

Troubleshoot the PGW 2200 Softswitch with SNMP

Document ID: 62683

Introduction

Prerequisites

Requirements

Components Used

Conventions

Troubleshoot SNMP Information on the Cisco PGW 2200

Related Information

Introduction

This document provides troubleshooting information for the Simple Network Management Protocol (SNMP) on the Cisco PGW 2200 Public Switched Telephone Network (PSTN) Gateway (referred to as simply Cisco PGW 2200 in this document). The information in this document applies specifically to the Cisco PSTN Gateway Solution for both call control and call signaling modes. This document contains tips and warnings on the use of SNMP components with the solution, as well as troubleshooting steps for solving potential problems.

The SNMP agent provides a simple network management task. The SNMP exchanges information about the status of a device, in this case a device linked to the Cisco PGW 2200, within the management framework using Protocol Data Units (PDUs) coded in Abstract Syntax Notation (ASN) format.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

Platform	Platform Name	Release
Cisco PGW 2200 Node	Cisco Media Gateway Controller (MGC)	<ul style="list-style-type: none">• 9.3(2) (From patch 9.3(2)S20) Release Notes for the Cisco Media Gateway Controller Software Release 9.3(2)• 9.4(1) (From patch 9.4(01)S06) Release Notes for the Cisco Media Gateway Controller Software Release 9.4(1)

		<ul style="list-style-type: none"> • 9.5(2) Integrated Release Notes for the Cisco Media Gateway Controller Software Release 9.5(2)
Cisco PGW 2200 Management Information Bases (MIB) Information		Cisco bug ID CSCeb37011 (registered customers only)

SNMP security enhancement

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Troubleshoot SNMP Information on the Cisco PGW 2200

The default SNMP security (community) string is public for read and notification purposes. The write security (community) string is randomly generated for the process recovery function. SNMP configurations vary; for specific defects, check Cisco bug ID CSCeb73838 (registered customers only) which is linked to a Cisco PGW 2200 **config-snmpp** command that needs to be used to configure the SNMP items on the Cisco PGW2200.

The **config-snmpp** command, located in the /opt/CiscoMGC/local directory, is a menu-driven tool which can be executed from the UNIX superuser mode. Its migration feature can limit the set operation to only two MIB objects which either enable or disable the process recovery. The security string of set operation is randomly generated and limited to local host access. The **config-snmpp** command also provides the user the capability to add and delete the security (community) string and trap destination. This is sample output of the **config-snmpp** command:

```

mgcusr@mgc-bru-20% su - root
Password:
# config-snmpp

Migrating snmpd.cnf into a more secure setting...

=====      SNMPD Configuration Main Menu      =====

1. View Configuration Entries
2. Add an SNMP Community
3. Delete an SNMP Community
4. Add a Trap Destination
5. Delete a Trap Destination
6. Activate the New Settings

Enter a selection (1 through 6) or 'q' to quit:  1

=====      Entries Menu      =====

1. sysDescr
2. sysObjectID
3. sysLocation

```

```

4. sysContact
5. sysName
6. snmpEnableAuthenTraps
7. MAX_THREADS
8. MAX_PDU_TIME
9. MAX_OUTPUT_WAITING
10. MAX_SUBAGENTS
11. subagent
12. snmpCommunityEntry
13. communityEntry
14. snmpEngineBoots
15. usmUserEntry
16. vacmAccessEntry
17. vacmSecurityToGroupEntry
18. vacmViewTreeFamilyEntry
19. snmpNotifyEntry
20. snmpTargetAddrEntry
21. snmpTargetParamsEntry
22. snmpNotifyFilterProfileEntry
23. snmpNotifyFilterEntry
24. httpUserNameEntry
Enter a selection (1 through 24) or 'q' to quit to Main Menu:
=====  SNMPD Configuration Main Menu  =====

```

- ```

1. View Configuration Entries
2. Add an SNMP Community
3. Delete an SNMP Community
4. Add a Trap Destination
5. Delete a Trap Destination
6. Activate the New Settings

```

Enter a selection (1 through 6) or 'q' to quit: **2**

```

===== Add CommunityString Menu =====

```

```

SnmpCommunityName CommunitySecurityName
public ReadAndNotifyToAll

```

-- Where:

| CommunitySecurityName | SecurityModel | Read          | Write         | Notification  |
|-----------------------|---------------|---------------|---------------|---------------|
| ReadAndNotifyToAll    | snmpv1        | AllMibObjects | -             | AllMibObjects |
| ReadAndNotifyToAll    | snmpv2c       | AllMibObjects | -             | AllMibObjects |
| ReadWriteAll          | snmpv1        | AllMibObjects | AllMibObjects | -             |
| ReadWriteAll          | snmpv2c       | AllMibObjects | AllMibObjects | -             |

Would you like to proceed with the Add [n]/[y]?

From this level you can change the SnmpCommunityName on the Cisco PGW 2200.

