SOLARWINDS TECH TIPS

A Guide to Understanding SNMP

Read about SNMP v1, v2c & v3 and Learn How to Configure SNMP on Cisco® Routers

Share:

solarwinds
Unexpected Simplicity™

In small networks with only a few devices confined to a single location, network engineers can individually inspect devices and check for anomalies. However, as the number of devices increases, especially in growing networks with hundreds or thousands of devices, manual device monitoring becomes increasingly difficult. **Simple Network Management Protocol (SNMP)** is a popular technology that lets you monitor network devices such as switches, routers, servers, printers and other IP-based devices from a single management host. Provided the device is SNMP capable, you can configure SNMP, collect information, and monitor any number of devices from a single system.

Some uses of SNMP are:

- Monitoring traffic flowing through the device
- Detecting and notifying faults encountered on network devices
- Collecting device performance data over long periods and identifying trends
- Remotely configuring network devices
- Remotely accessing and controlling network devices

What is SNMP?

SNMP is a standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. System management software uses SNMP to allow administrators to remotely monitor and manage thousands of systems on a network, often by presenting the data gathered from monitored devices in a snapshot or dashboard view.

Hence by definition:

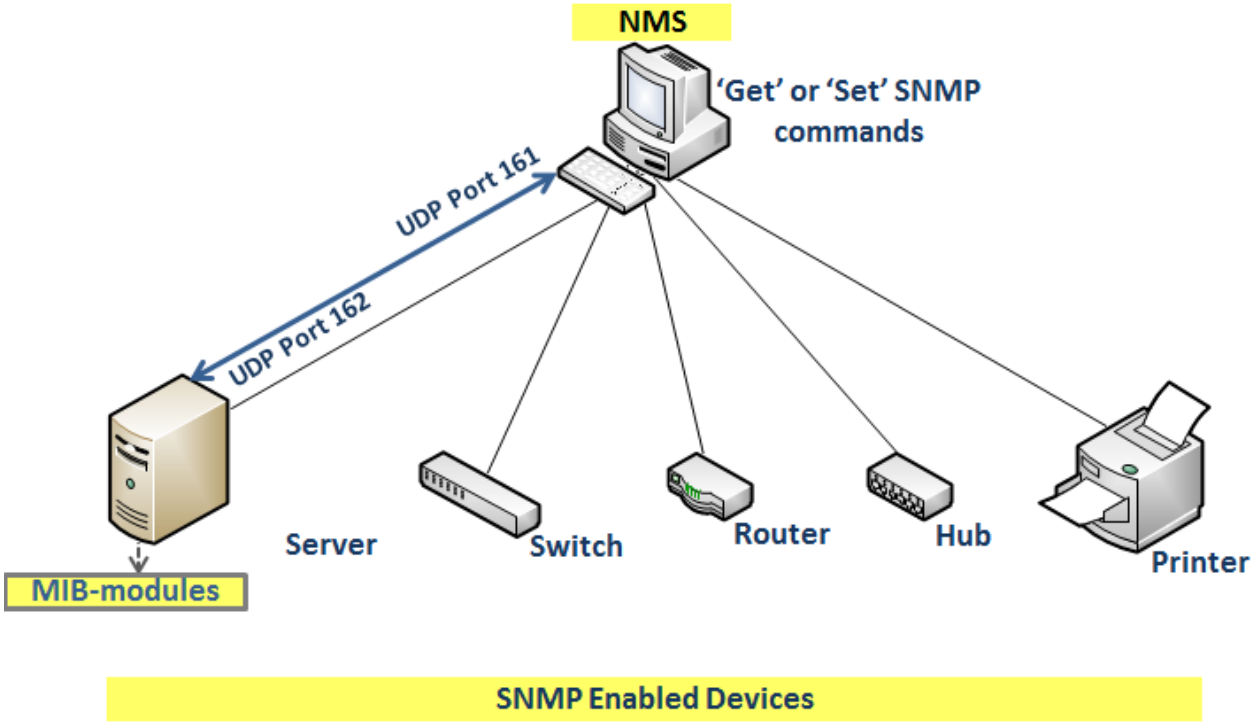
Simple Network Management Protocol (SNMP) is a standard that defines how communication occurs between SNMP-capable devices and defines the SNMP message types.

How Does SNMP Work?

As networks expand, technologies like SNMP become more useful and essential for network administration. For SNMP to work, network devices make use of a data store called the Management Information Base (MIB). All SNMP compliant devices contain an MIB that consists of information on valid attributes of a device. Some attributes in the MIB are fixed, while others are dynamic values calculated by the Network Management System (NMS).

