



Enabling Live Communications at the Edge of IP Networks

Reference Manual

MIB Structure

H.323/MGCP/NCS/SIP Version

MIB Version 1.5r3.109

Document Revision 01

August 31, 2011

Media5 Corporation
4229 Garlock Street
Sherbrooke, Québec, Canada J1L 2C8

MIB Structure Reference Manual

© 2011, Media5 Corporation

All rights reserved. No part of this publication may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the express written permission of the publisher.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.

Trademarks

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated.

All other trademarks and registered trademarks are the property of their respective owners.

Third-Party Software Copyright Information

The MIB Structure firmware aggregates some third-party software modules (open source and commercial) that are distributed to you in accordance with their respective licenses. Refer to the *Third Party Software Copyright Information* addendum available on the Mediatrix Download Portal, which lists the third-party software modules along with any copyright and license information.

Contents

Preface

MIB Structure and SNMP	xix
Simple Network Management Protocol (SNMP).....	xix
Definitions.....	xix
SNMP Messages.....	xx
SNMP Behaviour.....	xxi
SNMPv3 Special Behaviour	xxii
MIB Structure.....	xxiii
Textual Conventions.....	xxiv
Objects, Conformance, and Events.....	xxv
IP Addresses	xxv
IP Addresses Formats.....	xxv
Persistence.....	xxvi
Changing a Parameter Value	xxvi
Switching Protocols	xxvi
Working with Tables	xxvii
Generic Variables	xxvii
Variables for Administrative Commands	xxviii
Manual Conventions	xxix

Administration MIBs

Chapter 1

Administration Parameters – sysAdmin MIB.....	3
sysAdminMIBObjects.....	3

Chapter 2

Administration Parameters – groupAdmin MIB	5
Introduction	5
groupAdminMIBObjects	7

Chapter 3

Administration Parameters – IfAdmin MIB	9
Introduction	9
ifAdminMIBObjects	11

Management MIBs

Chapter 4

Management Parameters – ipAddressStatus	15
ipAddressStatusLocalHost	15
ipAddressStatusImage	16
ipAddressStatusMs	16
ipAddressStatusSyslog	17
ipAddressStatusMgcpCallAgent	17
ipAddressStatusNcsCallAgent	17
ipAddressStatusSipServer	18
ipAddressStatusSntp	19
ipAddressStatusConfigFileFetching	19
ipAddressStatusTelephonyDns	19
ipAddressStatusStun	20
stunTable	20

Chapter 5

Management Parameters – sysMgmt MIB.....	21
sysMgmtMIBObjects	21

Chapter 6

Management Parameters – rtp MIB	23
rtpMIBObjects	23
rtpStats	23
rtpConfig	25

Configuration MIBs

Chapter 7

Configuration Parameters – ipAddressConfig	29
ipAddressConfigLocalHost	29
ipAddressConfigLocalHostStatic	30
ipAddressConfigImage	31
ipAddressConfigImageStatic	31
ipAddressConfigImageDhcp	31
ipAddressConfigFileFetching	32
ipAddressConfigFileFetchingStatic	32
ipAddressConfigFileFetchingDhcp	32
ipAddressConfigMs	33
ipAddressConfigMsStatic	33
ipAddressConfigMsDhcp	33
ipAddressConfigSyslog	34
ipAddressConfigSyslogStatic	34
ipAddressConfigSyslogDhcp	34

ipAddressConfigMgcpCallAgent	35
ipAddressConfigMgcpCAStatic	35
ipAddressConfigMgcpCADhcp	35
ipAddressConfigNcsCallAgent	36
ipAddressConfigNcsCAStatic	36
ipAddressConfigNcsCADhcp	36
ipAddressConfigSipServer	37
ipAddressConfigSipServerStatic	37
ipAddressConfigSipServerDhcp	38
ipAddressConfigSntp	38
ipAddressConfigSntpStatic	38
ipAddressConfigH323	39
ipAddressConfigH323Static	39
ipAddressConfigH323Dhcp	40
ipAddressConfigLanInterface	40
ipAddressConfigHttpServer	41
ipAddressConfigTelephonyDns	41
ipAddressConfigTelephonyDnsStatic	41
ipAddressConfigStun	42
ipAddressConfigStunStatic	42

Chapter 8

Configuration Parameters – sysConfig MIB 43

sysConfigMIBObjects	43
sysConfigStats	45
sysConfigDownloadConfig	45

Chapter 9

Configuration Parameters – image MIB 47

imageMIBObjects	47
imageTransfer	47
imageAutomaticUpdate	48
imageStatus	49
imageEvents	49
image Notifications Control	49
image Notifications	49
image Notifications Params.....	49

Chapter 10

Configuration Parameters – ms MIB 51

msMIBObjects	51
msEvents	51
ms Notifications	51

Chapter 11

Configuration Parameters – Syslog MIB..... 53

syslogMIBObjects	53
syslogLocalMsgTable	53

syslogMsgCustomization.....	54
-----------------------------	----

Chapter 12

Configuration Parameters – qos MIB 55

qosMIBObjects	55
qosDiffServ	55
qosleee8021q.....	55

Chapter 13

Configuration Parameters – Telephony MIB..... 59

telephonyMIBObjects.....	59
countryCustomizationToneGroup.....	61

Chapter 14

Configuration Parameters – voicelf MIB 63

voicelfMIBObjects	63
voicelfTable	63
voicelfCodecTable.....	66
voicelfDtmfTransportTable	69
voicelfDtmfDetectionTable	70

Chapter 15

Configuration Parameters – dataIf MIB 73

dataIfMIBObjects	73
dataIfTable	74
dataIfCodecTable	74

Chapter 16

Configuration Parameters – fxs MIB 77

fxsMIBObjects.....	77
fxsEpSpecificLoopCurrentTable	79
fxsEmergencyBypass.....	79

Chapter 17

Configuration Parameters – Digit Maps MIB 81

digitMapMIBObjects.....	81
digitMapAllowedTable	81
digitMapRefusedTable	83
digitMapTimeouts	83

Chapter 18

Configuration Parameters – Telephony Attributes MIB	85
telephonyAttributesMIBObjects	85
telephonyAttributesIfFeaturesTable	85
telephonyAttributesIpAddressCallCustomization	87

Chapter 19

Configuration Parameters – Emergency Call MIB	89
emergencyCallMIBObjects	89
emergencyCallUrgentGatewayCustomization	89

Chapter 20

Configuration Parameters – Subscriber Services MIB	91
subscriberServicesMIBObjects	91
subscriberServicesIfEnablingTable	91
subscriberServicesIfStatusTable	93
subscriberServicesIfCallForwardActivationTable	93
subscriberServicesActivationDigitmaps	94
subscriberServicesProcessing	95

Chapter 21

Configuration Parameters – SNTP MIB	97
sntpMIBObjects	97
sntpTimeZoneConfig	98

Chapter 22

Configuration Parameters – Line Grouping MIB	99
lineGroupingMIBObjects	99
lineGroupingIfAssociationTable	99
lineGroupingGroupConfigTable	100

Chapter 23

Configuration Parameters – Line Selection MIB	101
lineSelectionMIBObjects	101
lineSelectionIfCustomizationTable	101

Chapter 24

Configuration Parameters – Analog SCN Gateway MIB	103
analogScnGwMIBObjects	103
analogScnGwIfDialingTable	103

Chapter 25

Configuration Parameters – FXO MIB	105
fxoMIBObjects	105
fxoLinePropertiesCustomization.....	105
fxoLineFaultDetection.....	106
fxoIfLineStatusTable.....	106
fxoIfAnsweringDelayTable.....	106
fxoForcedEndOfCallCustomization	107
fxoIfAnalogLineTypeTable.....	108
fxoIfIncomingCallNotAllowedBehaviorTable	108

Chapter 26

Configuration Parameters – Message Waiting Indicator MIB	109
mwiMIBObjects	109
mwIfConfigurationTable.....	109

Chapter 27

Configuration Parameters – PPPoE MIB.....	111
pppoeMIBObjects	111

Chapter 28

Configuration Parameters – IP Routing MIB.....	113
ipRoutingMIBObjects	113
ipRoutingDhcp	114
ipRoutingQos.....	115
ipRoutingMacSpoof	116
ipRoutingBandwidthControl	116
ipRoutingStatus	116

Chapter 29

Configuration Parameters – HTTP Server MIB	117
httpServerMIBObjects.....	117
httpServerMIBCustomisation.....	118

Chapter 30

Configuration Parameters – Configuration File Fetching MIB.....	119
configFileFetchingMIBObjects	119
configFileTransfer.....	119
configFileAutomaticUpdate	120
configFilePrivacy	121

Chapter 31

Configuration Parameters – SNMP Agent MIB	123
snmpAgentMIBObjects	123

Chapter 32

Configuration Parameters – Boot Behavior MIB	125
bootBehaviorMIBObjects	125

Chapter 33

Configuration Parameters – PIN Dialing MIB.....	127
pinDialingMIBObjects	127
pinDialingIfTable.....	127

Chapter 34

Configuration Parameters – STUN MIB.....	129
stunMIBObjects	129

Chapter 35

Configuration Parameters – ATM MIB.....	131
atmMIBObjects	131
atmStatus	131
oamTools.....	133

Chapter 36

Configuration Parameters – DSL MIB	135
dslMIBObjects.....	135
dslStatus.....	135

Chapter 37

Configuration Parameters – PPPoA MIB.....	137
pppoaMIBObjects	137

Chapter 38

Configuration Parameters – Security Certificates MIB.....	139
securityCertificatesMIBObjects	139
certificateTable	139

Chapter 39

Configuration Parameters – Interop MIB	141
mxInteropMIBObjects	141

Chapter 40

Configuration Parameters – NAT MIB	143
natMIBObjects	143
natPortForwarding	143
natSyslog	144

Chapter 41

Configuration Parameters – Firewall MIB	145
firewallMIBObjects	145
firewallSecurity	145
firewallSyslog	147

IP Telephony Signalling H.323 MIBs

Chapter 42

H.323 Protocol Parameters – Registration MIB	151
h323RegistrationMIBObjects	151
h323RegistrationSingleRegistration	152
h323RegistrationMultipleRegistrationIfTable	154
h323RegistrationMultipleRegistrationGroupTable	157
h323RegistrationStatusIfTable	160

Chapter 43

H.323 Protocol Parameters – Attributes MIB	161
h323AttributesMIBObjects	161
h323AttributesQ931	161
h323IfSignalingAttributesTable	163
h323IfTelephonyAttributesTable	166

Chapter 44

H.323 Protocol Parameters – Aliases MIB	167
h323AliasesMIBObjects	167
h323AliasesIfAliasesTable	167
h323AliasesGroupAliasesTable	168

Chapter 45

H.323 Protocol Parameters – Experimental MIB	169
h323ExperimentalMIBObjects	169
h323Interop	169

IP Telephony Signalling MGCP MIBs

Chapter 46

MGCP Protocol Parameters – MGCP MIB	173
mgcpMIBObjects	173
mgcpEndpointId	174
mgcpRetransmission	174
mgcpDtmfPackage	175
mgcpGenericMediaPackage	175
mgcpLinePackage	175
mgcpStats	176
mgcpFirewall	177

Chapter 47

MGCP Protocol Parameters – FXS Meter Pulse MIB.....	179
fxsMeterPulseMIBObjects	179
fxsMeterPulseTable	179

Chapter 48

MGCP/NCS Protocol Parameters – Experimental MIB.....	181
mgcpncsExperimentalMIBObjects	181
mgcpncsInterop	181

IP Telephony Signalling NCS MIBs

Chapter 49

NCS Protocol Parameters – NCS MIB	187
ncsMIBObjects	187
ncsEndpointId	187
ncsRetransmission	188
ncsLinePackage	189
ncsStats	189

Chapter 50

NCS Protocol Parameters – NCS Compatibility MIB.....	191
ncsCompatibilityMIBObjects	191

IP Telephony Signalling SIP MIBs

Chapter 51

SIP Protocol Parameters – SIP MIB	195
sipMIBObjects	195
sipUAIfTable	195
sipUAIfAuthenticationTable	197
sipUnitAuthenticationTable	197
sipRegistration	198
sipTransport	198
sipPenaltyBox	199
sipGrouping	200
sipPublication	201
sipConference	202
sipTrustedSources	202

Chapter 52

SIP Protocol Parameters – Experimental MIB	203
sipExperimentalMIBObjects	203
sipNatCustom	205

Chapter 53

SIP Protocol Parameters – Interop MIB.....	207
sipInteropMIBObjects	207
sipInteropDtmfTransportBySipProtocol	215
sipInteropInternationalCodeMapping	216

Appendices

Appendix A

List of MIB Parameters	219
-------------------------------------	------------

List of Tables

Table 1	— SNMPv1 Message Types	xx
Table 2	— SNMPv2 Message Type	xx
Table 3	— Structure of Management Information	xxiii
Table 4	— Textual Conventions	xxiv
Table 5	— MIB Data Types	xxv
Table 6	— IP Addresses.....	xxv
Table 7	— IP Addresses Formats	xxv
Table 8	— Storage Clauses	xxvi
Table 9	— Protocols Supported	xxvi
Table 10	— ifTable Example	xxvii
Table 11	— groupAdmin Parameters	xxviii
Table 12	— ifAdmin Parameters	xxviii
Table 13	— MIB Parameters Example	xxix
Table 14	— System Administration Parameters.....	3
Table 15	— Factors Affecting Management State of Object	5
Table 16	— groupAdmin Parameters	7
Table 17	— Factors Affecting Management State of Objects	9
Table 18	— ifAdmin Parameters	11
Table 19	— IP Address Status Parameters – Local Host.....	15
Table 20	— IP Address Status Parameters – Image.....	16
Table 21	— IP Address Status Parameters – Management Server	16
Table 22	— IP Address Status Parameters – Syslog.....	17
Table 23	— IP Address Status Parameters – Call Agent.....	17
Table 24	— IP Address Status Parameters – Call Agent.....	17
Table 25	— IP Address Status Parameters – SIP Server	18
Table 26	— IP Address Status Parameters – SNTP	19
Table 27	— IP Address Status Parameters – Configuration File Fetching.....	19
Table 28	— IP Address Status Parameters – Image.....	19
Table 29	— IP Address Status Parameters – STUN.....	20
Table 30	— System Management Parameters	21
Table 31	— RTP Statistics – Last Connection	23
Table 32	— RTP Statistics – Current	24
Table 33	— RTP Statistics – Cumulated	24
Table 34	— RTP Configuration	25
Table 35	— IP Address Configuration – Local Host.....	29
Table 36	— IP Address Configuration – Local Host Static	30
Table 37	— IP Address Configuration – Image	31
Table 38	— IP Address Configuration – Image Static	31
Table 39	— IP Address Configuration – Image DHCP.....	31
Table 40	— IP Address Configuration – Configuration File Fetching	32
Table 41	— IP Address Configuration – Configuration File Fetching Static	32
Table 42	— IP Address Configuration – Configuration File Fetching DHCP	32
Table 43	— IP Address Configuration – Management Server	33
Table 44	— IP Address Configuration – Management Server Static	33
Table 45	— IP Address Configuration – Management Server DHCP	33
Table 46	— IP Address Configuration – Syslog	34
Table 47	— IP Address Configuration – Syslog Static	34
Table 48	— IP Address Configuration – Syslog DHCP	34
Table 49	— IP Address Configuration – MGCP Call Agent.....	35
Table 50	— IP Address Configuration – MGCP Call Agent Static.....	35
Table 51	— IP Address Configuration – MGCP Call Agent DHCP	35

Table 52	— IP Address Configuration – NCS Call Agent.....	36
Table 53	— IP Address Configuration – NCS Call Agent Static.....	36
Table 54	— IP Address Configuration – NCS Call Agent DHCP.....	36
Table 55	— IP Address Configuration – SIP Servers.....	37
Table 56	— IP Address Configuration – SIP Servers Static.....	37
Table 57	— IP Address Configuration – SIP Servers DHCP.....	38
Table 58	— IP Address Configuration – SNTP.....	38
Table 59	— IP Address Configuration – SNTP Static.....	38
Table 60	— IP Address Configuration – H.323 Configuration Source.....	39
Table 61	— IP Address Configuration – H.323 Registration, Gatekeeper Addresses.....	39
Table 62	— IP Address Configuration – H.323 Registration, DHCP.....	40
Table 63	— IP Address Configuration – LAN Interface Static Information.....	40
Table 64	— IP Address Configuration – HTTP Server.....	41
Table 65	— IP Address Configuration – Telephony DNS.....	41
Table 66	— IP Address Configuration – Static Telephony DNS.....	41
Table 67	— System Configuration Parameters.....	43
Table 68	— System Configuration – Statistics.....	45
Table 69	— System Configuration – Download.....	45
Table 70	— Image Parameters.....	47
Table 71	— Image Parameters – Transfer.....	47
Table 72	— Image Parameters – Automatic Update.....	48
Table 73	— Image Parameters – Status.....	49
Table 74	— Image Events – Notifications Control.....	49
Table 75	— Image Events – Notifications.....	49
Table 76	— Image Events – Notifications Parameters.....	49
Table 77	— Management Server Parameters.....	51
Table 78	— Management Server Events – Notifications.....	51
Table 79	— Syslog Parameter.....	53
Table 80	— Syslog Parameter – Local Message Table.....	53
Table 81	— Syslog Parameter – Message Customization.....	54
Table 82	— QoS Parameters – DiffServ.....	55
Table 83	— QoS Parameters – IEEE 802.1q.....	55
Table 84	— QoS Parameters – IEEE 802.1q (VLAN).....	57
Table 85	— QoS Parameters – IEEE 802.1q (VLAN) Substitution.....	57
Table 86	— QoS Parameters – Interop.....	58
Table 87	— Telephony Parameters.....	59
Table 88	— Customization Tone Parameters.....	61
Table 89	— Voice Interface Parameters.....	63
Table 90	— Voice Interface – voicelfTable.....	63
Table 91	— Voice Interface – voicelfCodecTable.....	66
Table 92	— Voice Interface – voicelfDtmfTransportTable.....	69
Table 93	— Voice Interface – voicelfDtmfDetectionTable.....	70
Table 94	— T.38 Base Port Parameter.....	73
Table 95	— Data Interface Parameters.....	74
Table 96	— Data Interface Parameters.....	74
Table 97	— FXS Parameters.....	77
Table 98	— Specific Loop Current Parameters.....	79
Table 99	— FXS Parameters.....	79
Table 100	— Digit Maps Parameters.....	81
Table 101	— Allowed Digit Maps Parameters.....	81
Table 102	— Refused Digit Maps Parameters.....	83
Table 103	— Digit Maps Timeouts Parameters.....	83
Table 104	— Telephony Attributes Parameters.....	85
Table 105	— Telephony Attributes – IP Address Call.....	87
Table 106	— Emergency Call – Urgent Gateway.....	89

