M7 Modem SNMP Guide

M7 Modem Technical Note

Revision History

Rev 0.1	2-10-2015	Initial Release.
Rev 0.2	2-13-2015	Minor corrections and proper settings for local and remote modems.
Rev 0.3	3-2-2015	Figures added with associated text.

1.0 M7 Modem SNMP Overview

SNMP stands for Simple Network Management Protocol. This document describes the resources and procedures necessary to use the SNMP facilities provided by the Datum System's M7 modem. It does not describe SNMP itself or methods and procedures for network management other than basic concepts.

The M7 modem utilizes a custom OS for modem operation and control including an SNMP agent (server) which responds to requests from valid SNMP browsers (clients).

The current M7 SNMP agent is capable of operating with v1 and v2c protocol versions.

The Datum Systems “PEN” for SNMP is 31968 which is used for the branch of the standard SNMP tree dealing with Datum System’s Private Enterprise Network objects.

The M7 Modem SNMP implementation is unique in that it is capable of gathering information from modems on the far end of a link not served by the Internet.

1.0.1 SNMP – Some Definitions

For the purposes of the remainder of this document the conventions for naming the different objects that are part of SNMP are:

- “***Manager” or “Client”*** The controlling device or computer. This can be a Windows, Linux or other computer with a SNMP manager or browser programs installed.
- “***Agent***” The controlled device, in this case, typically a M7 modem. The agent performs server functionality; providing information in response to requests from a client or manager.
- “***Trap***” A background task runs as a daemon and determines if a parameter is outside normal bounds. Boundary exception conditions are identified and an autonomous message is sent to a specified client/manager.
- “**MCC**” or Modem Control Channel. An internal modem service which sends and receives binary messages for maintenance and control purposes.
- “***MIB***” The Management Information Base. This is the database of the individual elements (objects) that can be managed via SNMP. The MIB basically is an address book of object identifiers and the parameters they control. The MIB can be textual or compiled and may have extensions of either “.mib”, “.txt”, or no extension – all with the same content. It's worth noting that MIBs typically use the line endings from Linux which is slightly different from Windows.
- “***OID***” short for Object Identifier - The unique number that represents the position of a particular parameter in the SNMP tree structure. Standard Internet management OIDs begin with 1.3.6.1.2 followed by additional object identifiers. Datum Systems private OIDs begin with 1.3.6.1.4.1. followed by the “PEN” of the company developing the MIB (Datum

Systems - 31968) and followed by additional numbers separated by decimal points. Each of these numbers represents a node in the MIB tree. All proprietary Datum System OIDs begin with 1.3.6.1.4.1.31968. There may be additional nodes representing discovery items.

1.0.2 SNMP – Basic Model

SNMP consists of three main elements: The “Manager”, the “Agent” and the device(s) that the agent controls. We are expressly differentiating between the agent and the device that it controls. The manager is distinct from the computer that it is installed on, just as the agent is distinct from the device that operates its control processes.

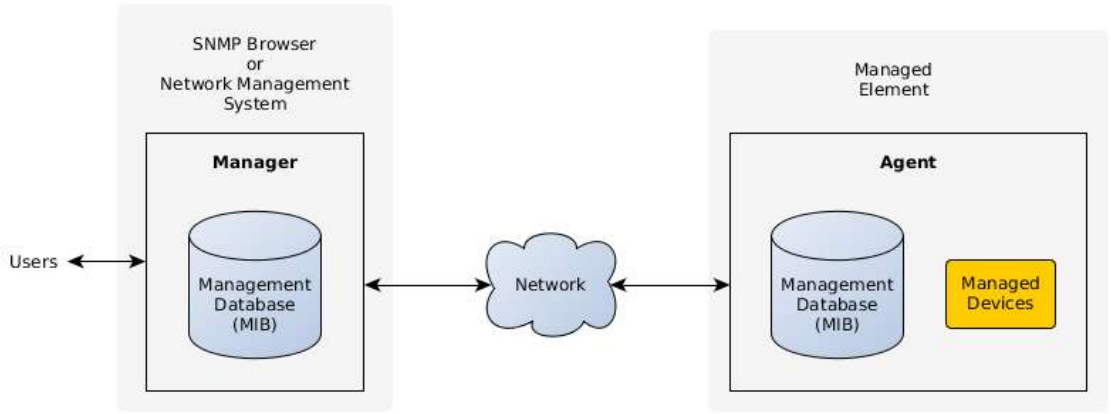

FIGURE 1: SNMP Components

The manager and agent use a Management Information Base or “MIB” to identify data. Notice that both the manager and agent must have the same MIB versions -- although they may be in different formats where the agent is compiled with knowledge of the MIB and the methods of retrieving the values the MIB refers to while the manager typically loads a text version of the MIB, and can load many MIBs.

The manager and agent communicate using the SNMP Protocol over the network between them. You can also think of the system as a client-server, where the agent is the server providing information in response to a client that requests it is somewhat like a web server providing web pages in response to a browser client requests. Notice also that the user or information requester only interfaces with the Manager, not the agent directly.

Figure 2 below shows a small portion of a satellite based communications system.

