



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Securing your Cisco Router when using SNMP

Charles Carter

December 11, 2000

Managing your Cisco Equipment

Every Network Manager is confronted with the requirement to manage and control their Cisco routed network. The ability to remotely manage your router base is a necessity, and since it requires access to each router, poses a number of security risks. The Simple Network Management Protocol provides the opportunity to remotely monitor, configure and receive notification of important or useful events from your routers. As with any capability, we need to also concern ourselves with insuring that only authorized personnel use it. SNMP version 1 was introduced over twelve years ago, and has become very popular among vendors, including Cisco.

What exactly is SNMP?

The Simple Network Management Protocol is a mechanism that uses a workstation as the point of entry and control for the Network Manager. In the Cisco environment, the router will contain an SNMP agent and Management Information Block (MIB). You will need some kind of software application to communicate to and possibly from your router. The following example shows a typical configuration using a workstation that could communicate to and with the routers in your network.

© SANS Institute 2000 - 2002
Author retains full rights.

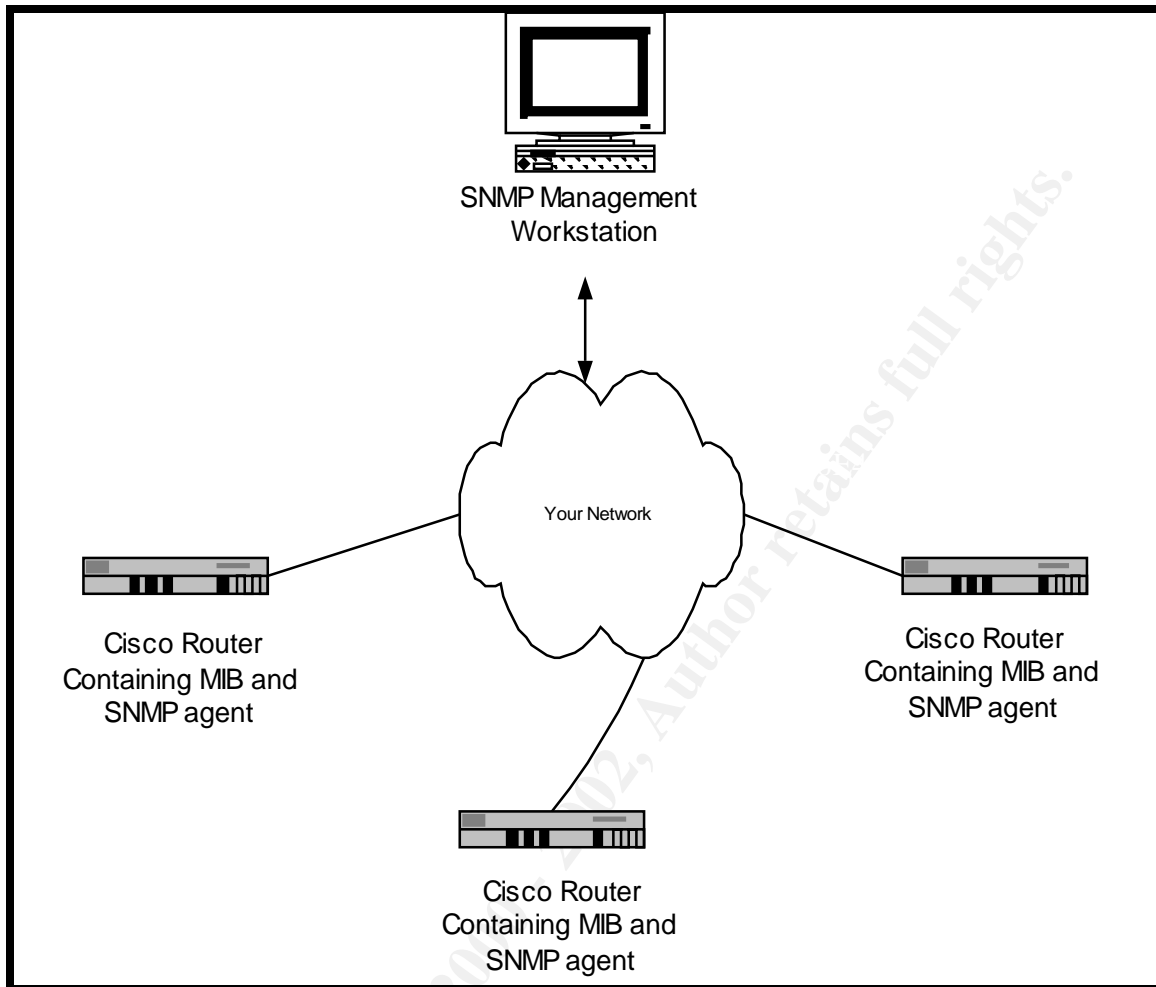


Figure 1 Typical SNMP Configuration

In determining how you want to leverage SNMP enabled devices, you need to consider whether you will use software that will poll the devices for useful information, enable Traps on the device which causes the device to automatically send back information, or some combination of both.

