APPENDIX D

MIBs Used and SNMP Traps Generated

MIBS Used

Service Monitor uses the CISCO-SYSLOG-MIB to generate SNMP traps.

SNMP Traps Generated

Cisco Prime Unified Service Monitor (Service Monitor) generates the following traps:

- MOS Violation—For details, see Table D-1.
- Sensor Unreachable—For details, see Table D-2.
- Sensor Reconnect—For details, see Table D-3.

Trap details are provided as name-value pairs in the clogHistMsgText field of the clogMessageGenerated notification. Table D-1 lists details of the MOS violation SNMP trap. Some information that is exclusive to a sensor or to a cluster is included only when the trap pertains to a sensor or a cluster as shown throughout Table D-1.

Table D-1 MOS Violation SNMP Trap Details

TAG	Description	Value
Information Included for Sensor and Cluster		
TT	Trap type	1: Data from sensor 3: Data from Cisco Unified Communications Manager (Unified Communications Manager) cluster
01	When TT = 1, one of these: • MAC address (Cisco 1040) • IP address (NAM). When TT = 3, Unified Communications Manager cluster ID.	Text string.
A	Flag indicating actual or sampled data	0: Actual 1: Sampled (not used)
B	Source device IP address. The source device can be: • A Cisco Unified IP Phone or a voice gateway (when TT = 1 and TT = 3). • A remote Unified Communications Manager (when TT = 3 and the call is an intercluster call).	IPv4 address, for example: `172.20.4.18`

Table D-1 MOS Violation SNMP Trap Details (continued)

TAG	Description	Value
C	Recipient device IP address. The recipient device can be: • A Cisco Unified IP Phone or a voice gateway (when TT = 1 and TT = 3). • A remote Unified Communications Manager (when TT = 3 and the call is an intercluster call).	IPv4 address, for example: `172.20.5.12`
D	Codec of call data record (see also CDC in this table).	One of these: 2: G711Alaw 64k 3: G711Alaw 56k 4: G711Ulaw 64k 5: G711Ulaw 56k 6: G722 64k 7: G722 56k 8: G722 48k 9: G723.1 10: G728 11: G729 12: G729AnnexA 15: G729AnnexB 16: G729AnnexAwAnnexB 18: GSM Full Rate 19: GSM Half Rate 20: GSM Enhanced Full Rate 40: G.722.1 32k 41: G.722.1 24k 42: AAC 80: GSM 82: G726_32K 83: G726_24K 84: G726_16K 89: iSAC (used when TT = 3 only)
E	MOS score calculated by the sensor (when TT = 1) or CVTQ (when TT = 3).	Sample value: 3.4
F	Primary cause of call degradation.	When TT = 1: • J: Jitter • P: Packet Loss When TT = 3, N/A

Table D-1 MOS Violation SNMP Trap Details (continued)

TAG	Description	Value
G	Actual packet loss in the previous minute.	Sample value: 0.0.
H	Actual jitter in milliseconds in the previous minute.	Sample value: 0 Value is NA when TT = 3
CDC	Codec of call data record.	One of these: • G711Alaw64k • G711Alaw56k • G711Ulaw64k • G711Ulaw56k • G722 64k • G722 56k • G722 48k • G723.1 • G728 • G729 • G729AnnexA • G729AnnexB • G729AnnexAwAnnexB • GSM • GSM Full Rate • GSM Half Rate • GSM Enhanced Full Rate • G.722.1 32k • G.722.1 24k • AAC • G726_32K • G726_24K • G726_16K • iSAC (used when TT = 3 only)
Information Included for Cluster Only		
CCR	Cumulative Concealment Ratio—Cumulative ratio of concealment time over speech time observed after starting a call.	Sample value: 0.0
ICR	Interval Concealment Ratio—Interval-based average concealment rate; the ratio of concealment time over speech time for the last three seconds of active speech.	Sample value: 0.0
ICRmx	Interval Concealment Ratio Max—Maximum concealment ratio observed during the call.	Sample value: 0.0

Table D-1 MOS Violation SNMP Trap Details (continued)