The SNMP management application together with the PC on which it runs is the NMS. This provides the bulk of the processing and memory resources required for network management. Therefore, the NMS executes applications that monitor and control managed devices.

The NMS uses SNMP commands to read data that is stored in the device MIB. 'Get' commands typically retrieve data values, while 'set' commands typically initiate some action on the device.



As seen in the above diagram, SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. Each managed component has a corresponding subagent and MIBs. SNMP-compliant devices listen for PDUs on port 162 and return the data stored in the MIB to the SNMP requesters via port 161. A network can have multiple SNMP managers.

An NMS can request the following types of information from the device it monitors:

- Network protocol identification and statistics
- Dynamic identification (discovery) of devices attached to the network
- Hardware and software configuration data
- Performance and usage statistics of network devices
- Error and event messages from devices
- Application usage statistics

SNMP Versions

There are three SNMP messaging protocols: SNMPv1, SNMPv2 and SNMPv3.

SNMPv1

This was the first protocol introduced and it is still widely used. It implements ‘get’, ‘getnext’, ‘getresponse’, ‘set’, and ‘trap’ operations. The SNMP ‘get’ operation is performed by an NMS to retrieve SNMP object variables. Listed below are some of the operations and what they do:

- GET - Retrieves the exact object instance from the SNMP agent
- GETNEXT - Retrieves the next object variable
- GETBULK - Retrieves a large amount of object variable data, without the need for repeated GETNEXT operations
- SET – Tells the NMS to modify the value of an object variable
- TRAPS - Alerts the SNMP manager about a condition on the network
- INFORMS - Traps that include a request for confirmation of receipt from the SNMP manager

SNMPv1 operates over both User Datagram protocol (UDP) and Internet Protocol (IP). The SNMPv1 SMI (Structure of Management Information) defines the MIBs that contain information on the device. The rows in the MIBs are indexed, so SNMP can retrieve or alter an entire row with a supported command. In SNMPv1, the SNMP Manager issues a request, and the SNMP enabled devices return responses. Agents use the ‘trap’ operation to asynchronously inform the SNMP Manager of a significant event.

Security for SNMPv1 is based on a ‘community string’ that is transmitted with each message. The ‘community string’ acts as a password. If the Manager includes the correct password in a request to an agent, the agent will send a response. The community string is not encrypted and thus the security it provides is weak.

SNMPv2

Also referred to as SNMPv2c, this was the most stable second version that survived. SNMPv2 introduced the ability to transmit SMIv2 MIB-definitions of type “Counter64”. SNMPv2c utilizes the same ‘community string’ security as SNMPv1. The operations that are used in SNMPv1 are similar to those that are used in SNMPv2. SNMPv2c also provides expanded messaging operations: ‘getbulk’, ‘inform’, ‘report’, and a new ‘v2trap’ operation. This also introduced enhanced error responses by agents on the device. The SNMPv2 ‘trap’ operation serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 ‘trap.’

SNMPv2c messages use different header and protocol data unit (PDU) formats from SNMPv1 messages. SNMPv2c also uses two protocol operations that are not specified in SNMPv1. Hence, SNMPv2c is incompatible with SNMPv1 in two areas: message formats and protocol operations.

SNMPv3

SNMPv3 is the latest introduction and was developed as an improvement to SNMPv1 and SNMPv2. SNMPv3 comes with improved security, with its key benefits being:

- **User Authentication:** This involves the verification of the identity of the SNMP Manager or SNMP Agent sending the request. Managers and Agents share information of valid users, and there is a shared secret key defined for each user. When a device sends an SNMPv3 message, the secret key is used to create a hash of the message, and this hashed value is included with the message. If the receiving device can recreate this hash, then the message is said to be "authenticated" and is from a valid user. This authentication helps assure that the message originated from a valid source.
- **Encryption:** Scrambles the packet contents to prevent it from being seen by unauthorized sources. Message payload can be optionally encrypted based on a second shared key. That is, there is no plain-text SNMP data lying around on the network.
- **Message Integrity:** Ensures that a packet has not been tampered with in-transit.

Most network admins today use v2, but the advantage of using v3 is that it offers many more robust security features. To prevent SNMP packets from being exposed on your network, you should configure encryption with SNMPv3.