Table 107	— Subscriber Services – Activation Parameters	91
Table 108	— Subscriber Services – Status Parameters	93
Table 109	— Subscriber Services – Call Forward Activation	93
Table 110	— Subscriber Services – Call Forward Digit Maps	94
Table 111	— Subscriber Services – Processing	95
Table 112	— SNTP Parameters	97
Table 113	— SNTP Parameters – Time Zone	98
Table 114	— Line Grouping – Number of Group	99
Table 115	— Line Grouping – Association	99
Table 116	— Line Grouping – Attributes	100
Table 117	— Line Selection – Parameters	101
Table 118	— Analog SCN Gateway Parameters – Dialing	103
Table 119	— FXO Parameters – Line Properties	105
Table 120	— FXO Parameters – Line Fault Detection	106
Table 121	— FXO Parameters – Line Status	106
Table 122	— FXO Parameters – Answering Delay	106
Table 123	— FXO Parameters – Forced End of Call	107
Table 124	— FXO Parameters – End of Call Custom Tone	107
Table 125	— FXO Parameters – Analog Line Type	108
Table 126	— FXO Parameters – Incoming Call	108
Table 127	— MWI Parameters – General	109
Table 128	— MWI Parameters – Configuration	109
Table 129	— PPPoE Parameters – General	111
Table 130	— IP Routing Parameters – General	113
Table 131	— IP Routing Parameters – DHCP	114
Table 132	— IP Routing Parameters – QoS	115
Table 133	— IP Routing Parameters – MAC Address Spoofing	116
Table 134	— IP Routing Parameters – Bandwidth Control	116
Table 135	— IP Routing Parameter – Status	116
Table 136	— Web-Based Service Parameters	117
Table 137	— Web-Based Service Parameters – Customizing	118
Table 138	— Configuration File Fetching Parameters	119
Table 139	— Configuration File Fetching Parameters – Transfer	119
Table 140	— Configuration File Fetching Parameters – Automatic Update	120
Table 141	— Configuration File Fetching Parameters – Automatic Update	121
Table 142	— MWI Parameters – General	123
Table 143	— Boot Behavior Parameters – General	125
Table 144	— PIN Dialing Parameters – General	127
Table 145	— STUN Parameters – General	129
Table 146	— ATM Parameters – VC Table	131
Table 147	— ATM Parameters – AAL5 Statistics	132
Table 148	— ATM Parameters – OAM Statistics	133
Table 149	— ATM Parameters – OAM Tools	133
Table 150	— ATM Parameters – OAM Tools Parameters	133
Table 151	— DSL Parameters – General Parameters	135
Table 152	— DSL Parameters – DSL Modem Statistics	136
Table 153	— DSL Parameters – Interleaved Path Statistics	136
Table 154	— DSL Parameters – Fast Path Statistics	136
Table 155	— PPPoA Parameters – General	137
Table 156	— Security Certificates Parameters	139
Table 157	— Interop Parameters	141
Table 158	— NAT Parameters – General	143
Table 159	— NAT Parameters – Syslog	144
Table 160	— Firewall Parameters – General	145
Table 161	— Firewall Parameters – Security	145

Table 162	— Firewall Parameters – Security Spoof.....	147
Table 163	— Firewall Parameters – Security Spoof Table.....	147
Table 164	— Firewall Parameters – Syslog	147
Table 165	— H.323 Parameters – Registration Method.....	151
Table 166	— H.323 Parameters – Single Registration.....	152
Table 167	— H.323 Parameters – Multiple Registration	154
Table 168	— H.323 Parameters – Group Registration.....	157
Table 169	— H.323 Parameters – Registration Status	160
Table 170	— H.323 Parameters – Q.931 Attributes	161
Table 171	— H.323 Parameters – Q.931 Called Party Number.....	162
Table 172	— H.323 Parameters – Signaling Attributes.....	163
Table 173	— H.323 Parameters – Telephony Attributes.....	166
Table 174	— H.323 Parameters – Aliases	167
Table 175	— H.323 Parameters – Group Aliases	168
Table 176	— H.323 Parameters – Interop.....	169
Table 177	— H.323 Parameters – Interop, G.729.....	170
Table 178	— MGCP Parameters.....	173
Table 179	— MGCP Parameters – Endpoint	174
Table 180	— MGCP Parameters – Retransmission	174
Table 181	— MGCP Parameters – DTMF Package.....	175
Table 182	— MGCP Parameters – Generic Media Package	175
Table 183	— MGCP Parameters – Line Package.....	175
Table 184	— MGCP Parameters – Statistics	176
Table 185	— MGCP Parameters – Current Statistics	176
Table 186	— MGCP Parameters – Cumulated Statistics.....	176
Table 187	— MGCP Parameters – Firewall Keep-Alive.....	177
Table 188	— FXS Meter Pulse Frequency Parameter.....	179
Table 189	— FXS Meter Pulse Duration Parameters.....	179
Table 190	— MGCP/NCS Experimental Parameters	181
Table 191	— NCS Parameters.....	187
Table 192	— NCS Parameters – Endpoint.....	187
Table 193	— NCS Parameters – Retransmission	188
Table 194	— NCS Parameters – Line Package	189
Table 195	— NCS Parameters – Statistics	189
Table 196	— NCS Parameters – Current Statistics	189
Table 197	— NCS Parameters – Cumulated Statistics	189
Table 198	— NCS Compatibility Parameters	191
Table 199	— SIP Parameters – Basic.....	195
Table 200	— SIP Parameters – SIP User Agents	195
Table 201	— SIP Parameters – User Agent Authentication.....	197
Table 202	— SIP Parameters – Unit Authentication	197
Table 203	— SIP Parameters – Registration	198
Table 204	— SIP Parameters – Transport	198
Table 205	— SIP Parameters – Transport Configuration.....	199
Table 206	— SIP Parameters – Penalty Box	199
Table 207	— SIP Parameters – User Agent Group.....	200
Table 208	— SIP Parameters – Authentication per Group.....	201
Table 209	— SIP Parameters – Publication	201
Table 210	— SIP Parameters – Conference	202
Table 211	— SIP Parameters – Trusted Sources	202
Table 212	— SIP Parameters – Trusted Sources Table	202
Table 213	— SIP Parameters – Experimental.....	203
Table 214	— SIP Parameters – SIP NAT.....	205
Table 215	— SIP Interop Parameters	207
Table 216	— SIP Interop Parameters – DTMF Transport.....	215

Table 217 — SIP Interop Parameters – International Code Mapping216



MIB Structure and SNMP

This document describes the Media5 Management Information Base (MIB) structure. A description and possible values of all parameters are provided to help you make the required changes to your system. Please read the comments very carefully before changing a parameter's value.

Simple Network Management Protocol (SNMP)

Mediatrix units use the Simple Network Management Protocol (SNMP) for initial software configuration provisioning and subsequent software configuration.

SNMP is a simple request-reply protocol for Internet network management services. It consists of *network management stations* (in this document, they are referred to as a management server) communicating with *network elements*. Management stations are normally workstations that display relevant facts about the elements being monitored.

SNMP works over the IP (Internet Protocol) communication stack. SNMP network management consists of three pieces:

- ▶ The protocol between the manager and the element (SNMP). This details the format of the packets exchanged. Although a wide variety of transport protocols could be used, UDP is normally used with SNMP.
- ▶ A set of common structures and an identification scheme used to reference the variables in the MIB. This is called the *Structure of Management Information (SMI)*. See [“Structure of Management Information \(SMI\)” on page xix](#) for more details.
- ▶ A MIB that specifies what variables the network elements maintain (the information that can be queried and set by the manager). See [“MIB Structure” on page xxiii](#) for more details.

Definitions

Structure of Management Information (SMI)

The SMI is the set of rules for specifying the management information that a device maintains. The management information is actually a collection of managed objects, and these rules are used to both name and define these managed objects.

Management Information Base (MIB)

A MIB is a structured collection of all the managed objects a device maintains. The managed objects are structured in the form of a hierarchical tree. At the top of the tree is the most general information available about a network. Each branch of the tree then gets more detailed into a specific network area, with the leaves of the tree as specific as the MIB can get.

Object Identifier (OID)

Object Identifiers (OID) are strings of numbers. They are allocated in a hierarchical manner, so that, for instance, the authority for “1.2.3” is the only one that can say what “1.2.3.4” means. The formal definition of OIDs comes from ITU-T recommendation X.208 (ASN.1), which is available from the ITU.

SNMP Messages

Three (3) versions of SNMP are supported: SNMPv1, SNMPv2c, and SNMPv3. SNMP defines a few types of messages that are exchanged between the manager and agent.

SNMPv1

The following messages are specific to SNMPv1.

Table 1: SNMPv1 Message Types

Operator	Description
messages sent from the manager to the agent	
get-request	Get the value of one or more variables.
get-next-request	Get the next variable after one or more specified variables.
set-request	Set the value of one or more variables.
messages sent from the agent to the manager	
get-response	Return the value of one or more variables. This is the message returned by the agent to the manager in response to the get-request , get-next-request , and set-request operators.
trap	Notify the manager when something happens on the agent.

SNMPv2c

There are a few flavours of SNMPv2, SNMPv2c being the most common. The following message is specific to SNMPv2.

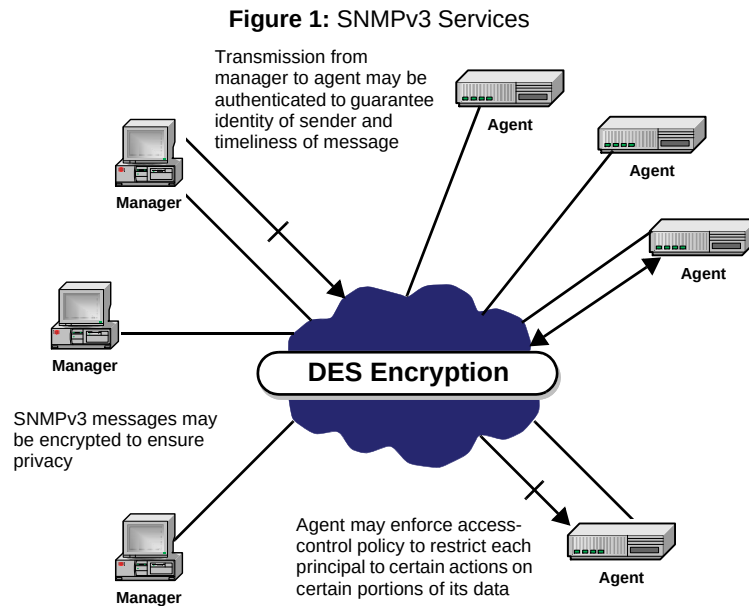
Table 2: SNMPv2 Message Type

Operator	Description
get-bulk	Uses BULK Requests to query for a tree of information about a network entity. A variable put in command line specifies which portion of the object identifier space will be searched using BULK Requests. All variables in the subtree below the given variable are queried as a single request and their values presented to the user.

This message is sent from the manager to the agent.

SNMPv3

To correct the security deficiencies of SNMPv1/v2, SNMPv3 was defined with an overall SNMP architecture and a set of security capabilities. SNMPv3 includes three important services: *authentication*, *privacy*, and *access control* (Figure 1). To deliver these services in a flexible and efficient manner, SNMPv3 introduces the concept of a *principal*, which is the entity on whose behalf services are provided or processing takes place.



Note: Some versions of the Mediatrix 1102 do not support the SNMPv3 feature. Please refer to the *Mediatrix 1102 Administration Manual* to see if your version supports SNMPv3.

SNMP Behaviour

When using SNMP, the following rules apply:

- ▶ Media5 recommends to copy the SNMPv3 user attributes only twice.
- ▶ The administrator may edit the SNMPv3 user attributes:
 - Authentication algorithm (none, MD5, or SHA)
 - Authentication password
 - Encryption algorithm (NULL or DES)
 - Encryption password
 - All SNMPv3 passwords (encryption and authentication) must be at least 8 characters long. You should use the *Unit Manager Network* product to perform SNMPv3 setup. Whatever the MIB browser you use, the unit follows the SNMPv3 standard RFCs.

SNMP can be used in a non-secure or secure management mode.



Warning: The SNMPv3 method for changing the password or encryption key contains a flaw which may result in setting the incorrect password. This problem can happen if you use an incorrect "oldpassword" when changing your password. Always exercise great caution when changing your password or encryption key. Note that depending on the software version running in your unit, it may be possible to use the factory reset to clear the SNMPv3 password.

Non-Secure Management Mode

In non-secure management mode, the unit responds to SNMP requests as follows:

- ▶ SNMPv1: read-write on all MIB tree
- ▶ SNMPv2c: read-write on all MIB tree
- ▶ SNMPv3: read-write on all MIB tree using:
 - MD5 authentication
 - Authentication password: "Md5Password" (initial password)
 - DES encryption
 - Encryption password: "DesPassword" (initial password)
- ▶ SNMPv3: read-write on all MIB tree using:
 - SHA authentication
 - Authentication password: "ShaPassword" (initial password)
 - DES encryption
 - Encryption password: "DesPassword" (initial password)

Secure Management Mode

In secure management mode, the unit responds to SNMP requests as follows:

- ▶ SNMPv1: read-only on all MIB tree
- ▶ SNMPv2c: read-only on all MIB tree
- ▶ SNMPv3: the same values as for SNMPv3 in non-secure management mode



Note: If you forget or lose a password, perform a Factory Reset to reset the unit to the non-secure management mode. See the *Administration Manual* for more details.

Notes

- ▶ When using SNMPv3 with encryption (DES), you may experience delays when accessing MIB variables. This is normal because encrypting an IP packet takes in general longer than sending it over IP. If you experience any timeout, simply add some seconds to the timeout period of your MIB browser, and then try to reach the unit again.
- ▶ Suppose that the Mediatrix unit accepts requests with authentication only. If you perform requests by using encryption and authentication, assuming that the authentication password is valid, the SNMP agent still responds as if the requests were only authenticated.
- ▶ If you clone an SNMPv3 user, and then remove authentication or privacy for it, ensure that a row in *vacmGroupName* matches its new constraints. If not, the unit is not accessible by using the new clone parameters.

SNMPv3 Special Behaviour

Mediatrix units coming out of factory are set so that you can use all MIB variables by using SNMPv1, SNMPv2c, or SNMPv3. However, you can decide to accept only SNMPv3 access by using passwords known by administrators only for enhanced security. In this case, you should manually disable SNMPv1 / SNMPv2 so that SNMPv3 works properly. The Mediatrix unit will thus refuse any SNMPv1 or SNMPv2 request directed to it.

You can disable / enable SNMPv1 / SNMPv2 by using the MIB Browser included in the Media5 Unit Manager Network (or any other MIB Browser) to modify the permissions related to SNMPv1 / SNMPv2 (security model). These permissions are located in the *VacmAccessTable* of the SNMP-VIEW-BASED-ACM-MIB (RFC 2575).

When using exclusively SNMPv3, a row from one of the following tables:

- ▶ *usmUserTable*
- ▶ *vacmSecurityToGroupTable*
- ▶ *vacmAccessTable*

- ▶ `vacmViewTreeFamilyTable`

is saved in flash memory only if these conditions are met:

- ▶ The `RowStatus` variable (e.g., `vacmAccessRowStatus`) is equal to **active(1)**
- ▶ The `StorageType` variable (e.g., `vacmAccessStorage Type`) is equal to **nonVolatile(3)**



Note: The `vacmContextTable` is not saved under any condition.

MIB Structure

The current MIB structure is defined in the SMI file, called *MX-SMI.my*. The SMI contains seven main groups.

Table 3: Structure of Management Information

Group	Description
<code>mediatrixProducts</code>	Each Media5 product has been assigned with its own <code>sysObjectID</code> value.
<code>mediatrixAdmin</code>	Root of the modules used for the administration of the products. See “Administration MIBs” on page 1 for more details.
<code>mediatrixMgmt</code>	Root of the modules used to manage the products. See “Management MIBs” on page 13 for more details.
<code>mediatrixConfig</code>	Root of the modules used to configure the products. See “Configuration MIBs” on page 27 for more details.
<code>mediatrixIpTelephonySignaling</code>	Root of the modules used to configure the signalling protocols. For more details, see: • “IP Telephony Signalling H.323 MIBs” on page 149 • “IP Telephony Signalling MGCP MIBs” on page 171 • “IP Telephony Signalling NCS MIBs” on page 185 • “IP Telephony Signalling SIP MIBs” on page 193
<code>mediatrixModules</code>	Provides a root in which modules can register their module entity. No MIB variables actually appear under this node.
<code>mediatrixExperimental</code>	The experimental sub-tree is the area where objects and events in MIBs under development can be placed without fear of conflicting with other MIBs. When the items rooted under an experimental sub-tree are ready for release, the sub-tree is re-attached under a permanent branch. Please note that Media5 configuration tool – the Unit Manager Network – does not support MIBs that are located under the <i>mediatrixExperimental</i> branch of the MIB structure. The Unit Manager Network does not have specific tasks to manage variables in experimental MIBs. Even though the Unit Manager Network can view experimental MIBs, SNMP operations may not work properly on them.

All parameters in the MIBs have been configured by default upon start up. However, if you need to modify some of these parameters (for example, parameters related to the country in which you are), use a MIB browser.

Textual Conventions

Textual conventions are defined in a module to ensure that all variables throughout the MIB structure use the same syntax and types. The type of each variable is defined in the *Composed syntax* line.

