Debugging SNMP using CLI

Topic Covered

Featured Brands

lumbergautomation A BELDEN BRAND
HIRSCHMANN A BELDEN BRAND
TOFINO SECURITY A BELDEN BRAND
GarrettCom A BELDEN BRAND

General Information

1 SNMP Description:

The Simple Network Management Protocol (SNMP) is a widely deployed protocol that is commonly used to monitor and manage network devices. SNMP-compliant devices, have an embedded application called an SNMP agent. The SNMP agent can access data about the network device it is running on using predefined Object Identifiers (OIDs) contained in a Management Information Base (MIB) and return this data to an SNMP requester.

There is one exception to the request/reply operation of SNMP. That is when SNMP Traps are enabled. SNMP Traps are unrequested messages sent to the SNMP requester by the SNMP agent on the network device containing information on critical events that occur to the network device.

The SNMP requester (MIB Browser, SNMP Trap Receiver, Network Management Software or Network Monitoring Software) is software that runs on another piece of equipment that uses the MIBs to request specific information of Network devices and can store, summarize and/or notify IT personnel of problems on the network.

There are three major versions of the SNMP protocol. They are described by IETF Request For Comment (RFC) documents as listed below.

SNMPv1 RFC

The SNMP Version 1 RFC is:

RFC 1157. Simple Network Management Protocol

SMIv1 RFCs also apply to all SNMPv1 entities.
MIB-II RFCs also apply to all SNMPv1 agent entities.

SNMPv2 RFCs

The SNMP Version 2 RFCs are:

- RFC 1901. Introduction to Community-based SNMPv2
- RFC 1908. Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
- RFC 3416. Version 2 of SNMP Protocol Operations
- RFC 3417. Transport Mappings

SMIv1 and SMIv2 RFCs also apply to all SNMPv2c entities.
MIB-II RFCs also apply to all SNMPv2c agent entities.

SNMPv3 RFCs

The SNMP Version 3 RFCs are:

- RFC 3410. Introduction and Applicability Statements for Internet Standard Management Framework

- RFC 3411. An Architecture for Describing SNMP Management Frameworks
- RFC 3412. Message Processing and Dispatching
- RFC 3413. SNMP Applications
- RFC 3414. User-based Security Model
- RFC 3415. View-based Access Control Model
- RFC 3416. Version 2 of SNMP Protocol Operations
- RFC 3417. Transport Mappings
- RFC 3584. Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
- RFC 3826. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- RFC 5343. Simple Network Management Protocol (SNMP) Context EngineID Discovery

Additional SNMPv3 RFCs including the Datagram Transport Layer Security RFCs (also known as DTLS or (D)TLS) are:

- RFC 5590. Transport Subsystem for the Simple Network Management Protocol (SNMP)
- RFC 5591. Transport Security Model for the Simple Network Management Protocol (SNMP)
- RFC 5953. Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)

SMIv1 and SMIv2 RFCs also apply to all SNMPv3 entities.
MIB-II RFCs also apply to all SNMPv3 agent entities.

MNS-DX supports the following MIBs:

- MIB-II
- TARGET-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-USER-BASED-SM-MIB

And each GarrettCom Product family also has its own Enterprise MIB

- DX ENTERPRISE MIB
- MNS ENTERPRISE MIB
- INOS ENTERPRISE MIB

2 Initial Preparation

Gather the information, tools and equipment needed to complete this task. The example values given in this document are not meant to be thought of as recommended as each installation is unique and has its own requirements.

2.1 Tools and equipment:

2.1.1 Cables

2.1.1.1 10RX, 6KL Console

Console cable RJ45 to DB9 for systems with serial port (**Model CONSOLE-CBLQD**) or

Console cable RJ45 to USB for systems with only USB ports **(Model CONSOLE-CBLQU)**

RJ45 Ethernet cable

1	**RTS**	**Request to Send**
2	**Not Used**	**No Connection**
3	**TXD**	**Transmit Data (out)**
4	**GND**	**Signal ground**
5	**Not Used**	**No Connection**
6	**RXD**	**Receive Data (in)**
7	**Not Used**	**No Connection**
8	**CTS**	**Clear to Send**

RJ45 Console port pin assignments 10RX, 6KL

2.1.1.2 DX, 10XTS Console

Console cable DB9 to DB9 for systems with serial port (**Model CONSOLE-CBLQD**) or

Console cable DB9 to USB for systems with only USB ports **(Model CONSOLE-CBLQU)**

RJ45 Ethernet cable

Pin	Name	Dir.	Description
1	DCD	In	Data Carrier Detect from DCE.
2	RXD	In	Receive Data from DCE.
3	TXD	Out	Transmit Data to DCE.
4	DTR	Out	Data Terminal Ready to DCE.
5	GND	Power Reference	Signal Ground.
6	DSR	In	Data Set Ready from DCE.
7	RTS	Out	Request To Send.
8	CTS	In	Clear to Send.
9	RI	In	Ring Indicator from DCE.

DB9 Console port pin assignments DX, 10XTS

2.1.2 Software

Terminal Server Software for a Windows PC supporting serial and SSH connections to access the MNS, MNS-DX, INOS CLI;

Recommended, not supplied by Belden.

Examples: TeraTerm (http://en.osdn.jp/projects/ttssh2/releases/)

Putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html)

Internet Browsers used to access the MNS, MNS-DX, INOS Graphical User Interface, hereafter called the GUI.

Examples: Firefox (https://www.mozilla.org/)

Chrome (https://www.google.com/chrome/)

MIB Browsers used to query SNMP Agents

Examples: MG-Soft MIB Browser (Commercial Product, must be purchased)

(https://www.mg-soft.si/download.html)

Snmpwalk (a component of Linux SNMP, CygWin windows Linux subsystem)

(https://www.cygwin.com/)

Industrial HiVision (Commercial Product, a 16 agent version is free)

(http://www.hivision.de/English/Free_Version/index.phtml)

Other than Industrial HiVision these are third party software and as such are not supported by Belden.

2.1.3 Laptop or Desktop Personal Computer required

These devices are not supplied nor supported by Belden

2.2 Information to get before starting:

This information may be supplied by your IT department or the network administrator for the network where the MNS, MNS-DX, INOS system will be installed.

2.2.1 IP address assigned to the SNMP Agent

Example Value Used: 192.168.1.2 (Default address for MNS, MNS-DX and INOS devices)

2.2.2 Protocol used by the SNMP Agent

Example Value Used: UDP (UDP and TCP are available)

2.2.3 UDP or TCP port used by the SNMP Agent

Example Value Used: 161 (default for UDP or TCP)

Example Value Used: 162 (default for UDP Trap or TCP Trap)

2.3 Special Note for DX Firmware Versions 4.1.0 and above

The following changes for the management station feature were done during implementation of Zero Touch Provisioning required by Industrial HiVision software.

Current default behavior for the management station is:

- By default SNMP V3 is enabled, and a default user of manager is configured.
- If no management station IP is configured, then the device will process the SNMP queries from all IP addresses. (This was done as the IP address of Industrial HiVision Software could be any address)
- If a management station IP is configured, the device will process the SNMP queries only from the IP addresses of the listed management stations.

3 Connecting to the DUT

3.1 Console Port Connections

The console port of the 10RX is an RJ45 connector that can be located on either the front or rear of the system. It is always located with the LED indicators (power, activity or connectivity)

Use the appropriate cable to connect from the laptop to the console port. Start the Terminal program installed on your PC (TeraTerm in this document), select the appropriate serial port (this will vary from system to system depending on the cable and the adapter used) and configure the serial port properties as follows:

- 38400 Baud rate
- 8 Data bits
- 1 Stop bit
- No Parity
- No Flow Control

After completing this and hitting the enter key you should see a **login:** prompt. The default username and password is **manager**.

3.2 SSH Connections

Before connecting to the Ethernet port on the DUT the IP address of the Laptop/PC must be set to be in the same subnet as the default IP of the DUT, **in this example it is set to 192.168.1.2 mask 255.255.255.0.**

Only Ethernet port 1/1 is enabled when the 10RX is first powered up. This port is always the top left port set when facing the system. The 10RX Ethernet ports 1 and 2 are RJ45/SFP socket port pairs only one or the other can be used. When first setting up the system it is recommended that the fiber port not be used till all initial setup is done. The default address is 192.168.1.2.

Some Terminal Server software will take what seems a long time to make the first connection, do not despair a lot of back and forth occurs just this once and usually once all this has completed you will be asked to accept a key (not accepting this key will not allow you to login).

After this you will see a **login:** prompt. The default username and password is **manager**.

NOTE: Remember that once the IP address of the DUT has been changed this initial SSH connection will no longer be valid and a new session with the new address must be started to continue.

3.3 Web/GUI Connections

Before connecting to the Ethernet port on the DUT the IP address of the Laptop/PC must be set to be in the same subnet as the default IP of the DUT, **in this example it is set to 192.168.1.1 mask 255.255.255.0.**

Only Ethernet port 1/1 is enabled when the 10RX is first powered up. This port is always the top left port set when facing the system. The 10RX Ethernet ports 1 and 2 are RJ45/SFP socket port pairs only one or the other can be used. When first setting up the system it is recommended that the fiber port not be used till all initial setup is done. The example address is 192.168.1.2 and a secure connection is required. Thus the URL/Address to access will be **https://192.168.1.2**.

NOTE: All newer web browsers and all older browsers that have all of the security updates installed are configured by default to reject self-signed certificates (these certificates are used to setup the SSL secure connection). However you are offered as the user the opportunity to bypass this block and continue to the web page. You will be required to do this for the DUT.

After this you will see a **login:** screen. The default username and password is **manager**.

4 Debugging SNMP V1/V2c

This document DOES NOT show you how to configure SNMP on any of the GarrettCom devices. Please refer to the Admin documents for the device you are using for information on how to configure SNMP.

https://garrettcom-support.belden.com/ is the GarrettCom Support Portal where you can access these documents.

4.1 First Step Check Network Connectivity

Ping from the SNMP Server to the SNMP Agent

An example of a successful Ping;

C:\Users\mrbrown>ping 96.233.66.245

Pinging 96.233.66.245 with 32 bytes of data:

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Ping statistics for 96.233.66.245:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

An example of a failed Ping;

C:\Users\mrbrown>ping 96.233.66.245

Pinging 96.233.66.245 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 96.233.66.245:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\mrbrown>

The above is an example of 2 ping requests from the System that hosts the SNMP Servers to the system (DX40 in this example) with the SNMP Agent. The first shows 4 good ping request/replies, with this result it is time to continue to the next step. The second shows a ping request timeout a timeout indicates a network problem. This problem needs to be solved before continuing, this document does not cover debugging network problems.