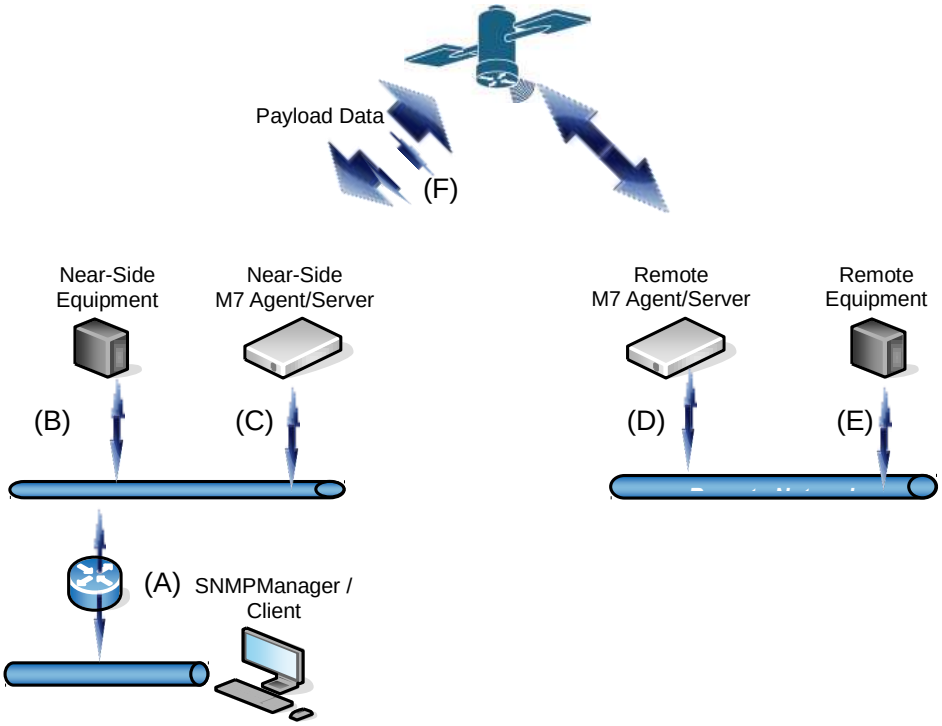

FIGURE 2: Satellite Link with SNMP

Throughout this document Figure 2 will be used to describe requirements and potential pitfalls in using the SNMP locally and remotely. The reader should keep in mind that each lettered link (A-F) must be configured for the SNMP to function properly. Configuration includes setting IP addresses, IP ports, Modem Control Channel addresses, channel bandwidth, SNMP community names for reading and writing and of course enabling the SNMP agent and MCC agent.

For now we'll quickly overview the data paths for Monitor and Control messaging and later in the document describe the steps to configure and test the SNMP exchanges.

The simplest case is a local SNMP manager controlling or monitoring a local (Near-Side) M7 agent. Communication must be established from:

SNMP Manager → A → C → Near Side M7 Agent

and a reply path must be available from

Near Side M7 Agent → C → A → SNMP Manager.

For the same command to be successful to the Remote M7 Agent a communication path must be available for the Monitor and Control (M&C) traffic. In this case the satellite link must provide the data bridge for the messages and their responses.

If the Near-Side and the Far-Side agents both have Ethernet interfaces installed; then, the M&C information can be placed onto the LANs along with the payload data. In this scenario, the payload and M&C modem ports would both be connected to their respective LANs; so, the M&C data travels undistinguished from the payload carried over the satellite link. This can be advantageous in some cases; but, this is impossible when either modem does not have an

Ethernet LAN connected to an interface. It should be noted that some customers will not want to have their payload information interspersed with M&C data.

Datum Systems provides a mechanism for exchanging the SNMP packets between the two modems by using an overhead Modem Control Channel (MCC). The overhead Modem Control Channel, (F) in the figure, can be set up explicitly in the modem configuration. For I7 and E7 IP interface cards an on-demand embedded channel can be configured.

The MCC bandwidth is manageable by the customer and keeps the payload separate from M&C data. See Section 3 for information and examples on this capability.

The remote communication path is now

SNMP Manager → A → C → Near Side M7 Agent → F → Remote M7 Agent

with a symmetric reply path of

Remote M7 Agent → F → Near Side M7 Agent → C → A → SNMP Manager

This in turn can be extended so that the remote agent can provide communications with remote equipment via (D → E). Far end devices are addressed via special formatting of the community names in the SNMP messages.

1.0.3 SNMP – Tree Structure

SNMP information is arranged in a tree like structure with branches and leaves. The first few digits of the tree are defined by the ISO organization and begin with 1.3.6.1.4.1 which stands for iso.org.dod.internet.private.enterprises.manufacturer.device.model.

1 3 6 1 4 1 31968

Several identity items which can be used by standard discovery processes begins at the OID 1.3.6.1.2.1.1.1 through 7.

And the top level OID for the M7 modem as controlled by a M7 modem device is:
1.3.6.1.4.1.31968.3.1.3

All objects and events for the M7 series of modems will begin with this OID number. For example the full OID for the modem modulator IF output level is:
1.3.6.1.4.1.31968.3.1.3.1.2.1.4.1.1.5.1

A quick note here if you are not familiar with SNMP. The individual parameters in the tree are sometimes called a “leaf”, and a scalar leaf uses “.0” after its OID to access that parameter. If the parameter is part of a table the individual parameters have designations of “.1”, “.2” and so forth representing the columns of the table.

A lengthy tree structure defined as a series of numbers would be very difficult to work with. One purpose of the MIB database is to provide a textual definition and translation between the numeric OID and human readable names for each of the parameters.

When the proper MIBs for a device such as the M7 modem are loaded into the manager/browser or into a command line version of the Net-SNMP manager/client programs, then much simpler names can be used. For example:

DATUM-M7-MODEM::modIfIFLevel.1

or more simply

modIfIFLevel.1

Obviously each OID is unique and the named element referenced by it must be unique. MIB node names follow a naming convention called camelback where the first character is always lower case letter, and upper case is used to clarify the word beginnings.

