APPLICATION NOTE-SNMP V1/V2C

Simple Network Management Protocol (SNMP) 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 System (NMS).

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

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 raw data (e.g. port interface speed) is called an 'object' that resides within the device in the MIB database, and every object (e.g. device statistics) is uniquely identified with an object identifier **(OID)**. There are many OIDs (hundreds, even thousands at times) on a single device that are pollable by the SNMP server to monitor and manage the status of the entire communications network that the administrator wants to monitor.

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's 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 provide supporting information to recommend the addition of new hardware if needed.
4. **Device management** – An NMS can provide 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. Useful in 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.

While there are other commands that are less utilized, these are the primary commands used.

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

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

The SNMP Community String acts as a user id or password that allows access to a network device's statistics and operational information.

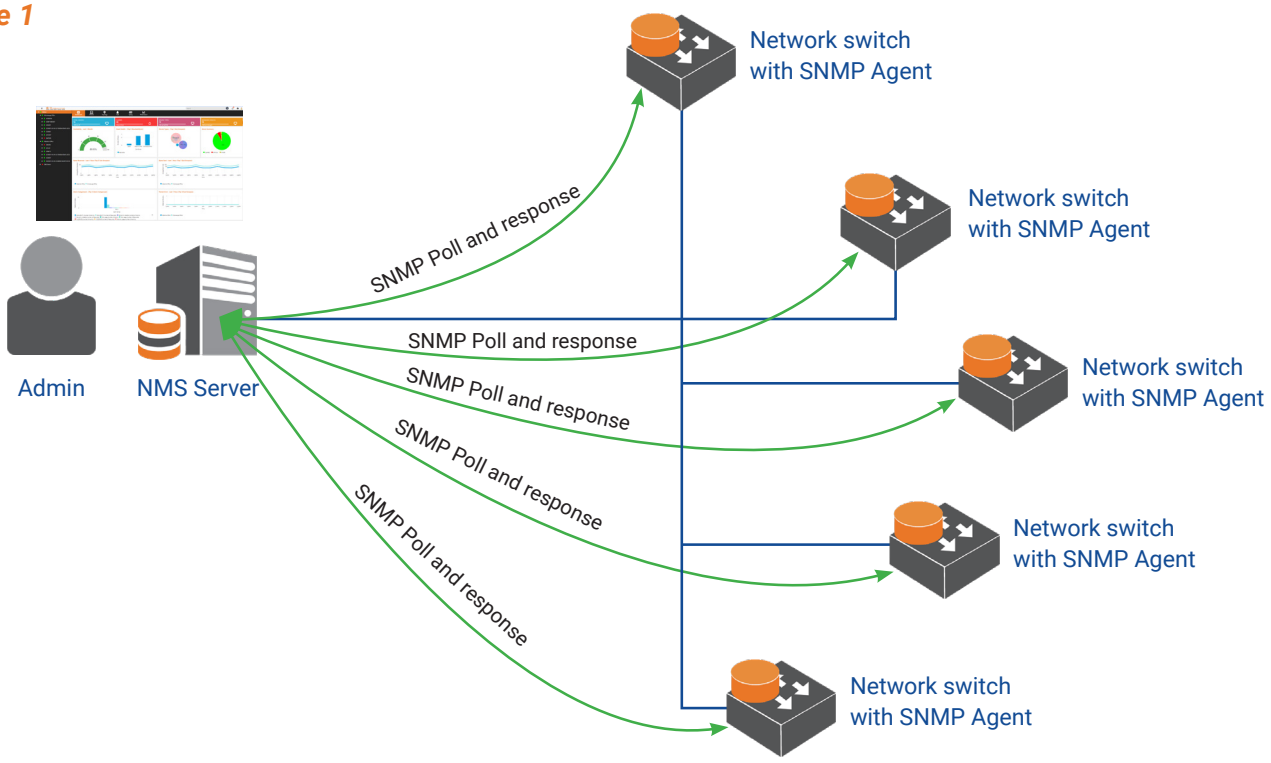
NMS's send the community string along with all SNMP requests.

- If correct, the device responds with the requested information.
- If incorrect, the device discards the request and does not respond.

Note: SNMP Community strings are used only by devices which support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

Typically, most SNMPv1 and v2c equipment ships from the factory with a read-only community string set to **"public"**. It is recommended to change the default community names during device configuration.

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

FOR SNMP V2C:

At SNMP Agent (IN CLI):
Configure the community details – think of Community as something very similar to a user name. The community details must match on the managed device as well as the NMS.
– Enter the Global Configuration Mode.

iS5comm# configure terminal
– Configure the SNMP Community (with the name is5Com) and its associated parameters to establish SNMP v1/v2 access.

iS5comm(config)# snmp community index *com* **name** *is5Com* **security** *none*
– Exit the Global Configuration Mode.

iS5comm(config)# end
Configuring SNMP community with security name
– Enter the Global Configuration Mode.

iS5comm# configure terminal
– Configure the SNMP Community and its associated parameters to establish SNMP v1/v2 access.

iS5comm(config)# snmp community index *com1* **name** *is5Com1* **security** *user1*

Or

iS5comm(config)# snmp community index *com2* **name** *is5Com2* **security** *user2*

– Create and configure the parameters for the user (security name)

iS5comm(config)# snmp user *user1*

Or

iS5comm(config)# snmp user *user2*
– Configure the SNMP Group.

iS5comm(config)# snmp group *group1* **user** *user1* **security-model** *v1*

Or

iS5comm(config)# snmp group *group2* **user** *user2* **security-model** *v2c*
– Configure the access details for the group. Group must be created using the command snmp group command before configuring the group access details.

iS5comm(config)# snmp access *group1 v1* **read** *iso* **write** *iso* **notify** *iso*

Or

iS5comm(config)# snmp access *group2 v2c* **read** *iso* **write** *iso* **notify** *iso*
– Exit the Global Configuration Mode.

iS5comm(config)# end

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 has its own NMS, RAPTOR*Eye*, which supports third party SNMP based products as well as iS5Com devices.

For any additional information or questions, please touch base 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