4.2 Second Step Check Access to the SNMP Agent

Start the SNMP MIB browser you have selected or use the Linux Snmpwalk command

CygWin SNMPWalk Get Request

mrbrown@BNATECH-PC ~

$ snmpwalk -v 2c -c public 96.233.66.245 1.3.6.1.2.1.1.1.0

Timeout: No Response from 96.233.66.245

MG-Soft MIB Browser Contact Request

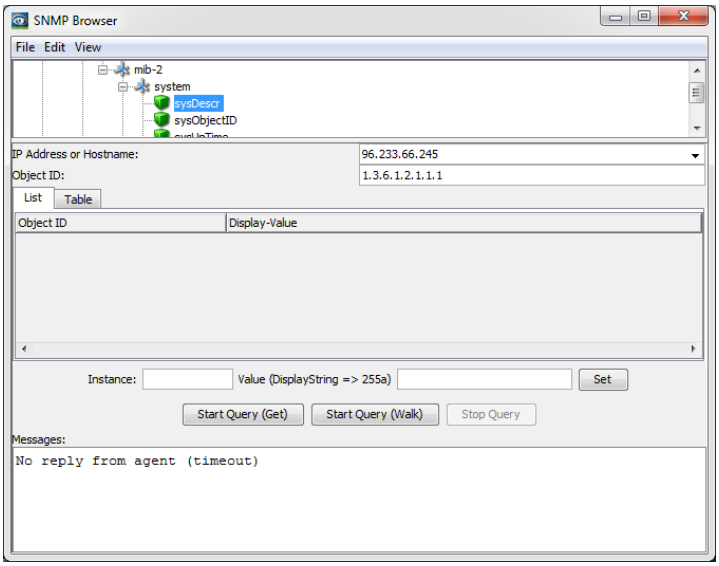
Remote address: 96.233.66.245 port: 161 transport: IP/UDP

Local address: 96.233.66.242 port: 61785 transport: IP/UDP

Protocol version: SNMPv2c

TIMEOUT

Industrial HiVision Get Requests



If you see a timeout;

- Check to see if SNMP is Enabled on the DUT
- Check to see if SNMP Agent Read community setting matches the SNMP Server Settings
- Check to see that SNMP management IP address is set on the DUT

➢ Example CLI commands to check configurations

- DX Example of Show SNMP Settings

```
C4F1DX# snmp show sett

        Mode : V1/V2 Enabled

        Local IP : Any

        Write Access : Disabled

        Traps : Disabled

        Read Community String : public

        Write Community String : private

        Engine Id : 000039cd0300206104c4f100
```

```
                Engine Boots : 45

                Engine Time (secs) : 3372205

        C4F1DX# snmp show station

                Station Name

                ============================

                96.233.66.242

        C4F1DX#
```

- MNS 6K Example of Show SNMP Settings

```
        00:20:06:4a:b3:e0 6KL##show snmp

                SNMP CONFIGURATION INFORMATION

                ------------------------------

                SNMP Get Community Name  :  public

                SNMP Set Community Name  :  private

                SNMP Trap Community Name :  public

                AuthenTrapsEnableFlag    :  disabled

                SNMP Access Status       :  enabled

                SNMP MANAGERS INFO

                ------------------

                IP Address = 192.168.1.4

                SNMP TRAP STATIONS INFO

                ----------------------

                IP Address = 192.168.1.4 Trap Type = SNMP,
               Enterprise

        00:20:06:4a:b3:e0 6KL## show active-snmp

                SNMP Agent supports v1 only.

        00:20:06:4a:b3:e0 6KL##
```

- INOS 10RX Example of Show SNMP Settings

```
10RX-5BB0## show snmp community

    Community Index : private

    Community Name  : private

    Security Name   : private

    Transport Tag   :

    Row Status      : Active

    ------------------------------

    Community Index : public

    Community Name  : public

    Security Name   : public

    Transport Tag   :

    Row Status      : Active

    ------------------------------

10RX-5BB0## show snmp group

    Security Model : v2c

    Security Name  : public

    Group Name     : public

    Row Status     : Active

    ------------------------------

    Security Model : v2c

    Security Name  : private

    Group Name     : private

    Row Status     : Active

    ------------------------------
```

```
10RX-5BB0## show snmp access

    Group Name   : public

    Read View    : defaultv2c

    Write View   : defaultv2c

    Notify View  : defaultv2c

    Row Status   : Active

    ------------------------------

    Group Name   : private

    Read View    : defaultv2c

    Write View   : defaultv2c

    Notify View  : defaultv2c

    Row Status   : Active

    ------------------------------

10RX-5BB0## show snmp view

    View Name    : defaultv2c

    Subtree OID  : 1

    Subtree Mask : 1

    View Type    : Included

    Row Status   : Active

    ------------------------------

10RX-5BB0## show snmp targetaddr

    Target Address Name : HighvisionL3

    IP Address          : 172.29.1.99

    Port                : 162

    Tag List            : 1

    Parameters          : ParamHV
```

```
Row Status          : Active

------------------------------

10RX-5BB0##
```

4.3 Third Step See If a Full Walk of the DUT Works

A full walk can be done by default with CygWin snmpwalk by leaving the OID value blank this becomes a series of get next commands automatically executed till the first failure of that command

```
mrbrown@BNATECH-PC ~

$ snmpwalk -v 2c -c public 96.233.66.245

SNMPv2-MIB::sysDescr.0 = STRING: DX40

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.553

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (339094705) 39 days, 5:55:47.05

SNMPv2-MIB::sysContact.0 = STRING: Mike Brown

SNMPv2-MIB::sysName.0 = STRING: DX40 Extended Test C4F1

SNMPv2-MIB::sysLocation.0 = STRING: BNA Tech Support

SNMPv2-MIB::sysServices.0 = INTEGER: 79

IF-MIB::ifNumber.0 = INTEGER: 5

Cut approximately 450 lines of output to make it more readable

IF-MIB::ifAlias.2 = STRING:

IF-MIB::ifAlias.101 = STRING:

IF-MIB::ifAlias.102 = STRING:

IF-MIB::ifAlias.10001 = STRING:

IF-MIB::ifCounterDiscontinuityTime.1 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.2 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.101 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.102 = Timeticks: (0) 0:00:00.00
```

```
IF-MIB::ifCounterDiscontinuityTime.10001 = Timeticks: (0) 0:00:00.00

IF-MIB::ifStackStatus.0.10001 = INTEGER: active(1)

IF-MIB::ifStackStatus.0.100001 = INTEGER: active(1)

IF-MIB::ifStackStatus.10001.0 = INTEGER: active(1)

IF-MIB::ifStackStatus.100001.0 = INTEGER: active(1)

IF-MIB::ifRcvAddressStatus.10001.". a..." = INTEGER: active(1)

IF-MIB::ifRcvAddressStatus.10001."..^..." = INTEGER: active(1)

IF-MIB::ifRcvAddressType.10001.". a..." = INTEGER: nonVolatile(3)

IF-MIB::ifRcvAddressType.10001."..^..." = INTEGER: nonVolatile(3)

IF-MIB::ifTableLastChange.0 = Timeticks: (0) 0:00:00.00

IF-MIB::ifStackLastChange.0 = Timeticks: (0) 0:00:00.00
```

Snmpwalk only scans the public MIBs NOT the enterprise (private) MIBs as the enterprise MIBs are not by default loaded

If you only see a few (less than 5 lines output) from this test

- Check that you have not restricted what the agent can output via configuration
- The application (MIB Browser, SNMPWalk or HiVision) is not configured properly (MIB's not loaded)
    - This document will not cover the possible fixes to this situation

➢ **Sample CLI commands to look at view restrictions**

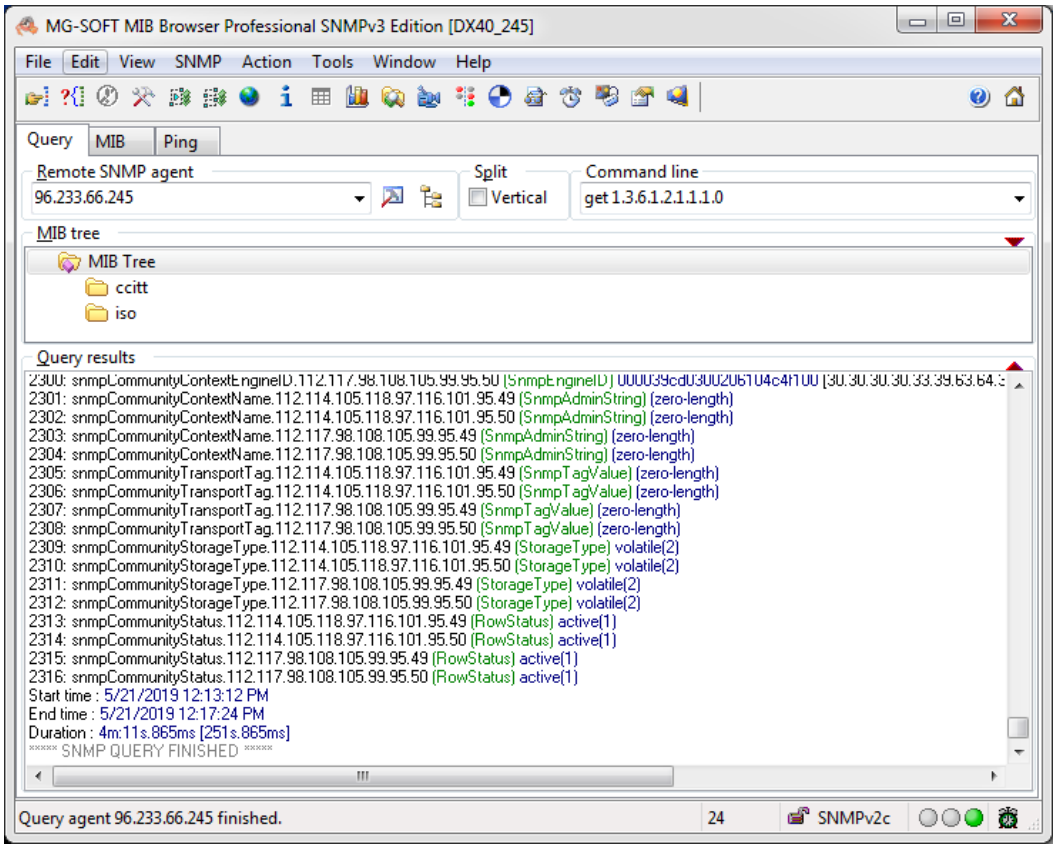
- The DX does not have a configuration option to restrict MIB access
- The MNS 6K Example of the MIB access restrictions (allow all is the example) this command is only available for SNMPV3

```
00:20:06:4a:b3:e0 6KL#(snmpv3)##show-view

 ID View Name      Type      Subtree                Mask

 ========================================

  1 all              included       .1                   ff

00:20:06:4a:b3:e0 6KL#(snmpv3)##
```