1.0.4 SNMP Additional Resources

If you are unfamiliar with SNMP and its operation there is a wealth of information available on the web. A good starting point might be to Google for “SNMP Tutorial” and “SNMP Tools”.

There are also free and commercial programs that allow one to browse the MIBs of controlled device agents. These programs run on Windows, Linux and Mac computers to provide either a textual or graphic displays of information. There are multiple open source tools available for Linux variants such as Fedora and Ubuntu among others.

The MIB provided by Datum Systems, Inc. has been tested and is believed to work without error using the free iReasoning version 10.0 MIB browser.

2.0 SNMP Configuration

Proper SNMP requires configuring and enabling the M7 modem agent and also configuring and running an SNMP manager or “browser”.

2.1 SNMP M7 modem Configuration

M7 modem SNMP configuration consists of setting the correct values for your system in the SNMP configuration parameters and enabling SNMP and or SNMP trap operations. This configuration can be done from the front panel or the web interface. Since in most cases the manager/browser is talking to multiple modems in a system the configuration will be the same for all local modems except for its unique IP address.

2.1.1 SNMP Configuration Basics

When enabled, the SNMP agent processes wait and listen for messages on the Ethernet control interface port containing the SNMP protocol. If the messages are addressed to this unit’s IP Address and are properly formed the agent will act upon the message and return a response. The modem also listens for messages on the MCC channel with its MCC receive address.

Link configuration for SNMP involves setting the SNMP parameters properly plus setting up the MCC channel if required.

Common settings for SNMP operation are identified in this document with the following color keys:

- Common modem settings are highlighted in yellow, while
- Modems with a LAN connection are highlighted in blue, and
- Modems for the remote site are in green.

Notice that a response port is not specified; all messages are returned to the incoming port.

SNMP Settings

Name	Type	Options
Server Mode	Selection	0 = Disable, 1 = Read Only, 2 = Full Access
Server Type	Selection	0 = V1, 1 = V2c
Server Port Number	Entry	Default 161, use keypad to change
Read Only Community	Entry	Default “public”
Read/Write Community	Entry	Default “private”
Trap Community	Entry	Default “datum”
Trap Path	Selection	0 – Out IP Control Port, 1 = Out MCC Port,
Trap Address	Entry	IP Address to send traps to.
Trap Port Number	Entry	Default 162, use keypad to change
Activity	Selection	0 = None, 1 = Beep, 2 = Blink Online Lamp, 3 = Beep and Blink Lamp

Also, most operators will want to set unique community strings as a minimal protection.

This list does not include the control port IP Address which should already be set. The control port IP Address is currently common to three modem controllers: the remote binary control, web control and SNMP control.

As we've mentioned, if a remote unit is not accessible on an Ethernet LAN, it may still be controlled via SNMP using MCC accesses. However, you must configure the remote modem for SNMP operation as though it were connected to a LAN. The Control port IP Address must be set and it can be different than the control address at the local end.

When the MCC is being used the remote modem must also have its MCC Rcv Address set and the MCC overhead channel operating. In fact, we recommend that a unique MCC Rcv address always be set in all modems in your network. Once the addressing is set, the channel can be enabled on an as needed basis. See the instructions in Section 3.1 and 3.1.1 on setting up the MCC channel.

2.1.1.2 Configuring SNMP via Web User Interface

Log into a M7 modem control web address and select the “Unit” page from the links on the left and then click the “SNMP” tab. The display should be similar to the figure below and configuration is simple since all the table options available are shown in a single view.

