CHAPTER 17

Simple Network Management Protocol

Revised: July 24, 2009, OL-3743-42

This chapter describes the tables and commands pertaining to the Simple Network Management Protocol (SNMP) in the Cisco BTS 10200 Softswitch.

Note In this chapter, an asterisk preceding a token name means the token is mandatory. A token without an asterisk is optional.

Simple Network Management Protocol Community

The Simple Network Management Protocol (SNMP) Agent uses the SNMP Community (snmpcommunity) table using the snmpconfig command to:

- manually block particular IP addresses (or hostnames) due to abuse, unauthorized access, or access attempts using the SNMP blocking command. In addition, if the Agent detects what appear to be multiple failed attempts from a particular source, it automatically blocks that source IP address, or hostname. To unblock either the manual or automatically blocked hosts, the blocked entries from this table must be manually deleted.
- configure settings for conformance to RFC 1213 using the MIB to System (MIB2SYS) configuration command.
- couple or decouple the SNMP Agent to the Sun Solaris SNMP subagent using the SNMP setting command.
- stores community strings for SNMP agents, which can be modified using the snmpconfig command. A community string is a password-like variable used for Cisco BTS 10200 Softswitch SNMP Agent access.

At installation, this table is initially provisioned with the value PUBLIC for both the READCOMMUNITY and WRITECOMMUNITY tokens. Service providers can delete either value and specify their own value(s). During upgrades, whatever values are in these tables are maintained. READCOMMUNITY and WRITECOMMUNITY are case insensitive. The PUBLIC value is case sensitive.

Table Name: SNMPCOMMUNITY

Table Containment Area: OAMP

Command Types

Show, add change and delete

Examples

Block Command Examples:

```
show snmpconfig type=MANUALBLOCKED
show snmpconfig type=AUTOBLOCKED
add snmpconfig type=MANUALBLOCKED; value=hostnameABC
add snmpconfig type=MANUALBLOCKED; value=192.168.1.192
delete snmpconfig type=MANUALBLOCKED; value=hostnameABC
delete snmpconfig type=AUTOBLOCKED; value=hostnameABC
```

MIB2SYS Command Examples:

```
show snmpconfig type=MIB2SYS; value=sys_name;
add snmpconfig type=MIB2SYS; value=sys_name;
change snmpconfig type=MIB2SYS; value=sys_location; value1=Cisco Systems
delete snmpconfig type=MIB2SYS; value=sys_name;
```

Setting Command Examples:

```
show snmpconfig type=SETTING;
add snmpconfig type=SETTING; value=COUPLE_SUN_AGENT;
delete snmpconfig type=SETTING;
```

Store Command Examples:

```
show snmpconfig type=readcommunity
show snmpconfig type=writecommunity
add snmpconfig type=readcommunity; Value=whateverreadvalue
add snmpconfig type=writecommunity; Value=whateverwritevalue
delete snmpconfig type=readcommunity; Value=whateverreadvalue
delete snmpconfig type=writecommunity; Value=whateverwritevalue
```

Usage Guidelines

Primary Key Token(s): type, value

Add Rules: None.

Delete Rules: None.

Syntax Description

* TYPE	Primary key. Mandatory for show, add, change and delete. Type of blockage. VARCHAR(64): 1–64 ASCII characters. Permitted values are: AUTOBLOCKED—SNMP Agent detects what it perceives are suspicious sources trying to access the system. MANUALBLOCKED—Operator manually blocks a source from accessing the system using SNMP. MIB2SYS—MIB2 definition. SETTING—Setting using the add command couples Agents; setting using the delete command uncouples Agents. READCOMMUNITY—Variable to read agent data. WRITECOMMUNITY—Variable to set agent data.
* VALUE	Mandatory for add, change and delete. Valid for commands: show, add, change and delete. Primary key. IP Address or hostname of the blocked source. VARCHAR(64): 1–64 ASCII characters. Actual value of a community string. Valid only if type=READCOMMUNITY or WRITECOMMUNITY. SYS_NAME—System name. Valid only if type=MIB2SYS. SYS_CONTACT—System contact. Valid only if type=MIB2SYS. SYS_LOCATION—System location. Valid only if type=MIB2SYS. COUPLE_SUN_AGENT—Couples the Cisco BTS 10200 Softswitch SNMP Agent with the Sun SNMP Agent. Valid only if type=SETTING. Use underscores (_) for this value. Do not use hyphens (-).
KEY1	Valid for Commands: show, add, change and delete. Used to specify a privilege level similar to the CLI noun privilege level. This is required when accessing "status" command branches for the SNMP MIB such as when accessing statuses of a media gateway, Call Agent, and so forth. See the Command Level section in the Security chapter for more information. VARCHAR (14): 1–14 ASCII characters. Permitted value is COMMAND-LEVEL.
VALUE1	Valid for commands: show, add, change and delete. Used to further define the type and value tokens. Defined by service provider. VARCHAR(64): 1–64 ASCII characters.

Simple Network Management Protocol Trap Destination

The Simple Network Management Protocol (SNMP) Agent uses the SNMP Trap Destination (snmptrapdest) table to send traps to the network management systems (NMSs) listed in the table. This provides the SNMP Agent with a persistent list of NMSs to send SNMP traps to. When performing trap retransmission, valid destination addresses must be provisioned here.

Table Name: SNMPTRAPDEST

Table Containment Area: EMS

Command Types

Show, add, change, and delete

Examples

```
show snmptrapdest;
add snmptrapdest; trapdestaddress=190.10.100.199; trapdestport=162;
change snmptrapdest trapdestindex=1; trapdestport=16222;
delete snmptrapdest trapdestindex=1;
```

Usage Guidelines

Primary Key Token(s): trapdestindex

Add Rules: None.

Change Rules: None.

Delete Rules: None.

*TRAPDESTADDRESS	IP address, or host name, of the NMS machine. VARCHAR(15): 7–15 ASCII characters in formats ranging from: n.n.n.n to nnn.nnn.nnn.nnn.
*TRAPDESTPORT	Port number to which the NMS machine is listening for incoming traps. INTEGER: 1–65535.
TRAPDESTINDEX	Primary Key. Mandatory for change and delete. Index into the table. INTEGER: 1–4294967296.
TRAPDEST COMMUNITY (Not used)	Community name associated with the trap to be sent to the NMS. VARCHAR(64): 1–64 ASCII characters.
TRAPDESTOWNER (Not used)	Owner of this NMS. VARCHAR(64): 1–64 ASCII characters.
TRAPDESTSTATUS (Not used)	Status state of this entry. INTEGER: 1–6.

FILTERTYPES	Specifies which subsystem events to filter on, or permit to be sent to, this address. Used in combination with FILTERLEVELS to provide a granular filter for traps from the SNMP Agent side. VARCHAR(12) 1–12 ASCII characters. Permitted values are: BILLING CALLP CONFIG DATABASE MAINTENANCE OSS SECURITY SIGNALING STATISTICS SYSTEM AUDIT
FILTERLEVELS	Specifies which event levels to filter on, or permit to be sent to, this address. Used in combination with FILTERTYPES to provide a granular filter for traps from the SNMP Agent side. VARCHAR(8) 1–8 ASCII characters. Permitted values are: DEBUG INFO WARNING MINOR MAJOR CRITICAL