# Simple Network Management Protocol SNMP Tutorial

June 16th, 2014 Go to comments

Building a working network is important but monitoring its health is as important as building it. Luckily we have tools to make administrator's life easier and SNMP is one among of them. SNMP presents in most of the network regardless of the size of that network. And understanding how SNMP works is really important and that what we will learn in this tutorial.

Understand SNMP

SNMP consists of 3 items:

+ **SNMP Manager** (sometimes called Network Management System – NMS): a software runs on the device of the network administrator (in most case, a computer) to monitor the network.
+ **SNMP Agent:** a software runs on network devices that we want to monitor (router, switch, server…)
+ **Management Information Base** (MIB): is the collection of managed objects. This components makes sure that the data exchange between the manager and the agent remains structured. In other words, MIB contains a set of questions that the SNMP Manager can ask the Agent (and the Agent can understand them). MIB is commonly shared between the Agent and Manager.
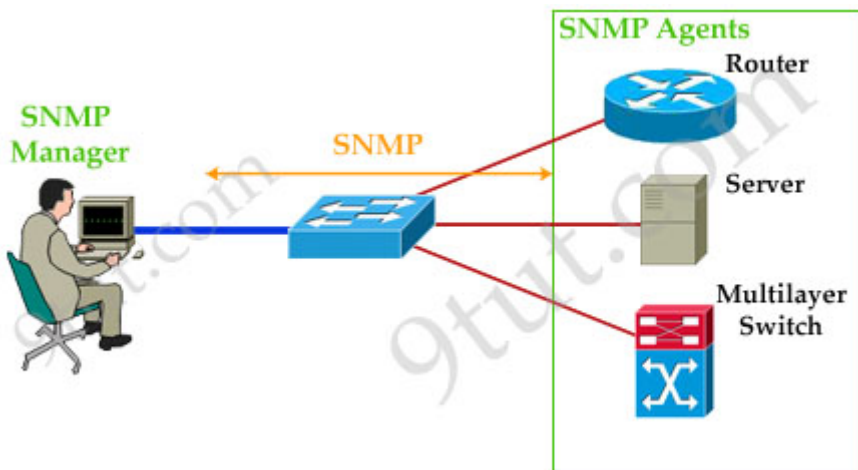
For example, in the topology above you want to monitor a router, a server and a Multilayer Switch. You can run SNMP Agent on all of them. Then on a PC you install a SNMP Manager software to receive monitoring information. SNMP is the protocol running between the Manager and Agent. SNMP communication between Manager and Agent takes place in form of messages. The monitoring process must be done via a MIB which is a standardized database and it contains parameters/objects to describe these networking devices (like IP addresses, interfaces, CPU utilization, …). Therefore the monitoring process now becomes the process of GET and SET the information from the MIB.

SNMP Versions

SNMP has multiple versions but there are three main versions:

+ **SNMP version 1**
+ **SNMP version 2c**
+ **SNMP version 3**

SNMPv1 is the original version and is very legacy so it should not be used in our network. SNMPv2c updated the original protocol and offered some enhancements. One of the noticeable enhancement is the introduction of INFORM and GETBULK messages which will be explain later in this tutorial.

Both SNMPv1 and v2 did not focus much on security and they provide security based on **community string** only. Community string is really just a clear text password (without encryption). Any data sent in clear text over a network is vulnerable to packet sniffing and interception. There are two types of community strings in SNMPv2c:

+ **Read-only (RO)**: gives read-only access to the MIB objects which is safer and preferred to other method.
+ **Read-write (RW)**: gives read and write access to the MIB objects. This method allows SNMP Manager to change the configuration of the managed router/switch so be careful with this type.

The community string defined on the SNMP Manager must match one of the community strings on the Agents in order for the Manager to access the Agents.

SNMPv3 provides significant enhancements to address the security weaknesses existing in the earlier versions. The concept of community string does not exist in this version. SNMPv3 provides a far more secure communication using entities, users and groups. This is achieved by implementing three new major features:
+ **Message integrity:** ensuring that a packet has not been modified in transit.
+ **Authentication:** by using password hashing (based on the HMAC-MD5 or HMAC-SHA algorithms) to ensure the message is from a valid source on the network.
+ **Privacy (Encryption):** by using encryption (56-bit DES encryption, for example) to encrypt the contents of a packet.

Note: Although SNMPv3 offers better security but SNMPv2c however is still more common. Cisco has supported SNMPv3 in their routers since IOS version 12.0.3T.

In the next part we will learn the SNMP messages used in each version.

SNMP Messages

SNMP Messages are used to communicate between the SNMP Manager and Agents. SNMPv1 supports five basic SNMP messages:

+ **SNMP GET**
+ **SNMP GET-NEXT**
+ **SNMP GET-RESPONSE**
+ **SNMP SET**
+ **SNMP TRAP**

In general, the GET messages are sent by the SNMP Manager to retrieve information from the SNMP Agents while the SET messages are used by the SNMP Manager to modify or assign the value to the SNMP Agents.

Note: GET-NEXT retrieves the value of the next object in the MIB.

The GET-RESPONSE message is used by the SNMP Agents to reply to GET and GET-NEXT messages.