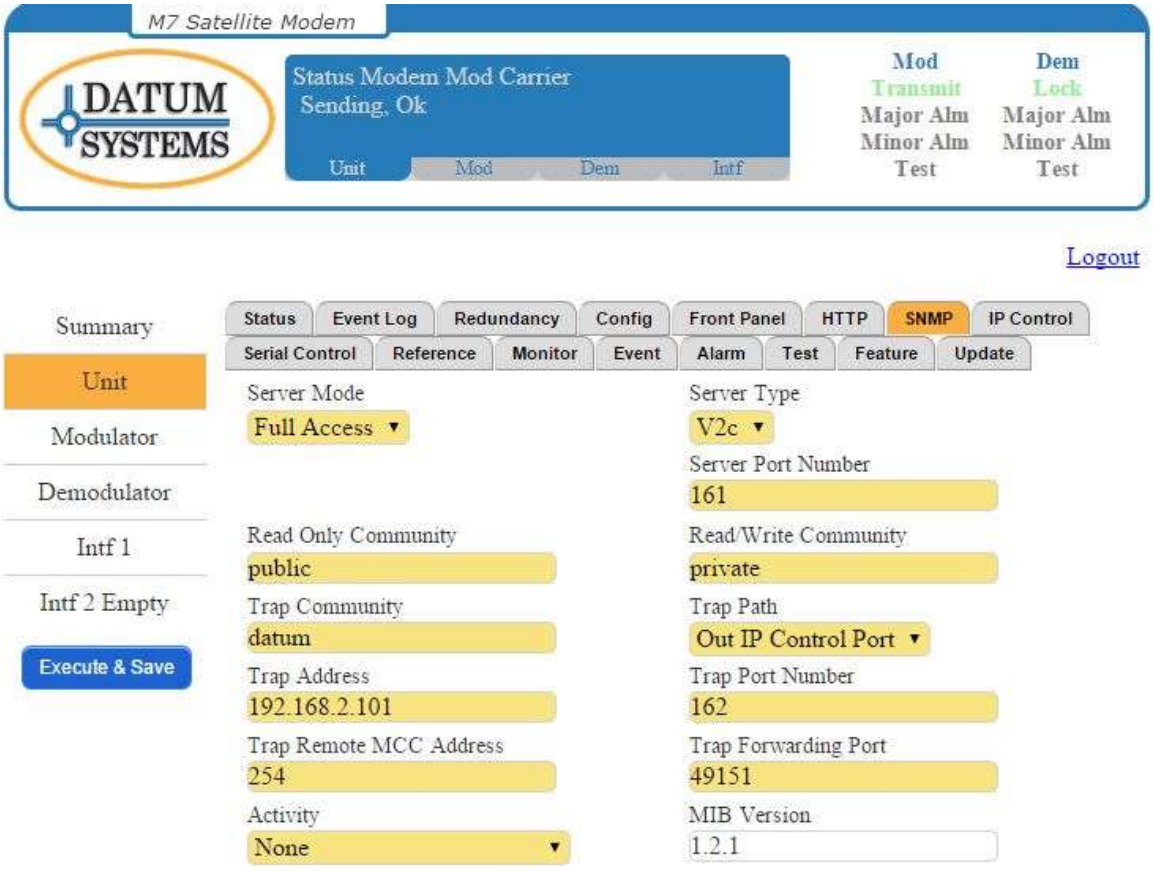

FIGURE 3 - SNMP Web Control Page

2.1.1.3 Configuring SNMP via Front Panel Controls

You can think of the modem's LCD as displaying a single cell of large matrix of available parameters, very much like a multi-page spreadsheet. The buttons below the display select the page, representing the functional element, while the arrow keys allow scrolling up, down, left and

right within the cell array. The upper left displays the column name while the upper center displays the current parameter name within that column.

On the modem front panel first press the “Unit” button under the LCD display, then scroll right until you see the label “SNMP” in the upper left of the LCD display. All of the SNMP configuration items are in this column reachable by scrolling up and down.

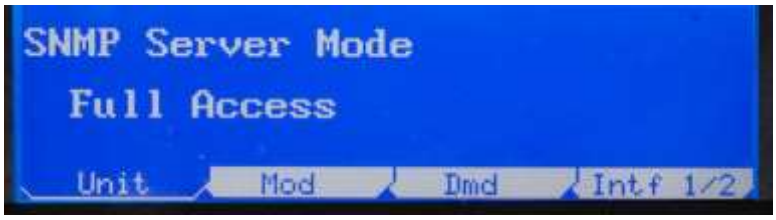

FIGURE 4 - Front Panel LCD SNMP Control

To set an item in a selection list you can either press “Edit” and then scroll up and down to locate the proper selection, or number keys directly if you know the selection number desired. Press “Enter” to confirm the selection, or “Clear” to escape the selection process.

To set an item in a manual entry parameter you can either press “Edit” and then scroll back and forth within the current setting to edit it, or enter the value directly. This is difficult on the front panel because you need to enter each character using its ASCII code. It is best to enter text items from the web interface. When finished press “Enter” to confirm the entry, or “Clear” to escape the process.

The modified parameters will be set immediately, including enabling and disabling the SNMP modem agent itself.

2.1.3 M7 Modem Agent – Built-in Parameter Organization

The parameter list in the M7 modem is too extensive to show fully here. One of the best ways to view the parameter list is to use a graphical browser and show the MIB in a “Tree” view.

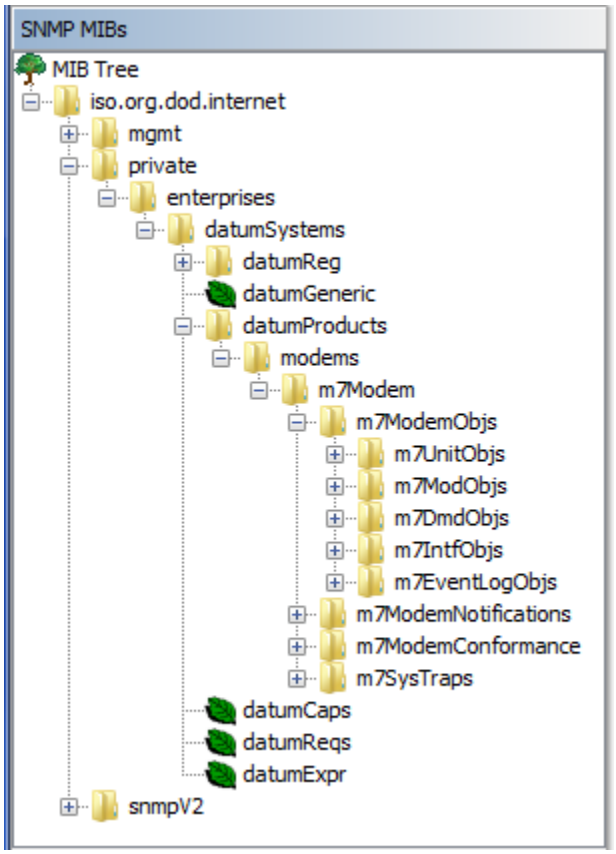

FIGURE 5 - Example Tree View of the M7 Upper-Level MIB

The parameters are divided into sections based on the installed functional cards which are plugged into the internal “slots” of the modem. There is one controller slot, two RF card slots and two interface slots.

