



## Network Management Configuration Templates

Peter J. Welcher

## Introduction

I'm writing this just after Christmas, 2002. I think I've found a topic that is easy for me to write about, it being vacation time. At the same time I hope to provide you with some useful information.

This article is about what to configure in your Cisco routers and switches to maximize their manageability. I had posted the raw configuration templates previously on our web site, but I think it helps to have some explanation of what the intent is, in case you have to alter something.

These configuration templates represent what I consider to be current Best Practices. I see part of the potential value as consisting of pulling together bits and pieces of things that are scattered throughout the Cisco manuals. The CiscoWorks course provides a minimal starter configuration, which has its drawbacks. That course is not the place to get into the details of all the options for configuring Cisco devices for management, and certainly there is no other course explaining the ins and outs of configuring these features. There are increasing numbers of good Tech Tips at Cisco on Network Management, but nowhere do I see one document telling you all you need to do. Hence, this document.

## Prior Articles About Network Management

Some of these may be a bit old, but the basics haven't changed much. Some of these articles explain various SNMP or other configuration commands and what they might be good for. This article differs in trying to show the actual configuration you'd put into your devices.

Managing Cisco Routers	<a href="http://www.netcraftsmen.net/welcher/papers/manage.htm">http://www.netcraftsmen.net/welcher/papers/manage.htm</a>
Configuring for Manageability, Part I	<a href="http://www.netcraftsmen.net/welcher/papers/cfgmgt1.htm">http://www.netcraftsmen.net/welcher/papers/cfgmgt1.htm</a>
Configuring for Manageability, Part II	<a href="http://www.netcraftsmen.net/welcher/papers/cfgmgt2.htm">http://www.netcraftsmen.net/welcher/papers/cfgmgt2.htm</a>
Configuring for Manageability, Part III	<a href="http://www.netcraftsmen.net/welcher/papers/cfgmgt3.htm">http://www.netcraftsmen.net/welcher/papers/cfgmgt3.htm</a>
Performance Monitoring	<a href="http://www.netcraftsmen.net/welcher/papers/perfmgmt.htm">http://www.netcraftsmen.net/welcher/papers/perfmgmt.htm</a>
RMON	<a href="http://www.netcraftsmen.net/welcher/papers/rmon.htm">http://www.netcraftsmen.net/welcher/papers/rmon.htm</a>
Threshold Manager	<a href="http://www.netcraftsmen.net/welcher/papers/thresh.htm">http://www.netcraftsmen.net/welcher/papers/thresh.htm</a>
CiscoWorks 2000	<a href="http://www.netcraftsmen.net/welcher/papers/cw2000.html">http://www.netcraftsmen.net/welcher/papers/cw2000.html</a>
Configuring SNMP in Cisco Routers	<a href="http://www.netcraftsmen.net/welcher/papers/snmprouter.html">http://www.netcraftsmen.net/welcher/papers/snmprouter.html</a>
Configuring SNMP on Switches, and Syslog	<a href="http://www.netcraftsmen.net/welcher/papers/snmpswitch.html">http://www.netcraftsmen.net/welcher/papers/snmpswitch.html</a>
Switching: CiscoWorks 2000/CWSI	<a href="http://www.netcraftsmen.net/welcher/papers/cwsi.html">http://www.netcraftsmen.net/welcher/papers/cwsi.html</a>
Service Assurance Agent (SAA) and the Management Engine	<a href="http://www.netcraftsmen.net/welcher/papers/saa.html">http://www.netcraftsmen.net/welcher/papers/saa.html</a>
CiscoWorks 2000 Update	<a href="http://www.netcraftsmen.net/welcher/papers/cw2000update.html">http://www.netcraftsmen.net/welcher/papers/cw2000update.html</a>
Secure Management of Routers	<a href="http://www.netcraftsmen.net/welcher/papers/securemgmt.html">http://www.netcraftsmen.net/welcher/papers/securemgmt.html</a>
QoS Device Manager	<a href="http://www.netcraftsmen.net/welcher/papers/qdm.html">http://www.netcraftsmen.net/welcher/papers/qdm.html</a>

## Template Assumptions

Management stations use addresses a.b.c.d and e.f.g.h. We assume a.b.c.d has HP OpenView, CiscoWorks DFM, or other SNMP trap receiving software on it. We assume a syslog process is receiving syslog messages on a.b.c.d as well.

We assume m.n.o.p and q.r.s.t are NTP servers.