- The INOS 10RX Example of the MIB access restrictions (allow all is the example)

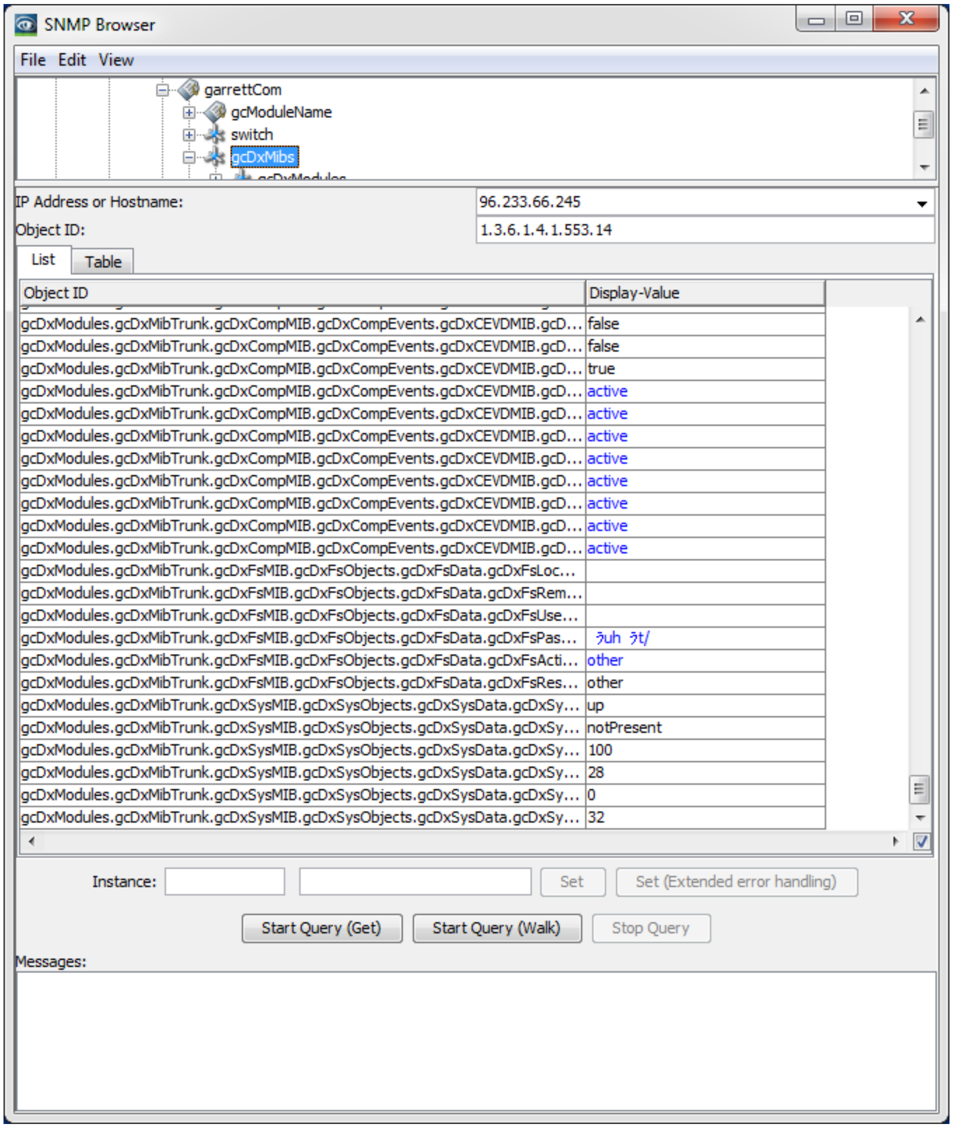
```
10RX-5BB0## show snmp view

    View Name    : defaultv2c

    Subtree OID  : 1

    Subtree Mask : 1

    View Type    : Included

    Row Status   : Active

    ------------------------------

10RX-5BB0##
```

Sample Output of MG-Soft MIB Browser with DX MIBs manually loaded walking through the MIBs



Note the 2316 MIB OIDs scanned more than 6 times the number using the basic snmpwalk

Sample Output of Industrial HiVision this software loads DX MIBs when a system is discovered during setup



The difference here is that ONLY the DX MIB was walked as the section of the MIBs you want to scan needs to be selected, see top window in browser

4.4 Sample Wireshark Capture of SNMP Get Request

Capture fully expanded and saved as text.

No. Time Source Destination Protocol Length Info

389 45.785048 192.168.1.4 96.233.66.245 SNMP 83 get-request 1.3.6.1.2.1.1.3.0

Frame 389: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0

Ethernet II, Src: Dell_6f:25:42 (5c:f9:dd:6f:25:42), Dst: Actionte_33:f2:71 (f8:e4:fb:33:f2:71)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 96.233.66.245

User Datagram Protocol, Src Port: 56186, Dst Port: 161

Simple Network Management Protocol

version: v2c (1)

community: public

data: get-request (0)

get-request

request-id: 210

error-status: noError (0)

error-index: 0

variable-bindings: 1 item

1.3.6.1.2.1.1.3.0: Value (Null)

Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)

Value (Null)

No. Time Source Destination Protocol Length Info

390 45.796169 96.233.66.245 192.168.1.4 SNMP 87 get-response 1.3.6.1.2.1.1.3.0

Frame 390: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0

Ethernet II, Src: Actionte_33:f2:71 (f8:e4:fb:33:f2:71), Dst: Dell_6f:25:42 (5c:f9:dd:6f:25:42)

Internet Protocol Version 4, Src: 96.233.66.245, Dst: 192.168.1.4

User Datagram Protocol, Src Port: 161, Dst Port: 56186

Simple Network Management Protocol

version: v2c (1)

community: public

data: get-response (2)

get-response

request-id: 210

error-status: noError (0)

error-index: 0

variable-bindings: 1 item

1.3.6.1.2.1.1.3.0: 347425620

Object Name: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)

Value (Timeticks): 347425620

5 Debugging SNMP V3 (No Encryption)

5.1 First Step Check Network Connectivity

Ping from the SNMP Server to the SNMP Agent

C:\Users\mrbrown>ping 96.233.66.245

Pinging 96.233.66.245 with 32 bytes of data:

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Ping statistics for 96.233.66.245:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\mrbrown>ping 96.233.66.245

Pinging 96.233.66.245 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 96.233.66.245:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\mrbrown>

The above is an example of 2 ping requests from the System that hosts the SNMP Servers to the system (DX40 in this example) with the SNMP Agent. The first shows 4 good ping request/replies, with this result it is time to continue to the next step. The second shows a ping request timeout a timeout indicates a network problem. This problem needs to be solved before continuing, this document does not cover debugging network problems.

5.2 Second Step Check Access to the SNMP Agent (No Encryption)

Start the SNMP MIB browser you have selected or use the Linux Snmpwalk command

CygWin SNMPWalk Get Request

mrbrown@BNATECH-PC ~

$ snmpwalk -v 3 -u admin -l AuthNoPriv -A password -a MD5 96.233.66.245 1.3.6.1.2.1.1.1.0

snmpwalk: Authentication failure (incorrect password, community or key)

mrbrown@BNATECH-PC ~

$ snmpwalk -v 3 -u manager -l AuthNoPriv -A garrettcom -a MD5 96.233.66.245 1.3.6.1.2.1.1.1.0

snmpwalk: Unknown user name

mrbrown@BNATECH-PC ~

$ snmpwalk -v 3 -u admin -l AuthNoPriv -A password -a SHA 96.233.66.245 1.3.6.1.2.1.1.1.0

snmpwalk: Authentication failure (incorrect password, community or key)

mrbrown@BNATECH-PC ~

$ snmpwalk -v 3 -u admin -l AuthNoPriv -A password -a MD5 96.233.66.245 1.3.6.1.2.1.1.1.0

snmpwalk: Timeout

MG-Soft MIB Browser Contact Request

Remote address: 96.233.66.245 port: 161 transport: IP/UDP

Local address: 192.168.1.4 port: 50151 transport: IP/UDP

Protocol version: SNMPv3

Request:

User profile name:

Security user name: admin

Security engine ID: (zero-length)

Context name: (zero-length)

Context engine ID:

Authentication protocol: HMAC MD5

Privacy protocol: None

Security level: Authentication

Security model: USM

Operation: Get next

1: sysUpTime (TimeTicks) null

TIMEOUT

Disabled ==========

Remote address: 96.233.66.245 port: 161 transport: IP/UDP

Local address: 192.168.1.4 port: 57043 transport: IP/UDP

Protocol version: SNMPv3

Request:

User profile name:

Security user name: manager

Security engine ID: (zero-length)

Context name: (zero-length)

Context engine ID:

Authentication protocol: HMAC MD5

Privacy protocol: None

Security level: Authentication

Security model: USM

Operation: Get next

1: sysUpTime (TimeTicks) null

Synchronize:

SNMPv3 report received from remote agent.

Security engine ID updated.

User profile name:

Security user name: manager

Security engine ID: 000039cd0300206104c4f100

Context name: (zero-length)

Context engine ID: 000039cd0300206104c4f100

Authentication protocol: HMAC MD5

Privacy protocol: None

Security level: Authentication

Security model: USM

1: usmStatsUnknownEngineIDs.0 (Counter32) 18

Response:

SNMPv3 report received from remote agent.