Table 4: Textual Conventions

Type	Definition
MxIpHostName	Represents an IP address or a domain name.
MxIpAddress	Represents an IP address.
MxIpPort	The TCP or UDP port number range. Values can be between 1 and 65535.
MxIpSubnetMask	Represents an Internet subnet mask.
MxIpSelectConfigSource	Indicates the source to use during the next boot sequence for the provisioning of the localHost MIB objects. - static: uses static values provided by the user such as DNS addresses, router etc. - dhcp: uses the DHCP server to retrieve the configuration of the localHost MIB objects.
MxIpConfigSource	Indicates the source used during the last boot sequence for the provisioning of the localHost MIB objects. - static: the user provided static values such as DNS addresses, router etc. - dhcp: the DHCP server was used to retrieve the configuration of the localHost MIB objects. - Default: hardcoded values for recovery mode were used.
MxIpDhcpSiteSpecificCode	Represents a DHCP site specific code. Values can be between 128 and 254 or 0. You can enter this code in your DHCP server to define IP addresses. Refer to the <i>Administration manual</i> for more details.
MxFloatingPoint	Represents a floating point number.
MxAdvancedIpPort	The TCP or UDP port number range. Values can be between 0 and 65535. The port number value 0 is used for special functionality defined in the variable definition.
MxEnableState	Represents an enabled/disabled state (boolean value).
MxActivation State	Represents an active/inactive state (boolean value).
MxSignaling Address	Represents a valid signaling address.
MxDigitMap	A digit map is a sequence used to determine when the dialing of DTMFs is completed. The permitted digit map syntax is taken from the core MGCP specification, RFC2705: ftp://ftp.rfc-editor.org/in-notes/rfc2705.txt, section 3.4. Legend: "x" ==> any digit "," ==> any number of <pre> DigitMap = DigitString / '(' DigitStringList ')' DigitStringList = DigitString 0* (' ' DigitString) DigitString = 1*(DigitStringElement) DigitStringElement = DigitPosition ['.'] DigitPosition = DigitMapLetter / DigitMapRange DigitMapLetter = DIGIT / '#' / '*' / 'A' / 'B' / 'C' / 'D' / 'T' DigitMapRange = 'x' / '[' 1*DigitLetter ']' DigitLetter = *((DIGIT '-' DIGIT) / DigitMapLetter) </pre> For example, the digit map "xx" will match after any two DTMFs that are dialed.

Objects, Conformance, and Events

Each MIB may have three types of data.

Table 5: MIB Data Types

Type	Description
Object	Represents the actual variables that can be set.
Conformance	Describes one or more groups to which the product may conform. This allows to have an exact idea of what a unit supports just by glancing at the conformance information.
Event	An event is sent to tell what type of data will be received, but not the data itself. This is used to “warn” in advance what is coming.

IP Addresses

The MIB structure contains many IP addresses that can be set or viewed. These IP addresses are physically located in their relevant MIB. For instance, the IP addresses for the Syslog Daemon are located in the Syslog MIB. However, when viewing the MIB structure in a MIB browser, the IP addresses are grouped in two distinct groups for easy management:

Table 6: IP Addresses

Action	Description
ipAddressStatus	All IP addresses used by the unit are grouped under the <i>ipAddressStatus</i> category in the <i>mediatrixMgmt</i> MIB. See “ Management Parameters – ipAddressStatus ” on page 15 for more details.
ipAddressConfig	All IP addresses you can set are grouped under the <i>ipAddressConfig</i> category in the <i>mediatrixConfig</i> MIB. See “ Configuration Parameters – ipAddressConfig ” on page 29 for more details.

IP Addresses Formats

You can use a number of formats when defining IP addresses in the DHCP server and MIB variables.

Table 7: IP Addresses Formats

Format	Description	Allowed Char.
Decimal	You can enter IP addresses in the widely-used (base 10) decimal format. For instance, a decimal IP address would be 192.168.0.9. IP addresses cannot contain decimal numbers higher than 255.	0..9
Hexadecimal	You can enter IP addresses in (base 16) hexadecimal format. Prepending “0x” to the value instructs the unit to interpret it as hexadecimal. For instance, the decimal IP address 192.168.0.9 translates to 0xC0.0xA8.0x0.0x9 in hexadecimal format.	0..9, A..F
Octal	You can enter IP addresses in (base 8) octal format. Prepending “0” to the value instructs the unit to interpret it as octal. For instance, the decimal IP address 192.168.0.9 translates to 0300.0250.00.011 in octal format.	0..7

You can make combinations of the three bases in a single string, because each number in the string is interpreted separately. For instance, 0300.0xA8.000.9 translates to the decimal IP address 192.168.0.9.

There may be some confusion between the three available IP address formats. In particular, it is important to understand that prefixing “0” to your values makes them interpreted as octal values. For instance, the string 192.168.0.009 is not valid because 009 is interpreted in octal, and the digit “9” does not exist in that base.

Persistence

A variable may either be persistent or volatile.

Table 8: Storage Clauses

Clause	Definition
Persistent	<i>Persistent</i> parameters are saved into the unit's memory and restored when it restarts. All the variables with the <i>Access = Read Write</i> attribute are persistent, except the variables representing commands (such as <i>sysAdminCommand</i>).
Volatile	<i>Volatile</i> parameters are lost every time the unit restarts. This type of parameter includes toggling parameters such as requesting a configuration file or a software download. <i>Statistics</i> are also volatile parameters that are lost every time the unit reboots.

Changing a Parameter Value

Changing a parameter value involves contacting the unit with any SNMP MIB browser. You can use the MIB browser built in the Media5's Unit Manager Network. Be sure to use the MIB files that match the version of the MIB located inside the current software build of the unit.

Locate the proper parameter to modify and change (SET) its value. Most of the parameters require to reboot the Mediatrix unit. A reboot may be software-initiated or manually initiated by unplugging the unit. It will delete all statistics stored and will overwrite all volatile parameter values in the configuration file. A reboot will also reinitiate the entire unit's initial provisioning sequence.



Note: When performing a SET operation on any MIB variable, Media5 recommends to wait at least 30 seconds before shutting down the unit. This gives time to the software to update configuration data in flash memory.

Switching Protocols

Depending on the Mediatrix units version, they support different protocols.

Table 9: Protocols Supported

Version	Protocols Supported
Version 4.0.x	H.323
Version 4.1.x	MGCP
Version 4.2.x	MGCP and NCS
Version 4.3.x	SIP or MGCP and NCS ^a
Version 4.4.x	SIP or MGCP and NCS ^b
Version 4.5.x	SIP
Version 4.6.x	MGCP
Version 5.0.x	MGCP or SIP

a. You cannot switch from SIP to MGCP/NCS, those are two different products

b. You cannot switch from SIP to MGCP/NCS, those are two different products

For more details, see:

- ▶ ["IP Telephony Signalling H.323 MIBs" on page 149](#)
- ▶ ["IP Telephony Signalling MGCP MIBs" on page 171](#)
- ▶ ["IP Telephony Signalling NCS MIBs" on page 185](#)
- ▶ ["IP Telephony Signalling SIP MIBs" on page 193](#)

If you are using a Mediatrix unit v4.2.x, v4.3.x or 4.4.x that runs the MGCP or NCS signalling protocol, you can switch between protocols and the proper settings are activated upon restart.

- **To switch protocols:**
 - In the *telephonyMIB*, set the *telephonyIpSignaling ProtocolSelection* variable to either **MGCP** or **NCS**.
The default value is **MGCP**. The unit restarts automatically. After the unit restarts, it uses the selected protocol.

Working with Tables

There are two types of tables used in the MIB structure. They contain:

- Generic variables that apply to each line of a unit. This avoids to repeat each set of variables for each line it has.
- The administrative commands and status related to a managed object.

Generic Variables

All tables used to set variables for one or more lines (such as the *voiceIfTable*) are based on the *ifTable*, or interface table.

The *ifTable* lists the interfaces of a unit. In other words, it basically defines the lines that are used by the unit. It contains an *ifIndex*, which defines the interfaces. It may also contain interfaces such as:

- the LoopBack (*lo*) and Ethernet (*eth0*) interfaces.
- the actual voice interfaces (lines) of the unit.

Table 10 gives an example of the *ifTable*.

Table 10: ifTable Example

ifIndex	Type	Description
1	LoopBack	lo
2	Ethernet(0)	eth0
3	Voice FXS	(0)
4	Voice FXS	(1)
5	Voice FXS	(2)
...	...	...
26	Voice FXS	(24)

Figure 2 shows a table built in the Unit Manager Network from the *voiceIfTable* parameters.

Figure 2: voiceIfTable Example

voiceIfAdaptiveJitterBu...	voiceIfTargetJitterBufferL...	voiceIfMaxJitterBufferLen...	voiceIfG711VoiceActivityD...
enable	30	125	conservative
enable	30	125	conservative
enable	30	125	conservative
enable	30	125	conservative

You can perform GET and SET operations on these parameters.

Variables for Administrative Commands

Administrative commands are built on a hierarchical structure of parents-children. A command applied on a parent is propagated to all of its children.

There are two tables used to define administrative commands to groups:

- ▶ *groupAdmin*: A group may be the unit itself (gateway) or other instances. There are no instances other than the gateway defined at this moment.
- ▶ *ifAdmin*: This table applies to each interface of the unit.

groupAdmin Table

The *groupAdmin* table sends administrative commands at the highest instance in a hierarchy (such as the gateway).

Table 11: groupAdmin Parameters

Parameter	Description
groupSetAdmin	Command to set the administrative state of the system.
groupAdminState	The administrative state of the group. Indicates the current maintenance state of a group. Available states are unlocked, shutting down, and locked.
groupOpState	The operational state of the group. It reflects the group's internal state. Available states are enabled and disabled.
groupUsageState	The usage state of the group. Indicates the running state of a group. Available states are idle, active, busy, and idle-unusable.
groupAdminType	The type of resources managed by the group.
groupAdminDescription	The description of the group.
groupAdminParentGroup	The parent's group. This is the index (<i>groupAdminIndex</i>), taken from this table (<i>groupAdminTable</i>), of the group that is the parent. In case there is no parent, the value "-1" is used.

The *groupAdmin* table is further described in ["Chapter 2 - Administration Parameters – groupAdmin MIB"](#) on page 5.

ifAdmin Table

The *ifAdmin* table is similar to the *groupAdmin* table, except that it applies to interfaces.

Table 12: ifAdmin Parameters

Parameter	Description
ifAdminSetAdmin	Command to set the administrative state of the current interface.
ifAdminAdminState	The administrative state of the current interface. It indicates the current maintenance state of a gateway component. Available states are unlocked, shutting down, locked, and permanentLock.
ifAdminOpState	The operational state of the current interface. This state reflects the component's internal state. Available states are enabled and disabled.
ifAdminUsageState	The usage state of the current interface. It indicates the running state of a voice component. Available states are idle, active, busy, and idle-unusable.
ifAdminParentType	The parents type of this interface.
ifAdminParent	The index of the parent of this interface.

The *groupAdmin* table is further described in ["Chapter 3 - Administration Parameters – IfAdmin MIB"](#) on page 9.

Manual Conventions

The MIB parameters are presented in a table such as the following:

Table 13: MIB Parameters Example

Name	Access	Description
voicelfAdaptativeJitterBufferEnable	R/W	Jitter is an abrupt and unwanted variation of one or more signal characteristics, such as the interval between successive pulses, or the frequency or phase of successive cycles. An adaptive jitter buffer usually consists of an elastic buffer in which the signal is temporarily stored and then retransmitted at a rate based on the average rate of the incoming signal. • disable(0) • enable(1) Default Value: enable

The tables contain the following information:

- ▶ **Name:** Full name of the parameter as displayed in the MIB.
- ▶ **Access:** The parameter may have one of four access types:
 - *R/W*: the parameter is "Read/Write" and can be edited.
 - *R-O*: the parameter is "Read-Only" and cannot be edited.
 - *A-N*: the parameter is accessible for Notify.
 - *N/A*: the parameter is not accessible.
- ▶ **Description:** Description of the parameter as displayed in the MIB. When possible, the default value for the parameter is provided.

Administration MIBs

Page Left Intentionally Blank

Administration Parameters – sysAdmin MIB

This MIB provide general system management information.

sysAdminMIBObjects

The System Administration parameters allow you to get an accurate status of the unit.

Table 14: System Administration Parameters

Name	Access	Description
sysAdminCommand	R/W	This variable controls the various commands that can be performed by the unit. - noOp: No action is taken. - checkRam: Launches the RAM check routine. The unit will restart, test the RAM, and start normally afterwards. This command can only be applied while the unit is in maintenance mode (<i>groupAdminState</i> must be 'locked'). If the unit is shutting down (<i>groupAdminState</i> is 'shuttingDown'), the command is delayed until the unit enters maintenance mode. - checkRom: This value's semantics are different depending on the protocol and hardware platform. Please refer to the documentation shipped with your device for more details. - downloadSoftware: Launches a software update. The unit will restart, download the new software version, and restart again running the new software version. This command can only be applied while the unit is in maintenance mode (<i>groupAdminState</i> must be 'locked'). If the unit is shutting down (<i>groupAdminState</i> is 'shuttingDown'), the command is delayed until the unit enters maintenance mode. - resetStats: Resets all cumulated call statistics. - setConfigSourcesStatic: This command will set all configuration sources supported by the unit to 'static'. This command can be used when no DHCP server is present in the network to easily configure the unit to use static values. This value's semantics are different depending on the protocol. Please refer to the documentation shipped with your device for more details. - updateConfiguration: Configuration files are fetched by the unit (see <i>configFileFetchingFileName</i>). The transfer protocol used is defined by <i>configFileTransferProtocol</i>. The unit is the initiator of the transfer sessions. The unit is automatically restarted after reception of the configuration file and the new settings are applied. This command can only be applied while the unit is in maintenance mode (<i>groupAdminState</i> must be 'locked'). If the unit is shutting down (<i>groupAdminState</i> is 'shuttingDown'), the command is delayed until the unit enters maintenance mode. Default Value: noOp(0)
sysAdminDefaultSettingsEnable	R/W	Indicates if the default settings button can trigger the factory reset. The factory reset reverts the configuration of the system to default factory settings. - enable: The default settings button can trigger the factory reset. - disable: The default settings button can not trigger the factory reset. Please refer to the documentation shipped with your device for more details on the factory reset and the default settings button. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: enable

Table 14: System Administration Parameters (Continued)

Name	Access	Description
sysAdminLastCheckRam	R-O	Last RAM check status. - notTested(0), - fail(1), - success(2) Default Value: notTested
sysAdminLastCheckRom	R-O	Last ROM check status. - fail(1), - success(2) Default Value: success
sysAdminLastDownloadSoftware	R-O	Status of the last download software command. - fail(1), - success(2) Default Value: success
sysAdminDownloadConfigFileStatus	R-O	Status of the last configuration file download. - idle - fail - success - inProgress - listening Default Value: idle
sysAdminAppMode	R-O	Application's current operational mode. - normal(0) - recovery(1) Refer to the documentation shipped with your device for a thorough description of the operational modes. Default Value: normal

Administration Parameters – groupAdmin MIB

This MIB defines the administrative command and status related to a managed object. These objects are managed by the combination of three attributes that are termed OSI States attributes.

Introduction

This MIB follows ISO/IEC 10164-2 CCITT Recommendation X.731 with the following interpretations and extensions.

This MIB contains manageable objects containers. The table *groupAdminTable* contains a group of entities that are manageable uniquely (in another admin table) or in group (*groupAdminTable*).

The management state of a managed object represents the instantaneous condition of availability and operability of the associated resource from the management point of view.

Managed objects have a variety of state attributes that express and control aspects of the operation of their associated resource that are peculiar to each. However, the management state is expected to be common to a large number of resources and, for this reason, is standardized; it expresses key aspects of their usability at any given time. There are three primary factors to affect the management state of a managed object. These are:

Table 15: Factors Affecting Management State of Object

Factor	Description
operability	Indicates whether or not the resource is operational.
usage	Indicates whether or not the resource is actively in use at a specific instant, and, if so, whether or not it has spare capacity for additional requests at that instant.
administration	Indicates the current maintenance state of a group. This attribute reflects the result of an operator-initiated maintenance request.

The managed object status is closely related to the status of its children. These status are affected by external events such as administrative commands. The behaviour of the managed object to these events is explained below.

► **Event: receive an administrative lock (graceful) command for a group:**

- 1 = The administrative state of the group (*groupAdminState*) is changed to SHUTTING DOWN.
- 2 = All children are notified to set their usage state to IDLE UNUSABLE gracefully.
- 3 = The children change their usage state to IDLE UNUSABLE as soon as their activities end.
- 4 = When the usage state of all children have been set to IDLE UNUSABLE, the usage state of the group (*groupUsageState*) is changed to IDLE UNUSABLE.
- 5 = The administrative state of the group (*groupAdminState*) is changed to LOCKED.

► **Event: receive an administrative lock command (non graceful) for a group:**

- 1 = All children are notified to set their usage state to IDLE UNUSABLE immediately.
- 2 = The children change their usage state to IDLE UNUSABLE abruptly.

3 = When the usage state of all children have been changed to IDLE UNUSABLE, the usage state of the group (*groupUsageState*) is changed to IDLE UNUSABLE.

4 = The administrative state of the group (*groupAdminState*) is changed to LOCKED.

► **Event: receive an administrative unlock command for a group**

1 = All children are notified to set their usage state to IDLE if:

- the administrative state of the child is UNLOCKED AND
- the administrative state of all its parents are also UNLOCKED AND
- the operational state of the child is ENABLED AND
- the operational state of all its parents are also ENABLED.

2 = The usage state of the group (*groupUsageState*) is set to IDLE if:

- the administrative state of all its parents are also UNLOCKED AND
- the operational state of the group is ENABLED AND
- the operational state of all its parents are also ENABLED.

3 = The administrative state of the group (*groupAdminState*) is set to UNLOCKED.

► **Event: An operational problem is discovered with a group**

1 = All children are notified to set their usage state to IDLE UNUSABLE abruptly.

2 = All children change their usage state to IDLE UNUSABLE abruptly.

3 = When the usage state of all children has been set to IDLE UNUSABLE, the usage state of the group (*groupUsageState*) is changed to IDLE UNUSABLE.

4 = The operational state of the group (*groupOpState*) is changed to DISABLED.

► **Event: An operational problem is resolved in a group**

1 = All children are notified to set their usage state to IDLE if:

- the administrative state of the child is UNLOCKED AND
- the administrative state of all its parents are also UNLOCKED AND
- the operational state of the child is ENABLED AND
- the operational state of all its parents are also ENABLED

2 = The usage state of the group (*groupUsageState*) is changed to IDLE if:

- the administrative state of the group is UNLOCKED AND
- the administrative state of all its parents are also UNLOCKED AND
- the operational state of all its parents are also ENABLED

3 = The operational state of the group (*groupOpState*) is changed to ENABLED.

groupAdminMIBObjects

The parameters are defined in a table called *groupAdminTable*.

