



Configuring SNMP in Cisco Routers

Peter J. Welcher

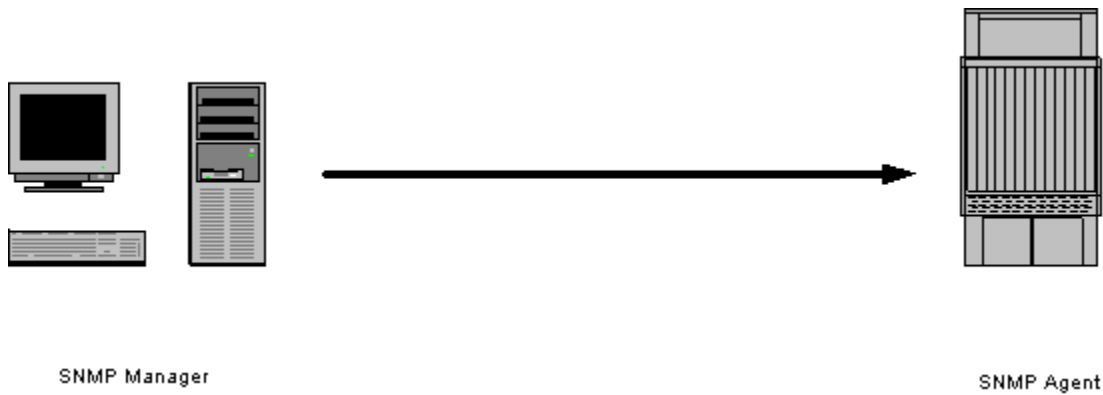
Introduction

I've been doing a fair amount of network management lately. Some of it has been consulting, and some preparation to deliver a new Cisco course, CEMS. This new CEMS course covers CiscoWorks 2000 (Resource Manager Essentials, CiscoWorks for Switched Internetworks, and Traffic Director). I'm eager to offer this course since it contains a lot of new and improved materials, plus many hands-on labs. It contains moderately deep coverage of the CW2000 products -- there's too much there to go into everything completely, and it would be too much for folks new to the products. The CEMS course also naturally leads into our four-day NetScout class for those making heavier use of the Cisco/NetScout probes and software (Traffic Director is essentially the NetScout reporting software -- and a good reason for buying CiscoWorks 2000).

From doing this network management work, it is apparent that Cisco has been adding a little here, a little there, to the SNMP capabilities of the routers and switches. Furthermore, my previous articles on Configuration for Manageability only scratch the surface of the topic. So it seems like it might be useful to us all to take a look at Cisco SNMP features and what they buy us in the way of router/switch manageability. There's enough to cover that this will be (at least) a two-article series.

Overview of Capabilities

Cisco routers and switches contain SNMP agents that can respond to standard SNMP get and set operations. That is, a management station can ask the Cisco device for information via an SNMP get, or it can tell the device to change some setting or take some actions, via a set operation. The device can also spontaneously originate traps or SNMPv2c inform notifications.



The Cisco IOS now (12.0) complies with SNMPv2c. They used to support the draft SNMPv2 Classic but pulled the security features in 11.3 when the version 2 standardization effort fell apart. SNMP version 3 is in 12.0(3) T. See the new features documentation for details (which would be an article in themselves), at

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm> .

The Cisco IOS also supports the router acting as an SNMP Manager. That means it can send SNMP get requests, receive replies, and receive traps or notifications.

This seems to have been in the documentation since 10.0. But other than enabling the feature, the documentation provides no information as to how to tell the router that it is supposed to send SNMP gets. Or maybe I'm missing something here. If anyone can point me in the right direction, I'd appreciate it (and pass it on in this CiscoWorld column).

For Service Providers, who need substantial information collection at remote sites, there is the system controller SC3640 and associated commands. You can read more about this at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cger/fun_c/fcprt3/fcsyscon.htm .

We won't go into that since it's presumably of interest only to a smaller audience.

Those who have been tracking my articles know about the RMON (version 1) capabilities in Cisco routers and switches ("mini-RMON"). This provides an excellent way to spot the devices, links, or ports that are getting into trouble. The 2500 and AS5200 routers provide full RMON version 1 support. (Beware what it may do to the router CPU). Since the prior articles are on my Web page, I won't go into more detail here. Some reasonably good information may also be found at

<http://www.cisco.com/warp/public/701/25.html> and <http://www.cisco.com/warp/public/79/17.html> .

Some slightly stale information is at

http://www.cisco.com/warp/partner/synchronicd/cc/cisco/mkt/enm/cwsiman/tech/rmon2_wp.html .

The Response Time Reporter (RTR) feature in Cisco routers allows the router to track response time information, using IP and SNA probe packets. You can send IP ICMP Echo, SNA SSCP echo, SNA LU type 0 to Cisco NSPECHO program, or SNA LU type 2 to Cisco NSPECHO program. The measurement can either be Echo Round Trip Time, or hop-by-hop analysis. The collected measurements can be used for longer-term trending. The router can report response time threshold violations via traps or SNA Alerts / Resolutions. This is another whole topic in itself. If you're interested, you might want to look into the Internetwork Performance Monitor software, which is intended to make it easier to access the RTR features in routers. See also

<http://www.cisco.com/warp/customer/cc/cisco/mkt/enm/cw2000/ipm/index.shtml> for the marketing

info, and also the Software Center page,

<http://www.cisco.com/kobayashi/sw-center/netmgmt/cw2000/IPM.html> .