User profile name:

Security user name: manager

Security engine ID: 000039cd0300206104c4f100

Context name: (zero-length)

Context engine ID: 000039cd0300206104c4f100

Authentication protocol: HMAC MD5

Privacy protocol: None

Security level: Authentication

Security model: USM

1: usmStatsUnknownUserNames.0 (Counter32) 9

UsernameWrong ==========

Remote address: 96.233.66.245 port: 161 transport: IP/UDP

Local address: 192.168.1.4 port: 61820 transport: IP/UDP

Protocol version: SNMPv3

Request:

User profile name:

Security user name: admin

Security engine ID: (zero-length)

Context name: (zero-length)

Context engine ID:

Authentication protocol: HMAC SHA

Privacy protocol: None

Security level: Authentication

Security model: USM

Operation: Get next

1: sysUpTime (TimeTicks) null

Synchronize:

SNMPv3 report received from remote agent.

Security engine ID updated.

User profile name:

Security user name: admin

Security engine ID: 000039cd0300206104c4f100

Context name: (zero-length)

Context engine ID: 000039cd0300206104c4f100

Authentication protocol: HMAC SHA

Privacy protocol: None

Security level: Authentication

Security model: USM

1: usmStatsUnknownEngineIDs.0 (Counter32) 22

AuthProtocolWrong ==========

Remote address: 96.233.66.245 port: 161 transport: IP/UDP

Local address: 192.168.1.4 port: 63825 transport: IP/UDP

Protocol version: SNMPv3

Request:

User profile name:

Security user name: admin

Security engine ID: (zero-length)

Context name: (zero-length)

Context engine ID:

Authentication protocol: HMAC MD5

Privacy protocol: None

Security level: Authentication

Security model: USM

Operation: Get next

1: sysUpTime (TimeTicks) null

Synchronize:

SNMPv3 report received from remote agent.

Security engine ID updated.

User profile name:

Security user name: admin

Security engine ID: 000039cd0300206104c4f100

Context name: (zero-length)

Context engine ID: 000039cd0300206104c4f100

Authentication protocol: HMAC MD5

Privacy protocol: None

Security level: Authentication

Security model: USM

1: usmStatsUnknownEngineIDs.0 (Counter32) 24

Response:

SNMPv3 report received from remote agent.

User profile name:

Security user name: admin

Security engine ID: 000039cd0300206104c4f100

Context name: (zero-length)

Context engine ID: 000039cd0300206104c4f100

Authentication protocol: HMAC MD5

Privacy protocol: None

Security level: Authentication

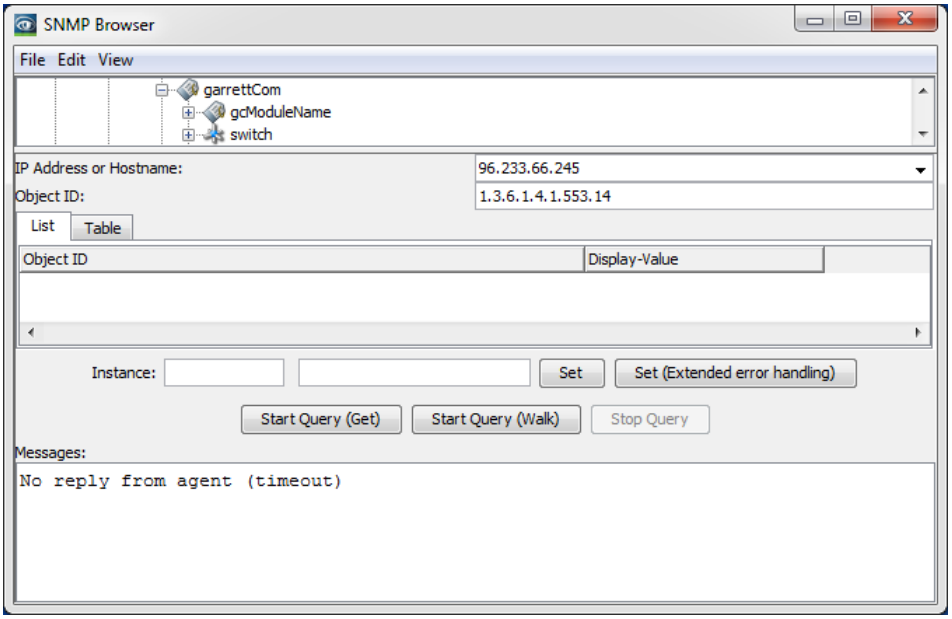
Security model: USM

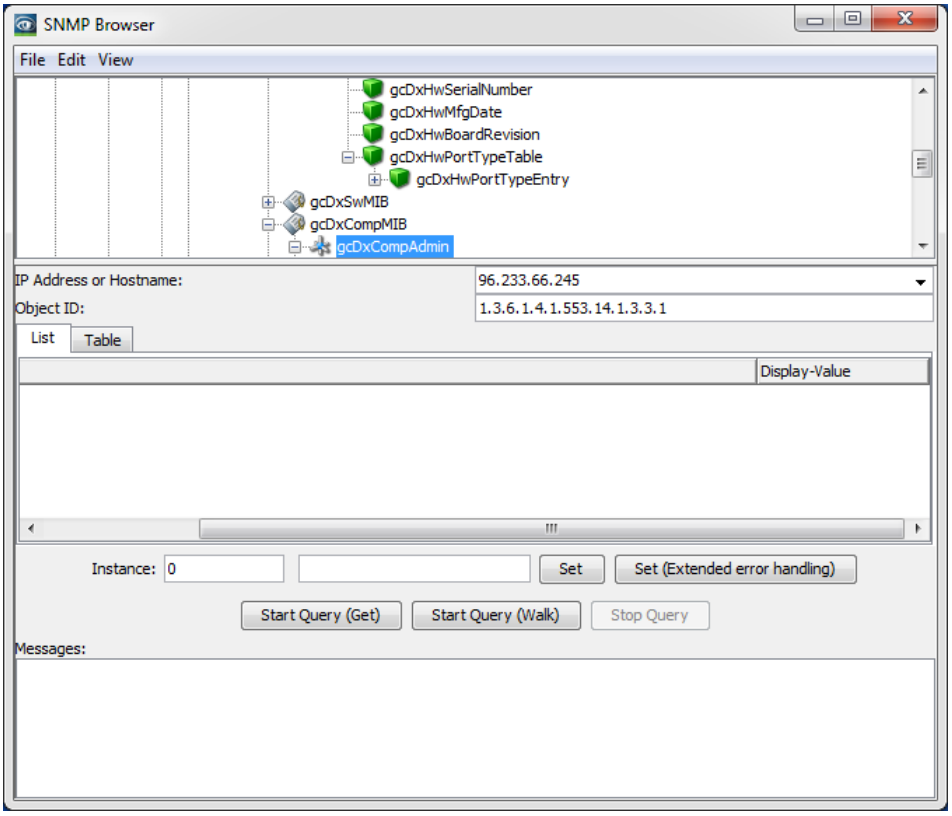
1: usmStatsWrongDigests.0 (Counter32) 3

WrongAuthPassword ==========

Industrial HiVision Get Requests

The HiVision Browser does not support the range of error messages as snmpwalk and the MG-Soft Browser





If you see an error message;

- Check to see if SNMP version 3 is Enabled on the DUT
- Check to see if SNMP Agent User is configured and setting matches the SNMP Server settings
- Check to see if SNMP Agent User password is configured and setting matches the SNMP Server settings (DX does not show password, saved records will have to do)
- Check to see that security mode/protocol setting matches SNMP Server settings
- Check to see that SNMP management IP address is set on the DUT

➢ Example CLI commands to check configurations

- DX Example of Show SNMP Settings

```
C4F1DX# snmp show settings

    Mode : V3 Enabled

    Local IP : Any

    Write Access : Disabled

    Traps : Disabled

    Read Community String : public

    Write Community String : private

    Engine Id : 000039cd0300206104c4f100

    Engine Boots : 45

    Engine Time (secs) : 3476648

C4F1DX# snmp show station

    Station Name

    ================================

    96.233.66.242

C4F1DX# snmp show user

              User       Security

    ID        Name       Mode

    ===  ===========  ========

     1        admin          MD5
```

- MNS 6K Example of Show SNMP Settings

```
00:20:06:4a:b3:e0 6KL##show active-snmp
     SNMP Agent supports all (v1/v2c/v3) versions.
00:20:06:4a:b3:e0 6KL##show snmp
    SNMPv3 Configuration Information
    ================================
     System Name        : 6KL_B3E0
     System Location    : Fremont, CA
     System Contact     : support@garrettcom.com
     Authentication Trap : Disabled
     Default Trap Comm.  : public
     V3 Engine ID       : 6K_v3Engine
00:20:06:4a:b3:e0 6KL#(snmpv3)##show-trap
     ID Trap Type      Host IP          Community      Port
     ========================================
     1 v1          192.168.1.4       --          --
     2 --          --              --          --
     3 --          --              --          --
     4 --          --              --          --
     5 --          --              --          --
00:20:06:4a:b3:e0 6KL#(snmpv3)##show-com2sec
     ID Sec. Name      Source        Community
     ======================================
     1 public        default       public
     2 --          --          --
     3 --          --          --
```

```
  4 --          --          --

  5 --          --          --

  6 --          --          --

  7 --          --          --

  8 --          --          --

  9 --          --          --

 10 --          --          --

00:20:06:4a:b3:e0 6KL#(snmpv3)##show-view

  ID View Name      Type      Subtree                  Mask

 ========================================

  1 all          included  .1                    ff

  2 --           --        --                    --

  3 --           --        --                    --

  4 --           --        --                    --

  5 --           --        --                    --

  6 --           --        --                    --

  7 --           --        --                    --

  8 --           --        --                    --

  9 --           --        --                    --

 10 --           --        --                    --

00:20:06:4a:b3:e0 6KL#(snmpv3)##show-user

  ID User Name  UType  AuthPass   PrivPass   AType   Level
Subtree

 ============================================

  1 admin      RW     ******           MD5      auth

  2 --         --     --         --         --       --      --

  3 --         --     --         --         --       --      --
```

```
4 --      --    --      --      --      --      --
5 --      --    --      --      --      --      --
00:20:06:4a:b3:e0 6KL#(snmpv3)##
```