The following configurations enable desirable features and disable certain "noisy" traps for network management. Note that some commands will not apply in all chassis. This will result in an error message and the command being ignored in the chassis or Cisco IOS version where the command does not apply.

## Router Configuration Template

Use this template for Cisco routers and Cisco IOS-based switches and other devices.

```
! IOS-based Devices (Routers and Switches)
! ACL for management stations permitted SNMP access
! List them individually here
access-list 60 permit a.b.c.d
access-list 60 permit e.f.g.h
!
snmp-server community <your-comm-string-here> RO 60
snmp-server community <your-comm-string-here> RW 60
! Make sure the RW community string is chosen well and not obvious. It is
! equivalent to the enable secret.
!
! Put in contact name/email/phone/whatever:
snmp-server contact noc@foo.com
! Source all SNMP traps from the same address:
snmp-server trap-source loopback 0
! Allow CiscoWorks to reboot the box after IOS upgrade:
```

```

snmp-server system-shutdown
!
! WHERE to send SNMP traps to, which traps to send
! (default is to send ALL traps)
snmp-server host a.b.c.d traps version 2c public
! Enable all traps to be sent.
snmp-server enable traps
! NOTE: verbose tty traps will get sent, we could configure to prevent
! it but it's a little awkward; use HPOV to tune them out
! Disable the other verbose or redundant traps.
no snmp-server enable traps snmp authentication
no snmp-server enable traps syslog
no snmp-server enable traps config
!
! Interfaces: turn off link status traps on user IOS switch ports
! or dialer interfaces on routers:
interface ...
no snmp-server trap link-status
!
logging buffered 128000 debugging
no logging monitor
no logging console
logging trap informational
! Send syslog messages to CW
logging a.b.c.d
! The following will be ignored on devices with no loopback
logging source-interface loopback 0
!
line con 0
logging synch
exec-timeout 0 0
line vty 0 4
logging synch
exec-timeout 10 0
!
! Enable RCP for config and IOS transfers:
ip rcmd rcp-enable
ip rcmd remote-host <dummy-cw-user> a.b.c.d <dummy-cw-user> enable
!
! Enable Web management unless the security people say otherwise:
ip http server
!
service timestamps log datetime show-timezone
service timestamps debug datetime show-timezone
! To use EST for CiscoWorks:
clock timezone EST -5
clock summer-time EDT recurring
! Pick two core routers and point them at the Internet sources
! for time. Point all others at them:
ntp server m.n.o.p
ntp server q.r.s.t
! For boxes with hardware clock/calendar:
ntp update-calendar
! Globally enable SNMP ifindex persistence, if available (new IOS):
snmp-server ifindex persist
!
! Limit SNMP-triggered TFTP to the Net Mgmt servers:
snmp-server tftp-server-list 60
! Force good sub-interface traps (only in newest IOS code)
snmp-server trap link ietf

```

The above turns on all SNMP traps then turns selected ones off. There is a Cisco TTY trap that is sent upon termination of a TCP session, including telnet. This gets annoying but there is apparently no direct way to disable this in recent Cisco IOS versions. ("no snmp enable traps tty" used to be the command.)

I don't want SNMP authentication traps since any mis-configured net management software that's polling will trigger one such trap from each device on each polling cycle. If you want to see if someone is probing to guess community strings, leave the authentication traps enabled on a couple of devices.

Configuration and syslog traps are turned off, because syslog messages will provide all such information -- it's not necessary to send more copies via SNMP traps. This assumes the syslog reporting tools in CiscoWorks are being used to track and view syslog messages.

You will want to turn off link status traps on all interfaces that go up and down a lot, e.g. dial interfaces or user PC interfaces on Cisco IOS-based switches.

RCP is enabled so CiscoWorks can use it to reliably update the devices. Note that Cisco IOS images larger than 16 MB may well require RCP not TFTP for transfer. The "dummy-cw-user" acts as a sort of password. The first of the RCP commands enables RCP, the second provides the user login access (sort of like a ".rhosts" file in UNIX). Yes, SCP would be better if it were available. I'm becoming a big believer in SSL where possible (and affordable) to avoid sending passwords across any network in cleartext.

The HTTP server in the device is enabled to permit use of QDM. An access list can be used to more tightly limit HTML access to the Cisco devices.

The ifindex persistence and IETF style link traps are nice new features but certainly not critical.