Table 16: groupAdmin Parameters

Name	Access	Description
groupAdminIndex	N/A	Index of the group admin table.
groupSetAdmin	R/W	Command to set the administrative state of the system. - noOp: no operation. - Unlock: The <i>groupAdminState</i> variable is set to unlocked. - Lock: If the <i>groupUsageState</i> variable's value is idle-unusable or idle, then the <i>groupAdminState</i> variable is set to locked. If activities are in progress, the <i>groupUsageState</i> variable's value is either busy or active, activities continue until normal completion and the <i>groupAdminState</i> variable is set to shuttingdown. - Forcelock: The <i>groupAdminState</i> variable is set to locked and the <i>groupUsageState</i> variable's value is updated to idle-unusable. All activities that are in progress will be terminated immediately. No new request may be initiated. Default Value: noOp
groupAdminState	R-O	The administrative state of the group. Indicates the current maintenance state of a group. This attribute reflects the result of an operator initiated maintenance request. - Unlocked: no operator initiated maintenance request is affecting the operation of the group. - ShuttingDown: the group is in a transition state between unlocked and locked state. A group will only transition to a locked state once all current activities are completed. No new activity will be accepted once all activities are terminated. - Locked: an operator-initiated request has been issued for this group. This group and all its children are unavailable for normal operation. Default Value: unlocked
groupOpState	R-O	The operational state of the group. It reflect the group's internal state. There are certain conditions that affect the internal state of a group. - Enabled: the group is operationally functional. - Disabled: the group is operationally non-functional due to an internal condition that would not allow it to participate in normal operation. Default Value: disabled
groupUsageState	R-O	The usage state of the group. Indicates the running state of a group. - Idle: the group is not currently active, but is available for use. - Active: the group is currently being used and available for processing and still has additional capacity. - Busy: the group is usable but is not available for any new additional processing requests, since all of its resources (child) are currently being used. - Idle-Unusable: the group is not currently active and not available for use. Default Value: idle-unusable
groupReset	R/W	Command to request a reset on the group. - NoOp: no operation. In case, the reset is not started, it will cancel the operation. - SoftReset: This will perform a software reset on the group under certain conditions: <i>groupAdminState</i> set to Locked: start reset immediately. <i>groupAdminState</i> set to ShuttingDown: wait for the state to be locked then start the reset. <i>groupAdminState</i> set to Unlock: command is discarded. Default Value: noOp
groupAdminType	R-O	The type of resources managed by the group. 1 = Gateway
groupAdminDescription	R-O	The description of the group.

Table 16: groupAdmin Parameters (Continued)

Name	Access	Description
groupAdminParentGroup	R-O	The parent's group. This is the index (<i>groupAdminIndex</i>), taken from this table (<i>groupAdminTable</i>), of the group that is the parent. In case there is no parent, value "-1" is used. Default Value: -1

Administration Parameters – IfAdmin MIB

This MIB defines the administrative command and status related to a managed object. These objects are managed by the combination of three attributes that are termed OSI States attributes.

Introduction

This MIB follows ISO/IEC 10164-2 CCITT Recommendation X.731 with the following interpretations and extensions.

The management state of a managed object represents the instantaneous condition of availability and operability of the associated resource from the management point of view.

Managed objects have a variety of state attributes that express and control aspects of the operation of their associated resource that are peculiar to each. However, the management state is expected to be common to a large number of resources and, for this reason, is standardized; it expresses key aspects of their usability at any given time. We used three primary factors to affect the management state of a managed object. These are:

Table 17: Factors Affecting Management State of Objects

Factor	Description
operability	Indicates whether or not the resource is operational.
usage	Indicates whether or not the resource is actively in use at a specific instant and if so, whether or not it has spare capacity for additional request at that instant.
administration	Indicates the current maintenance state. This attribute reflects the result of an operator initiated maintenance request.

The managed object status is closely related to the status of its children. These status are affected by external events such as administrative command. The behaviour of the managed object to these events is explained below.

► **Event: receive an administrative lock (graceful) command for an interface:**

- 1 = The administrative state of the interface (*groupAdminState*) is changed to SHUTTING DOWN.
- 2 = All children are notified to set their usage state to IDLE UNUSABLE gracefully.
- 3 = The children change their usage state to IDLE UNUSABLE as soon as their activities end.
- 4 = When the usage state of all children have been set to IDLE UNUSABLE, the usage state of the interface (*groupUsageState*) is changed to IDLE UNUSABLE.
- 5 = Its administrative state (*groupAdminState*) is changed to LOCKED.

► **Event: receive an administrative lock command (non graceful) for an interface:**

- 1 = All children are notified to set their usage state to IDLE UNUSABLE immediately.
- 2 = The children change their usage state to IDLE UNUSABLE abruptly.
- 3 = When the usage state of all children have been changed to IDLE UNUSABLE, the usage state of the interface (*groupUsageState*) is changed to IDLE UNUSABLE.
- 4 = Its administrative state (*groupAdminState*) is changed to LOCKED

► **Event: receive an administrative unlock command for an interface**

- 1 = All children are notified to set their usage state to IDLE if:
 - the administrative state of the child is UNLOCKED AND
 - the administrative state of all its parents are also UNLOCKED AND
 - the operational state of the child is ENABLED AND
 - the operational state of all its parents are also ENABLED.
- 2 = The usage state of the interface (*groupUsageState*) to IDLE if:
 - the administrative state of all its parents are also UNLOCKED AND
 - the operational state of the group is ENABLED AND
 - the operational state of all its parents are also ENABLED.
- 3 = The administrative state of the interface (*groupAdminState*) to UNLOCKED.

► **Event: An operational problem is discovered with an interface**

- 1 = All children are notified to set their usage state to IDLE UNUSABLE abruptly.
- 2 = All children change their usage state to IDLE UNUSABLE abruptly.
- 3 = When the usage state of all children have been set to IDLE UNUSABLE, the usage state of the interface (*groupUsageState*) is changed to IDLE UNUSABLE.
- 4 = Its operational state (*groupOpState*) is changed to DISABLED.

► **Event: An operational problem is resolved in an interface**

- 1 = All children are notified to set their usage state to IDLE if:
 - the administrative state of the child is UNLOCKED AND
 - the administrative state of all its parents are also UNLOCKED AND
 - the operational state of the child is ENABLED AND
 - the operational state of all its parents are also ENABLED.
- 2 = The usage state of the interface (*groupUsageState*) is changed to IDLE if:
 - the administrative state of the group is UNLOCKED AND
 - the administrative state of all its parents are also UNLOCKED AND
 - the s operational state of all its parents are also ENABLED.
- 3 = Its operational state (*groupOpState*) is changed to ENABLED.

ifAdminMIBObjects

The parameters are defined in a table called *ifAdminTable*.

Table 18: ifAdmin Parameters

Name	Access	Description
ifAdminSetAdmin	R/W	Command to set the administrative state of the current interface. Represents action on admin status. Lock indicates that component usage states of active or idle are updated with their admin state set to locked. Their usage state is updated to idle. For active calls in progress who's usage state is busy, calls remain established until normal call termination. The admin state is set to shuttingdown. Once the call is terminated the admin state is set to locked and usage state to idle. For forcetlock, admin state is set to locked. Their usage state is updated to idle. All active calls in progress are terminated immediately; there is no transition admin state of shuttingdown. No new calls may be initiated. For unlock, admin state is set to unlocked. The <i>permanentUnlock</i> and <i>permanentForcelock</i> commands are deprecated. Use the <i>ifAdminInitialAdminState</i> variable instead when a permanent setting is desired. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. • noOp(0) • permanentUnlock(1) • lock(2) • forcetlock(3) • permanentForcelock(4) • unlock(5) Default Value: noOp
ifAdminAdminState	R-O	The administrative state of the current interface. It indicates the current maintenance state of a gateway component. This attribute reflects the result of an operator initiated maintenance request. • Unlocked: no operator initiated maintenance request is affecting the operation of the component. • ShuttingDown: the component is in a transition state between unlocked and locked state. An active component will only transition to a locked state once activity, if present, has completed. No new request will be accepted once the activity is completed. • Locked: an operator-initiated request has been issued for this component. This component and all its children are unavailable for normal operation. The <i>permanentLock</i> state is deprecated. AdminState can now be made permanent through the variable <i>ifAdminInitialAdminState</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: unlocked
ifAdminOpState	R-O	The operational state of the current interface. This state reflects the component's internal state. There are certain conditions that affect the internal state of a voice component. • Enabled: the component is operationally functional. • Disabled: the component is operationally non-functional due to an internal condition that would not allow it to participate in normal VoIP call. Default Value: disabled
ifAdminUsageState	R-O	The usage state of the current interface. It indicates the running state of a voice component. • Idle: the component is not currently processing calls, but is available for use. • Active: the component is usable being used and available for processing and still has additional capacity. • Busy: the component is usable but is not available for any new processing requests, since all its resources are currently being used. • Idle-Unusable: the component is not currently processing calls and not available for use. Default Value: Idle-Unusable

Table 18: ifAdmin Parameters (Continued)

Name	Access	Description
ifAdminParentType	R-O	The parents type of this interface. - groupAdmin: the <i>ifAdminParent</i> represents the index (<i>groupAdminIndex</i>) of a group from the <i>groupAdminTable</i> (from the module MX-GROUPS-ADMIN-MIB). - ifAdmin: the <i>ifAdminParent</i> represents the index (<i>ifIndex</i>) of the <i>ifAdminTable</i> (this table) Default Value: groupAdmin
ifAdminParent	R-O	The index of the parent of this interface.
ifAdminInitialAdminState	R/W	Indicates the administrative state the current interface will have after the unit restarts. Refer to <i>ifAdminAdminState</i> for a description of the states. - unlocked(1) - locked(2) This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: unlocked

Management MIBs

Page Left Intentionally Blank

Management Parameters – ipAddressStatus

This MIB provide general system settings.

ipAddressStatusLocalHost

The following parameters allow you to see the IP addresses pertaining to the unit They can be located in the System Config MIB.

Table 19: IP Address Status Parameters – Local Host

Name	Access	Description
localHostConfigSource	R-O	Indicates the source used during the last boot sequence for the provisioning of the localHost objects. Default Value: dhcp
localHostAddress	R-O	Local IP address. Default Value: 192.168.0.1
localHostDhcpServer	R-O	This value indicates the DHCP server IP address obtained from the network after a DHCP broadcast had been sent. In the case no DHPC server were found or DHCP not used, this field will be empty. Default Value: 192.168.0.10
localHostPrimaryDns	R-O	Primary DNS (domain name server) IP address. Default Value: 192.168.0.10
localHostSecondaryDns	R-O	Secondary DNS (domain name server) IP address. This address is used in case the primary DNS can not be reached. Default Value: 192.168.0.10
localHostDefaultRouter	R-O	Default router IP address Default Value: 192.168.0.10
localHostSnmpPort	R-O	The port number used to reach the local host via SNMP protocol. Default Value: 161
localHostSubnetMask	R-O	Subnet mask. Default Value: 255.255.255.0
localHostFqdnConfigSource	R-O	Indicates the source used during the last boot sequence for the provisioning of the local FQDN. • none (0), • static (1), • dhcp (2), • dns (3) This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
localHostFqdn	R-O	Local Fully Qualified Domain Name (FQDN). This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
localHostWanAddressConfigSource	R-O	Indicates the source used during the last boot sequence for the provisioning of the wide area network (WAN) address. • localAddress(0) • static(1) • pppoe(2) • pppoa(3) Default Value: localAddress

Table 19: IP Address Status Parameters – Local Host (Continued)

Name	Access	Description
localHostWanAddress	R-O	The wide area network (WAN) address. This address is the public IP address to be used for incoming signaling, media and management traffic. Default Value: 0.0.0.0

ipAddressStatusImage

The following parameters allow you to see the IP addresses pertaining to the image server used by the unit when performing a software download. They can be located in the Image MIB.

Table 20: IP Address Status Parameters – Image

Name	Access	Description
imageConfigSource	R-O	Indicates the source used for the provisioning of the image MIB objects. Default Value: dhcp
imagePrimaryHost	R-O	Image primary server IP address or domain name. Default Value: 192.168.0.10
imagePrimaryPort	R-O	Image primary server IP port number. Default Value: 69
imageSecondaryHost	R-O	Image secondary server IP address or domain name. Default Value: 192.168.0.10
imageSecondaryPort	R-O	Image secondary server IP port number. Default Value: 69

ipAddressStatusMs

The following parameters allow you to see the IP addresses pertaining to the Management Server used by the unit. They can be located in the MS MIB.

A Management Server can be the Unit Manager Network or IP Communication Server products.

Table 21: IP Address Status Parameters – Management Server

Name	Access	Description
msConfigSource	R-O	Indicates the source used for the provisioning of the management server MIB objects. Default Value: dhcp
msHost	R-O	Management server IP address or domain name. Default Value: 192.168.0.10
msTrapPort	R-O	Management server IP port number on which the SNMP traps are received. Default Value: 162

ipAddressStatusSyslog

The following parameters allow you to see the IP addresses pertaining to the Syslog daemon used by the unit. They can be located in the Syslog MIB.

Table 22: IP Address Status Parameters – Syslog

Name	Access	Description
syslogConfigSource	R-O	Indicates the source used for the provisioning of the syslog MIB objects. Default Value: dhcp
syslogHost	R-O	Syslog server IP address or domain name. Default Value: 192.168.0.10
syslogPort	R-O	Syslog server IP port number. Default Value: 514

ipAddressStatusMgcpCallAgent

The following parameters allow you to see the IP addresses pertaining to the unit. They can be located in the MGCP MIB.

Table 23: IP Address Status Parameters – Call Agent

Name	Access	Description
mgcpCAConfigSource	R-O	Indicates the source used for the provisioning of the MGCP Call Agent MIB objects. Default Value: dhcp
mgcpCAHost	R-O	MGCP Call Agent IP address or domain name. Default Value: 192.168.0.10
mgcpCAPort	R-O	MGCP Call Agent IP port number. Default Value: 2727

ipAddressStatusNcsCallAgent

The following parameters allow you to see the IP addresses pertaining to the unit. They can be located in the NCS MIB.

Table 24: IP Address Status Parameters – Call Agent

Name	Access	Description
ncsCAConfigSource	R-O	Indicates the source used for the provisioning of the NCS Call Agent MIB objects. Default Value: dhcp
ncsCAHost	R-O	NCS Call Agent IP address or domain name. Default Value: 192.168.0.10
ncsCAPort	R-O	NCS Call Agent IP port number. Default Value: 2727

ipAddressStatusSipServer

The following parameters allow you to see the IP addresses pertaining to the unit. They can be located in the SIP MIB.

Table 25: IP Address Status Parameters – SIP Server

Name	Access	Description
sipServerConfigSource	R-O	Indicates the source used for the provisioning of the SIP Server MIB objects. Default Value: dhcp
sipHomeDomainProxyHost	R-O	SIP proxy server IP address or domain name. To disable the outbound proxy, set it to 0.0.0.0 . From RFC3261: A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a UA is manually configured with an outbound proxy, or can learn about one through auto-configuration protocols. When enabled, the initial route for all SIP requests will contain the outbound proxy address, suffixed with the loose routing parameter "lr". The Request-URI still contains the home domain proxy address. Requests are directed to the first route (the outbound proxy). Note: If using a domain name that is bound to a SRV record, see <i>sipHomeDomainProxyPort</i> . Default Value: 192.168.0.10
sipHomeDomainProxyPort	R-O	SIP proxy server IP port number. Note: If <i>sipHomeDomainProxyHost</i> corresponds to a domain name that is bound to a SRV record, the port must be set to 0 in order for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used. Default Value: 0
sipOutboundProxyHost	R-O	SIP outbound proxy server IP address or domain name. To disable the outbound proxy, set it to 0.0.0.0' From RFC3261: A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a UA is manually configured with an outbound proxy, or can learn about one through auto-configuration protocols. When enabled, the initial route for all SIP requests will contain the outbound proxy address, suffixed with the loose routing parameter 'lr'. The Request-URI still contains the home domain proxy address. Requests are directed to the first route (the outbound proxy). Note: If using a domain name that is bound to a SRV record, see <i>sipOutboundProxyPort</i> . Default Value: 0.0.0.0
sipOutboundProxyPort	R-O	SIP outbound proxy server IP port number. Note: If <i>sipOutboundProxyHost</i> corresponds to a domain name that is bound to a SRV record, the port must be set to 0 in order for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used. Default Value: 0
sipRegistrarHost	R-O	SIP registrar server IP address or domain name. A registrar is a server that accepts REGISTER requests, and places the information it receives in those requests into the location service for the domain it handles. Note: If using a domain name that is bound to a SRV record, see <i>sipRegistrarPort</i> . Default Value: 192.168.0.10
sipRegistrarPort	R-O	SIP registrar server IP port number. Note: If <i>sipRegistrarHost</i> corresponds to a domain name that is bound to a SRV record, the port must be set to 0 in order for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used. Default Value: 0
sipPresenceCompositorHost	R-O	SIP Presence Compositor server IP address or domain name. From RFC 3903: A Presence Compositor server is a User Agent Server (UAS) that processes PUBLISH requests, and is responsible for compositing event state into a complete, composite event state of a resource for a presentity. To disable publication, set it to '0.0.0.0'. Note: If using a domain name that is bound to a SRV record, see <i>sipPresenceCompositorPort</i> . Default Value: 0.0.0.0

Table 25: IP Address Status Parameters – SIP Server (Continued)

Name	Access	Description
sipPresenceCompositorPort	R-O	SIP Presence Compositor server IP port number. Note: If <i>sipPresenceCompositorHost</i> corresponds to a domain name that is bound to a SRV record, the port must be set to 0 in order for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used. Default Value: 0

ipAddressStatusSntp

The following parameters allow you to see the IP addresses pertaining to the unit. They can be located in the SNTP MIB.

Table 26: IP Address Status Parameters – SNTP

Name	Access	Description
sntpConfigSource	R-O	Indicates the source used for the provisioning of the SNTP MIB objects. Default Value: static
sntpHost	R-O	SNTP server IP address or domain name. Default Value: 192.168.0.10
sntpPort	R-O	SNTP server IP port number. Default Value: 123

ipAddressStatusConfigFileFetching

The following parameters allow you to see the IP addresses pertaining to the unit. They can be located in the configFileFetching MIB.

Table 27: IP Address Status Parameters – Configuration File Fetching

Name	Access	Description
configFileFetchingConfigSource	R-O	Indicates the source used for the provisioning of the TFTP server MIB objects. This server is used by the unit when fetching configuration files. Default Value: dhcp
configFileFetchingHost	R-O	TFTP server IP address or domain name used when the unit is fetching configuration files. Default Value: 192.168.0.10
configFileFetchingPort	R-O	TFTP server IP port number used when the unit is fetching configuration files. Default Value: 69

ipAddressStatusTelephonyDns

The following parameters allow you to see the IP addresses pertaining to the image server used by the unit when performing a software download. They can be located in the Image MIB.