Key Differences between SNMP v1, v2c and v3

SNMP v1	SNMP v2c	SNMP v3
Easy to set up. Only requires a plain text community string to authenticate packets	Identical to version 1	Setup is more complex. Does not use community strings but users with authentication and encryption.
Supports only 32 bit counters	Support for 64 bit counters	Adds security to the 64 bit counters.
Packet Types: • Get-Request • Get-Next-Request • Set Request • Get Response	Packet Types: • Get-Request • Get-Bulk-Request • Get-Next-Request • Set Request • Inform-Response	The basic functions of v3 are from v1 and v2. v3 has a new SNMP message format

	• SNMP v2 Trap	
Anybody with access to the network will be able to see the community string in plaintext	• Improved error handling • Improved SET commands	Adds both encryption and authentication, to the SNMP message.

Configuring SNMP v1 and v2c on a Cisco® Router

SNMP can be configured on devices with just a few commands. Before we get into the commands for configuration, let's discuss the SNMP privilege levels feature. This feature limits the types of operations that a management station can have on a device. There are two types of privilege level on devices: Read-Only (RO) and Read-Write (RW). The RO level only allows a management station to query the MIB for device data. It does not allow for configuration commands such as rebooting a router and shutting down interfaces to be performed. Only the RW privilege level can be used to perform such operations. You can specify the required access level while creating the community string.

In SNMP v1 or v2c, to enable device polling all you have to do is configure SNMP 'Community String'. A community string is like a password for access to the device. To create a community string, go into the configuration mode:

```
router#enable
Password:*****
router#configure terminal
router2950(config)#snmp-server community public RO
router2950(config)#exit
router#
```

Use this command to enable Read (R) community string where "public" is the Read community string.

```
router#enable
Password:*****
router#configure terminal
router2950(config)#snmp-server community private RW
router2950(config)#exit
router#
```

Use this command to enable Read-write (RW) community string where "private" is the Read-write community string.

The above commands allow the SNMP manager to both view (read) and modify device configurations and statistics (write).

Configuring SNMP v3

SNMP version 3 (SNMPv3) provides secure exchanges of management data between network devices and management stations. The encryption and authentication features in SNMPv3 ensure high security in transporting packets to a management console. This is another reason why it's preferred over SNMPv1 or v2c.

To configure SNMP v3:

Step1: Create an SNMP View

Step2: Create a GROUP for that View

Step3: Create Users under GROUP

```
router#enable
Password:*****
router#configure terminal
router2950(config)# snmp-server view target1 internet included
router2950(config)# snmp-server group mygroup v3 auth write target1
router2950(config)#snmp-server user myuser mygroup v3 encrypted auth md5 myuser
router2950(config)#exit
router#
```

Creating an SNMP View

Creating a GROUP

Creating USERS under that GROUP

Some Best Practices for SNMP in Your Network

Implementing SNMP helps you monitor and be alerted on the status of device hardware components. Here are a few best practices for using SNMP in your network.

- Setting too short a polling interval can add to the overhead on your network device as well as result in a flood of alerts, whereas long polling intervals may lead to missing an event as values are averaged out over time. Choose a polling interval that is appropriate to your network but based on the type of data you're collecting and on the devices being polled. If the data is critical and provides insight into network uptime, choose a lower polling interval whereas, non-critical stats can do with less frequent ones.

- Take care to assign appropriate ‘read only’ or ‘read/write’ permissions for each device based on the criticality of the device. Create strong community strings for your devices and avoid allowing incoming SNMP requests over the WAN. This adds to the security and prevents unauthorized users from gaining access to your network.
- Reduce the security risks associated with SNMP v1 and v2 by implementing SNMP v3 and choosing an NMS system that supports the same. SNMPv3 plugs the security holes associated with previous versions by adding user and message authentication as well as encryption to prevent data interception.

In short, SNMP provides an application-layer protocol that facilitates the exchange of management information between network devices and notifies the NMS accordingly. It enables network administrators to manage network performance, easily find and solve network problems before outages occur, and provide data to plan for network growth.