**Note:** If the SNMP daemon is disabled on the Cisco PGW 2200, there is no recovery feature for Cisco PGW 2200 processes (see /opt/CiscoMGC/snmp/critagt.cnf). Processes monitored by the Critical Application Subagent (critagt) cannot be recovered if this agent is killed unintentionally. There is no recovery support.

Once you have set all information correctly, you may still encounter some issues. Here are some troubleshooting steps:

1. Ensure the snmpdm process is running on the Cisco PGW 2200:

```
mgcusr@PGW 2200a% ps -ef | grep snmp
```

```

root 931 1 0 Mar 29 ? 3:20 /opt/CiscoMGC/snmp/snmpdm -tcplocal -d
root 932 1 0 Mar 29 ? 0:31 /opt/CiscoMGC/snmp/mib2agt -d
root 15519 1 0 Jun 29 ? 0:06 /opt/CiscoMGC/snmp/critagt -d
root 933 1 0 Mar 29 ? 1:26 /opt/CiscoMGC/snmp/hostagt -d
root 934 1 0 Mar 29 ? 0:25 /opt/CiscoMGC/snmp/fsagt -d
root 935 1 0 Mar 29 ? 4:34 /opt/CiscoMGC/snmp/brassagt -d

```

2. Critagt is supervised from init. Verify that you have this entry in the /etc/inittab directory:

```
ca:3:respawn:/opt/CiscoMGC/snmp/critagt -d
```

3. Critagt supervises the snmpdm, mib2agt, hostagt, fsagt, brassagt, procM and LogServer agents. Verify that you see these SNMP processes running in /opt/CiscoMGC/snmp/critagt.cnf:

```

mgcusr@PGW 2200a% ps -ef | grep snmp
root 931 1 0 Mar 29 ? 3:20 /opt/CiscoMGC/snmp/snmpdm -tcplocal -d
root 932 1 0 Mar 29 ? 0:31 /opt/CiscoMGC/snmp/mib2agt -d
root 15519 1 0 Jun 29 ? 0:06 /opt/CiscoMGC/snmp/critagt -d
root 933 1 0 Mar 29 ? 1:26 /opt/CiscoMGC/snmp/hostagt -d
root 934 1 0 Mar 29 ? 0:25 /opt/CiscoMGC/snmp/fsagt -d
root 935 1 0 Mar 29 ? 4:34 /opt/CiscoMGC/snmp/brassagt -d

```

4. Issue the UNIX command **netstat -a | grep 161** and check that the command returns an **idle** status for the User Datagram Protocol (UDP) SNMP ports.

```

mgcusr@PGW 2200a% netstat -a | grep 161
*.161 Idle
localhost.7161 *.* 0 0 24576 0 LISTEN
30006f41610 stream-ord 00000000 00000000 ../var/lsd_addr
mgcusr@PGW 2200a% netstat -a | grep 162
*.162 Idle
mgcusr@PGW 2200a%

```

**Note:** Standard SNMP sends responses to management requests over UDP port 161 and trap information over UDP port 162.

**Note:** You can issue the UNIX **snoop** command to find out what has been sent between the Cisco PGW 2200 and the network management system (NMS) station. On the NMS station, you can issue freeware command **snmpwalk** in combination with the UNIX **snoop** command.

5. Issue the **snoop -v <IP address NMS>** command on the Cisco PGW 2200 to find out what messages have been sent from and to the NMS station. Also read the **man snoop** command details; you may want to store them in a file. You can also capture this information and check the content using the Ethereal network protocol analyzer.
6. Issue the **snmpwalk -c public <PGW 2200 IP address>** command on your NMS system. This command queries for a tree of information.

The version of the **snmpwalk** command used for the purposes of this document is:

```

% snmpwalk
No hostname specified.
USAGE: snmpwalk [OPTIONS] AGENT [OID]

Version: 5.0.9
Web: http://www.net-snmp.org/
Email: net-snmp-coders@lists.sourceforge.net

```

This is a sample output of the **snmpwalk** command:

```

SNMPv2-MIB::sysDescr.0 = STRING: SNMPv3 agent from Cisco Systems, Inc.
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.2496.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1599337216)
185 days, 2:36:12.16
SNMPv2-MIB::sysContact.0 = STRING: Cisco Systems, Inc. +1 703 484 3000

```

```

SNMPv2-MIB::sysName.0 = STRING: NSSU - MGC
SNMPv2-MIB::sysLocation.0 = STRING: Herndon, Virginia
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 3
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifDescr.1 = STRING: lo0
IF-MIB::ifDescr.2 = STRING: eri0
IF-MIB::ifDescr.3 = STRING: eril
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifMtu.1 = INTEGER: 8232
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifMtu.3 = INTEGER: 1500
RFC1213-MIB::atNetAddress.2.1.50.0.0.1 = Network Address: 32:00:00:01
RFC1213-MIB::atNetAddress.2.1.224.0.0.0 = Network Address: E0:00:00:00
RFC1213-MIB::atNetAddress.3.1.10.48.85.20 = Network Address: 0A:30:55:14
RFC1213-MIB::atNetAddress.3.1.224.0.0.0 = Network Address: E0:00:00:00
IP-MIB::ipForwarding.0 = INTEGER: notForwarding(2)
IP-MIB::ipDefaultTTL.0 = INTEGER: 255
IP-MIB::ipInReceives.0 = Counter32: 535077888
IP-MIB::ipInHdrErrors.0 = Counter32: 0
IP-MIB::ipInAddrErrors.0 = Counter32: 0
IP-MIB::ipForwDatagrams.0 = Counter32: 0

```

```

!--- Output suppressed due to the enormity of information, which
!--- would require several HTML pages to display.