Table 28: IP Address Status Parameters – Image

Name	Access	Description
telephonyDnsPrimaryDns	R-O	If <i>telephonyDnsOverrideEnable</i> is disabled, the <i>telephonyDnsPrimaryDns</i> variable takes its value from the variable <i>localHostPrimaryDns</i> . If <i>telephonyDnsOverrideEnable</i> is enabled, the <i>telephonyDnsPrimaryDns</i> variable takes its value from the variable <i>telephonyDnsStaticPrimaryDns</i> . Default Value: 192.168.0.10

Table 28: IP Address Status Parameters – Image (Continued)

Name	Access	Description
telephonyDnsSecondaryDns	R-O	If <i>telephonyDnsOverrideEnable</i> is disabled, the <i>telephonyDnsSecondaryDns</i> variable takes its value from the variable <i>localHostSecondaryDns</i> . If <i>telephonyDnsOverrideEnable</i> is enabled, the <i>telephonyDnsSecondaryDns</i> variable takes its value from the variable <i>telephonyDnsStaticSecondaryDns</i> . Default Value: 192.168.0.10

ipAddressStatusStun

The following parameters allow you to see the IP addresses pertaining to the unit. They can be located in the STUN MIB.

stunTable

A table of STUN servers..

Table 29: IP Address Status Parameters – STUN

Name	Access	Description
stunHost	R-O	STUN server IP address or domain name. Default Value: 192.168.0.10
stunPort	R-O	STUN server IP port number. Default Value: 3478

Management Parameters – sysMgmt MIB

This MIB provide general system management information.

sysMgmtMIBObjects

The following parameters give system information on the unit such as its MAC address.

Table 30: System Management Parameters

Name	Access	Description
sysMacAddress	R-O	Ethernet MAC address.
sysHardwareVersion	R-O	Hardware version.
sysSoftwareVersion	R-O	Software version.
sysMibVersion	R-O	MIB version.
sysSerialNumber	R-O	Serial number.

Management Parameters – rtp MIB

This MIB contains RTP statistics data collected by the unit.

rtpMIBObjects

The following parameters allow you to collect statistics and define RTP settings.

rtpStats

The unit collects statistics. These statistics are saved in two sets of variables as Current statistics and Cumulated statistics.

rtpStatsLastConnectionStatistics

Table 31: RTP Statistics – Last Connection

Name	Access	Description
rtpStatsLastConnNumberOctetsTransmitted	R-O	Number of octets transmitted during the last connection.
rtpStatsLastConnNumberOctetsReceived	R-O	Number of octets received during the last connection.
rtpStatsLastConnNumberPacketsTransmitted	R-O	Number of packets transmitted during the last connection.
rtpStatsLastConnNumberPacketsReceived	R-O	Number of packets received during the last connection.
rtpStatsLastConnNumberPacketsLost	R-O	Number of packets lost during the last connection.
rtpStatsLastConnPercentPacketsLost	R-O	Percentage of packets lost during the last connection.
rtpStatsLastConnInterarrivalJitterMin	R-O	Minimum time, in milliseconds, between the arrival of packets during the last connection.
rtpStatsLastConnInterarrivalJitterMax	R-O	Maximum time, in milliseconds, between the arrival of packets during the last connection.
rtpStatsLastConnInterarrivalJitterAvg	R-O	Average time, in milliseconds, between the arrival of packets during the last connection.
rtpStatsLastConnLatencyMin	R-O	Minimum latency, in milliseconds, during the last connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.
rtpStatsLastConnLatencyMax	R-O	Maximum latency, in milliseconds, during the last connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.
rtpStatsLastConnLatencyAvg	R-O	Average latency, in milliseconds, during the last connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.

rtpStatsCurrentStatistics**Table 32: RTP Statistics – Current**

Name	Access	Description
rtpStatsCurrentTotalOctetsTransmitted	R-O	Total number of octets transmitted so far in the current statistics period.
rtpStatsCurrentTotalOctetsReceived	R-O	Total number of octets received so far in the current statistics period.
rtpStatsCurrentTotalPacketsTransmitted	R-O	Total number of packets transmitted so far in the current statistics period.
rtpStatsCurrentTotalPacketsReceived	R-O	Total number of packets received so far in the current statistics period.
rtpStatsCurrentTotalPacketsLost	R-O	Total number of packets lost so far in the current statistics period.
rtpStatsCurrentTotalPercentPacketsLost	R-O	Percentage of packets lost so far in the current statistics period..
rtpStatsCurrentTotalInterarrivalJitterMin	R-O	Minimum time, in milliseconds, between the arrival of packets so far in the current statistics period.
rtpStatsCurrentTotalInterarrivalJitterMax	R-O	Maximum time, in milliseconds, between the arrival of packets so far in the current statistics period.
rtpStatsCurrentTotalInterarrivalJitterAvg	R-O	Average time, in milliseconds, between the arrival of packets so far in the current statistics period.
rtpStatsCurrentTotalLatencyMin	R-O	Minimum latency, in milliseconds, so far in the current statistics period. The latency value is computed as one half of the round-trip time, as measured through RTCP.
rtpStatsCurrentTotalLatencyMax	R-O	Maximum latency, in milliseconds, so far in the current statistics period. The latency value is computed as one half of the round-trip time, as measured through RTCP.
rtpStatsCurrentTotalLatencyAvg	R-O	Average latency in milliseconds so far in the current statistics period. The latency value is computed as one half of the round-trip time, as measured through RTCP.

rtpStatsCumulatedStatistics**Table 33: RTP Statistics – Cumulated**

Name	Access	Description
rtpStatsCumulatedTotalOctetsTransmitted	R-O	Cumulated total of octets transmitted during the cumulated period.
rtpStatsCumulatedTotalOctetsReceived	R-O	Cumulated total of octets received during the cumulated period.
rtpStatsCumulatedTotalPacketsTransmitted	R-O	Cumulated total of packets transmitted during the cumulated period.
rtpStatsCumulatedTotalPacketsReceived	R-O	Cumulated total of packets received during the cumulated period.
rtpStatsCumulatedTotalPacketsLost	R-O	Cumulated total of packets lost during the cumulated period.
rtpStatsCumulatedTotalPercentPacketsLost	R-O	Percentage of packet lost during the cumulated period.
rtpStatsCumulatedTotalInterarrivalJitterMin	R-O	Minimum time, in milliseconds, between the arrival of packets during the cumulated period.
rtpStatsCumulatedTotalInterarrivalJitterMax	R-O	Maximum time, in milliseconds, between the arrival of packets during the cumulated period.
rtpStatsCumulatedTotalInterarrivalJitterAvg	R-O	Average time, in milliseconds, between the arrival of packets during the cumulated period.
rtpStatsCumulatedTotalLatencyMin	R-O	Minimum latency, in milliseconds, during the cumulated period. The latency value is computed as one half of the round-trip time, as measured through RTCP.
rtpStatsCumulatedTotalLatencyMax	R-O	Maximum latency, in milliseconds, during the cumulated period. The latency value is computed as one half of the round-trip time, as measured through RTCP.
rtpStatsCumulatedTotalLatencyAvg	R-O	Average latency, in milliseconds, during the cumulated period. The latency value is computed as one half of the round-trip time, as measured through RTCP.

rtpConfig

This is the root of the configurable RTP objects.

Table 34: RTP Configuration

Name	Access	Description
rtpConfigBasePort	R/W	UDP base port for the RTP/RTCP protocols. The RTP/RTCP ports are allocated starting from this base port. The unit may use two or four RTP/RTCP ports per FXS/FXO interface. It uses 2 ports in case of a standard call, while it uses 4 ports in other types of calls such as a conference call, a call transfer, etc. E.g.: let's say for instance that a unit has two FXS interfaces and the base port is defined on 5004: • if there is currently no ongoing call and FXS connector 1 has an incoming or outgoing call, it will use the RTP/RTCP ports 5004 and 5005. • if there is currently a standard call on FXS connector 1 and FXS connector 2 has a conference call, then FXS connector 2 will use the RTP/RTCP ports 5006, 5007, 5008, and 5009, which are the next available ports. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 5004

Configuration MIBs

Page Left Intentionally Blank

Configuration Parameters – ipAddressConfig

This MIB allows you to set general system parameters.

ipAddressConfigLocalHost

Use these parameters to define the configuration source of the unit. They can be located in the System Config MIB.

Table 35: IP Address Configuration – Local Host

Name	Access	Description
localHostSelectConfigSource	R/W	Indicates the source to be used for the provisioning of the following localHost objects: • localHostAddress • localHostDhcpServer • localHostPrimaryDns • localHostSecondaryDns • localHostDefaultRouter • localHostSubnetMask. If <i>localHostDnsOverrideEnable</i> is enabled, <i>localHostPrimaryDns</i> and <i>localHostSecondaryDns</i> objects are always set with static values. Default Value: dhcp
localHostFqdnSelectConfigSource	R/W	Indicates the source to be used for the provisioning of the local FQDN. • static(0) • dhcp(1) • dns(2) • none(3) This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: none
localHostWanAddressSelectConfigSource	R/W	Indicates the source to be used for the provisioning of the wide area network (WAN) address. The WAN address is the public IP address to be used for incoming signaling, media and management traffic. • localAddress: The WAN address is the one that is set in the <i>localHostAddress</i> variable, whereas the <i>localHostStaticWanAddress</i> is ignored. • static: The unit has a static WAN address. The address is configured in <i>localHostStaticWanAddress</i>. This setting allows a limited NAT traversal scheme. • pppoe: The unit uses the PPP over Ethernet in order to obtain its WAN IP address. The PPPoE service must be enabled. See also the <i>pppoeEnable</i> variable. • pppoa: The unit uses the PPP over ATM in order to obtain its WAN IP address. The PPPoA service must be enabled. See also the <i>pppoaEnable</i> variable. • automatic: If the PPPoE service is enabled, the unit uses 'pppoe' as the configuration source. If the PPPoA service is enabled, the unit uses 'pppoa' as the configuration source. Otherwise the unit uses 'localAddress'. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: automatic

Table 35: IP Address Configuration – Local Host (Continued)

Name	Access	Description
localHostDnsOverrideEnable	R/W	If <i>localHostDnsOverrideEnable</i> is enabled, the <i>localHostPrimaryDns</i> and <i>localHostSecondaryDns</i> objects are always overridden with static values. If <i>localHostDnsOverrideEnable</i> is disabled, the variable <i>localHostSelectConfigSource</i> indicates the source for the provisioning of the localHost objects: <i>localHostPrimaryDns</i> and <i>localHostSecondaryDns</i> . Default Value: disable

ipAddressConfigLocalHostStatic

The following parameters allow you to set static information pertaining to the unit if you don't want to use DHCP-provided information.

Table 36: IP Address Configuration – Local Host Static

Name	Access	Description
localHostStaticAddress	R/W	User defined local IP address. Default Value: 192.168.0.1
localHostStaticPrimaryDns	R/W	User defined static primary DNS (domain name server) IP address. The DNS is used mainly to resolve a FQDN (Fully qualified domain name) into the proper IP address or to get the FQDN from a specified IP address. Default Value: 192.168.0.10
localHostStaticSecondaryDns	R/W	User defined static secondary DNS (domain name server) IP address. This address is used in case the primary DNS can not be reached. Default Value: 192.168.0.10
localHostStaticDefaultRouter	R/W	User defined default router IP address. Default Value: 192.168.0.10
localHostStaticSnmpPort	R/W	The port number to use to reach the local host via SNMP protocol. Default Value: 161
localHostStaticSubnetMask	R/W	User defined subnet mask. Default Value: 255.255.255.0
localHostStaticFqdn	R/W	User-defined local Fully Qualified Domain Name (FQDN). This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
localHostStaticWanAddress	R/W	User-defined wide area network (WAN) address. Default Value: 0.0.0.0

ipAddressConfigImage

Use this parameter to define if you want the unit to get its image information via a DHCP server or to use static information. They can be located in the Image MIB.

Table 37: IP Address Configuration – Image

Name	Access	Description
imageSelectConfigSource	R/W	The source to use for the provisioning of the image MIB objects. Default Value: dhcp

ipAddressConfigImageStatic

The following parameters allow you to set static image information pertaining to the unit if you don't want to use DHCP-provided information.

Table 38: IP Address Configuration – Image Static

Name	Access	Description
imageStaticPrimaryHost	R/W	Static primary server IP address or domain name. Default Value: 192.168.0.10
imageStaticPrimaryPort	R/W	Static primary server IP port number. Default Value: 69
imageStaticSecondaryHost	R/W	Static secondary server IP address or domain name. Default Value: 192.168.0.10
imageStaticSecondaryPort	R/W	Static secondary server IP port number. Default Value: 69

ipAddressConfigImageDhcp

The following parameters allow you to set DHCP image information pertaining to the unit. You will have to define this information in your DHCP server by using vendor specific or site specific codes. This information will then be supplied to the unit during its provisioning sequence.

Table 39: IP Address Configuration – Image DHCP

Name	Access	Description
imageDhcpPrimarySiteSpecificCode	R/W	DHCP primary image server site specific code. If set to 0, use vendor-specific code #117. Default Value: 0
imageDhcpSecondarySiteSpecificCode	R/W	DHCP secondary image server site specific code. If set to 0, use vendor-specific code #118. Default Value: 0

ipAddressConfigFileFetching

Use this parameter to define if you want the unit to get its configuration file fetching information via a DHCP server or to use static information. They can be located in the configFileFetching MIB.

Table 40: IP Address Configuration – Configuration File Fetching

Name	Access	Description
configFileFetchingSelectConfigSource	R/W	The source to use for the provisioning of the TFTP server MIB objects. This server is used by the unit when fetching configuration files. Default Value: dhcp

ipAddressConfigFileFetchingStatic

The following parameters allow you to set static configuration file fetching information pertaining to the unit if you don't want to use DHCP-provided information.

Table 41: IP Address Configuration – Configuration File Fetching Static

Name	Access	Description
configFileFetchingStaticHost	R/W	Static TFTP server IP address or domain name to use when fetching configuration files. Default Value: 192.168.0.10
configFileFetchingStaticPort	R/W	Static TFTP server IP port number to use when fetching configuration files. Default Value: 69

ipAddressConfigFileFetchingDhcp

The following parameters allow you to set DHCP configuration file fetching information pertaining to the unit. You will have to define this information in your DHCP server by using vendor specific or site specific codes. This information will then be supplied to the unit during its provisioning sequence.

Table 42: IP Address Configuration – Configuration File Fetching DHCP

Name	Access	Description
configFileFetchingDhcpSiteSpecificCode	R/W	DHCP TFTP server site specific code to use when fetching configuration files. If set to 0, use vendor-specific code #201. Default Value: 0

ipAddressConfigMs

Use this parameter to define if you want the unit to get its Management Server information via a DHCP server or to use static information. They can be located in the MS MIB.

The Management Server could be the Unit Manager Network product.

Table 43: IP Address Configuration – Management Server

Name	Access	Description
msSelectConfigSource	R/W	Indicates the source to be used for the provisioning of the management server MIB objects. Default Value: dhcp

ipAddressConfigMsStatic

The following parameters allow you to set static Management Server information pertaining to the unit if you don't want to use DHCP-provided information.

Table 44: IP Address Configuration – Management Server Static

Name	Access	Description
msStaticHost	R/W	Static management server IP address or domain name. Default Value: 192.168.0.10
msStaticTrapPort	R/W	Static management server IP port number on which the SNMP traps are received. Default Value: 162

ipAddressConfigMsDhcp

The following parameters allow you to set DHCP Management Server information pertaining to the unit. You will have to define this information in your DHCP server by using vendor specific or site specific codes. This information will then be supplied to the unit during its provisioning sequence.

Table 45: IP Address Configuration – Management Server DHCP

Name	Access	Description
msDhcpSiteSpecificCode	R/W	DHCP management server site specific code. If set to 0, use vendor-specific code #200. Default Value: 0

ipAddressConfigSyslog

Use this parameter to define if you want the unit to get its Syslog daemon information via a DHCP server or to use static information. They can be located in the Syslog MIB.

Table 46: IP Address Configuration – Syslog

Name	Access	Description
syslogSelectConfigSource	R/W	Indicates the source to be used for the provisioning of the syslog MIB objects. Default Value: dhcp

ipAddressConfigSyslogStatic

The following parameters allow you to set static Syslog daemon information pertaining to the unit if you don't want to use DHCP-provided information.

Table 47: IP Address Configuration – Syslog Static

Name	Access	Description
syslogStaticHost	R/W	Static Syslog server IP address or domain name. Default Value: 192.168.0.10
syslogStaticPort	R/W	Static Syslog server IP port number. Default Value: 514

ipAddressConfigSyslogDhcp

The following parameters allow you to set DHCP Syslog daemon information pertaining to the unit. You will have to define this information in your DHCP server by using vendor specific or site specific codes. This information will then be supplied to the unit during its provisioning sequence.

Table 48: IP Address Configuration – Syslog DHCP

Name	Access	Description
syslogDhcpSiteSpecificCode	R/W	DHCP Syslog server site specific code. If set to 0, use vendor-specific code #110. Default Value: 0

ipAddressConfigMgcpCallAgent

Use this parameter to define if you want the unit to get its MGCP Call Agent information via a DHCP server or to use static information. They can be located in the MGCP MIB.

Table 49: IP Address Configuration – MGCP Call Agent

Name	Access	Description
mgcpCSelectConfigSource	R/W	Indicates the source to be used for the provisioning of the MGCP Call Agent MIB objects. Default Value: dhcp

ipAddressConfigMgcpCStatic

The following parameters allow you to set static MGCP Call Agent information pertaining to the unit if you don't want to use DHCP-provided information.

Table 50: IP Address Configuration – MGCP Call Agent Static

Name	Access	Description
mgcpCStaticHost	R/W	Static MGCP Call Agent IP address or domain name. Default Value: 192.168.0.10
mgcpCStaticPort	R/W	Static MGCP Call Agent IP port number. Default Value: 2727

ipAddressConfigMgcpCDhcp

The following parameters allow you to set DHCP MGCP Call Agent information pertaining to the unit. You will have to define this information in your DHCP server by using vendor specific or site specific codes. This information will then be supplied to the unit during its provisioning sequence.