- INOS 10RX Example of Show SNMP Settings

```
10RX-5BB0## show snmp group
    Security Model : v3
    Security Name  : admin
    Group Name     : Group1
    Row Status     : Active
    ------------------------------
10RX-5BB0## show snmp access
    Group Name   : Group1
    Read View    : defaultv3
    Write View   : defaultv3
    Notify View  : None
    Row Status   : Active
    ------------------------------
10RX-5BB0## show snmp view
    View Name    : defaultv3
    Subtree OID  : 1
    Subtree Mask : 1
    View Type    : Included
    Row Status   : Active
    ------------------------------
10RX-5BB0## show snmp targetaddr
```

```
        Target Address Name : HighvisionL3

        IP Address          : 172.29.1.99

        Port                : 162

        Tag List            : 1

        Parameters          : ParamHV

        Row Status          : Active

        ------------------------------

    10RX-5BB0## show snmp targetparam

        Target Parameter Name    : ParamHV

        Message Processing Model : v3

        Security Model           : v3

        Security Name            : admin

        Security Level           : Authentication, No Privacy

        Row Status               : Active

        Filter  Profile Name     : None

        Row Status               : Active

        ------------------------------

    10RX-5BB0##
```

5.3 Third Step See If a Full Walk of the DUT Works (No Encryption)

A full walk can be done by default with CygWin snmpwalk by leaving the OID value blank this becomes a series of get next commands automatically executed till the first failure of that command

```
mrbrown@BNATECH-PC ~

$ snmpwalk -v 3  -u admin -l AuthNoPriv -A garrettcom -a MD5 96.233.66.245
```

SNMPv2-MIB::sysDescr.0 = STRING: DX40

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.553

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (362971682) 42 days, 0:15:16.82

SNMPv2-MIB::sysContact.0 = STRING: Mike Brown

SNMPv2-MIB::sysName.0 = STRING: DX40 Extended Test C4F1

SNMPv2-MIB::sysLocation.0 = STRING: BNA Tech Support

SNMPv2-MIB::sysServices.0 = INTEGER: 79

IF-MIB::ifNumber.0 = INTEGER: 5

IF-MIB::ifIndex.1 = INTEGER: 1

IF-MIB::ifIndex.2 = INTEGER: 2

IF-MIB::ifIndex.101 = INTEGER: 101

IF-MIB::ifIndex.102 = INTEGER: 102

IF-MIB::ifIndex.10001 = INTEGER: 10001

Removed approximately 400 lines for readability

IF-MIB::ifCounterDiscontinuityTime.1 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.2 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.101 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.102 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.10001 = Timeticks: (0) 0:00:00.00

IF-MIB::ifStackStatus.0.10001 = INTEGER: active(1)

IF-MIB::ifStackStatus.0.100001 = INTEGER: active(1)

IF-MIB::ifStackStatus.10001.0 = INTEGER: active(1)

IF-MIB::ifStackStatus.100001.0 = INTEGER: active(1)

IF-MIB::ifRcvAddressStatus.10001.". a..." = INTEGER: active(1)

IF-MIB::ifRcvAddressStatus.10001."..^..." = INTEGER: active(1)

```
IF-MIB::ifRcvAddressType.10001.". a..." = INTEGER: nonVolatile(3)

IF-MIB::ifRcvAddressType.10001."..^..." = INTEGER: nonVolatile(3)

IF-MIB::ifTableLastChange.0 = Timeticks: (0) 0:00:00.00

IF-MIB::ifStackLastChange.0 = Timeticks: (0) 0:00:00.00
```

Snmpwalk only scans the public MIBs NOT the enterprise (private) MIBs as the enterprise MIBs are not by default loaded

If you only see a few (less than 5 lines output) from this test

- Check that you have not restricted what the agent can output via configuration
- The application (MIB Browser, SNMPWalk or HiVision) is not configured properly (MIB's not loaded)
    - This document will not cover the possible fixes to this situation

➢ **Sample CLI commands to look at view restrictions**

- The DX does not have a configuration option to restrict MIB access
- The MNS 6K Example of the MIB access restrictions (allow all is the example) this command is only available for SNMPV3

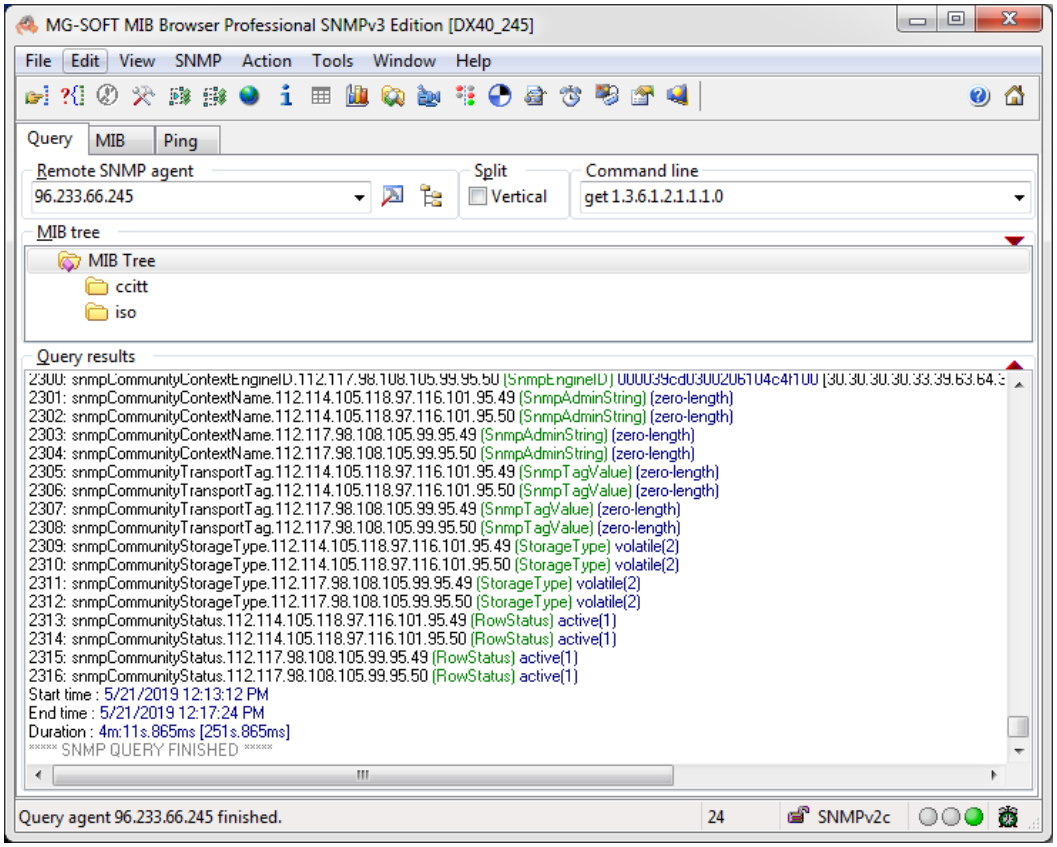
```
00:20:06:4a:b3:e0 6KL#(snmpv3)##show-view
 ID View Name      Type      Subtree              Mask
 ========================================
  1 all              included       .1                   ff
00:20:06:4a:b3:e0 6KL#(snmpv3)##
```

- The INOS 10RX Example of the MIB access restrictions (allow all is the example)

```
10RX-5BB0## show snmp view
    View Name    : defaultv2c
    Subtree OID  : 1
    Subtree Mask : 1
    View Type    : Included
    Row Status   : Active
```

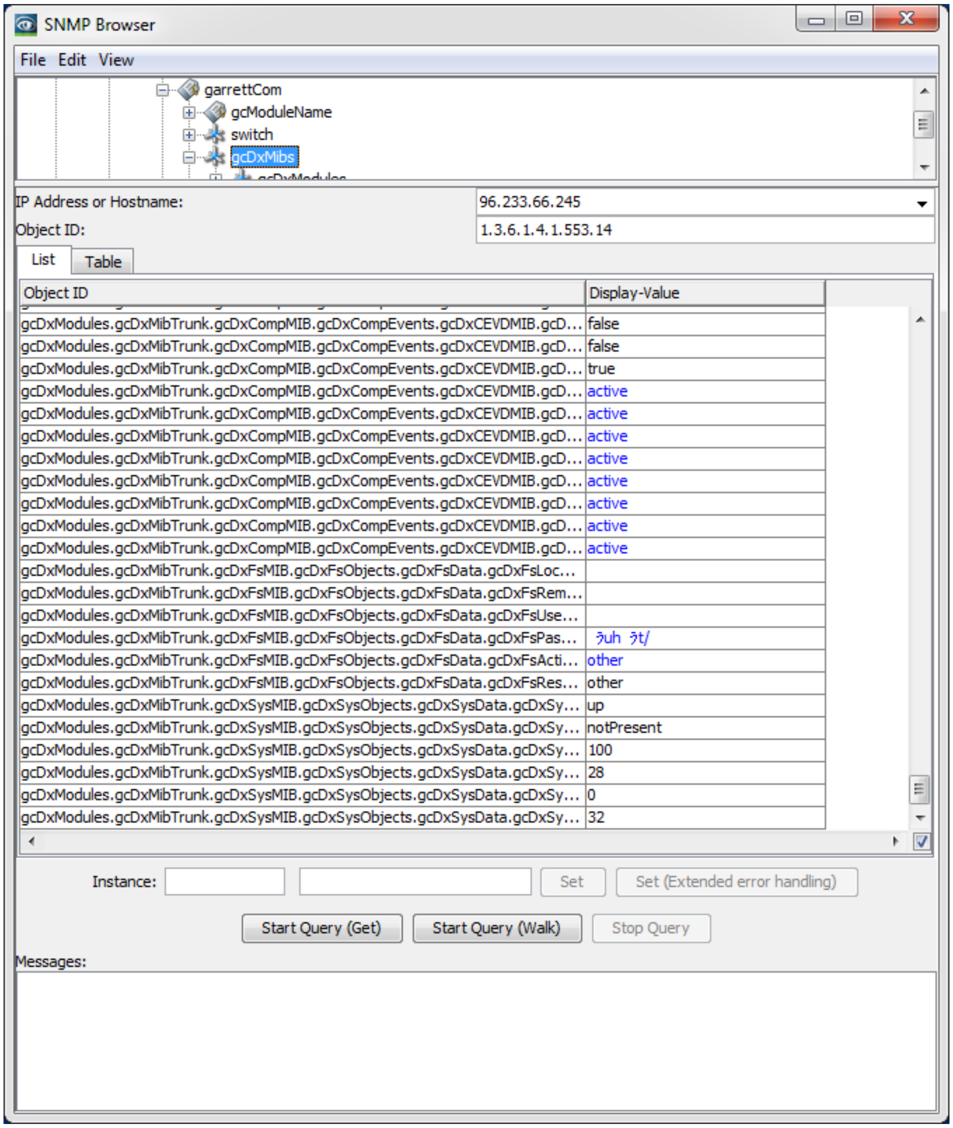
```
------------------------------

10RX-5BB0##
```