Every SNMP enabled device contains a database called a Management Information Block (MIB), which is a simple hierarchical tree structure that contains device information. SNMP version 1 also uses a very simple repertoire of commands. The basic commands are the GET, which will retrieve information from a MIB or the SET that places data into a MIB variable.

One of the more popular software tools in use in managing a Cisco router farm would be the Multi Router Traffic Grapher (MRTG) from Tobias Oetiker. This is a great tool and it's free! Another well-known product is WhatsUp Gold from Ipswitch. This is a modestly priced monitoring tool that is easy to setup and use.

If you want to both monitor and configure your system, you would probably want to acquire CiscoWorks from Cisco.

Why do we need to secure our SNMP capability?

SNMP version 1 also uses a two-password system, where passwords are called *Community* strings. One string is used only to retrieve data and is known as the *read only* community string and the other is the *read/write* community string, which can be used to both retrieve and place data in a MIB variable. The community strings are transmitted in clear text. While a later version of SNMP, called version 3 does provide enhancements in the area of security, most management applications only utilize SNMP version 1.

What do I need to do first?

You will need to issue basic commands to enable your router to use SNMP.

```
snmp-server community look RO  
snmp-server community touch RW
```

The first command allows read access to any software that presents the community string *look*.

The second command allows read and write access to any software that presents the community string *touch*.

It is important that you select strong passwords for your community strings! The ones I used in the above example are fairly weak. Do not use string names like *public* or *private*. Everyone can guess those names, since they are commonly used. If at all possible, you should avoid using the same community strings for all your routers; try using a different string for each device. Do not make a read-only string the same as a read-write string. There is an SNMP password review tool called SNMP Brute Force Attack available from SolarWinds that can be used to test the strength of your community strings. It allows you to execute a dictionary attack on your SNMP enabled routers. In fact, you can use it on any device that is SNMP enabled such as servers, switches, hubs or modems. Also, do not forget to periodically change your passwords!

Restricting the hosts that can access your SNMP enabled routers

It would also be a prudent security measure to restrict SNMP access to only management workstations on your own network, especially if you have INTERNET connections.

You can use an access-list and a modified version of the *snmp-server* command to restrict access to you own network. Let's assume you have a class C network address of 204.50.25.0.

```
access-list 5 permit 204.50.25.0 0.0.0.255
snmp-server community touch RW 5
```

The first command creates an access list with a number of 5 (5 in this case is an arbitrary number) and will only allow traffic from the 204.50.25.0 network. The second command allows read and write access to any software that presents the community string *touch*, as long as the request comes from the 204.50.25.0 network.

How do I find out if someone is trying to gain unauthorized access to my router by using SNMP?

We can use the trap capability of SNMP to have our router tell us when someone is sending SNMP commands with an incorrect community string. This facility requires that the management workstation have software such as CiscoWorks.

```
snmp-server enable traps
snmp-server trap-authentication
snmp-server host 204.50.25.5
```

The first command tells the router to enable traps. If this isn't active, no traps are forwarded.

The second command tells the router to send a trap if authentication of the community string fails.

The third command tells the router which host computer should be sent the trap.

Summary

SNMP is a simple but very powerful tool in managing your router network. It is equally important that you take a few simple precautions to insure that it never is abused. Using strong passwords, changing them periodically, and tracking access to your routers is a must.

Product References

MRTG	www.mrtg.org
WhatsUp Gold	www.ipswitch.com
CiscoWorks	www.cisco.com
SNMP check	www.solarwinds.net

References

Cisco." Improving Security on Cisco Routers".URL:
<http://www.ieng.com/warp/public/707/21.html#snmp>

Insecure.org. "Building Bastion Routers Using Cisco IOS".URL:
<http://www.insecure.org/news/P55-10.txt>

"Simple Network Management Protocol (SNMP)".URL:
<http://www.sce.carleton.ca/netmanage/snmp/cisco-intro.html>

Lewis, Chris, "Cisco TCP/IP Routing Professional Reference" McGraw Hill

Marr, Stephen and Rocci, Lenny. "Security Problems in Network Management"
Enterprise Systems Journal, March 2000

© SANS Institute 2000 - 2002, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event