Table 51: IP Address Configuration – MGCP Call Agent DHCP

Name	Access	Description
mgcpCDhcpSiteSpecificCode	R/W	DHCP MGCP Call Agent site specific code. If set to 0, use vendor-specific code #207. Default Value: 0

ipAddressConfigNcsCallAgent

Use this parameter to define if you want the unit to get its NCS Call Agent information via a DHCP server or to use static information. They can be located in the NCS MIB.

Table 52: IP Address Configuration – NCS Call Agent

Name	Access	Description
ncsCAslectConfigSource	R/W	Indicates the source to be used for the provisioning of the NCS Call Agent MIB objects. Default Value: dhcp

ipAddressConfigNcsCAStatic

The following parameters allow you to set static NCS Call Agent information pertaining to the unit if you don't want to use DHCP-provided information.

Table 53: IP Address Configuration – NCS Call Agent Static

Name	Access	Description
ncsCAStaticHost	R/W	Static NCS Call Agent IP address or domain name. Default Value: 192.168.0.10
ncsCAStaticPort	R/W	Static NCS Call Agent IP port number. Default Value: 2727

ipAddressConfigNcsCADhcp

The following parameters allow you to set DHCP NCS Call Agent information pertaining to the unit. You will have to define this information in your DHCP server by using vendor specific or site specific codes. This information will then be supplied to the unit during its provisioning sequence.

Table 54: IP Address Configuration – NCS Call Agent DHCP

Name	Access	Description
ncsCADhcpSiteSpecificCode	R/W	DHCP NCS Call Agent site specific code. If set to 0, use vendor-specific code #210. Default Value: 0

ipAddressConfigSipServer

Use this parameter to define if you want the unit to get its SIP Servers information via a DHCP server or to use static information. They can be located in the SIP MIB.

Table 55: IP Address Configuration – SIP Servers

Name	Access	Description
sipServerSelectConfigSource	R/W	Indicates the source to be used for the provisioning of the SIP Server registrar MIB objects. Default Value: dhcp

ipAddressConfigSipServerStatic

The following parameters allow you to set static SIP Servers information pertaining to the unit if you don't want to use DHCP-provided information.

Table 56: IP Address Configuration – SIP Servers Static

Name	Access	Description
sipHomeDomainProxyStaticHost	R/W	SIP proxy server IP address or domain name. A SIP proxy server is an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is passed on to another entity that can further process the request. Proxies are also useful for enforcing policy and for firewall traversal. A proxy interprets, and, if necessary, rewrites parts of a request message before forwarding it. Note: If using a domain name that is bound to a SRV record, see <i>sipHomeDomainProxyStaticPort</i> . Default Value: 192.168.0.10
sipHomeDomainProxyStaticPort	R/W	SIP proxy server IP port number. Note: If <i>sipHomeDomainProxyStaticHost</i> corresponds to a domain name that is bound to a SRV record, the port must be set to 0 in order for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used. Default Value: 0
sipOutboundProxyStaticHost	R/W	SIP outbound proxy server IP address or domain name. To disable the outbound proxy, set it to 0.0.0.0 . From RFC3261: A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a UA is manually configured with an outbound proxy, or can learn about one through auto-configuration protocols. When enabled, the initial route for all SIP requests will contain the outbound proxy address, suffixed with the loose routing parameter "lr". The Request-URI still contains the home domain proxy address. Requests are directed to the first route (the outbound proxy). Note: If using a domain name that is bound to a SRV record, see <i>sipOutboundProxyPort</i> . Note: If using a domain name that is bound to a SRV record, see <i>sipOutboundProxyStaticPort</i> . Default Value: 0.0.0.0
sipOutboundProxyStaticPort	R/W	SIP outbound proxy server IP port number. Note: If <i>sipOutboundProxyStaticHost</i> corresponds to a domain name that is bound to a SRV record, the port must be set to 0 in order for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used. Default Value: 0
sipRegistrarStaticHost	R/W	SIP registrar server IP address or domain name. A SIP registrar server is a server that accepts REGISTER requests, and places the information it receives in those requests into the location service for the domain it handles. Note: If using a domain name that is bound to a SRV record, see <i>sipRegistrarStaticPort</i> . Default Value: 192.168.0.10
sipRegistrarStaticPort	R/W	SIP registrar server IP port number. Note: If <i>sipRegistrarStaticHost</i> corresponds to a domain name that is bound to a SRV record, the port must be set to 0 in order for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used. Default Value: 0

Table 56: IP Address Configuration – SIP Servers Static (Continued)

Name	Access	Description
sipPresenceCompositorStaticHost	R/W	SIP Presence Compositor server IP address or domain name. From RFC 3903: A Presence Compositor server is a User Agent Server (UAS) that processes PUBLISH requests, and is responsible for compositing event state into a complete, composite event state of a resource for a presentity. To disable publication, set it to '0.0.0.0'. Note: If using a domain name that is bound to a SRV record, see <i>sipPresenceCompositorStaticPort</i> . Default Value: 0.0.0.0
sipPresenceCompositorStaticPort	R/W	SIP Presence Compositor server IP port number. Note: If <i>sipPresenceCompositorStaticHost</i> corresponds to a domain name that is bound to a SRV record, the port must be set to 0 in order for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used. Default Value: 0

ipAddressConfigSipServerDhcp

The following parameters allow you to set DHCP SIP Servers information pertaining to the unit. You will have to define this information in your DHCP server by using vendor specific or site specific codes. This information will then be supplied to the unit during its provisioning sequence.

Table 57: IP Address Configuration – SIP Servers DHCP

Name	Access	Description
sipRegistrarDhcpSiteSpecificCode	R/W	DHCP SIP server registrar site specific code. If set to 0, use vendor-specific code #203. Default Value: 0
sipHomeDomainProxyDhcpSiteSpecificCode	R/W	DHCP SIP server proxy site specific code. If set to 0, use vendor-specific code #204. Default Value: 0
sipOutboundProxyDhcpSiteSpecificCode	R/W	DHCP SIP outbound proxy server site specific code. If set to 0, use vendor-specific code #205. Default Value: 0
sipPresenceCompositorDhcpSiteSpecificCode	R/W	DHCP SIP Presence Compositor server site-specific code. If set to 0, use vendor-specific code #206. Default Value: 0

ipAddressConfigSntp

Use this parameter to define if you want the unit to get its SNTP (Simple Network Time Protocol) information via a DHCP server or to use static information. They can be located in the SNTP MIB.

Table 58: IP Address Configuration – “SNTP

Name	Access	Description
sntpSelectConfigSource	R/W	Indicates the source to be used for the provisioning of the SNTP MIB objects. Default Value: dhcp

ipAddressConfigSntpStatic

The following parameters allow you to set static SNTP information pertaining to the unit if you don't want to use DHCP-provided information.

Table 59: IP Address Configuration – SNTP Static

Name	Access	Description
sntpStaticHost	R/W	Static SNTP server IP address or domain name. Default Value: 192.168.0.10

Table 59: IP Address Configuration – SNTP Static (Continued)

Name	Access	Description
sntpStaticPort	R/W	Static SNTP server IP port number. Default Value: 123

ipAddressConfigH323

The following parameters allow you to define the IP information of H.323 units.

Table 60: IP Address Configuration – H.323 Configuration Source

Name	Access	Description
h323SelectConfigSource	R/W	Selection of the configuration source for IP addresses. For the gatekeeper registration, this variable indicates the source for the gatekeeper IP addresses. - static: the IP addresses are specified by the administrator. - dhcp: the IP addresses are provided by a DHCP server. This configuration applies to all the lines/groups of lines. Default Value: dhcp

ipAddressConfigH323Static

ipAddressConfigH323GatekeeperTable

This table holds the gatekeeper IP addresses used in the registration of the unit.

Table 61: IP Address Configuration – H.323 Registration, Gatekeeper Addresses

Name	Access	Description
ipAddressConfigH323GkStaticHost	R/W	A gatekeeper IP address. When the unit is configured with the single registration method, it uses this IP address if: - The unit is configured with the manual gatekeeper discovery mode. - The configuration source is static. When the unit is configured with the multiple registration method, it uses this IP address if: - The line/group of lines is configured with the manual gatekeeper discovery mode. - The registration for the line/group is enabled. - The configuration source is static.
ipAddressConfigH323GkStaticPort	R-O	The gatekeeper RAS port (well-known gatekeeper RAS Channel TSAP Identifier, 1719). Default Value: 1719

ipAddressConfigH323Dhcp

The following parameters allow you to set DHCP H.323 registration information pertaining to the unit. You will have to define this information in your DHCP server by using a vendor specific or site specific code. This information will then be supplied to the unit during its provisioning sequence.

Table 62: IP Address Configuration – H.323 Registration, DHCP

Name	Access	Description
h323GkDhcpSiteSpecificCode	R/W	DHCP H.323 gatekeeper site-specific code. If the value of this variable is 0, the unit uses the vendor-specific code #111. The unit expects an array of IP addresses from the DHCP server. This array contains gatekeeper IP addresses. The unit expects from one to five IP addresses. If there are more than five IP addresses, the unit ignores the additional IP addresses. When the unit is configured with the single registration method, it uses these IP addresses if: - The unit is configured with the manual gatekeeper discovery mode. - The configuration source is dhcp. When the unit is configured with the multiple registration method, it uses these IP addresses if: - The line/group of lines is configured with the manual gatekeeper discovery mode. - The registration for the line/group is enabled. - The source is dhcp. Default Value: 0

ipAddressConfigLanInterface

The following parameters allow you to define the LAN IP information of the Mediatrix unit's *Computer* interface.

Table 63: IP Address Configuration – LAN Interface Static Information

Name	Access	Description
lanStaticAddressActivation	R/W	Allows to use the LAN static IP address according to IP routing, VLAN substitution or always enabled configuration. - ipRouting: To set the <i>lanStaticAddress</i> as the Local Area Network (LAN) IP address used by the router's computer interface, set the variable <i>ipRoutingEnable</i> to enable. - vlanSubstitution: To set the <i>lanStaticAddress</i> as the Local Area Network (LAN) IP address used by the router's computer interface, set the variable <i>qosVlanIeee8021qSubstitutionEnable</i> to enable. - always: Sets the <i>lanStaticAddress</i> as the Local Area Network (LAN) IP address used by the router's computer interface. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: pRouting
lanStaticAddress	R/W	When the <i>ipRoutingEnable</i> variable is set to enable and <i>lanStaticAddressActivation</i> to ipRouting Or the <i>qosVlanIeee8021qSubstitutionEnable</i> variable is set to enable and <i>lanStaticAddressActivation</i> to vlanSubstitution: The <i>lanStaticAddress</i> is the Local Area Network (LAN) IP address used by the router's computer interface. Default Value: 192.168.10.1

Table 63: IP Address Configuration – LAN Interface Static Information (Continued)

Name	Access	Description
lanStaticNetworkMask	R/W	When the <i>ipRoutingEnable</i> variable is set to enable and <i>lanStaticAddressActivation</i> to ipRouting Or the <i>qosVlanIeee8021qSubstitutionEnable</i> variable is set to enable and <i>lanStaticAddressActivation</i> to vlanSubstitution : Or <i>lanStaticAddressActivation</i> is set to always : The <i>lanStaticNetworkMask</i> is the Local Area Network (LAN) subnet mask used by the router's computer interface. Default Value: 255.255.255.0

ipAddressConfigHttpServer

The following parameter allows you to define the HTTP server IP information.

Table 64: IP Address Configuration – HTTP Server

Name	Access	Description
httpServerPort	R/W	Set the TCP port on which to listen for HTTP requests. Default value: 80
httpServerAdminPort	R/W	Set the TCP port on which the administration website will listen for HTTP requests. Default value: 8080

ipAddressConfigTelephonyDns

The following parameters allow you to set telephony DNS information pertaining to the unit.

Table 65: IP Address Configuration – Telephony DNS

Name	Access	Description
telephonyDnsOverrideEnable	R/W	If <i>telephonyDnsOverrideEnable</i> is disabled, DNS IP addresses are provisioned by the variables <i>localHostPrimaryDns</i> and <i>localHostSecondaryDns</i> . If <i>telephonyDnsOverrideEnable</i> is enabled, DNS IP addresses are overridden by the variables <i>telephonyDnsPrimaryDns</i> and <i>telephonyDnsSecondaryDns</i> . This is useful when a unit and a networked PC (linked in a LAN with the unit) need to use a different DNS. Default Value: disable

ipAddressConfigTelephonyDnsStatic

The following parameters allow you to set static telephony DNS information pertaining to the unit.

Table 66: IP Address Configuration – Static Telephony DNS

Name	Access	Description
telephonyDnsStaticPrimaryDns	R/W	If <i>telephonyDnsOverrideEnable</i> is enabled, the unit uses this static primary DNS. If <i>telephonyDnsOverrideEnable</i> is disabled, this variable is not used. Default Value: 192.168.0.10
telephonyDnsStaticSecondaryDns	R/W	If <i>telephonyDnsOverrideEnable</i> is enabled, the unit uses this static secondary DNS. If <i>telephonyDnsOverrideEnable</i> is disabled, this variable is not used. Default Value: 192.168.0.10

ipAddressConfigStun

ipAddressConfigStunStatic

The following parameters allow you to set static STUN client information pertaining to the unit.

stunStaticTable

Name	Access	Description
stunStaticHost	R/W	Static STUN server IP address or domain name. Default Value: 192.168.0.10
stunStaticPort	R/W	Static STUN server IP port number. Default Value: 3478

Configuration Parameters – sysConfig MIB

This MIB allows you to set general system parameters.

sysConfigMIBObjects

Use this parameter to define the speed of the Ethernet connection of the unit.

Table 67: System Configuration Parameters

Name	Access	Description
sysConfigNetworkEthernetSpeed	R/W	Set the network connection speed. By default, autoDetect should handle most situations. In some cases however, it might be required to force the speed and duplex to certain setting. Whenever forcing a connection speed / duplex mode, make sure that the other device has the same configuration. Please refer to the documentation shipped with your device for more details. • autoDetect(0) • at-10Mbs-HalfDuplex(1) • at-100Mbs-HalfDuplex(2) • at-10Mbs-FullDuplex(3) • at-100Mbs-FullDuplex(4) Default Value: autoDetect
sysConfigComputerEthernetSpeed	R/W	Set the computer ethernet connection speed. By default, autoDetect should handle most situations. In some cases however, it might be required to force the speed and duplex to certain setting. Whenever forcing a connection speed / duplex mode, make sure that the other device has the same configuration. Please refer to the documentation shipped with your device for more details. • autoDetect(0) • at-10Mbs-HalfDuplex(1) • at-100Mbs-HalfDuplex(2) • at-10Mbs-FullDuplex(3) • at-100Mbs-FullDuplex(4) Default Value: autoDetect
sysConfigMinDynamicPort	R/W	Lower boundary for the range of dynamic UDP and TCP ports. The smallest acceptable range, between the lower and upper boundaries, is 500. When needed, the TCP/IP implementation of the unit randomly selects a dynamic port amongst the free ports of the range. For example, the dynamic ports range is configured from 41000 to 42000. The unit needs to download a new version of its software. The TCP/IP implementation of the unit selects a local UDP port for the TFTP client. The port is selected in the dynamic ports range so the port has a value between 41000 and 42000. The UDP and TCP ports are separated in three ranges: well-known ports (0 to 1023), registered ports (1024 to 49151) and dynamic ports (49152 to 65535). The IANA (Internet Assigned Numbers Authority, www.iana.org) assigns the well-known ports. The IANA also lists the registered ports. The dynamic ports are not under the authority of the IANA. Most TCP/IP implementations use the range 1025 to 65535 for dynamic ports instead of the range defined by the IANA. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 31001

Table 67: System Configuration Parameters (Continued)

Name	Access	Description
sysConfigMaxDynamicPort	R/W	Upper boundary for the range of dynamic UDP and TCP ports. The smallest acceptable range, between the lower and upper boundaries, is 500. When needed, the TCP/IP implementation of the unit randomly selects a dynamic port amongst the free ports of the range. For example, the dynamic ports range is configured from 41000 to 42000. The unit needs to download a new version of its software. The TCP/IP implementation of the unit selects a local UDP port for the TFTP client. The port is selected in the dynamic ports range so the port has a value between 41000 and 42000. The UDP and TCP ports are separated in three ranges: well-known ports (0 to 1023), registered ports (1024 to 49151) and dynamic ports (49152 to 65535). The IANA (Internet Assigned Numbers Authority, www.iana.org) assigns the well-known ports. The IANA also lists the registered ports. The dynamic ports are not under the authority of the IANA. Most TCP/IP implementations use the range 1025 to 65535 for dynamic ports instead of the range defined by the IANA. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 32000
sysConfigDhcpWait	R/W	Determines the restart behaviour of a unit that needs to issue a DHCP request to receive some options. This variable has no influence on the wait behaviour in effect when the unit is requesting an IP address lease from the DHCP server. - enable: The unit waits up to 130 seconds for DHCP options and then, in the absence of a response, proceeds to restart without a valid address for the requested servers. - disable: The unit restarts, without valid server addresses, if a DHCP response has not been received after the amount of time specified in the variable <i>sysConfigDhcpWaitDelay</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: enable
sysConfigDhcpWaitDelay	R/W	The amount of time (in seconds) a unit will wait for DHCP options before restarting without a valid address for the requested servers. This variable is only effective when the variable <i>sysConfigDhcpWait</i> is set to disable. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 10
sysConfigBootpFlags	R/W	Determines whether the Bootp BROADCAST flag is set in DHCP requests issued by the unit. See RFC 1542 for details. - noFlags - broadcastFlag This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: broadcastFlag
sysConfigProductNamePadding	R/W	A string that is appended to the content of the variable "productNamingPlatforms" to be used as Vendor Class identifier (Option 60) in a DHCP request. This option is useful when servers require that DHCP packets sent to them be of a minimum size. A string of arbitrary characters (including blanks) can then be used to artificially increase the size of DHCP requests. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.

sysConfigStats

The following parameters allow you to define how the unit is to collect system statistics. These statistics can then be viewed in the rtp management MIB. See “[Chapter 6 - Management Parameters – rtp MIB](#)” on page 23 for more details.