Sample Output of MG-Soft MIB Browser with DX MIBs manually loaded walking through the MIBs



Note the 2316 MIB OIDs scanned more than 6 times the number using the basic snmpwalk

Sample Output of Industrial HiVision this software loads DX MIBs when a system is discovered during setup



The difference here is that ONLY the DX MIB was walked as the section of the MIBs you want to scan needs to be selected, see top window in browser

5.4 Sample Wireshark Trace of SNMP V3 Get Request

No. Time Source Destination Protocol Length Info

618 85.276391 192.168.1.4 96.233.66.245 SNMP 182 get-request 1.3.6.1.2.1.1.1.0

Frame 618: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0

Ethernet II, Src: Dell_6f:25:42 (5c:f9:dd:6f:25:42), Dst: Actionte_33:f2:71 (f8:e4:fb:33:f2:71)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 96.233.66.245

User Datagram Protocol, Src Port: 55784, Dst Port: 161

Simple Network Management Protocol

msgVersion: snmpv3 (3)

msgGlobalData

msgAuthoritativeEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

[Group: Protocol]

msgAuthoritativeEngineBoots: 45

msgAuthoritativeEngineTime: 3631437

msgUserName: admin

msgAuthenticationParameters: c359720840e1d20168e3c4c8

msgPrivacyParameters: <MISSING>

msgData: plaintext (0)

plaintext

contextEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

[Group: Protocol]

contextName:

data: get-request (0)

get-request

request-id: 31

error-status: noError (0)

error-index: 0

variable-bindings: 1 item

1.3.6.1.2.1.1.1.0: Value (Null)

Object Name: 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0)

Value (Null)

No.	Time	Source	Destination	Protocol	Length	Info
619	85.289431	96.233.66.245	192.168.1.4	SNMP	185	get-response 1.3.6.1.2.1.1.1.0

Frame 619: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits) on interface 0

Ethernet II, Src: Actionte_33:f2:71 (f8:e4:fb:33:f2:71), Dst: Dell_6f:25:42 (5c:f9:dd:6f:25:42)

Internet Protocol Version 4, Src: 96.233.66.245, Dst: 192.168.1.4

User Datagram Protocol, Src Port: 161, Dst Port: 55784

Simple Network Management Protocol

msgVersion: snmpv3 (3)

msgGlobalData

msgAuthoritativeEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

[Group: Protocol]

msgAuthoritativeEngineBoots: 45

msgAuthoritativeEngineTime: 3631437

msgUserName: admin

msgAuthenticationParameters: a800e4a95c08ed637a83bc7b

msgPrivacyParameters: <MISSING>

msgData: plaintext (0)

plaintext

contextEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

[Group: Protocol]

contextName:

data: get-response (2)

get-response

request-id: 31

error-status: noError (0)

error-index: 0

variable-bindings: 1 item

1.3.6.1.2.1.1.1.0: 44583430

Object Name: 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0)

Value (OctetString): 44583430

Variable-binding-string: DX40

6 Debugging SNMP V3 (With Encryption)

6.1 First Step Check Network Connectivity

Ping from the SNMP Server to the SNMP Agent

C:\Users\mrbrown>ping 96.233.66.245

Pinging 96.233.66.245 with 32 bytes of data:

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Reply from 96.233.66.245: bytes=32 time=1ms TTL=63

Ping statistics for 96.233.66.245:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\mrbrown>ping 96.233.66.245

Pinging 96.233.66.245 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 96.233.66.245:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\mrbrown>

The above is an example of 2 ping requests from the System that hosts the SNMP Servers to the system (DX40 in this example) with the SNMP Agent. The first shows 4 good ping

request/replies, with this result it is time to continue to the next step. The second shows a ping request timeout a timeout indicates a network problem. This problem needs to be solved before continuing, this document does not cover debugging network problems.

6.2 Second Step Check Access to the SNMP Agent (With Encryption)

Start the SNMP MIB browser you have selected or use the Linux Snmpwalk command

This section will only cover the differences between no encryption and encryption

CygWin SNMPWalk Get Request

mrbrown@BNATECH-PC ~

$ snmpwalk -v 3 -u admin -l authPriv -A garrettcom -a MD5 -X goobldegoop -x AES 96.233.66.245 1.3.6.1.2.1.1.1.0

Timeout: No Response from 96.233.66.245

mrbrown@BNATECH-PC ~

$ snmpwalk -v 3 -u admin -l authPriv -A garrettcom -a MD5 -X MagnumDX40 -x DES 96.233.66.245 1.3.6.1.2.1.1.1.0

Timeout: No Response from 96.233.66.245

mrbrown@BNATECH-PC ~

$ snmpwalk -v 3 -u admin -l authPriv -A garrettcom -a MD5 -X MagnumDX40 -x AES 96.233.66.245 1.3.6.1.2.1.1.1.0

SNMPv2-MIB::sysDescr.0 = STRING: DX40

mrbrown@BNATECH-PC ~

$

MG-Soft MIB Browser Contact Request

Request binding:

1: sysDescr.0 (DisplayString) null

Synchronize binding (report):

SNMPv3 report received from remote agent.

User profile name:

Security user name: admin

Security engine ID: 000039cd0300206104c4f100

Context name: (zero-length)

Context engine ID: 000039cd0300206104c4f100

Authentication protocol: HMAC MD5

Privacy protocol: CFB AES 128

Security level: Authentication And Privacy

Security model: USM

1: usmStatsUnknownEngineIDs.0 (Counter32) 55

Response binding:

User profile name:

Security user name: admin

Security engine ID: 000039cd0300206104c4f100

Context name: (zero-length)

Context engine ID: 000039cd0300206104c4f100

Authentication protocol: HMAC MD5

Privacy protocol: CFB AES 128

Security level: Authentication And Privacy

Security model: USM

1: sysDescr.0 (DisplayString) DX40 [44.58.34.30 (hex)]

Remote address: 96.233.66.245 port: 161 transport: IP/UDP

Local address: 192.168.1.4 port: 56202 transport: IP/UDP

Protocol version: SNMPv3

Request:

User profile name:

Security user name: admin

Security engine ID: (zero-length)

Context name: (zero-length)

Context engine ID:

Authentication protocol: HMAC MD5

Privacy protocol: CBC DES

Security level: Authentication And Privacy

Security model: USM

Operation: Get next

1: sysUpTime (TimeTicks) null

Synchronize:

SNMPv3 report received from remote agent.

Security engine ID updated.

User profile name:

Security user name: admin

Security engine ID: 000039cd0300206104c4f100

Context name: (zero-length)

Context engine ID: 000039cd0300206104c4f100

Authentication protocol: HMAC MD5

Privacy protocol: CBC DES

Security level: Authentication And Privacy

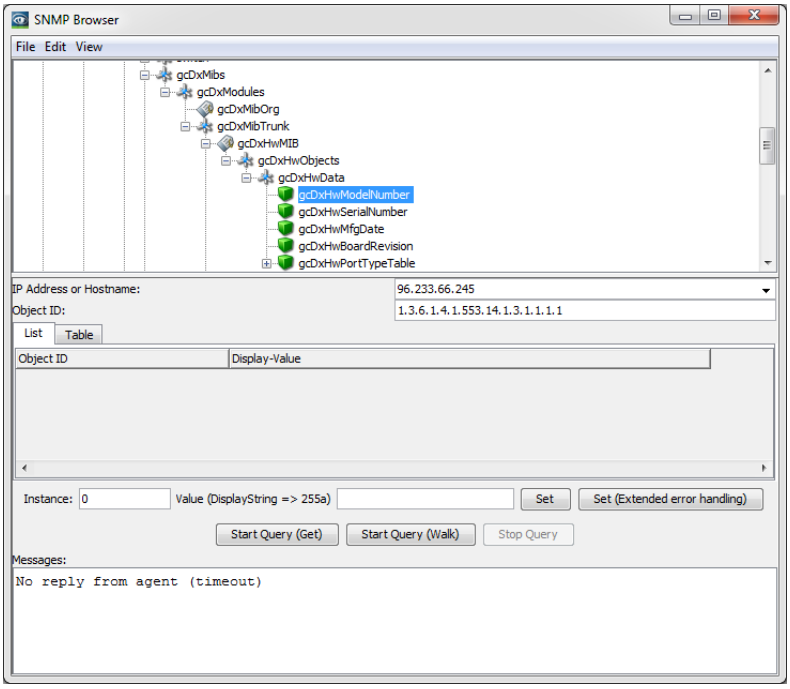
Security model: USM

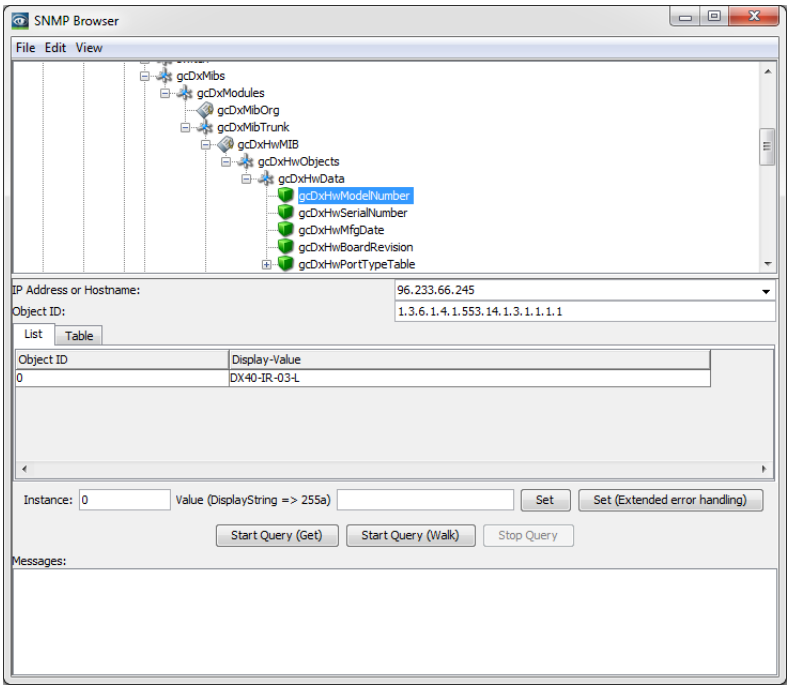
1: usmStatsUnknownEngineIDs.0 (Counter32) 108