```

You cannot start the snmpdm process in the /opt/CiscoMGC/snmp directory from the UNIX superuser mode, using the argument "-apall" as log all messages anymore. This is not possible because the software removes this argument and brings it back into the normal setup scenario as snmpdm -tcplocal -d, shown in this sample output. This results in this error message:

```

#/etc/init.d/snmpd stop
/opt/CiscoMGC/snmp/snmpdm -tcplocal -d -apall &

!--- Start the snmpdm process with the command snmpd -tcplocal -d -apall &.

SNMP Research SNMP Agent Resident Module Version 15.4.1.16
Copyright 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998,
1999, 2000, 2001, 2002, 2003 SNMP Research, Inc.
Successfully opened log file /tmp/snmpd.log
 at line 397 in file mastmain.c
Only APERROR and APWARN messages are being printed to the log file
(override with -log_tracefile)
 at line 421 in file mastmain.c

[1] 11204
init_fnames: searching for configuration files in /opt/CiscoMGC/snmp
from getenv("SR_AGT_CONF_DIR")
 at line 90 in file ../../snmpd/shared/fnames.c
AgentSocketCreate: bind failed: Address already in use
 at line 262 in file tcp.c
InitMaster: IPCFP[0].AgentSocketCreate failed
 at line 735 in file master.c
master agent initialization failed, exiting
 at line 478 in file mastmain.c

/opt/CiscoMGC/snmp/snmpdm -h

```

```
usage: ./snmpdm [options]
```

```
options:
```

```
-d execute in the foreground window
-trap_send_port PORT send SNMP trap/inform messages from port PORT
-tcpany accept connections from any TCP subagent
-tcplocal accept connections from local TCP subagents
-tcptimeout disallow connections from TCP subagents (default)
-apnone no log messages
-apwarn log warning messages
-aperror log error messages
-apconfig log config file i/o messages
-appacket log SNMP packet build/parse messages
-aptrap log trap/inform messages
-apaccess log agent processing messages
-apemanate log master/subagent messages
-aptimer log timer debug messages
-apthread log thread debug messages
-apverbose log verbose debug messages
-apuser log user messages
-hexdump dump packets in hex
-vbdump dump packets as varbinds
-aptrace trace packet in application
-apaudit audit SET processing in application
-apall log all messages
-log_mtos allow sending log messages to Subagents
-log_nomtos disallow sending log messages to Subagents
-log_stom allow receiving log messages from Subagents
-log_nostom disallow receiving log messages from Subagents
-log_format 0 use traditional log message format
-log_format 1 use new log message format
-log_stdout allow log messages to go to standard output
-log_nostdout disallow log messages to go to standard output
-log_stderr allow log messages to go to standard error
-log_nostderr disallow log messages to go to standard error
-log_file allow log messages to go to snmpd.log
-log_nofile disallow log messages to go to snmpd.log
-log_tracefile allow APTRACE messages to go to snmpd.log
-log_notracefile disallow APTRACE messages to go to snmpd.log
-log_append append log messages to snmpd.log
-log_noappend discard previous contents of snmpd.log, if any
-large_vl_pdu lift 484 byte restriction for v1/v2c PDUs
-help print this usage line
-pkt_size value use supplied value as max packet size
```

```
mgcusr@PGW 2200a%
```

The critagt.cnf file in the /opt/CiscoMGC/snmp directory, shown here, is responsible for the above error message:

```
mgcusr@pw2200a% more critagt.cnf
Entry type: critAppProcEntry
Entry format: integer
octetString
octetString
octetString
integer
integer
integer
integer
integer
integer
critAppProcEntry 1 snmpdm "/opt/CiscoMGC/snmp/snmpdm -tcplocal -d"
- 1 true 0 true true true
```

Because critagt restarts the SNMP daemon and once it is started, the port becomes busy, you encounter the error message described.

**Note:** You cannot change any entry in the critagt.cnf file, because after you restart the Cisco PGW 2200 application, it automatically restores the default settings.

**Note:** For detailed information on the snmpd.log file, check under the /tmp directory.

For DDTS records linked to Cisco PGW 2200 snmpd details, refer to Cisco bug ID CSCef55514 ( registered customers only) Missing SNMP generic traps for link down and up.

---

## Related Information

- [Cisco PGW 2200 Softswitch Tech Notes](#)
- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Recommended Reading: Troubleshooting Cisco IP Telephony](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jul 23, 2008

Document ID: 62683

---