Table 68: System Configuration – Statistics

Name	Access	Description
sysConfigStatsPeriodLength	R/W	Duration of time that statistics are collected in the current statistics buffer. At expiration, the current statistics are added to the cumulated statistics buffer and then reset. These are units of 5 minutes. 1 = 5 minutes. 12 = 1 hour. 288 = 24 hours. Changing this value resets all the statistics buffers. Default Value: 1
sysConfigStatsNumberPeriods	R/W	Number of statistics period used for cumulating statistics. Changing this value resets all the statistics buffers. 0 = Disable cumulated statistics. Default Value: 0
sysConfigStatsBySyslogEnable	R/W	Enables or disables statistics by syslog feature. This feature allows the unit to send by syslog all RTP statistics at the end of a connection (at the end of the call or the fax). Default Value: disable

sysConfigDownloadConfig

The following parameters allow you to define how the unit must get its configuration file.

Table 69: System Configuration – Download

Name	Access	Description
sysConfigDownloadConfigFile	R/W	Indicates if a configuration file is downloaded and how it is downloaded. - noFileDownload: Do not perform a configuration file download. - requestFileDownload: A configuration file is sent by the management server on request (see <i>sysConfigDownloadConfigMode</i>). The management server is the initiator of the TFTP session. - automaticInitiateFileDownload: Configuration files are automatically fetched by the unit (see <i>configFileFetchingFile Name</i>). Refer to <i>configFileAutoUpdateOnRestartEnable</i> and <i>configFileAutoUpdatePeriodicEnable</i> for details. The unit is the initiator of the transfer sessions (see <i>configFileTransferProtocol</i>). This method facilitates the NAT traversal. Default Value: requestFileDownload
sysConfigDownloadConfigMode	R/W	The unit configuration mode when a configuration file is sent by the management server. See <i>sysConfigDownloadConfigFile</i> . - request: The unit requests a configuration from the management server. A notification, <i>msTrapConfigInformation</i>, is sent to the management server. - record: The unit is recording the new configuration from the management server. Note that the new settings will not be applied until the configuration mode is set to <i>commit(1)</i>. A notification, <i>msTrapStatusInformation</i>, is sent to the management server to confirm that the configuration mode was modified. - commit: Commit the new recorded settings. A notification, <i>msTrapStatusInformation</i>, is sent to the management server to confirm that the configuration mode was modified. The unit is automatically restarted. - undo: Undo all recorded settings. The new recorded configuration is dismissed. A notification, <i>msTrapStatusInformation</i>, is sent to the management server to confirm that the configuration mode was modified. Default Value: request

Table 69: System Configuration – Download (Continued)

Name	Access	Description
sysConfigDownloadConfigPathname	R/W	Pathname (= path/filename) of the configuration file fetched by the unit (see <i>sysConfigDownloadConfigFile</i>). The pathname is relative to the root of the TFTP server. Use "/" to separate subdirectories and to separate the path from the filename. The TFTP server is located on the management server host (see <i>msHost</i>). The default TFTP port, i.e. 69, is used. NOTE: The default value is set by substituting <i>\$sysMacAddress</i> by the <i>sysMacAddress</i> MIB object value. Default Value: \$sysMacAddress.cfg

Configuration Parameters – image MIB

This MIB is used to define how to perform for the update of the binary image of the application running on the current device. The update is done through a software download using common file transfer protocols such as tftp or ftp.

imageMIBObjects

The following parameters allow you to define the file names used in the image download process.

Table 70: Image Parameters

Name	Access	Description
imageLocation	R/W	The path of the "Setup.inf" file location, and of the location of the binary image to be downloaded, on the remote image server. This setting applies when <i>imageLocationProvisionSource</i> is set to static .
imageSelectionFileLocation	R/W	The path of the image selection file on the remote image server. The selection file is named from concatenation of the product name (see variable <i>productNamingPlatformName</i>) and the prefix 'targetimage.inf'. All spaces are stripped and all cases are lowered. For a product named 'Xyz 123', the selection file name would be 'xyz123targetimage.inf'. This file contains the path of the "Setup.inf" file location, and of the location of the binary image to be downloaded. This setting applies when <i>imageLocationProvisionSource</i> is set to remoteFile .
imageLocationProvisionSource	R/W	Source of the image location. - static: The image location is defined by <i>imageLocation</i>. - remoteFile: The image location is obtained by fetching the information present in a file located in <i>imageSelectionFileLocation</i>. Default Value: static

imageTransfer

The following parameters allow you to define the image transfer process.

Table 71: Image Parameters – Transfer

Name	Access	Description
imageTransferProtocol	R/W	The protocol to use for downloading the image. - tftp: Trivial File Transfer Protocol. - http: Hypertext Transfer Protocol. - https: Hypertext Transfer Protocol over Transport Layer Security (HTTP over TLS). This option requires that the appropriate security certificate be installed on the unit. Furthermore, because HTTPS relies on the system clock for server authentication, the SNTP client (see <i>sntpMIB</i>) must be enabled and properly configured. Please refer to the documentation shipped with your device for more details. Default Value: tftp
imageTransferUsername	R/W	The user name to use for authentication when downloading the image. Only applies when using HTTP or HTTPS as the transfer protocol.
imageTransferPassword	R/W	The password to use for authentication when downloading the image. Only applies when using HTTP or HTTPS as the transfer protocol.

imageAutomaticUpdate

The following parameters allow you to define the image automatic update process.

Table 72: Image Parameters – Automatic Update

Name	Access	Description
imageAutoUpdateOnRestartEnable	R/W	Enables/Disables the automatic update of the image on restart. - disable: The image is not automatically updated at each restart. - enable: The image is updated at each restart." Default Value: disable
imageAutoUpdatePeriodicEnable	R/W	Enables/Disables the periodic image updates. - disable: The image is not periodically updated. - enable: The image is periodically updated." Default Value: disable
imageAutoUpdateTimeUnit	R/W	The time base for periodic image updates. Modification to this setting resets the update timer. - minutes: The image is updated every x minutes. - hours: The image is updated every x hours. - days : The image is updated every x days. Note that x is defined by <i>imageAutoUpdatePeriod</i> . Default Value: days
imageAutoUpdatePeriod	R/W	The waiting period between each image update. Modification to this setting resets the update timer. This value is expressed in units defined by <i>imageAutoUpdateTimeUnit</i> . Default Value: 1
imageAutoUpdateTimeOfDay	R/W	This object is deprecated. It is recommended to use the variable <i>imageAutoUpdateTimeRange</i> because it has precedence over this variable. The time of the day, based on <i>sntpTimeZoneString</i> , when the unit periodically initiate a image software download. The image software download is initiated at the first occurrence of this value and thereafter with a period defined by <i>imageAutoUpdatePeriod</i> . Let's say for instance the automatic update is set with the time of day at 14h00 and the update period at every 2 days. If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on. -1: The time of the day at which the unit first fetches the configuration files is randomly selected. Only applies when <i>imageAutoUpdateTimeUnit</i> is set to days . Default Value: -1
imageAutoUpdateTimeRange	R/W	The time of the day, based on <i>sntpTimeZoneString</i> , when the unit periodically initiates an image software download. If a time range is specified, the unit will initiate the image software download at a random time within the interval specified. The format should be one of the following: hh[:mm[:ss]] hh[:mm[:ss]] - hh[:mm[:ss]] Where: hh: Hours. mm: Minutes. ss: Seconds. The image software download is initiated at the first occurrence of this value and thereafter with a period defined by <i>imageAutoUpdatePeriod</i> . Let's say for instance the automatic update is set with the time of day at 14h00 and the update period at every 2 days. If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on. If the time range is set to '14:00 - 15:00' and the automatic update is enabled within those hours, the first update will take place the following day. This means that a range of '00:00:00 - 23:59:59' will always take place the next day. Note that the SNTP server needs to be enabled (see <i>sntpEnable</i>). Modification to this setting resets the update timer. It only applies when <i>imageAutoUpdateTimeUnit</i> is set to days .

imageStatus

The following parameter gives you the status of the image location.

Table 73: Image Parameters – Status

Name	Access	Description
imageLocationStatus	R-O	The path of the "Setup.inf" file location, and of the location of the binary image, that was last successfully downloaded from the remote image server.

imageEvents

The following are the events produced during the image download process.

image Notifications Control

The following is the notification control event.

Table 74: Image Events – Notifications Control

Name	Access	Description
imageCompletionControl	R/W	This value specifies whether or not a notification should be issued on completion of the software download. If such a notification is desired, it is the responsibility of the SNMP manager to properly configure the notification parameters to insure that the notification will be delivered • disable(0) • enable(1) Default Value: enable

image Notifications

The following is the notification event.

Table 75: Image Events – Notifications

Name	Access	Description
imageCompletion	N/A	A message notification is sent after the software download completed successfully or not. • imageFilenameDownloaded, • imageServerAddress, • sysAdminLastDownloadSoftware, • imageErrorCause, • imageTimeStarted, • imageTimeCompleted

image Notifications Params

The following are the notification parameters.

Table 76: Image Events – Notifications Parameters

Name	Access	Description
imageLocationUsed	A-N	The path of the <<Setup.inf>> file location, and of the binary image location, on the remote image server used in the last software download. Parameters used in image notifications.
imageCompletion	N/A	A message notification is sent after the software download completed successfully or not.

Configuration Parameters – ms MIB

This MIB describes the parameters to configure the Management Server. The Management Server could be the Unit Manager Network product.

msMIBObjects

The following parameters allow you to define how to use the Management Server.

Table 77: Management Server Parameters

Name	Access	Description
msEnable	R/W	Enable/Disable the management server. - disable: No notification (SNMP trap) is sent to the management server. - enable: Notifications (SNMP traps) can be sent to the management server. Default Value: enable
msTrapRetransmissionPeriod	R/W	Retransmission period for the SNMP trap <i>msTrapConfigInformation</i> . The trap is retransmitted with this period until the management server replies or the <i>msTrapRetransmissionRetryCount</i> is reached. This value is expressed in milliseconds (ms). Default Value: 60000
msTrapRetransmissionRetryCount	R/W	Retransmission retry count for the SNMP trap <i>msTrapConfigInformation</i> . The trap is retransmitted until the management server replies or this retry count is reached. -1 = infinite (always retransmit) Default Value: 10

msEvents

The following are the events produced for the management server.

ms Notifications

The following are the management server notifications.

Table 78: Management Server Events – Notifications

Name	Access	Description
msTrapConfigInformation	N/A	The Management system is trapped with the sysObjectID, the MAC address and the request configuration of the Mediatrix unit (the Mediatrix unit requests a configuration from the Management system).
msTrapStatusInformation	N/A	The Management system is trapped with the MAC address and the configuration mode of the Mediatrix unit (the Mediatrix unit confirms its configuration mode modification).
msTrapStatusConfigFile	N/A	The Management system is trapped with the MAC address and the config file download status.

Configuration Parameters – Syslog MIB

This MIB describes the parameters used by the syslog messaging system.

syslogMIBObjects

Use the following parameter to define the level of Syslog information you want to use.

Table 79: Syslog Parameter

Name	Access	Description
syslogMsgMaxSeverity	R/W	This value indicates which syslog message will be processed. Any syslog message with a severity value greater than this value will be ignored by the agent. - disabled(0) - critical(1) - error(2) - warning(3) - informational(4) - debug(5) Default Value: informational
syslogMsgLocalMaxSeverity	R/W	This value indicates which syslog message will be processed by the local agent. Any syslog message with a severity value greater than this value will be ignored by the agent. - disabled(0) - critical(1) - error(2) - warning(3) - informational(4) - debug(5) Default Value: informational
syslogMsgLocalMaxNbr	R/W	This value indicates the maximum number of syslog messages handled by the local agent. If the local agent receives a new syslog message and the maximal number of message is reached, the oldest one is removed." Default Value: 0

syslogLocalMsgTable

This table holds the last *syslogMsgLocalMaxNbr* syslog sent by the unit.

Table 80: Syslog Parameter – Local Message Table

Name	Access	Description
syslogMsgLocalSeverity	R-O	Severity level of the syslog.
syslogMsgLocalTime	R-O	Time when the syslog occurred.
syslogMsgLocalModule	R-O	Module that sent the syslog.
syslogMsgLocalMsg	R-O	Syslog message.

syslogMsgCustomization

Use the following parameters to customize the way the syslog messages are sent.

Table 81: Syslog Parameter – Message Customization

Name	Access	Description
syslogMsgDisplayMacAddress	R/W	Enables/Disables displaying the unit's MAC address as part of the prefix for all syslog messages. - disable: The MAC address is not displayed in the prefix of the syslog messages. - enable: The MAC address is displayed in the prefix of the syslog messages. This affects only syslog messages sent on the network and not the local syslog messages. Default Value: disable
syslogMsgDisplayTime	R/W	Enables/Disables displaying the unit's current local time as part of the prefix for all syslog messages. - disable: The time is not displayed in the prefix of the syslog messages. - enable: The time is displayed in the prefix of the syslog messages. This affects only syslog messages sent on the network and not the local syslog messages. Default Value: enable
syslogMsgDisplayTimeFormat	R/W	Selects the timestamp format of the syslog messages. - trueRfcFormat: The timestamp complies with the RFC 3164 format. - pseudoRfcFormat: The timestamp uses a pseudo-RFC 3164 format. Timestamp in true RFC 3164 format: Jan 1 09:05:06 Timestamp in pseudo-RFC 3164 format: Jan 1 9:5:6 This applies only to syslog messages sent on the network and not the local syslog messages. Default Value: pseudoRfcFormat
syslogMsgDisplayLocalHost	R/W	Enables/Disables displaying the unit's current local host as part of the prefix for all syslog messages. - disable: The local host is not displayed in the prefix of the syslog messages. - enable : The local host is displayed in the prefix of the syslog messages. This affects only syslog messages sent on the network and not the local syslog messages. Default Value: enable

Configuration Parameters – qos MIB

This MIB provides configuration of Quality of Services field value.

qosMIBObjects

QoS information is broken down in two categories: Differentiated Service (DiffServ) and IEEE 802.1q.

qosDiffServ

The following parameters are used to define the DiffServ QoS information.

Table 82: QoS Parameters – DiffServ

Name	Access	Description
qosSignalingDiffServ	R/W	Signalling QoS Differentiated Services field value. Refer to the Quality of Service section of your Administration Manual for a detailed description. Default Value: 184
qosVoiceDiffServ	R/W	Voice QoS Differentiated Services field value. Refer to the Quality of Service section of your Administration Manual for a detailed description. Default Value: 184
qosT38FaxDiffServ	R/W	T38 QoS Differentiated Services field value. Refer to the Quality of Service section of your Administration Manual for a detailed description. Default Value: 184
qosVbdDiffServ	R/W	Voice-band data QoS Differentiated Services field value. Refer to the Quality of Service section of your Administration Manual for a detailed description. Default Value: 184

qosleee8021q

The following parameters are used to define the IEEE 802.1q QoS information.

Table 83: QoS Parameters – IEEE 802.1q

Name	Access	Description
qosSignalingleee8021qEnable	R/W	Enabling IEEE 802.1Q VLAN user priority tagging for VoIP signalling packet. This filter applies to any VoIP signalling protocol in use (e.g. MGCP or SIP). When the filter is disabled (as well as VLAN), no tag is added to the Ethernet header. Otherwise, each signalling packet is tagged with the user priority defined below. • disable(0) • enable(1) Default Value: disable

Table 83: QoS Parameters – IEEE 802.1q (Continued)

Name	Access	Description
qosSignalingIeee8021qUserPriority	R/W	IEEE 802.1Q VLAN user priority value for VoIP signalling packet. This value is used to set the user priority in the TCI field of the VLAN tag. Tagging user priority is applied only when the filter is enabled. In the case where the filter for signalling protocol is disabled and the VLAN option is enabled, the default user priority declared under the VLAN group will be used. Otherwise, the user priority set for signalling has precedence over the VLAN default user priority. 7 = High priority 0 = Low priority Default Value: 6
qosVoiceIeee8021qEnable	R/W	Enabling IEEE 802.1Q VLAN user priority tagging for VoIP packet. This filter applies to any VoIP voice protocol in use (e.g. RTP). When the filter is disabled (as well as VLAN), no tag is added to the Ethernet header. Otherwise, each signalling packet is tagged with the user priority defined below. - disable(0) - enable(1) Default Value: disable
qosVoiceIeee8021qUserPriority	R/W	IEEE 802.1Q VLAN user priority value for VoIP packet. This value is used to set the user priority in the TCI field of the VLAN tag. Tagging user priority is applied only when the filter is enabled. In the case where the filter for media protocol is disabled and the VLAN option is enabled, the default user priority declared under the VLAN group will be used. Otherwise, the user priority set for media has precedence over the VLAN default user priority. 7 = High priority 0 = Low priority Default Value: 6
qosT38FaxIeee8021qEnable	R/W	Enabling IEEE 802.1Q VLAN user priority tagging for T38 fax packet. When the filter is disabled (as well as VLAN), no tag is added to the Ethernet header. Otherwise, each signalling packet is tagged with the user priority defined below. - disable(0) - enable(1) Default Value: disable
qosT38FaxIeee8021qUserPriority	R/W	IEEE 802.1Q VLAN user priority value for T38 fax packet. This value is used to set the user priority in the TCI field of the VLAN tag. Tagging user priority is applied only when the filter is enabled. In the case where the filter for T38 protocol is disabled and the VLAN option is enabled, the default user priority declared under the VLAN group will be used. Otherwise, the user priority set for T38 has precedence over the VLAN default user priority. 7 = High priority 0 = Low priority Default Value: 6
qosVbdIeee8021qEnable	R/W	Enabling IEEE 802.1Q VLAN user priority tagging for voice-band data packet. This filter applies to any voice-band data protocol in use. When the filter is disabled (as well as VLAN), no tag is added to the Ethernet header. Otherwise, each signalling packet is tagged with the user priority defined below. - disable(0) - enable(1) Default Value: disable
qosVbdIeee8021qUserPriority	R/W	IEEE 802.1Q VLAN user priority value for voice-band data packet. This value is used to set the user priority in the TCI field of the VLAN tag. Tagging user priority is applied only when the filter is enabled. In the case where the filter for VBD protocol is disabled and the VLAN option is enabled, the default user priority declared under the VLAN group will be used. Otherwise, the user priority set for VBD has precedence over the VLAN default user priority. 7 = High priority 0 = Low priority Default Value: 6

qosVlanIeee8021q

Table 84: QoS Parameters – IEEE 802.1q (VLAN)