TAG	Description	Value
CustomerName	The customer name. Valid only if the installation is in MSP Network Deployment mode.	Sample value: *Cust-C*
Information Included for Sensor and Cluster		
CS	Concealment Seconds—Number of seconds within the report period that contain at least one concealment event. **Note** Cisco 1040 does not report concealed seconds.	Sample value: 2
SCS	Severely Concealed Seconds WhenTT = 1, number of seconds during which the percent packet loss (including jitter buffer discards) is greater than the SCS threshold. The threshold is fixed at 5%. **Note** Cisco 1040 does not report severely concealed seconds. When TT = 3, number of seconds during which a significant amount of concealment is observed.	Sample value: 1
Information Included for Cluster Only		
MLQK	MOS Listening Quality or CVTQ Score—The Cisco Voice Transmission Quality (CVTQ) algorithm provides an objective estimate of the mean opinion score (MOS) for listening quality (LQK), rating it from 5 (excellent) to 1 (bad). This score is based on audible concealment events due to frame loss in the preceding 8-second interval of the voice stream. **Note** The CVTQ score can vary based on the codec that the Cisco Unified IP Phone uses.	Sample value: 4.5
MLQKmn	MOS Listening Quality CVTQ Min—Minimum score observed since the beginning of a call; represents the worst-sounding eight-second interval.	Sample value: 4.1
MLQKmx	MOS Listening Quality CVTQ Max—Maximum score observed since the beginning of a call; represents the best sounding eight-second interval.	Sample value: 4.5
MLQKvr	Version of the CVTQ calculation.	Sample value: .95
DRTN	Duration of the call, in seconds.	Sample value: 120
Information Included for Sensor and Cluster		
NST	Number of suppressed traps from start time to end time when TT = 1. For more information, see the entry for Send traps every *n* minutes in Setting Up the Cisco 1040 Sensor Default Configuration, page 4-3.	Sample value: 9 Value is 0 when TT = 3
ST	Start time. When TT = 1, time when the first trap was sent out for the endpoint. When TT = 3, 10 minutes before the call disconnect time; used by Operations Manager to launch reports.	UTC time

Table D-1 MOS Violation SNMP Trap Details (continued)

TAG	Description	Value
ET	End time. When TT = 1, time when the most recent trap was sent out. When TT= 3, call disconnect time; used by Operations Manager to launch reports.	UTC time
Information Included for Sensor Only		
I	Percent network packet loss. Number of packets lost/total packets expected.	Sample value: 2.4
J	Adjusted packet loss—Percentage packet loss due to high jitter. This value is computed based on a reference jitter buffer with a fixed length delay. This value is not affected by network loss.	Sample value: 3.5
K	Integer representing the number of milliseconds between the first and last packet that is analyzed. This value will be 60000 for calls spanning a reporting interval. The value will most likely be less than 60000 for the initial and final streams.	Sample value: 60000
N	TOS/DSCP value.	Sample value: 3
O	Minimum MOS (3-second interval). The minimum MOS score for a given 3-second interval within the current report interval.	Sample value: 35 (for 3.5)
P	SSRC.	Sample value: 23435214
Q	Source UDP Port.	Sample value:13565
R	Destination UDP Port.	Sample value: 24245
S	Maximum single packet reception deviation, in milliseconds.	Sample value: 32
T	Protocol.	0: Skinny call control protocol—Used by Cisco 1040 1: Http—Used by NAM 2: Https—Used by NAM
U	HTTP or HTTPS port used by NAM.	Sample value: 443

Service Monitor generates a Sensor Unreachable trap when either of the following occurs:

- A Cisco 1040 that is registered to the Service Monitor no longer sends keepalives.
- A NAM is unreachable when Service Monitor tries to obtain data from it.

Note If you configure Operations Manager to receive traps from Service Monitor, the Sensor Unreachable trap is displayed on the Alerts and Events monitoring dashboard under the unidentified trap device type.

Table D-2 lists details of the Sensor Unreachable SNMP trap.

Table D-2 Sensor Unreachable SNMP Trap

TAG	Description	Value
TT	Trap type	2
01	ID	One of these: • MAC address—Indicates trap is for a Cisco 1040 sensor • IP address—Indicates trap is for a NAM
02	Time stamp	<YYYYMMDDhhmm>

When a sensor that has been unreachable becomes reachable, Service Monitor sends a Sensor Reconnect SNMP trap.

Note If you configure Operations Manager to receive traps from Service Monitor, the Sensor Reconnect trap is displayed on the Alerts and Events monitoring dashboard under the unidentified trap device type.

Table D-3 lists details of the Sensor Reconnect SNMP trap.

Table D-3 Sensor Reconnect SNMP Trap

TAG	Description	Value
TT	Trap type	4
01	ID	One of these: • MAC address—Indicates trap for a Cisco 1040 sensor • IP address—Indicates trap for a NAM
02	Time stamp	<YYYYMMDDhhmm>