## Switch Template

The following is a version of the above for CatOS Switches. Some commands will not apply in some chassis versions.

```

set snmp enable

```

```

set snmp rmon enable
# Default values:
set snmp rmonmemory 100
#
set snmp community read-only      your-secret-word-here
set snmp community read-write     really-secret-word
set snmp community read-write-all really-secret-word
set ip permit enable snmp
# List of addresses permitted to do SNMP to this box:
set ip permit a.b.c.d
set ip permit e.f.g.h
#
set snmp trap enable all
set snmp trap disable auth
set snmp trap disable syslog
set snmp trap disable config
#
# Where to send traps to:
set snmp trap a.b.c.d public
#
set logging buffer 500
set logging console disable
set logging history 1
set logging server enable
# The next two are the defaults:
set logging session enable
set logging telnet enable
# send syslog to CW server
set logging server a.b.c.d
#
set logging server facility LOCAL7
set logging server severity 6
set logging timestamp enable
#
# Start all logging at level 5, later adjust the
# over-complainers.
set logging level all 5 default
# The following two are chatty:
set logging pagp 4
set logging protfilt 4
#
set rcp username dummy-cw-user
#
# Set NTP to key off the core devices:
set ntp server m.n.o.p
set ntp server q.r.s.t
set ntp timezone EST -5
#
# Something in the above, turns on port traps as a side
# effect. Turn them back off on most ports (user ports):
set port trap mod/port disable
# Selected switch-switch, router, and switch ports need
# to have port traps enabled, to detect when key ports lose
# link status. You do not want to end up tracking when
# end user PC's are turned off, however

```

The comment above also apply to this configuration. The main switch-related tweak is to only send the more serious PAGP and PROTFILT messages, since these two subsystems in the switch tend to send a lot of messages. You do want to go in and enable link status traps on server or network ports. You probably do not want a trap anytime a user powers their PC on or off, so do not enable such traps across all ports.

**Added (6/1/2003):** you might want to consider the `set errdisable-timeout` command, if it is available to you. This greatly reduces the need to manually re-enable ports that have been errdisabled. You can specify which errdisable causes time out, if you wish to be selective about using this feature.

## Cisco Network Management Links

The first two of these provide tips about configuring for network management.

Technology: Network Management Protocols	<a href="http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Technologies&amp;f=2882">http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Technologies&amp;f=2882</a>
Technology: Network Management Protocols:SNMP	<a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Internetworking:SNMP&amp;s=Implementation_and_Configuration">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Internetworking:SNMP&amp;s=Implementation_and_Configuration</a>
Hardware: NAM and SwitchProbe Devices	<a href="http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Hardware%20Products&amp;f=472">http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Hardware%20Products&amp;f=472</a>

Software: Network Management Products	<a href="http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Software%20Products&amp;f=947">http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Software%20Products&amp;f=947</a>
Software: Network Management, CiscoWorks	<a href="http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Software%20Products&amp;f=854">http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Software%20Products&amp;f=854</a>

## Conclusion

**Tech tip:** next time you're logged into a switch, you might try "show snmp counters?". There's some interesting information available!

**Tech tip:** many people have basic HP OpenView Network Node Manager. The built-in reporting with this has some pretty severe limitations and is not very useful. One approach is to add more HPOV application packages -- but that costs. Instead, you can use the Applet builder to package up reporting for other SNMP variables. The Cisco local interface MIB can report on the locIfInBitsSec and locIfOutBitsSec bits per second counters, which are pretty useful. Another thing to do is to look into the HPOV conf directory, and look at the mibExpr.conf file. It contains expressions in Reverse Polish notation, including in and out interface utilization percentages (if%Util is the full duplex additive utilization, which is not as useful). You can use these with the data collection and reporting within HPOV. Using Show Data and then the Graph buttons in the HPOV Data Collection window is the best way of cutting through the clutter and getting per-device/per-interface graphs. The recent HPOV Web reports are a good first step towards better reporting within the HPOV NNM software.

Who knows what the next month will bring? I've been thinking about doing articles on the network management tools DFM, QPM, NAM and RTM using lots of screen captures, like the QDM article. I'm very impressed with NAM and DFM. And I've seen a lot of folks who have but don't use the DFM and RTM CiscoWorks components, so "making them more visible" might be useful. As far as QPM, it's well-documented and the tool of choice when doing QoS. I've been thinking about QoS and wireless a lot lately, complete with new posted seminar slides for QoS, so articles in those areas are likely. It's about time for more security and IP telephony as well. As always, your suggestions and comments are welcome!

---

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 [piw@netcraftsmen.net](mailto:piw@netcraftsmen.net).

1/2/2003

Copyright (C) 2003 Peter J. Welcher