- The controller card is named “Unit” and this category contains all of the parameters that are related to the unit as a whole plus those related to the control functions. SNMP MIB node names in this category all begin with “unit”.
- The RF slots contain modulator and/or demodulator cards of different types installed for specific applications. They usually contain one modulator and one demodulator, but could contain only one card or two demodulators. SNMP MIB node names in this category all begin with “mod” or “dmd” as appropriate followed by the type. For example “modIf” for an IF frequency range modulator, or “modLb” for an L-Band frequency range modulator.
- The interface slots can contain a wide variety of cards including Sync Serial, G.703, IP Extended Bridging (E7) and programmable IP (I7) types plus more. SNMP MIB node names in this category all begin with “int” followed by the type. For example “intSs” for a Sync Serial card, or “intG2” for a dual G.703 port.

Since there can be more than one RF card or interfaces these are arranged in an SNMP table format where the first of one particular card is followed by “.1” while the second instance is followed by “.2”. If the unit contains a dual IF based demodulator, the first instance is dmdIf.....1 and the second is dmdIf.....2. However if the cards are different, each one is followed by “.1”.

[Note 1] The exact list of available parameters may change. The web site will have information when new MIBs are released.

2.2 SNMP Browser/Manager Configuration

The Browser or Manager program is what queries the M7 modem for information. It needs a copy of MIBs for all equipment that it wants to access, as well as, knowledge of the community string and security arrangements for each piece of that equipment.

For access to the M7 modem a standard set of MIBs are used to traverse the tree from the top "iso" level down to the Private Datum Systems Products. These standard MIBs are typically distributed with the browser being used. The unique Datum Systems' M7 series modems the MIBs loaded have the file names:

1. DATUM-REG-MIB – The base Datum Systems Global Registration MIB.
2. DATUM-M7-MODEM-MIB – The M7 series modem MIB.

Note that these files have no extension, but some browsers may require the addition of ".txt" or ".mib" to operate properly. Just rename the MIB(s) to add the extension if required. Note also that Net-SNMP does not load MIBs by their file name, but instead the MIBs must be located in specific folders and the MIB is loaded using its "Definition" name. For the two MIBs above those are:

1. DATUM-GLOBAL-REG
2. DATUM-M7-MODEM-MIB

2.2.1 Net-SNMP Specific Information

The Net-SNMP suite of Master processes is common to Linux and those will be briefly described in Section 3 with examples to show their use. Our original MIB versions are created in Linux and use the Linux new line conventions which may not display correctly using a Windows program such as "Notepad". We attempt to reformat the ".txt" versions of these programs with the standard Windows new line characters.

Assuming Net-SNMP is installed on a Linux computer, the MIBs are most commonly maintained in the computer's **"/usr/share/snmp/mibs**" directory. This directory may be in **"/usr/share/mibs/netsnmp**" on versions of Net-SNMP after 5.4.2.1. Download the current "DATUM-REG-MIB" and "DATUM-M7-MODEM-MIB" from the DatumSystems.com website and place the files in that directory. Alternately you can always get the MIBs from the M7 modem itself, as they are maintained in the M7 modem's files.

To put the mibs into a Linux computer you will probably need root access or use of "sudo" to access that directory. SNMP commands such as walk, get, set, etc may scan the MIBs located there for your given parameter name. But the proper method is to tell Net-SNMP which MIBs to load beyond its standard set. A typical sequence to load the Datum Systems M7 modem MIBs might be:

```
export MIBS=+DATUM-GLOBAL-REG
export MIBS=+DATUM-M7-MODEM-MIB
```

Note that the top level MIB definition inside the DATUM-REG-MIB file does **not** match the name of the file. Net-SNMP always looks into the files to determine the MIB definition names.

After loading the MIBs you can then issue commands using the shorthand names of parameters. For example to get the current Demodulator Rcv IF Frequency you could use "snmpget" as in:

$ snmpget -v 2c -c public 192.168.15.64 demodIfFrequency.0

SNMP is also possible without loading the MIB, but you will have to know the full "OID" address of the modem parameters. They start at 1.3.6.1.4.1.31968.3.1.3 as described above.

2.2.2 Ubuntu 10.10 or others using Net-SNMP 5.4.3 and above

If you have recently updated your Linux computer and the new version of Net-SNMP is 5.4.3 or above then file locations may have changed and Net-SNMP may not work correctly with the M7 modem. The following changes to your Linux computer may be needed to recover a working system.

Beginning with Ubuntu 10.10 Net-SNMP was upgraded from Version 5.4.2.1 to 5.4.3 and all of the standard mibs were removed. The default location was also moved to a different directory, now in ***/usr/share/mibs/netsnmp*** or ietf or iana.

A) To get back the standard mibs you need to install a new package

sudo apt-get install snmp-mibs-downloader

The package installation normally downloads the standard mibs and puts them into three folders under /usr/share/mibs. There is also a resulting program named "download-mibs" but you probably won't need to use this.

B) You need to modify the snmp.conf configuration file by removing the comment # on the last line which reads "**#**mibs :"

sudo gedit /etc/snmp/snmp.conf

The last line should now be -

mibs :

C) Then you need to move the Datum System's mibs from the /usr/share/snmp/mibs folder to one of the new ones in /usr/share/mibs, for example in the netsnmp folder. They may work equally well in another folder.

sudo cp /usr/share/snmp/mibs/DATUM-* /usr/share/mibs/netsnmp/

You could also get these MIB files from the M7 modem itself if you did not have them in the snmp/mibs folder.

3.0 Basics for Using SNMP – Commands and Examples

The M7 modem is mainly intended as an agent, returning responses to SNMP commands. It can also act as a manager, getting information from other M7 modems or devices, but that application is not covered here except to note that the capability exists.

