with typical applications, SNMP does not use the terms client and server to refer to SNMP applications. Instead, SNMP uses the terms manager and agent.

In general, managers and agents communicate by sending UDP packets. These packets are encoded according to the Abstract Syntax Notation.1 (ASN.1) specification.

The data exchanged between the managers and agents is defined in a “database” called a Management Information Base (MIB). A MIB is formatted into a tree like structure, with data or events representing the leaf nodes. The MIB structure is technically called Structure of Management Information (SMI), but that term doesn’t come up very often, and it is often confused with ASN.1.

For 802.11 there is a MIB standard, but it is unclear which (if any) vendors follow it. The Atmel MIB on the Linksys WAP11 is not standards compliant. But that may be typical...

Communication between a manager and an agent is fairly simple. The manager issues either a get command or a set command to an agent. There are actually 5 types of commands, called Protocol Data Units (PDU), which includes three types of get, one set, and a trap message. The get command(s) allow the manager to monitor the device, while the set command allows the manager to send control commands to an agent (the agent may or may not issue these commands to the device). The agent does not issue any commands, but may generate a trap.

A trap can be thought of as an alert since it is normally generated when an exception on the device occurs, but this can vary by device. A manager should receive a trap, but the details of how the manager receives the trap are complicated. When it comes to traps, SNMP is not so simple.

Managers and Agents

A manager is a client application that runs on a central host, such as slodev1. An agent is a server application that runs on a device such as the Linksys WAP11.

Slodev1 is configured with net-snmp, which is a SNMP manager tool set, while the Linksys WAP11 (and other Access Points) includes an SNMP agent application that

responds to requests from a SNMP manager. Not much is known about the agent on the Linksys WAP11, other than the fact it originated from Atmel, the OEM for the WAP11.

The net-snmp tools `snmpget` and `snmpset` can be used to manage and control the Linksys WAP11 from `slodev1` or any other manager computer. These commands can be sent either through a wired link to the AP or wirelessly.

This behavior will vary for other AP's.

ASN.1 Notation

The ASN.1 specification is very low level and is not discussed here. Just remember it defines how the frames are organized in the UDP packets exchanged between managers and agents.

MIBs

As mentioned above, a MIB is organized in a tree like manor. The leaf nodes of this tree are Objects, which describe some aspect of the managed device. Each Managed Object is unique and has an Object ID (OID). The OID's are often expressed as a long string of numbers (separated by dots). The MIB can be used to translate these long string numbers into a human readable string of characters.

For example the textual representation of the object `sysDescr` in the Atmel MIB looks like this:

```
.iso.org.dod.internet.private.enterprises.atmel.atmelmib.atmelSys.sysCtrlGRP.sysDescr
```

However, the agent will see `sysDescr` as:

```
.1.3.6.1.4.1.410.1.1.1.1
```

Or it might be easier to combine these, in which case the OID looks like this:

```
.iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).atmel(410).atmelmib(1).atmelSys(1).sysCtrlGRP(1).sysDescr(1)
```

Here are some more examples using the above format:

- `.iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).atmel(410).atmelmib(1).atmelSys(1).sysCtrlGRP(1).sysDeviceInfo(5)`
- `.iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).atmel(410).atmelmib(1).atmelSys(1).OperBridgeOperationalMode(4).bridgeOperationalMode(1)`
- `.iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).atmel(410).atmelmib(1).Wireless(2).OperationalSettingsGRP(1).operAuthenticationType(7)`

Better yet see the diagram below of the top-level nodes in the Atmel MIB

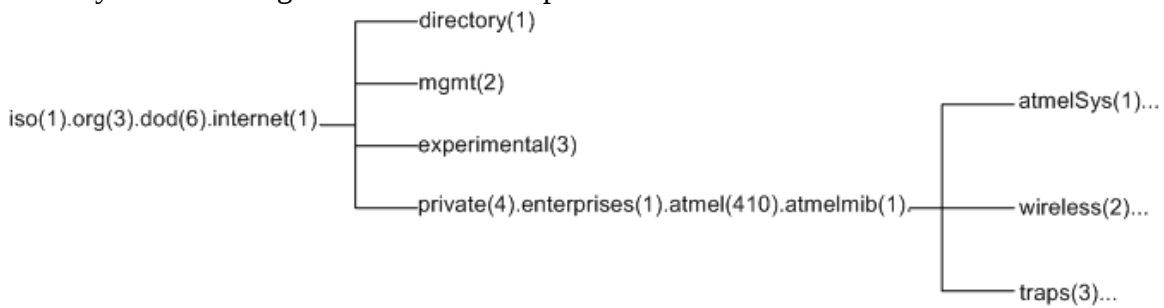


Figure 1 Top-Level Nodes in the Atmel MIB

There are a number of free tools that can be used to browse or translate a MIB. net-snmp's `snmptranslate` can be used to explore a MIB. See the net-snmp notes for more information on using `snmptranslate`.

Security

Security is very poor in SNMPv1, and SNMPv2. The primary weakness in the first two versions of SNMP originated from the use of the community string, which was used as a password. The community string was passed as clear text in SNMP packets so a sniffer could easily capture it. SNMPv3 has done away with the community string and now allows the use of an encrypted password.

SNMPv3 is still a new standard, and it doesn't appear to be widely used.