APPLICATION NOTE - SNMP V3

Simple Network Management Protocol (SNMP) Version 3 and the RAPTOR® and *Micro*RAPTOR®

Simple Network Management Protocol (SNMP) is a series of Internet standards defined for collecting and organizing information about managed devices on IP networks. SNMP also allows modification of information to change device functionality.

There are three versions of SNMP:

V1- Established in 1988, the first SNMP functions were defined.

V2c- Established an established MIB database that covered most of the switch and routing functions within Ethernet devices, including end devices such as PC, servers, relays and other IEDs.

V3- The latest version of SNMP that incorporates security into the standard and encrypts the SNMP information that is passed between the network device being polled and the Network Management Server (NMS). **This note provides guidance for SNMPv3.**

All three versions of SNMP are still in use, with V2c the most used. V3 is always recommended for extended data security.

Why use SNMPv3?

SNMPv1/v2 utilizes a pseudo password called a community string. This is inherently insecure as the community string is carried in the clear between the network device and the SNMP management server. SNMPv3 encrypts the community string so it is not visible to eavesdropping. SNMPv3 provides an encryption mechanism that encrypts the SNMP poll and response data (and the community String) and renders it obscured if it is captured with a tool such as Wireshark.

You can also use SNMPv3 to create individual or group login credentials that can restrict or allow SNMP information based on the MIBs and whether they are read-only or read-write accessible.

SNMP utilizes a Management Information Database (MIB) - A MIB database is used for managing the entities in a communication network. Most often associated with SNMP, it is comprised of Object Identifier (OID) entries.

The functionality of SNMP utilizing MIB databases filled with OIDs is incorporated into a variety of tools and software applications. The main application using SNMP is called a Network Management System. NMS systems serve multiple functions, including:

1. **Network monitoring** – NMS software monitors network elements to ensure all devices are operating optimally. Alerts and alarms can be sent to network administrators if a problem is detected.
2. **Device detection** – When a new device is installed, configured, and connected to the managed network, the NMS detects it so that it can be recognized and added to the network for monitoring.
3. **Performance analysis** – An NMS can monitor the current performance of a network, including the overall performance of the network and individual devices and connections. For example, the NMS may detect aspects of a network where bandwidth utilization is nearing the maximum bandwidth available. This data can be used to provide supporting information to recommend the addition of new hardware if needed.
4. **Device management** – An NMS can provide a central platform to manage multiple devices from multiple locations. It can be used to configure a device, remove unused devices or modify settings based on the performance analysis.
5. **Fault management** – If a network device or communications fails, an NMS may be able to automatically provide notification of the issue and the location of the failure. When a fault occurs, a network alert or notification is sent network administrators and is monitored on the NMS until resolved and cleared.

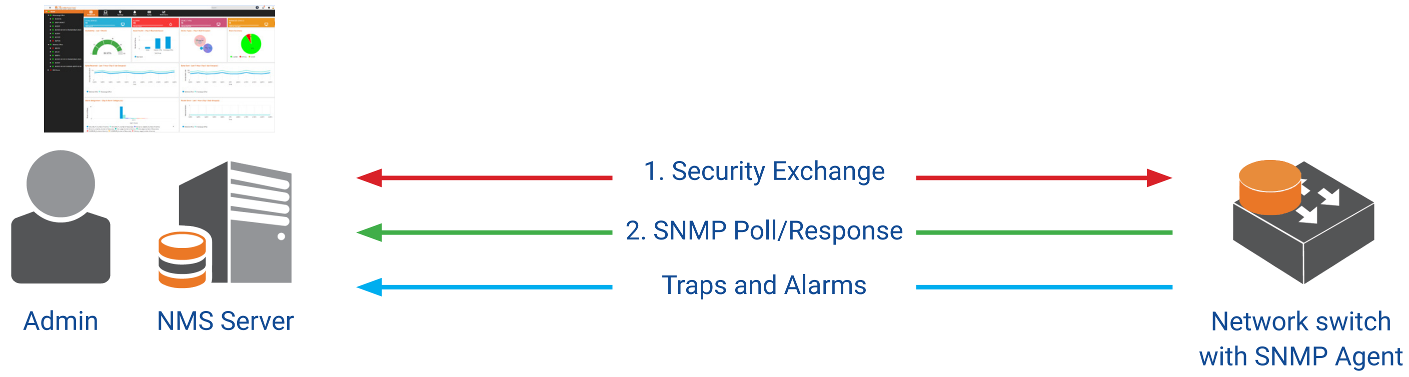
There are several widely used SNMP commands:

- **SNMPGet** - command retrieves the value of a MIB object.
- **SNMPGetnext** - command retrieves the value of the next MIB object in a sequence or table. It is useful for retrieving multiple MIB entries without continuous SNMPGet commands.
- **SNMPSet** - if the OID has write/set capable, SNMPSet will facilitate the settings change for the OID.

SNMP is poll-based, so these commands are issued primarily as polls to each device that the NMS Server manages. The polls are done on a scheduled periodic basis to not overutilize the available bandwidth. SNMPv3 provides encryption for these commands and responses.