The following commands and examples are representative of operations and responses from a Linux computer running standard Net-SNMP, which is the only base system we can describe for non-proprietary SNMP functions. For operating any commercial or proprietary browser or NMS you should consult their documentation. Before these operations will succeed you must have checked the computer's package manager to determine if Net_SNMP is loaded and if not then install it.

Before being able to access SNMP information from the M7 modem you must know its "community" string that is defined for specific areas in the SNMP configuration file located in and named **"/etc/snmp/snmpd.conf"**. This file is located in the M7 modem itself. It has been set up with a base configuration to allow you to check the functioning of SNMP on the M7 modem, but should be configured properly by the user for system, security and control methods desired. That subject is beyond the scope of this document.

A typical command typed at the console of an SNMP controller might be something like the following. The $ is the prompt from the command line in Linux and is not entered as part of a command.

$ snmpget -v1 192.168.15.68 -c public iso.3.6.1.2.1.1.1.0

Which would mean: Get the public community value of the numbered iso parameter shown from the M7 modem at the IP Address shown using version 1 protocol. A response in this case might be:

iso.3.6.1.2.1.1.1.0 = STRING: "M7 Series Modem"

The M7 modem is set up by default with the "***community string***" value of "**public**" for read operations. This next example will walk through the full tree for the "SNMPv2-MIB" which is normally a predefined MIB loaded into Net-SNMP by default and is also part of the standard MIBs configured into the M7 modem's SNMP master agent.

$ snmpwalk –v 2c -c public 92.168.15.68 iso.3.6.1.2.1.1

This will produce about 7 lines of information containing The basic M7 modem identification information. Some of the information returned above can be set via the web interface on each modem to help identify it. This specific command does not return the modem parameters however since this branch of the MIB ends before connecting to the modem parameters themselves. To see everything the modem has you can end the above command after the "iso" entry.

Assuming that the M7 Modem MIBs have been loaded as described above, commands can be issued to view parameters or blocks of parameters as shown in the following examples:

Get the Demodulator IF Data Bit Rate setting from the modem/M7 modem at IP address 192.168.15.64:

$ snmpget -v 2c -c public 192.168.15.64 dmdIfDataBitRate.1

DATUM-M7-MODEM-MIB::dmdIfDataBitRate.1 = Gauge32: 2000000 1 bps

Set the Modulator Data Bit Rate to 2.048 Mbps

$ snmpset -v 2c -c private 192.168.15.64 modIfDataBitRate.1 u 2048000

DATUM-M7-MODEM-MIB::modIfDataBitRate.1 = Gauge32: 2048000 1 bps

Note that in these examples the name of the parameter must be followed by a ".1". That is because there are 2 slots for RF cards and therefore the card parameters are part of a table.

The response from the second example for "set" is shown below the command. Also note that an Unsigned32 value is returned as a Guage32 in this particular version of Net-SNMP, but the "u" type in the set command is required. Also note in the "Set" example that we had to use the read-write community value of "private" for the command to work.

Many SNMP agents attempts to "parse" the names given and searches through the available MIBs for matching entries. So for example a "Walk" command can find all items beginning with (and in some cases containing) a name. Names are not case sensitive either. So the following is an example of looking for all modulator alarms.

$ snmpwalk -v 2c -c public 192.168.15.68 modIfStatus

DATUM-M7-MODEM-MIB::modIfStatusCarrier.1 = INTEGER: sendingInterfaceAlarm(12)
DATUM-M7-MODEM-MIB::modIfStatusInterface.1 = INTEGER: summaryAlarm(2)
DATUM-M7-MODEM-MIB::modIfStatusTest.1 = INTEGER: normal(0)
DATUM-M7-MODEM-MIB::modIfTestTotalOccupiedBW.1 = Gauge32: 1733333 1 Hz
DATUM-M7-MODEM-MIB::modIfFeatureBitRateLimit.1 = INTEGER: hardwareLimits(9)
DATUM-M7-MODEM-MIB::modIfFeatureModulation.1 = INTEGER: bqoq8psk816q(2)
DATUM-M7-MODEM-MIB::modIfFeatureFEC.1 = INTEGER: vitTcmRsTpcL16k(5)

The same response would have resulted from using "**modIfSt**" or "**modIfst**". This does not always work as it depends on the sophistication of the agent. Note also that the "**walk**" command does not use the ".0" on the name end as get and set require.

If you want to see all of the parameters available in the modem then you can use the walk command from some point in the tree at the top M7 level or higher. So the following will show it all.

$ snmpwalk –Os -v 2c -c public 192.168.15.68 iso

We added the -Os option in this case that removes all the preceding "DATUM-M7-MODEM-MIB::" from the output.

3.0.1 Aggregating SNMP Commands for Interdependent Parameters

Several parameters in the modem are interdependent and may be very difficult to set as individual values. For example the FEC Type, Options and Code Rate are dependent on each other and on the modulation mode currently in force. The key to getting desirable results is to use the SNMP browser and agents' ability to send multiple elements in the same request and have the modem act upon them as a group. To read, or write, multiple parameters – names are placed in the same line with only a space between them.