TIMEOUT

Industrial HiVision Get Requests

The HiVision Browser does not support the range of error messages as snmpwalk and the MG-Soft Browser





If you see an error message;

- Check to see if SNMP version 3 is Enabled on the DUT
- Check to see if SNMP Agent User is configured and setting matches the SNMP Server settings
- Check to see if SNMP Agent User password is configured and setting matches the SNMP Server settings (DX does not show password, saved records will have to do)
- Check to see that security mode/protocol setting matches SNMP Server settings
- Check to see that SNMP management IP address is set on the DUT

➢ Example CLI commands to check configurations

- DX Example of Show SNMP Settings

```
C4F1DX# snmp show settings
    Mode : V3 Enabled
    Local IP : Any
    Write Access : Disabled
    Traps : Disabled
    Read Community String : public
    Write Community String : private
    Engine Id : 000039cd0300206104c4f100
    Engine Boots : 45
    Engine Time (secs) : 3476648
C4F1DX# snmp show station
    Station Name
    ================================
    96.233.66.242
C4F1DX# snmp show user
              User       Security
    ID        Name       Mode
    === =========== ========
     1        admin          MD5-AES
```

- MNS 6K Example of Show SNMP Settings
  - **The 6K only supports DES-56 encryption many SNMP servers DO NOT support this**

```
00:20:06:4a:b3:e0 6KL##show active-snmp
    SNMP Agent supports all (v1/v2c/v3) versions.
00:20:06:4a:b3:e0 6KL##show snmp
    SNMPv3 Configuration Information
    ================================
     System Name        : 6KL_B3E0
     System Location    : Fremont, CA
     System Contact     : support@garrettcom.com
     Authentication Trap : Disabled
     Default Trap Comm.  : public
     V3 Engine ID       : 6K_v3Engine
00:20:06:4a:b3:e0 6KL#(snmpv3)##show-trap
     ID Trap Type      Host IP          Community      Port
     ========================================
     1 v1          192.168.1.4       --          --
     2 --          --            --          --
     3 --          --            --          --
     4 --          --            --          --
     5 --          --            --          --
00:20:06:4a:b3:e0 6KL#(snmpv3)##show-com2sec
     ID Sec. Name      Source        Community
     ======================================
     1 public        default       public
```

```
2 --          --          --

3 --          --          --

4 --          --          --

5 --          --          --

6 --          --          --

7 --          --          --

8 --          --          --

9 --          --          --

10 --          --          --

00:20:06:4a:b3:e0 6KL#(snmpv3)##show-view

 ID View Name      Type      Subtree                  Mask

==========================================

 1 all          included   .1                    ff

 2 --          --        --                    --

 3 --          --        --                    --

 4 --          --        --                    --

 5 --          --        --                    --

 6 --          --        --                    --

 7 --          --        --                    --

 8 --          --        --                    --

 9 --          --        --                    --

 10 --          --        --                    --

00:20:06:4a:b3:e0 6KL#(snmpv3)##show-user

 ID User Name  UType  AuthPass   PrivPass   AType   Level
Subtree

==============================================

 1 admin      RW    ******     *****        MD5     priv
```

```
2 --      --   --      --      --      --      --
3 --      --   --      --      --      --      --
4 --      --   --      --      --      --      --
5 --      --   --      --      --      --      --
00:20:06:4a:b3:e0 6KL#(snmpv3)##
```

- INOS 10RX Example of Show SNMP Settings

```
10RX-5BB0## show snmp group
    Security Model : v3
    Security Name  : admin
    Group Name     : Group1
    Row Status     : Active
    ------------------------------
10RX-5BB0## show snmp access
    Group Name   : Group1
    Read View    : defaultv3
    Write View   : defaultv3
    Notify View  : None
    Row Status   : Active
    ------------------------------
10RX-5BB0## show snmp view
    View Name    : defaultv3
    Subtree OID  : 1
    Subtree Mask : 1
    View Type    : Included
    Row Status   : Active
```

```
------------------------------
10RX-5BB0## show snmp targetaddr
    Target Address Name : HighvisionL3
    IP Address          : 172.29.1.99
    Port                : 162
    Tag List            : 1
    Parameters          : ParamHV
    Row Status          : Active
    ------------------------------
10RX-5BB0## show snmp targetparam
    Target Parameter Name    : ParamHV
    Message Processing Model : v3
    Security Model           : v3
    Security Name            : admin
    Security Level           : Authentication, Privacy
    Row Status               : Active
    Filter  Profile Name     : None
    Row Status               : Active
    ------------------------------
10RX-5BB0## show snmp user
Engine ID             : 80.00.08.1c.04.46.53
User                  : admin
Authentication Protocol : MD5
Privacy Protocol      : AES_CFB128
Row Status            : Active
------------------------------
```

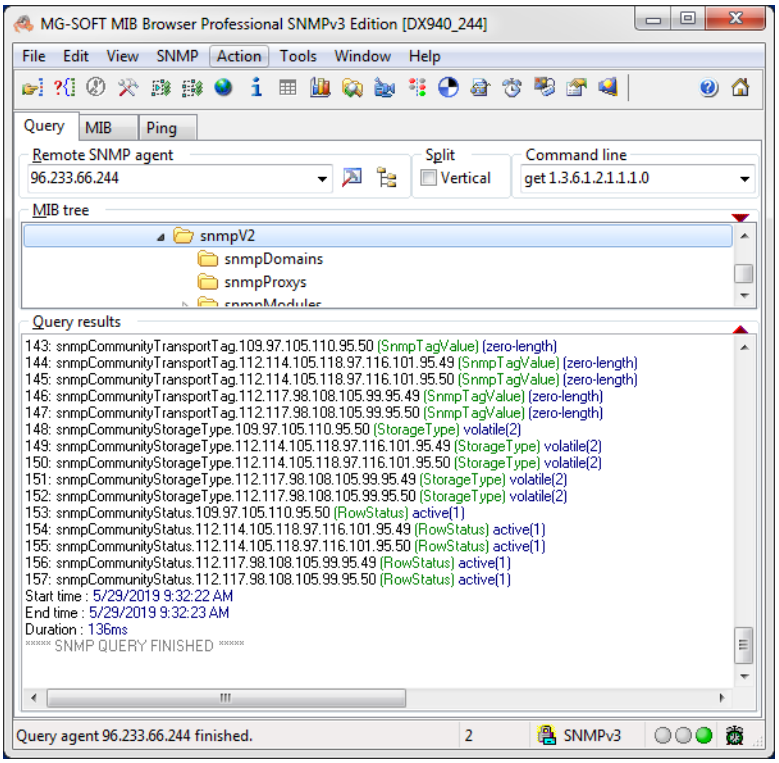
```
Engine ID              : 80.00.08.1c.04.46.53
User                   : public
Authentication Protocol : None
Privacy Protocol       : None
Row Status             : Active
------------------------------
Engine ID              : 80.00.08.1c.04.46.53
User                   : private
Authentication Protocol : None
Privacy Protocol       : None
Row Status             : Active
------------------------------

10RX-5BB0##
```