Unlike GET or SET messages, TRAP messages are initiated from the SNMP Agents to inform the SNMP Manager on the occurrence of an event. For example, suppose you want to be alarmed when the CPU usage of your server goes above 80%. But it would be very annoying if the administrator has to actively use the GET message to check the CPU usage from time to time. In this case, the TRAP message is very suitable for

that purpose because the administrator would only be informed from the CPU itself when that event occurs. The figure below shows the direction of SNMP messages:
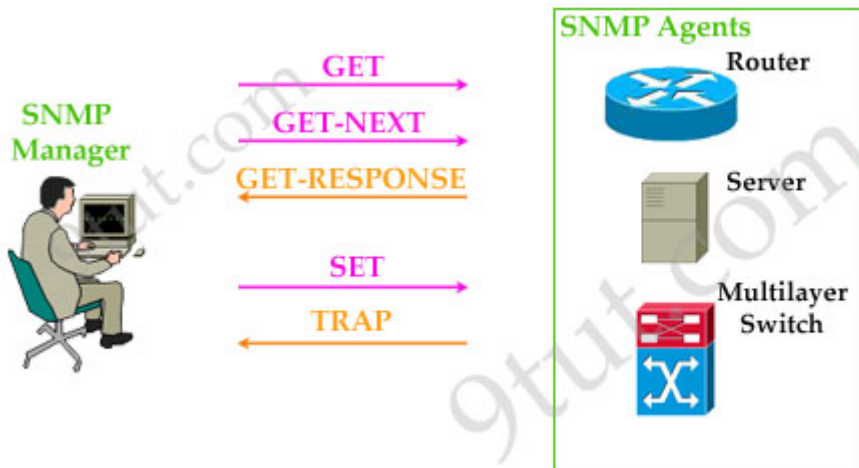
From SNMPv2c, two new messages were added: INFORM and GETBULK.

INFORM: An disadvantage of TRAP message is unreliable. SNMP communicates via UDP so it is unreliable because when the SNMP Agents send TRAP message to the SNMP Manager it cannot know if its messages arrive to the SNMP Manager. To amend this problem, a new type of message, called INFORM, was introduced from SNMPv2. With INFORM message, the SNMP Manager can now acknowledge that the message has been received at its end with an SNMP response protocol data unit (PDU). If the sender never receives a response, the INFORM can be sent again. Thus, INFORMs are more likely to reach their intended destination.

GETBULK: The GETBULK operation efficiently retrieve large blocks of data, such as multiple rows in a table. GETBULK fills a response message with as much of the requested data as will fit.

Note: There is no new message types on SNMPv3 compared to SNMPv2c.

SNMP Configuration

In the last part we will go through a simple SNMP configuration so that you can have a closer look at how SNMP works. SNMPv2c is still more popular than SNMPv3 so we will configure SNMPv2c.

1. Configure a community string

```
Router(config)#snmp-server community 9tut ro
```

In this case our community string named "9tut". The **ro** stands for read-only method.

2. Configure the IP address of a host receiver (SNMP Manager) for SNMPv2c TRAPs or INFORMs

```
Router(config)#snmp-server host 10.10.10.12 version 2c TRAPCOMM
```

"TRAPCOMM" is the community string for TRAP.

3. Enable the SNMP Traps

```
Router(config)#snmp-server enable traps
```

If we don't want to enable all trap messages we can specify which traps we want to be notified. For example, if you only want to receive traps about link up/down notification type then use this command instead:

```
Router(config)#snmp-server enable traps link cisco
```

Of course we have to configure an SNMP Manager on a computer with these community strings so that they can communicate.

Good resource and reference: http://docwiki.cisco.com/wiki/Simple_Network_Management_Protocol.

[Comments (1)](#) Comments

1. Hoangcisco
   March 5th, 2021

   very clear, thanks

Add a Comment

[   ] Name

[   ]

Submit Comment
[Subscribe to comments feed](#)
[EIGRP Troubleshooting Sim](#) [Syslog Tutorial](#)

Premium Member Zone

Welcome [Gurjeet singh](#)!

- [Welcome Premium Member](#)
- [CCNA – New Questions Part 5](#)
- [CCNA – New Questions Part 6](#)
- [CCNA – New Questions Part 7](#)
- [CCNA – New Questions Part 8](#)
- [CCNA – New Questions Part 9](#)
- [Composite Quizzes](#)

- [Logout](#)

CCNA 200-301

- [Basic Questions](#)
- [Topology Architecture Questions](#)
- [Cloud & Virtualization Questions](#)
- [CDP & LLDP Questions](#)
- [Switch Questions](#)
- [VLAN & Trunking Questions](#)
- [VLAN & Trunking Questions 2](#)
- [STP & VTP Questions](#)
- [EtherChannel Questions](#)
- [TCP & UDP Questions](#)
- [IP Address & Subnetting Questions](#)

CCNA Self-Study

- [Cisco Command Line Interface CLI](#)
- [Cisco Router Boot Sequence Tutorial](#)
- [OSI Model Tutorial](#)
- [Subnetting Tutorial – Subnetting Made Easy](#)
- [Frame Relay Tutorial](#)
- [Wireless Tutorial](#)
- [Virtual Local Area Network VLAN Tutorial](#)
- [VLAN Trunking Protocol VTP Tutorial](#)
- [IPv6 Tutorial](#)
- [Rapid Spanning Tree Protocol RSTP Tutorial](#)
- [Spanning Tree Protocol STP Tutorial](#)
- [Network Address Translation NAT Tutorial](#)
- [Access List Tutorial](#)
- [RIP Tutorial](#)
- [EIGRP Tutorial](#)
- [OSPF Tutorial](#)

Network Resources

- [Free Router Simulators](#)
  - [CCNA Website](#)
  - [ENCOR Website](#)
  - [ENSDWI Website](#)
  - [ENARSI Website](#)
  - [DevNet Website](#)
  - [CCIE R&S Website](#)
  - [Security Website](#)
  - [Wireless Website](#)
  - [Design Website](#)
  - [Data Center Website](#)
  - [Service Provider Website](#)
  - [Collaboration Website](#)

[Top](#)