For example the 3 FEC parameters could be get and set in a single request as:

$ snmpget -v 2c -c public 192.168.15.68 modIfDataFECMode.1 modIfDataFECOption.1 modIfDataFECCodeRate.1

DATUM-M7-MODEM-MIB::modIfDataFECMode.1 = INTEGER: viterbi(1)
DATUM-M7-MODEM-MIB::modIfDataFECOption.1 = Gauge32: 0
DATUM-M7-MODEM-MIB::modIfDataFECCodeRate.1 = Gauge32: 1

Now if we want to set it to TPC, Option 0 and Code Rate 4:

$ snmpset -v 2c -c private 192.168.15.68 modIfDataFECMode.1 i 4 modIfDataFECOption.1 u 0 modIfDataFECCodeRate.1 u 4

DATUM-M7-MODEM-MIB::modIfDataFECMode.1 = INTEGER: tpc(4)
DATUM-M7-MODEM-MIB::modIfDataFECOption.1 = Gauge32: 0
DATUM-M7-MODEM-MIB::modIfDataFECCodeRate.1 = Gauge32: 4

There are similar methods for creating these multi-parameter packets in graphical MIB browsers. We'll return to this example when we discuss error handling and best practices.

3.1 Basics for Using SNMP – Remote Device Control

In managing a network of satellite modems a problem arises for SNMP if the remote system does not use IP traffic as its data transfer method. Remote modems, and possibly equipment at those remote locations, have no traditional access to allow SNMP control.

When a remote IP medium is not available, the M7 modem can provide an alternate method for achieving SNMP access to the far-side modem and equipment. The user can modify the community string to act as additional addressing. In the M7 modem the community string can take three forms depending on the item to be addressed:

1. Local M7 modem directly connected to the IP LAN – "communityString"
2. Remote M7 modem directly connected via the RF link – "communityString#xxx" where xxx is the 3 digit decimal address of the MCC Receive channel at the remote modem. The "#" symbol is used as a token to denote the address.
3. Remote device on the same LAN as the remote M7 modem in Form 2 above – "communityString#xxxabbb.ccc.ddd.eee" where xxx is addressing the remote modem as above. The "a" literal character is used as a token to denote the address following and bbb.ccc.ddd.eee is the IP address of the device connected to the LAN at the remote location. The LAN must be attached to the modems control port and be within the mask of the other controlled devices.

In the methods above the community string with the added address components should not have any included spaces and must use 3 characters for each address element. The modified community string would be used in a Net-SNMP command after the "-c" argument flag. In a graphical browser you would need to define each device with its full community string, but using the same local IP address as the local modem that links to those devices.

To allow control communications with remote modems an overhead Modem Control Channel, MCC, must be provided. The MCC channel must be enabled in the modems on both ends of the link

Note: the E7 and I7 IP interfaces automatically allow for MCC overhead communications within the allowable data bandwidth. So, if both ends of the link are either the E7 or I7 IP interfaces; then, the MCC is already in place.

3.1.1 Setting Up the MCC channel

The more bandwidth that can be allocated to the MCC channel the faster the data can be retrieved from the far end. However that this process begins with a 500 mS round trip delay over the satellite plus the communications time for the given baud rate. For example a 9600 baud bi-directional MCC channel will require approximately 1 mS for each character in each direction.

You cannot perform this this setup in an operating link without an operator at the remote end. The local and remote end parameters must match.

Important: As noted earlier, you do not need to perform Steps 1 - 3 if you are using either an I7 or E7 as your operating data interface on both ends! For I7 or E7 Interfaces, skip to Step 4.

Set the

1. Send and Rcv Mux Mode to Advanced
2. Send and Rcv Mux ESC Rate to 0 unless required for other purposes.
3. Send and Rcv Mux MCC Rate to no lower than 1200 bps and preferably 9600 bps or higher.
4. Set MCC Local Modem Send and Rcv address to a unique number, such as Send/Rcv 1.
5. Set MCC Remote modem Send and Rcv Address to a unique number, such as Send/Rcv 2.
6. The MCC protocol should be already at M7 Binary Packet.
7. MCC Mode to "Full Access"

3.1.2 SNMP Control of Remote Modems

In a network with the overhead Mux and MCC channels enabled you should be able to communicate over the link. To verify this.... ***What would be a good test here?***

We should now be able to get information on the far end modem, and as an example from the local LAN browser you want to perform a complete walk over all the parameters. As an example if you are in Internet contact with a local modem at 192.168.15.68 and you want to get the parameters for the remote modem with MCC Rcv Address 2 you could use:

$ snmpwalk -Os -v 2c -c public#002 192.168.15.68 iso

The browser requests specific data from the local LAN connected M7 modem who in turn requests the information from the far end modem. That modem sends the data back over the MCC channel and the local modem prepares it as a response to the browser.

3.2 Basics for Using SNMP – Best Practices and Cautions

Neither SNMP nor the satellite modem is “magic”. SNMP is designed as a general purpose tool for networking and parameter monitoring and control. There are cases where it does not match well with modem or link capabilities. It is also intended more for machine to machine communications rather than human readability.

3.2.1 Aggregate SNMP Commands

A satellite modem is a complex piece of equipment and SNMP has a rigid set of rules that cannot easily accommodate some types of settings easily. A good example of this are the interdependent modulator, or demodulator, FEC settings.

There are three interdependent and interactive settings for the FEC Type, FEC Option and FEC Code Rate which will return an error in attempting to set them in the wrong order. To avoid the problem parameters should be sent as a single command as described in Section 3.0.1. Methods for handling this complex case are handled differently on the modem front panel and on the web page configuration.

The modem will make a best effort and set the value to the maximum (or minimum) constraints; but, you should be cautioned about specifying settings that are “out of range”.

As an example, this is true of the mod and demod data bit rate and the lower level alarm limits on the demodulator carrier level. The maximum or minimum for these values can vary considerably depending on modulation mode, interface types, installed options, FEC types, etc.

