

Устранение неполадок PGW 2200 Softswitch с SNMP

ID документа: 62683

Обновлено : 23 июля 2008



[Загрузка PDF](#)



[Печать](#)

[_ Обратная связь](#)

Родственные продукты

- [Сигнальный контроллер Cisco SC 2200](#)
- [Cisco PGW 2200 Softswitch](#)
- [Signaling System 7 \(SS7\)](#)

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Сведения SNMP устранения неполадок на Cisco PGW 2200](#)

[Дополнительные сведения](#)

[Соответствующие дискуссии сообщества технической поддержки Cisco](#)

Введение

Этот документ предоставляет сведения об устранении проблем для Протокола SNMP на Открытой коммутируемой телефонной сети (PSTN) шлюз Cisco PGW 2200 (называемый как просто Cisco PGW 2200 в этом документе). Сведения в этом документе применяются в частности к решению шлюза Cisco PSTN и для управления вызовами и для режимов передачи вызовов. Этот документ содержит советы и предупреждения на использовании компонентов SNMP с решением, а также действия по устранению проблем для решения потенциальных проблем.

Агент SNMP предоставляет задачу управления простой сетью. Обмен данными SNMP о статусе устройства, в этом случае устройство связалось с Cisco PGW 2200 в инфраструктуре управления с помощью Протокольных информационных единиц (PDU), закодированные в формате Абстрактного синтаксического обозначения (ASN).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Платформа	Имя платформы	Выпуск
Узел Cisco PGW 2200	Cisco Media Gateway Controller (MGC)	<ul style="list-style-type: none">• 9.3 (2) (Из исправления 9.3 (2) S20) — Комментарии к выпуску для Выпуска 9.3 (2) Cisco Media Gateway Controller Software• 9.4 (1) (Из исправления 9.4 (01) S06) — Комментарии к выпуску для Выпуска 9.4 (1) Cisco Media Gateway Controller Software• 9.5 (2) Интегрированный — Комментарии к выпуску для выпуска 9.5 (2) Cisco Media Gateway Controller Software
PGW Cisco 2200 информации об информационных базах управления (MIB)		Идентификатор ошибки Cisco CSCeb37011 (только зарегистрированные клиенты) — Усовершенствование безопасности SNMP

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

Сведения SNMP устранения неполадок на Cisco PGW 2200

Безопасность SNMP по умолчанию (сообщество) строка обще в целях уведомления и чтении. Безопасность записи (сообщество) строка случайным образом генерируется для функции восстановления процесса. Конфигурации SNMP варьируются; для определенных дефектов проверьте идентификатор ошибки Cisco [CSCeb73838 \(только зарегистрированные клиенты\)](#), который связан с командой `config-snmp` Cisco PGW 2200, которая должна использоваться для настройки элементов SNMP на Cisco PGW2200.

Команда `config-snmp`, расположенная в `/opt/CiscoMGC/local` каталоге, является управляемым с помощью меню программным средством, которое может быть выполнено от режима привилегированного пользователя Unix. Его функция миграции может ограничить операцию присвоения только двумя объектами MIB, которые или включить или отключают восстановление процесса. Строка защиты назначения операции случайным образом генерируется и ограничивается доступом локального хоста. **Команда `config-snmp`** также предоставляет пользователю возможность добавить и удалить безопасность (сообщество) строка и адрес назначения ловушки. Это - пример выходных данных команды `config-snmp`:

```
mgcusr@mgc-bru-20% su - root Password: # config-snmp 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.
```

Примечание: Если демон SNMP отключен на Cisco PGW 2200, нет никакой функции восстановления для процессов Cisco PGW 2200 (см. `/opt/CiscoMGC/snmp/critagt.cnf`). Если этот агент уничтожен непреднамеренно, процессы, проверенные Второстепенным агентом Критически важного приложения (`critagt`), не могут быть восстановлены. Нет никакой поддержки восстановления.