In addition to SNMP, Cisco routers can also be managed via syslog reporting. As I've mentioned in a prior article, the CiscoWorks 2000 Resource Manager Essentials syslog reporting tool gives very useful access and reporting of this data. As we'll see below, there's a tie-in to SNMP.

Configuring SNMP Access in Routers

The first thing you need to do is enable SNMP access. This is done by configuring community strings, which act somewhat like passwords. (The difference is that there can be several community strings, and that each one may grant different forms of access). Here's what this might look like when configured:

```
snmp-server community public ro
snmp-server community ourCommStr ro
snmp-server community topsecret rw 60
snmp-server community hideit ro view noRouteTable

access-list 60 permit 10.1.1.1
access-list 60 permit 10.2.2.2
```

The first two lines allow read-only (get) SNMP access using either string. We configure our management stations with "ourCommStr" so we can easily cut off access via the well-known community string "public" if we so wish. (Note: non-IOS-based Cisco switches apparently do not allow multiple read-only community strings).

The third line configures the read-write (get/set) SNMP community string. This should **not** be the well-known string "private" (unless you like having an insecure network). The "60" restricts access to sources permitted via standard access-list 60 (the sample shown lists the individual network management stations permitted to do read-write SNMP operations, you could also use a wildcard mask to allow all stations on selected subnets access).

The fourth line says that those using the community string "hideit" are restricted to information in the view named "noRouteTable". This might be used to keep management stations (and HPOV Network Node Manager) from pulling huge BGP / Internet routing tables from selected routers, for example:

```
snmp-server view noRouteTable internet included
snmp-server view noRouteTable ip.21 excluded
snmp-server view noRouteTable ip.22 excluded
snmp-server view noRouteTable ifMIB excluded
```

Configuring SNMP Traps in Routers

The next thing you'll probably want to do is get those very useful trouble-indicators, SNMP traps, sent to your management station(s). The way to configure this is as follows:

```
snmp-server host 10.1.1.1 public
```

This sends any and all SNMP traps the router sends to host 10.1.1.1 using community string "public". (There's no point in exposing your real community strings here -- I'd just use "public" unless I ran across some incredibly picky network management software that was silly enough to try to enforce "correct" community strings on inbound traps).

If you wish to be more selective, you can list all the varieties of traps that go to each host:

```
snmp-server host 10.1.1.1 public snmp bgp
snmp-server host 10.2.2.2 public snmp frame-relay
```

This says that 10.1.1.1 is to get any SNMP or BGP traps, and 10.2.2.2 gets SNMP and frame relay traps.

This is a good way to nip any undesired messages at the source, rather than wasting network bandwidth on them, only to throw them away using HPOV or your trouble ticket system. On the other hand, life is too short to be diddling what traps go where on more than a few routers.

There is a long list of flavors of traps you can control in this fashion. Check the IOS manual or the router help for the latest items. Note that all the flavors of traps for a particular destination host go on one and the same (long!) line. Omitting any flavors list means they **all** get sent to that host.

You can also alter whether SNMP version 1 or 2c traps are sent, and what UDP port the traps are sent to.

If the above is all you configure, you may notice some deafening silence. You need to turn on the sending of traps in the first place -- the above commands just control who gets which traps. Turn on trap sending by configuring:

```
snmp-server enable traps
```

This turns on all the varieties of traps. You can also turn on specific traps, by appending them to the above command, one trap variant at a time. Some allow for further specificity. For example

```
snmp-server enable traps frame-relay
snmp-server enable traps envmon temperature
snmp-server enable traps bgp
snmp-server enable traps snmp
```

This says the router should send the standard SNMP traps, and also BGP, Frame Relay, and Environmental Monitor traps (but only the temperature type of envmon traps).

One intriguing variety of traps you can enable is the **config** traps. This records on your management station that someone has configured the router. If you have way too many hands with enable password access, this can be a valuable trouble-shooting tool ("what changed, and who did it").

Another useful variety of traps is the **syslog** option to this command. This causes router console messages to be repackaged as SNMP traps and sent to (selected) management stations. I see this as primarily useful in a PC environment, where you don't wish to run freeware syslog on NT, and are perhaps using HPOV ProSuite or SNMPC as trap receiver. If you wish to use the syslog reporting in CiscoWorks 2000 (CW2000) Resource Manager Essentials (RME), you will need to send console message to management station via syslog. Turning on the syslog trap option would then double the amount of such traffic on your network.

You probably do **not** want to invoke the "tty" option on the snmp-server enable traps command. The TTY traps inform you of termination of a telnet session, which can get rather chatty and annoying. They are primarily for "milking machine" situations, where protocol translation maps some bit stream across a TCP connection between paired access servers.