So if a modulator bit rate setting requests 12 Mbps; but, the maximum possible for the FEC type is 5 Mbps, then the modem would be limited to setting the value to at most 5 Mbps. Either disqualifying the request or setting the value to 5 Mbps would be reasonable actions. SNMP has no explicit response or error type to represent this case and will return a general error.

It is good practice to read the value of a parameter again when an error is reported after attempting to set it.

3.2.2 SNMP Bandwidth Caution

As you may have noticed doing some basic “walk” experiments, SNMP can easily return a significant amount of information. SNMP is also very inefficient from a bandwidth standpoint. Considering that much SNMP monitor traffic will be over a satellite link with limited bandwidth and resources, care should be exercised to reduce the amount of SNMP traffic to a minimum. If a

management system is polling every possible parameter every second; then, the system performance will suffer.

3.2.3 Far End SNMP Modem Control Caution

This might be a good place to say “think before you act”. Satellite links often connect to remote unmanned sites. It is extremely easy to change a setting on the far end of a link at a remote site and cause the link to lose connectivity and control. Then someone will have to go to that site to restore operation.

The M7 series of modems are designed with the ability to automatically go to several predefined configurations if the receive carrier is lost for longer than a specified period of time. If thought out in advance and the consequences of signal loss are known to operations personnel; then this should be part of a recovery strategy. See the main M7 modem manual for more information on the “ACR” or Automatic Configuration Recovery feature.

4.0 Troubleshooting

Does none of this seem to work for you? If you cannot get SNMP to work with the M7 modem or the modem then it’s time to do some basic checking and troubleshooting.

4.1 Basic Requirements for SNMP to Work and Tests

SNMP can be difficult for newcomers. All of the following must be in place for SNMP to work:

1. The M7 modem must be at a valid IP Address and Mask for the connected network.
2. You must have a valid browser/manager computer to access the M7 modems' SNMP agent.
3. The management computer and the M7 modem must be mutually accessible. All intervening routers and firewalls must allow access to the ports and protocols to be used.
4. The SNMP agent software must be enabled on the M7 modem. Check the front panel Unit: SNMP Mode setting.
5. The manager computer must be running Net-SNMP or an SNMP Browser program.
6. The SNMP browser/manager must have the appropriate MIBs loaded.
7. Community names are case sensitive and must match exactly between communicating elements.

Test Connectivity:

One first test that will determine if 1, 2 and 3 conditions are met is to “ping” the M7 modem from the management computer. If you do not get a response then several things might be at fault:

1. The most common issue is that the network addresses are incorrect.
2. ICMP messaging, which IP ping relies on, may be blocked by the router on the local network, (A) in Figure 2. Keep in mind that routers may allow ping replies originated from a ping request on a local node; but, may also disallow ping requests originating on the “hot” side of a firewall.
3. Similarly, the protocol may be allowed but may require a non-standard port.
4. Routes in the gateway, (A) in Figure 2, are usually not the main culprit; but, tracert may be helpful to determine that the messaging is using the path you expect. Modern computers typically have a wired and a wireless interface – insure you're using the connection you want.

Check with your IT group and make sure you can at least ping the local modem before you try any advanced testing. Keep in mind the issues mentioned for the ICMP ping can also be true for the SNMP and HTTP protocols and ports. If non-standard ports are necessary make sure to make the adjustments to Modem protocol configuration.

Test M7 Agent Running:

The agent is running if you get a response to a known good SNMP request. If not then check the modem configuration to insure that SNMP in enabled.

The web interface also contains a page at Unit in the SNMP tab which allows both immediate and persistent SNMP agent control.

Test Manager/Browser Functionality:

If you've made it this far and you cannot get information in the browser or Net-SNMP from the M7 modem then you should double check the browser configuration again. Make sure you are using the correct IP Addresses and community string in the configuration. For Net-SNMP this is on the command line for each command. For browsers this is typically a GUI configuration item. For example iReasoning's browser has a configuration setup at Tools>>Options and the Agents tab which is used to set up the version and read and write community strings for each IP Address.

Test Manager/Browser MIB Load: Insure that the MIBs are loaded in the browser or Net-SNMP. Read Section 2.2 and check that the proper MIBs and directories exist and are being used for loading. Graphical browsers normally show which MIBs are loaded as part of their window presentation. With Net-SNMP the standard MIBs loaded by default should allow operation with the M7 modem.

It is often beneficial to change the file name or directory name and make sure that the tool fails to load the file with the name altered. If the tool still loads the MIB in the same way, there's a duplication, or cache, which must be accounted for.

5.0 SNMP Traps

Notifications and Traps serve the same purpose – to asynchronously inform a client of an event. The names of the messages and the datagram formats differ between the two types of messages as they were introduced in different revisions of the SNMP protocol. Traps are the SNMP v1 form of messaging and this was usurped by Notifications in SNMP v2c.

However, most users refer to both with the same term – traps. The changes in the packet format are handled transparently by the MIB browser/query tool and the differences become superfluous to the end user. So we'll refer to both datagram types as traps – regardless of the protocol version.

SNMP Traps are generated by background processes that monitor specified parameters. If the parameter falls outside of proper range then a “trap” message is generated and the manager is notified.

5.1 Configuring SNMP Traps

5.1.1 SNMP Notification Setup Procedure

The setup to send Traps to a SNMP client/manager involves the following steps:

1. Setting the SNMP Trap Address

2. Setting the SNMP Trap Port Number
3. Setting the SNMP Trap Community
4. Setting the SNMP Trap Path

These configuration values can be manipulated on the front panel or can be changed using the Web interface.

--End of Document.