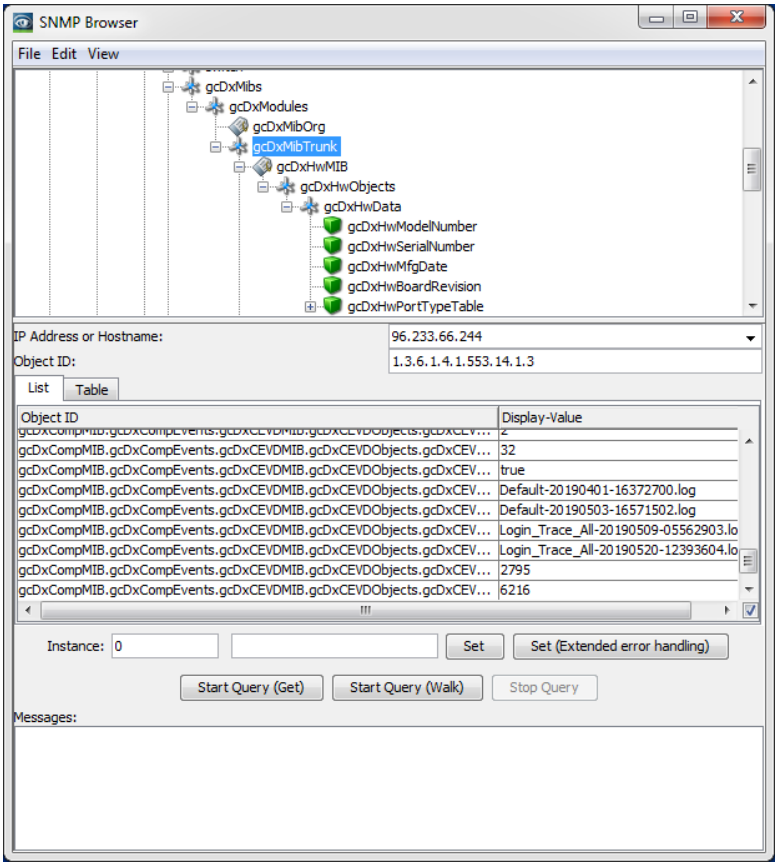
6.3 Third Step See If a Full Walk of the DUT Works (With Encryption)

```
mrbrown@BNATECH-PC ~

$ snmpwalk -v 3  -u admin -l authPriv -A garrettcom -a MD5 -X MagnumDX40 -x AES
96.233.66.245


SNMPv2-MIB::sysDescr.0 = STRING: DX40

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.553

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (29983) 0:04:59.83

SNMPv2-MIB::sysContact.0 = STRING: Mike Brown
```

```
SNMPv2-MIB::sysName.0 = STRING: DX40 Extended Test C4F1

SNMPv2-MIB::sysLocation.0 = STRING: BNA Tech Support

SNMPv2-MIB::sysServices.0 = INTEGER: 79

IF-MIB::ifNumber.0 = INTEGER: 5

IF-MIB::ifIndex.1 = INTEGER: 1

IF-MIB::ifIndex.2 = INTEGER: 2

IF-MIB::ifIndex.101 = INTEGER: 101

IF-MIB::ifIndex.102 = INTEGER: 102

IF-MIB::ifIndex.10001 = INTEGER: 10001

IF-MIB::ifDescr.1 = STRING: Eth1

IF-MIB::ifDescr.2 = STRING: Eth2

IF-MIB::ifDescr.101 = STRING: Serial1

IF-MIB::ifDescr.102 = STRING: Serial2

Removed ~400 Lines for readability

IF-MIB::ifLinkUpDownTrapEnable.102 = INTEGER: disabled(2)

IF-MIB::ifLinkUpDownTrapEnable.10001 = INTEGER: disabled(2)

IF-MIB::ifHighSpeed.1 = Gauge32: 0

IF-MIB::ifHighSpeed.2 = Gauge32: 0

IF-MIB::ifHighSpeed.101 = Gauge32: 0

IF-MIB::ifHighSpeed.102 = Gauge32: 0

IF-MIB::ifHighSpeed.10001 = Gauge32: 0

IF-MIB::ifPromiscuousMode.1 = INTEGER: false(2)

IF-MIB::ifPromiscuousMode.2 = INTEGER: false(2)

IF-MIB::ifPromiscuousMode.101 = INTEGER: false(2)

IF-MIB::ifPromiscuousMode.102 = INTEGER: false(2)

IF-MIB::ifPromiscuousMode.10001 = INTEGER: false(2)
```

```
IF-MIB::ifConnectorPresent.1 = INTEGER: false(2)

IF-MIB::ifConnectorPresent.2 = INTEGER: false(2)

IF-MIB::ifConnectorPresent.101 = INTEGER: false(2)

IF-MIB::ifConnectorPresent.102 = INTEGER: false(2)

IF-MIB::ifConnectorPresent.10001 = INTEGER: false(2)

IF-MIB::ifAlias.1 = STRING:

IF-MIB::ifAlias.2 = STRING:

IF-MIB::ifAlias.101 = STRING:

IF-MIB::ifAlias.102 = STRING:

IF-MIB::ifAlias.10001 = STRING:

IF-MIB::ifCounterDiscontinuityTime.1 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.2 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.101 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.102 = Timeticks: (0) 0:00:00.00

IF-MIB::ifCounterDiscontinuityTime.10001 = Timeticks: (0) 0:00:00.00

IF-MIB::ifStackStatus.0.10001 = INTEGER: active(1)

IF-MIB::ifStackStatus.0.100001 = INTEGER: active(1)

IF-MIB::ifStackStatus.10001.0 = INTEGER: active(1)

IF-MIB::ifStackStatus.100001.0 = INTEGER: active(1)

IF-MIB::ifRcvAddressStatus.10001.". a..." = INTEGER: active(1)

IF-MIB::ifRcvAddressStatus.10001."..^..." = INTEGER: active(1)

IF-MIB::ifRcvAddressType.10001.". a..." = INTEGER: nonVolatile(3)

IF-MIB::ifRcvAddressType.10001."..^..." = INTEGER: nonVolatile(3)

IF-MIB::ifTableLastChange.0 = Timeticks: (0) 0:00:00.00

IF-MIB::ifStackLastChange.0 = Timeticks: (0) 0:00:00.00
```





6.3 Sample Wireshark Capture of SNMP Get Request with Encryption

No. Time Source Destination Protocol Length Info

3648 108.628666 192.168.1.4 96.233.66.245 SNMP 199 encryptedPDU: privKey Unknown

Frame 3648: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface 0

Ethernet II, Src: Dell_6f:25:42 (5c:f9:dd:6f:25:42), Dst: Actionte_33:f2:71 (f8:e4:fb:33:f2:71)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 96.233.66.245

User Datagram Protocol, Src Port: 50278, Dst Port: 161

Simple Network Management Protocol

msgVersion: snmpv3 (3)

msgGlobalData

msgAuthoritativeEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

[Group: Protocol]

msgAuthoritativeEngineBoots: 46

msgAuthoritativeEngineTime: 8850

msgUserName: admin

msgAuthenticationParameters: 4f5bd7bcfe65ec8335b6ddf9

msgPrivacyParameters: 000000001eb8d790

msgData: encryptedPDU (1)

encryptedPDU: 26de77fe082f7d8c2073f4cd0c7b7f94cc2ea4839c03de0b...

No. Time Source Destination Protocol Length Info

3649 108.638079 96.233.66.245 192.168.1.4 SNMP 214 encryptedPDU: privKey Unknown

Frame 3649: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0

Ethernet II, Src: Actionte_33:f2:71 (f8:e4:fb:33:f2:71), Dst: Dell_6f:25:42 (5c:f9:dd:6f:25:42)

Internet Protocol Version 4, Src: 96.233.66.245, Dst: 192.168.1.4

User Datagram Protocol, Src Port: 161, Dst Port: 50278

Simple Network Management Protocol

msgVersion: snmpv3 (3)

msgGlobalData

msgAuthoritativeEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

[Group: Protocol]

msgAuthoritativeEngineBoots: 46

msgAuthoritativeEngineTime: 8850

msgUserName: admin

msgAuthenticationParameters: 267a0b3ed5e21929c5f41eb9

msgPrivacyParameters: 2dedfde0d9688331

msgData: encryptedPDU (1)

encryptedPDU: b77070162ae4330c13408db5f811ee534985396bd4df8a88...

No.	Time	Source	Destination	Protocol	Length	Info
3765	114.062926	192.168.1.4	96.233.66.245	SNMP	101	get-request

Frame 3765: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0

Ethernet II, Src: Dell_6f:25:42 (5c:f9:dd:6f:25:42), Dst: Actionte_33:f2:71 (f8:e4:fb:33:f2:71)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 96.233.66.245

User Datagram Protocol, Src Port: 50278, Dst Port: 161

Simple Network Management Protocol

msgVersion: snmpv3 (3)

msgGlobalData

msgAuthoritativeEngineID: <MISSING>

msgAuthoritativeEngineBoots: 0

msgAuthoritativeEngineTime: 0

msgUserName:

msgAuthenticationParameters: <MISSING>

msgPrivacyParameters: <MISSING>

msgData: plaintext (0)

plaintext

contextEngineID: <MISSING>

contextName:

data: get-request (0)

get-request

request-id: 12382

error-status: noError (0)

error-index: 0

variable-bindings: 0 items

No. Time Source Destination Protocol Length Info

3766 114.067066 96.233.66.245 192.168.1.4 SNMP 168 report 1.3.6.1.6.3.15.1.1.4.0

Frame 3766: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0

Ethernet II, Src: Actionte_33:f2:71 (f8:e4:fb:33:f2:71), Dst: Dell_6f:25:42 (5c:f9:dd:6f:25:42)

Internet Protocol Version 4, Src: 96.233.66.245, Dst: 192.168.1.4

User Datagram Protocol, Src Port: 161, Dst Port: 50278

Simple Network Management Protocol

msgVersion: snmpv3 (3)

msgGlobalData

msgAuthoritativeEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

```
        [Group: Protocol]
msgAuthoritativeEngineBoots: 46
msgAuthoritativeEngineTime: 8855
msgUserName:
msgAuthenticationParameters: <MISSING>
msgPrivacyParameters: <MISSING>
msgData: plaintext (0)
  plaintext
    contextEngineID: 3030303033396364303330303230363130346334663130 30
      0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)
      Engine Enterprise ID: Unknown (808464432)
      Data not conforming to RFC1910
        [Expert Info (Warning/Protocol): Data not conforming to RFC1910]
          [Data not conforming to RFC1910]
          [Severity level: Warning]
          [Group: Protocol]
    contextName:
    data: report (8)
      report
        request-id: 12382
        error-status: noError (0)
        error-index: 0
        variable-bindings: 1 item
          1.3.6.1.6.3.15.1.1.4.0: 338
            Object Name: 1.3.6.1.6.3.15.1.1.4.0 (iso.3.6.1.6.3.15.1.1.4.0)
```

Value (Counter32): 338

No. Time Source Destination Protocol Length Info

3767 114.067303 192.168.1.4 96.233.66.245 SNMP 192 encryptedPDU: privKey Unknown

Frame 3767: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface 0

Ethernet II, Src: Dell_6f:25:42 (5c:f9:dd:6f:25:42), Dst: Actionte_33:f2:71 (f8:e4:fb:33:f2:71)

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 96.233.66.245

User Datagram Protocol, Src Port: 50278, Dst Port: 161

Simple Network Management Protocol

msgVersion: snmpv3 (3)

msgGlobalData

msgAuthoritativeEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

[Group: Protocol]

msgAuthoritativeEngineBoots: 46

msgAuthoritativeEngineTime: 8855

msgUserName: admin

msgAuthenticationParameters: 735ffffde3c3c2f71d861954

msgPrivacyParameters: 000000001eb8d791

msgData: encryptedPDU (1)

encryptedPDU: a17ff89212b73de038a2698c2ddf16660e010fb0f09313ac...

No. Time Source Destination Protocol Length Info

3768 114.082731 96.233.66.245 192.168.1.4 SNMP 214 encryptedPDU: privKey Unknown

Frame 3768: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0

Ethernet II, Src: Actionte_33:f2:71 (f8:e4:fb:33:f2:71), Dst: Dell_6f:25:42 (5c:f9:dd:6f:25:42)

Internet Protocol Version 4, Src: 96.233.66.245, Dst: 192.168.1.4

User Datagram Protocol, Src Port: 161, Dst Port: 50278

Simple Network Management Protocol

msgVersion: snmpv3 (3)

msgGlobalData

msgAuthoritativeEngineID: 3030303033396364303330303230363130346334663130 30

0... .... = Engine ID Conformance: RFC1910 (Non-SNMPv3)

Engine Enterprise ID: Unknown (808464432)

Data not conforming to RFC1910

[Expert Info (Warning/Protocol): Data not conforming to RFC1910]

[Data not conforming to RFC1910]

[Severity level: Warning]

[Group: Protocol]

msgAuthoritativeEngineBoots: 46

msgAuthoritativeEngineTime: 8855

msgUserName: admin

msgAuthenticationParameters: d6a97838507a927e0ed0395a

msgPrivacyParameters: 286e33d4612f59e7

msgData: encryptedPDU (1)

encryptedPDU: 7f9740f580387459a792831185db578f7692b6703de23853...