You can control linkUp/linkDown traps on the interface level. To avoid hearing about every call your ISDN backup interface makes, configure:

```
interface bri 0/0
no snmp trap link-status
```

Other SNMP Commands in Routers

The above is the most important part of SNMP. To keep this brief, here is a sample of some other things you might wish to configure:

```
snmp-server contact Orville Wright, Network Operations, (999) 123-4567
snmp-server location Engineering Dept., Floor 6, Building A-20, New York
City
snmp-server system-shutdown
snmp-server tftp-server-list 60
no snmp-server trap-authentication

interface loopback 0
ip address 10.5.5.5 255.255.255.255
snmp-server trap-source loopback 0
```

The first two lines specify the SNMP-retrievable contact and location. Useful, particularly if you have a lot of devices with different owners.

The **system-shutdown** command allows a certain SNMP set operation to trigger a router reboot. CiscoWorks and RME use this when upgrading routers.

The TFTP server list allows you to restrict the TFTP servers used by SNMP-triggered TFTP operations. CiscoWorks and RME can use TFTP to move configuration files and IOS images, so you might well want to restrict the sources/destinations for better security. The list of servers might well be the same access list 60 that lists management stations permitted to do SNMP set operations.

You might well want to set the trap source address to be that of the loopback interface. Many sites wish to use this as the official management address of the router. This is a good practice, since when a key interface is down, network management software may be unable to talk to the router. If you ensure that the device name always resolves first to the loopback address (which depends on knowing you DNS server software), then there is less likely to be a problem with connectivity due to downed interface. Setting the trap source to this address then ensures that when reverse name mapping resolves the loopback address to a hostname, the correct name is used. This means the network management software will be able to identify the device in question and, if appropriate, turn the icon red.

Less important SNMP-related router commands:

```
snmp-server chassis-id 123-45678
snmp-server packetsize 1500
snmp-server queue-length 1
snmp-server trap-timeout 30
```

The chassis ID defaults to the software chassis id, burned into the CPU card on the router. You may wish to change this to the external serial number, for automated SNMP updating of your records. (Generally this is under-appreciated until you try to RMA a dead router that you don't know the serial number of, or didn't purchase support for). I'm not quite sure doing this is best practice, but it might be convenient.

Packetsize specifies how big an SNMP get or set is allowed. The default is now 1500 bytes. Increasing

the setting may allow more information to be transferred in one operation. If you have MIB's with table with many entries in a row, then this is useful to avoid tooBig errors. (SunNet Manager used to do this with the old Cisco MIB). Increasing the number with older IOS releases, from 484 to 1500, seems like a good bet.

Queue-length and trap-timeout refer to retransmission queue for SNMP traps. When an interface fails, the router may be temporarily unable to send the linkDown trap. This might be due to routing protocol convergence, the need to dial up HQ, or other causes. The router will then periodically (every 30 seconds, by default) re-try sending the SNMP trap(s) it couldn't send. The trap-timeout changes this retry interval, default 30 seconds. The queue-length is how many traps get saved for retransmission in this fashion, default 10.

If you don't have dial backup, you might wish to set the queue-length to 1. (Is zero allowed?) Otherwise, when a link outage is resolved, you then get a bunch of very stale and old traps telling you about the outage you just fixed.

Next Month

The next article will look at configuring SNMP in switches, and, if space permits, also at syslog and how it interacts with network management software (CiscoWorks and CiscoWorks 2000 RME) on your network management station. I've also been looking at RSH and RCP (did you know the routers support them?). And I've been asked the interesting question "Just how **do** I predict how much SNMP traffic HP OpenView is going to put out onto my network?" (I have most of the answer, and hope to do some Sniffer work to verify some numbers, if time permits).

References

CCO Documentation on SNMP	http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3
Cisco Network Management Toolkit page	http://www.cisco.com/public/sw-center/netmgmt/cmtk/
Cisco MIB information	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

I have a short Cisco Network Management wishlist:

- 1) A separate HTML document containing **just** the SNMP traps for various Cisco devices and Cisco MIB's.

Take a look at <ftp://ftp.cisco.com/pub/mibs/traps/> . A GUI-based FTP client (with multi-select) will make your life a whole lot easier.

- 2) One ZIP or TAR file with all the latest Cisco MIB's (so I can pull them all, without clicking

etc. 50+ times!)

See <ftp://ftp.cisco.com/pub/mibs/> . Again, think GUI FTP!

Dr. Peter J. Welcher (CCIE #1773, CCSI #94014) is a Senior Consultant with Chesapeake NetCraftsmen. NetCraftsmen is a high-end consulting firm and Cisco Premier Partner dedicated to quality consulting and knowledge transfer. NetCraftsmen has nine CCIE's, with expertise including large network high-availability routing/switching and design, VoIP, QoS, MPLS, network management, security, IP multicast, and other areas. See <http://www.netcraftsmen.net> for more information about NetCraftsmen. Pete's links start at <http://www.netcraftsmen.net/welcher> . New articles will be posted under the Articles link. Questions, suggestions for articles, etc. can be sent to pjw@netcraftsmen.net .

5/31/99

Copyright 1999, Peter J. Welcher