SolarWinds® Network Performance Monitor

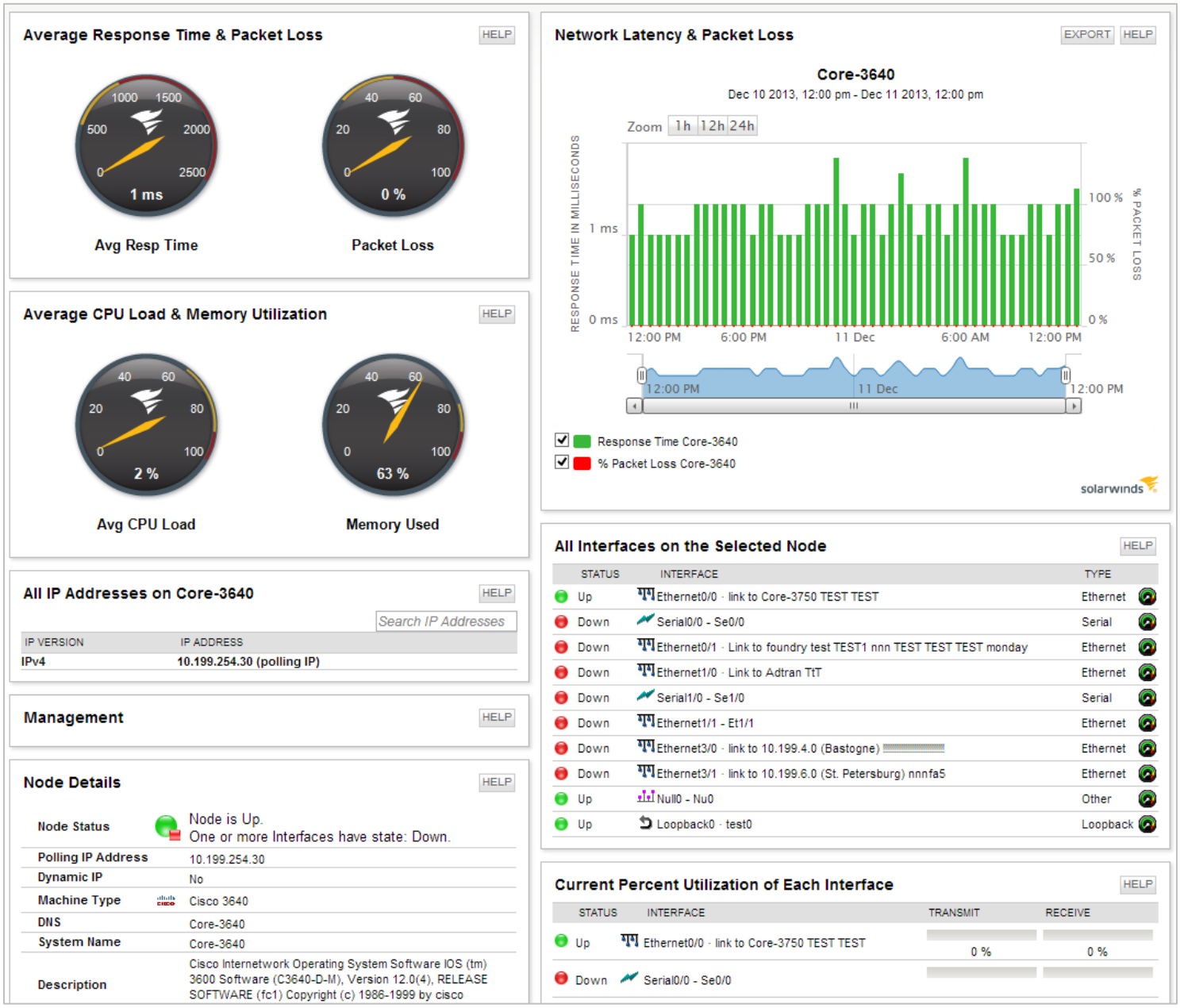
SolarWinds Network Performance Monitor (NPM) is a simple yet powerful network management system (NMS) that performs network fault, availability and performance monitoring for your growing, multi-vendor network.

NPM uses SNMP as one of its data polling methods to obtain performance metrics from network devices such as routers, switches, firewalls and any SNMP-enabled devices. Allowing you to monitor network devices from hundreds of manufacturers and thousands of device types, SolarWinds NPM provides valuable and actionable network statistics such as response time, packet loss, network latency, throughput, CPU memory utilization, and more — right from the device level to the interface level.

Highlights of SolarWinds NPM:

- Simplifies detection, diagnosis & resolution of network issues before outages occur
- Tracks response time, availability & uptime of routers, switches, & other SNMP-enabled devices
- Shows performance statistics in real time via dynamic, drillable network maps
- Includes out-of-the-box dashboards, alerts, reports & expert guidance on what to monitor & how
- Automatically discovers SNMP-enabled network devices & typically deploys in less than an hour

Right from a single, intuitive Web console, SolarWinds NPM provides out-of-the box network alerts, reports and interactive charts to understand your network health and isolate performance bottlenecks.



References:

- http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_0_1/ccmsrva/sasnmpv1.html
- http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_0_1/ccmsrva/sasnmpv3.html#wp1028007

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. In all of our market areas, our approach is consistent. We focus exclusively on IT Pros and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack (http://www.thwack.com/), to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at http://www.solarwinds.com/.