Faults and alarms are sent proactively by the managed network device to the NMS for monitoring and are not poll-based. These provide notifications in the event of an issue such as a dead power supply or if a physical port goes inoperable. They are stored in the NMS server. They can be cleared if they are acknowledged on the NMS system.

Figure 1

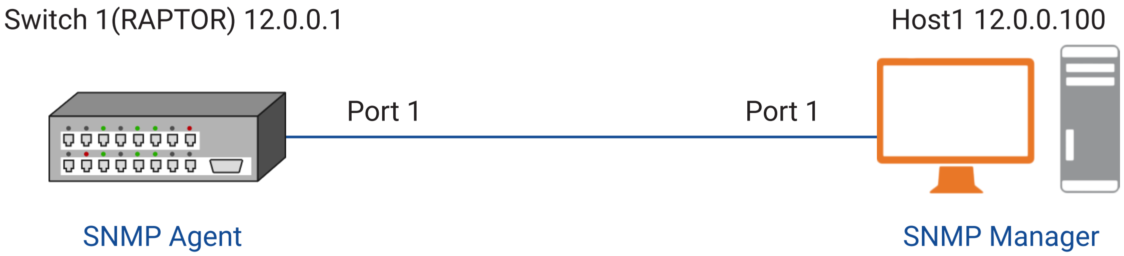


Settings for the iMX350/950 RAPTOR and iMR320 *Micro*RAPTOR

These examples are shown by using the CLI commands.

We will be referring to this example for the configurations for the Network switch (RAPTOR or *Micro*RAPTOR).

Figure 2 (Reference)



For SNMP V3:

The guidelines for configuration are as follows:

1) SNMPv3 framework has three security levels: noAuthNoPriv, authNoPriv, and authPriv can be configured.

– If the required security level is noAuthNoPriv, auth parameter must be configured as none (no Authentication) and there is no need to specify group access for both authentication and privacy (Encryption).

– If the required security level is authNoPriv, auth parameter and group access for authentication must be configured and there is no need to specify group access for privacy (Encryption).

– If the required security level is authPriv, auth parameter and group access for authentication and privacy (Encryption) must be configured.

Refer to the Agent/Manager figure for the Topology Setup. Execute the following commands in the SNMP Agent (switch1) to allow SNMPv3 access with SNMP manager (Host1).

Configure the SNMP engine ID. SNMP engine ID is an administratively unique identifier.

– Enter the Global Configuration Mode.

```
iS5comm# configure terminal
```

– Configure the SNMP engine ID.

```
iS5comm(config)# snmp engineid 80.00.08.1c.04.46.64
```

The engine ID can be the MAC Address of the RAPTOR

– Create and configure the parameters for the user user3 (example).

```
iS5comm(config)# snmp user user3 auth SHA sha12345 priv DES des12345 engineid 80.00.08.1c.04.46.64
```

User3 is an example name. Sha12345 is an example. Des 12345 is an example

– Configure the SNMP Group as group3 (example) and the associated group parameters. The group must be created using the command SNMP group command before configuring the group access details.

```
iS5comm(config)# snmp group group3 user user3 security-model v3
```

group3 is an example name

– Configure the access details for the group group3.

```
iS5comm(config)# snmp access group3 v3 auth read v3read write v3write notify none
iS5comm(config)# snmp access group3 v3 priv read v3read write v3write notify none
```

– Configure the parameters associated with SNMP view.
– Configure the view as v3read.

```
iS5comm(config)# snmp view v3read 1.3.6.1.2.1.17.7.1.4.5.1 mask 1.1.1.1.1.1.1.1.1.1.1.1 included nonvolatile
```

– Configure the view as v3write.

```
iS5comm(config)# snmp view v3write 1.3.6.1.2.1.17.7.1.4.5.1 mask 1.1.1.1.1.1.1.1.1.1.1.1 included nonvolatile
```

– Exit from the Global Configuration Model.

```
iS5comm(config)# end
```

Always remember to save your settings with the *wr Startup-config* command.

CONCLUSION

The RAPTOR and *Micro*RAPTOR series of network switches support standards-based SNMP v1/v2c and v3 operations and are interoperable with numerous Network Management systems on the market. iS5 Communications also offers its own NMS, RAPTOR*Eye*, which supports iS5's SNMP managed devices as well as third-party devices supporting SNMP.

For any additional information or questions, please get in touch with us at **is5com.com**.

ABOUT iS5 COMMUNICATIONS INC.

iS5 Communications Inc. ("iS5Com") is a global provider of integrated services and solutions, and manufacturer of intelligent Industrial Ethernet products. Our products are designed to meet the stringent demand requirements of utility sub-stations, roadside transportation, rail, and industrial applications. iS5Com's services and products are key enablers of advanced technology implementation such as the Smart Grid, Intelligent Transportation Systems, Intelligent Oil Field, and Internet of Things. All products have the ability to transmit data efficiently without the loss of any packets under harsh environments and EMI conditions.

iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

For more information, visit: is5com.com

toll free: +1-844-520-0588 | fax: +1-289-401-5206 | info@is5com.com
technical support: +1-844-475-8324 | support@is5com.com
Address: 5895 Ambler Dr, Mississauga, ON L4W 5B7