Как только вы установили всю информацию правильно, можно все еще встретиться с некоторыми проблемами. Вот некоторые действия по устранению проблем:

1. Гарантируйте, что процесс `snmpdm` работает на 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. `Criatgt` контролируется от `Init`. Проверьте, что у вас есть эта запись в `/etc/inittab` каталоге: `ca:3:respawn:/opt/CiscoMGC/snmp/critagt -d`

3. Critagt контролирует snmpdm, mib2agt, hostagt, fsagt, brassagt, procM и агенты LogServer. Проверьте, что вы видите, что эти процессы SNMP работают

```
v/opt/CiscoMGC/snmp/criagt.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. Выполните netstat команды UNIX-а | grep 161 и проверьте, что команда возвращает простаивающий статус для портов SNMP Протокола UDP.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% **Примечание:** Стандартный SNMP передает ответы на запросы управления по порту 161 UDP и сведения о ловушке по порту 162 UDP.**Примечание:** Можно выполнить команду ищейки UNIX для обнаружения то, что было передано между Cisco PGW 2200 и станцией системы управления сетью (NMS). На Станции NMS можно выполнить бесплатную команду snmpwalk в сочетании с командой ищейки UNIX.
5. Выполните ищейку-v команда NMS> адреса <IP на Cisco PGW 2200 для обнаружения то, какие сообщения были переданы от и до Станции NMS. Также считайте подробные данные команды man snmp; можно хотеть сохранить их в файле. Можно также перехватить эту информацию и проверить содержание с помощью Эфирного сетевого протокола анализатор.

6. Выполните snmpwalk-с общий <PGW 2200 IP-адресов> команда на вашей системе NMS. Эта команда делает запрос для дерева сведений.Версия команды snmpwalk, используемой в целях этого документа:% 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 Это - пример выходных данных команды snmpwalk: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: eri1
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.

Вы не можете запустить процесс snmpdm в/opt/CiscoMGC/snmp каталоге от режима привилегированного пользователя Unix, с помощью аргумента "-apall" как журнал все сообщения больше. Это не возможно, потому что программное обеспечение удаляет этот аргумент и возвращает его в сценарий обычной установки как snmpdm-tcplocal-d, показанный в этом примере выходных данных: Это приводит к этому сообщению об ошибках:

```
#!/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 -tcp any accept connections from any TCP subagent -
tcplocal accept connections from local TCP subagents -tcpnone 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 -apacket 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_nontos 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_v1_pdus 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%
```

critagt.cnf файл в/opt/CiscoMGC/snmp каталоге, показанном здесь, ответственен за вышеупомянутое сообщение об ошибках:

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

Поскольку critagt перезапускает демон SNMP и как только это запущено, порт становится занятым, вы встречаетесь с описанным сообщением об ошибках.

Примечание: Вы не можете изменить запись в critagt.cnf файле, потому что после перезапуска приложения Cisco PGW 2200 это автоматически восстанавливает настройки по умолчанию.

Примечание: Для получения дальнейшей информации на snmpd.log файле, проверьте в соответствии с / временным каталогом.

Для записей DDTS, связанных с подробными данными Cisco PGW 2200 snmpd, обратитесь к идентификатору ошибки Cisco [CSCef55514 \(только зарегистрированные клиенты\)](#) — Недоступный SNMP trap-сообщения общего назначения для ссылки вниз и.

[Дополнительные сведения](#)

- [Технические примечания программного коммутатора Cisco PGW 2200](#)
- [Поддержка голосовых технологий](#)
- [Поддержка продуктов Голосовой и Унифицированной связи](#)
- [Устранение неполадок в системах IP-телефонии Cisco](#)
- [Cisco Systems – техническая поддержка и документация](#)

Был ли этот документ полезен? [Да](#) [нет](#)

Спасибо за ваш отзыв.

[Адресовать вопрос техподдержке \(требуется контракт сервиса Cisco.\)](#)

Соответствующие дискуссии сообщества технической поддержки Cisco

[Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.](#)

[См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.](#)

Обновлено : 23 июля 2008

ID документа: 62683