Name	Access	Description
qosVlanIeee8021qTaggingEnable	R/W	Enabling IEEE 802.1Q VLAN tagging. With this option enabled, all packets are tagged with the Virtual ID (VID) specified below. The default user priority is to be applied in case of general protocol or when signalling or media protocol filtering is disabled. WARNING: Enable this option only on compatible LAN with equipment supporting the VLAN tagging. Otherwise, the Unit may be unreachable. In this case, please use the reset button to access and disable VLAN tagging - in the reset mode, tagging is not permitted. See IEEE 802.1Q for more information on this topic. • disable(0) • enable(1) Default Value: disable
qosVlanIeee8021qVirtualLanID	R/W	IEEE 802.1Q Virtual LAN ID. This is the VID to be applied in the TCI field when tagging is enabled. The value 1 is the default Port VID (PVID) for bridge port. The 4095 VID (0xFFF) is reserved for implementation use and it shall not be used in tag header. Values can range from 1 to 4095 NOTE: As per standard, some bridges may not support the full range of VID. Default Value: 1
qosVlanIeee8021qDefaultUserPriority	R/W	IEEE 802.1Q Virtual LAN default user priority. This is the user priority to be applied in the TCI field when tagging is enabled. This value applies to all protocols for which no priority filtering is enabled (e.g. ARP, ICMP). • 7 = High priority • 0 = Low priority Default Value: 6

qosIeee8021qSubstitution

Table 85: QoS Parameters – IEEE 802.1q (VLAN) Substitution

Name	Access	Description
qosVlanIeee8021qSubstitutionEnable	R/W	Indicates whether the packets relayed from the LAN port to the WAN port will be tagged with the VLAN ID defined in the <i>qosVlanIeee8021qSubstitutionVlanID</i> variable. • enable : The QoS 802.1q fields of the packets sent from the LAN to the WAN are assigned the value defined in the <i>qosVlanIeee8021qSubstitutionVlanID</i> and <i>qosVlanIeee8021qSubstitutionUserPriority</i> variables. • disable: The QoS 802.1q fields of the packets sent from the LAN to the WAN are left as is. This variable's semantics are different depending on protocol and/or hardware platforms. The name of the LAN and WAN ports differ depending on the product. Please refer to the documentation shipped with your device for more details. Default Value: disable
qosVlanIeee8021qSubstitutionVlanID	R/W	The IEEE 802.1Q Virtual LAN ID applied when the variable <i>qosVlanIeee8021qSubstitutionEnable</i> is set to enable. The value 1 is the default Port VID (PVID) for bridge port. The 4095 VID (0xFFF) is reserved for implementation use and it must not be used in the tag header. Note: As per the standard, some bridges may not support the full range of VID. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 1
qosVlanIeee8021qSubstitutionUserPriority	R/W	IEEE 802.1Q Virtual LAN default user priority. This is the user priority applied when the variable <i>qosVlanIeee8021qSubstitutionEnable</i> is set to enable. This value applies to all protocols for which no priority filtering is enabled (e.g. ARP, ICMP). • 7 = High priority • 0 = Low priority This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 0

Table 85: QoS Parameters – IEEE 802.1q (VLAN) Substitution (Continued)

Name	Access	Description
qosVlanIeee8021qSubstitutionFiltering	R/W	Indicates whether packets sent to the Computer port will pass through the VLAN ID filtering. It is especially useful to restrain the broadcast domain between each port's subnet. It is applied when the variable <i>qosVlanIeee8021qSubstitutionEnable</i> is set to enable. - enable : Packets sent to the Computer port must have the right VLAN ID. Packets with a different VLAN ID, or untagged packets, will be dropped. - disable : Packets sent to the Computer port (tagged or not) with any tag are forwarded from the Network to the Computer port. This effectively extends the broadcast domain and allows nodes behind the computer port to share the same IP subnet as the unit itself. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable

qosInterop

Table 86: QoS Parameters – Interop

Name	Access	Description
qosInteropUseVoiceQoSForRtcpEnable	R/W	Indicates whether or not the configuration related with the voice QoS (<i>qosVoiceDiffServ</i> and <i>qosVoiceIeee8021qUserPriority</i> variables) is also applied to the RTCP packets generated by the device. - enable: The voice QoS configuration (<i>qosVoiceDiffServ</i> and <i>qosVoiceIeee8021qUserPriority</i> variables) is also applied to the RTCP packets. - disable: The RTCP packets are not tagged by the <i>qosVoiceDiffServ</i> and <i>qosVoiceIeee8021qUserPriority</i> variables. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable

Configuration Parameters – Telephony MIB

This MIB provides telephony-specific settings.

telephonyMIBObjects

The following parameters allow you to define the signalling protocol to use in the unit and the country where it is located.

Table 87: Telephony Parameters

Name	Access	Description
telephonyIpSignalingProtocolSelection	R/W	The signalling protocol which will be used by the endpoints. - mgcp(1): Media Gateway Control Protocol. - sip(2): Session Initiation Protocol. - ncs(3): PacketCable Network-based Call Signalling protocol. - h323(4) : Packet-Based Multimedia Communications Systems - proprietary(99): Proprietary signaling protocol When '<i>proprietary</i>' is selected, the name of the proprietary signaling protocol is available through the <i>telephonyIpSignalingProtocolProprietary</i> variable. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: mgcp
telephonyIpSignalingProtocolProprietary	R-O	Name of the proprietary signaling protocol used by the endpoint. This variable is meaningful only if the <i>telephonyIpSignalingProtocolSelection</i> variable was previously set to '<i>proprietary</i>'. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.

Table 87: Telephony Parameters (Continued)

Name	Access	Description
telephonyCountrySelection	R/W	The country selection permits the selection of predefined country settings for the tone profiles, the ring patterns and other parameters such as input and output gains. For some countries, the caller ID standard can be selected with this variable. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the Administration Manual shipped with your device for more details. • northAmerica1(1) • northAmerica2(2) • austria(3) • france(4) • germany1(5) • germany2(6) • uk(7) • italy(8) • spain(9) • switzerland(10) • sweden(11) • australia1(12) • japan(13) • israel(14) • thailand(15) • indonesia(16) • australia2(12) • china(18) • hongKong(19) • malaysia(20) • russia(21) • netherlands(22) • brazil(23) • mexico(25) • denmark(26) • australia3(27) • newZealand(28) • austria2(29) • germany3(30) • czechRepublic(31) • chile1(32) • chile2(33) • uae2(34) • uk-bellcore(100) • uk-cca(101) • uk-etsi-fsk(102) • france-etsi-fsk(110) • france-etsi-dtmf(111) • austria-etsi-fsk(120) • austria2-etsi-fsk(130) Default Value: northAmerica1

countryCustomizationToneGroup

countryCustomizationToneTable

This table allows to override the default country tone configuration. The configuration applies to all interfaces.

Table 88: Customization Tone Parameters

Name	Access	Description
countryCustomizationToneTone	R/W	Tone to customize. • busy (100) • confirmation (200) • congestion(300) • dial(400) • intercept (600) • messageWaiting (700) • preemption(800) • reorder(900) • ringback (1000) • roh(1100) • sit (1200) • stutter(1300)
countryCustomizationToneOverride	R/W	Allows overriding of the default country tone setting. • disable: The unit uses the default country tone setting. • enable: The unit uses the tone configuration contained in the associated <i>countryCustomizationTonePattern</i> variable. Default Value: disable
countryCustomizationTonePattern	R/W	Description string for the custom tone. Only in effect when the corresponding <i>countryCustomizationToneOverride</i> variable is set to 'enable'. See the documentation for a description of the syntax.

Configuration Parameters – voicelf MIB

This MIB provides information to configure voice interface (such as analog line, etc.) on a per interface basis.

voicelfMIBObjects

The following parameters allow you to define voice parameters.

Table 89: Voice Interface Parameters

Name	Access	Description
voicelfAllowDtmfOobRecovery	R/W	Allows faster recovery when playing back an out-of-band DTMF whose end bit has not been received. - disable: The DTMF stops playing after 700 RTP packets are received (~7-60 seconds). - enable: The DTMF stops playing after 10 RTP packets are received (~1 second). This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: disable

voicelfTable

A table of configuration for each voice over IP interface. The parameters are defined in a table called *voicelfTable*.

Table 90: Voice Interface – voicelfTable

Name	Access	Description
voicelfAdaptativeJitterBufferEnable	R/W	Jitter is an abrupt and unwanted variation of one or more signal characteristics, such as the interval between successive pulses, or the frequency or phase of successive cycles. An adaptive jitter buffer usually consists of an elastic buffer in which the signal is temporarily stored and then retransmitted at a rate based on the average rate of the incoming signal. - disable(0) - enable(1) Default Value: enable
voicelfTargetJitterBufferLength	R/W	The adaptive jitter buffer attempts to hold packets to the target holding time. This is the minimum delay the jitter buffer adds to the system. The target jitter buffer length is in ms. The target jitter buffer MUST be equal to or smaller than maximum jitter buffer. Default Value: 30
voicelfMaxJitterBufferLength	R/W	This is the maximum jitter the adaptive jitter buffer can handle. The jitter buffer length is in ms. The maximum jitter buffer MUST be equal to or greater than the target jitter buffer. The maximum jitter buffer length allowed on some Medatrix products is smaller than 300 ms. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 125

Table 90: Voice Interface – voicelfTable (Continued)

Name	Access	Description
voicelfG711VoiceActivityDetectionEnable	R/W	If Voice Activity Detection (VAD) is enabled, then speech frames are only sent during talkspurts (periods of audio activity). During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent (c.f. RFC3389). This variable specifies the sensitivity of the VAD algorithm to silence periods. Note that this setting will also be applied in case G.726 is enabled. • disable: VAD disabled • transparent: VAD enabled - low sensitivity to silence period) • conservative: VAD enabled - normal sensitivity to silence period Default Value: conservative
voicelfEchoCancellationEnable	R/W	An echo is a signal that has been reflected or otherwise returned with sufficient magnitude and delay to be perceived. The echo cancellation is usually an active process in which echo signals are measured and cancelled or eliminated by combining an inverted signal with the echo signal. • disable: The DSP does not use echo cancellation on the related port. • enable: The default state. The DSP proceeds to cancel signals that are recognized as echo when appropriate. Default Value: enable
voicelfG711ComfortNoiseGenerationEnable	R/W	During silence periods, Comfort Noise (CN) packets containing information about background noise may be received (c.f. RFC3389). If Comfort Noise Generation (CNG) is enabled, then those packets are used to generate local comfort noise. This variable specifies the type of this comfort noise. Changing this variable requires a reboot of the unit in order to take effect. Note that this setting will also be applied in case G.726 is enabled. Note that G.723 and G.729 CNG is not configurable because it is built-in in the codec, while it is generic in G.711 and G.726. • disable: CNG disabled • whiteNoise: CNG enabled - white noise • customNoise: CNG enabled - custom noise (better) Default Value: customNoise
voicelfBaseGainConfigurationSource	R/W	This object is deprecated. This means some agents may implement it and some agents may not implement it. Specify how the base gain is configured. • useCustomConfiguration(0) • useDefaultCountryConfiguration(1) Note: When using the custom configuration, you must set the following variables: • voicelfBaseInputGain • voicelfBaseOutputGain • voicelfBaseInputGainOffset • voicelfBaseOutputGainOffset Warning: Custom configuration should be used with care. Default Value: useDefaultCountryConfiguration
voicelfUserInputGainOffset	R/W	The user input gain offset is added to the base input gain to compute the total input gain. The user input gain is in dB. Valid input gain range is between -30 dB and 20 dB. Default Value: 0
voicelfUserOutputGainOffset	R/W	The user output gain offset is added to the base output gain to compute the total output gain. The user output gain is in dB. Valid output gain range is between -30 dB and 20 dB. Default Value: 0
voicelfBaseInputGain	R/W	This object is deprecated. This means some agents may implement it and some agents may not implement it. The base input gain. This is an absolute value which is used in conjunction with the user input gain and the base input gain offset to compute the total input gain. Default Value: 5785
voicelfBaseOutputGain	R/W	This object is deprecated. This means some agents may implement it and some agents may not implement it. The base output gain. This is an absolute value which is used in conjunction with the user output gain and the base output gain offset to compute the total output gain. Default Value: 2052

Table 90: Voice Interface – voicelfTable (Continued)

Name	Access	Description
voicelfBaseInputGainOffset	R/W	This object is deprecated. This means some agents may implement it and some agents may not implement it. The base input gain offset. This value is used in the calibration to adjust the total input gain to an offset in dB from the base input gain. This value is in dB. Default Value: 0
voicelfBaseOutputGainOffset	R/W	This object is deprecated. This means some agents may implement it and some agents may not implement it. The base output gain offset. This value is used in the calibration to adjust the total output gain to an offset in dB from the base output gain. This value is in dB. Default Value: 0
voicelfNlpThresholdLevel	R/W	This object is deprecated. This means some agents may implement it and some agents may not implement it. The echo cancellation NLP threshold level. 0 : Strongest echo cancellation, weakest double-talk detection. 4 : Weakest echo cancellation, strongest double-talk detection. Increase the value if cuts in the voice stream are present, decrease it if too much echo can be heard. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 0
voicelfG729VoiceActivityDetectionEnable	R/W	If Voice Activity Detection (VAD) is enabled, then speech frames are only sent during talkspurts (periods of audio activity). During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent in accordance with annex B of G.729. - disable: G.729 uses annex A only - enable: G.729 annex A is used with annex B Default Value: enable
voicelfG723VoiceActivityDetectionEnable	R/W	If Voice Activity Detection (VAD) is enabled, then speech frames are only sent during talkspurts (periods of audio activity). During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent in accordance with annex A of G.723.1. - disable: G.723.1 is used without annex A - enable: G.723.1 is used with annex A This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: enable
voicelfSignalLimiterLevel	R/W	When enabled, the Signal Limiter attenuates or removes peaks in voice signal. This may reduce the presence of echo but may impair DTMF detection because of signal distortion. 0: Disable Signal Limiter 1: Most aggressive ... 5: Least aggressive This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 0

voicelfCodecTable

The *voicelfCodecTable* table holds the parameters that define the codecs used.

Table 91: Voice Interface – voicelfCodecTable

Name	Access	Description
voicelfCodecPreferred	R/W	Indicates the preferred type of codec for voice transmission. If the selected codec is disabled, this preferred type of codec will be ignored. - pcmu(1) - pcma(2) - g723(3) - g729(4) - g726-16kbps(5) - g726-24kbps(6) - g726-32kbps(7) - g726-40kbps(8) This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: pcmu
voicelfCodecPcmuEnable	R/W	Indicates if the codec can be selected for voice transmission. If enabled, this codec will be listed as supported for this specific endpoint. Otherwise, it will be ignored. - disable(0) - enable(1) Default Value: enable
voicelfCodecPcmuMinPTime	R/W	Shortest packetization period allowed for the PCMU codec. Expressed in milliseconds. Authorized values start at 10 and come in discrete steps of 10 ms up to the one specified by variable <i>voicelfCodecPcmuMaxPTime</i> . This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 10
voicelfCodecPcmuMaxPTime	R/W	Longest packetization period allowed for the PCMU codec. Expressed in milliseconds. Authorized values go up to 100, in discrete steps of 10 ms, and start at the one specified by variable <i>voicelfCodecPcmuMinPTime</i> . This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 100
voicelfCodecPcmaEnable	R/W	Indicates if the codec can be selected for voice transmission. If enabled, this codec will be listed as supported for this specific endpoint. Otherwise, it will be ignored. - disable(0) - enable(1) Default Value: enable
voicelfCodecPcmaMinPTime	R/W	Shortest packetization period allowed for the PCMA codec. Expressed in milliseconds. Authorized values start at 10 and come in discrete steps of 10 ms up to the one specified by variable <i>voicelfCodecPcmaMaxPTime</i> . This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 10
voicelfCodecPcmaMaxPTime	R/W	Longest packetization period allowed for the PCMA codec. Expressed in milliseconds. Authorized values go up to 100, in discrete steps of 10 ms, and start at the one specified by variable <i>voicelfCodecPcmaMinPTime</i> . This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 100
voicelfCodecG723Enable	R/W	Indicates if the codec can be selected for voice transmission. If not disabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored. - disable: Disable G.723 - g723-53kbs: Use G.723 at 5.3 kbps - g723-63kbs: Use G.723 at 6.3 kbps This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: g723-63kbs

Table 91: Voice Interface – voicellCodecTable (Continued)

Name	Access	Description
voicellCodecG723MinPTime	R/W	Shortest packetization period allowed for the G.723 codec. Expressed in milliseconds. Authorized values start at 30 and come in discrete steps of 30 ms up to the one specified by variable <i>voicellCodecG723MaxPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 30
voicellCodecG723MaxPTime	R/W	Longest packetization period allowed for the G.723 codec. Expressed in milliseconds. Authorized values go up to 120, in discrete steps of 30 ms, and start at the one specified by variable <i>voicellCodecG723MinPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 120
voicellCodecG729Enable	R/W	Indicates if the codec can be selected for voice transmission. If enabled, this codec will be listed as supported for this specific endpoint. Otherwise, it will be ignored. • disable(0) • enable(1) Default Value: enable
voicellCodecG729MinPTime	R/W	Shortest packetization period allowed for the G.729 codec. Expressed in milliseconds. Authorized values start at 10 and come in discrete steps of 10 ms up to the one specified by variable <i>voicellCodecG729MaxPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 10
voicellCodecG729MaxPTime	R/W	Longest packetization period allowed for the G.729 codec. Expressed in milliseconds. Authorized values go up to 100, in discrete steps of 10 ms, and start at the one specified by variable <i>voicellCodecG729MinPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 100
voicellCodecG72616kbpsEnable	R/W	Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored. Note that if G.726 at 16 kbps is enabled, voice activity detection and comfort noise generation can be controlled via the <i>voicellG711VoiceActivityDetectionEnable</i> and <i>voicellG711ComfortNoiseGenerationEnable</i> variables. • disable: Disable G.726 at 16 kbps • enable: Enable G.726 at 16 kbps This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: disable
voicellCodecG72616kbpsPayloadType	R/W	When enabling G.726 at 16 kbps for voice transmission, this variable determines the actual RTP dynamic payload type used in an initial offer. The payload types available are as per RFC 3551. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 97
voicellCodecG72616kbpsMinPTime	R/W	Shortest packetization period allowed for the G.726-16kbps codec. Expressed in milliseconds. Authorized values start at 10 and come in discrete steps of 10 ms up to the one specified by variable <i>voicellCodecG72616kbpsMaxPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 10
voicellCodecG72616kbpsMaxPTime	R/W	Longest packetization period allowed for the G.726-16kbps codec. Expressed in milliseconds. Authorized values go up to 100, in discrete steps of 10 ms, and start at the one specified by variable <i>voicellCodecG72616kbpsMinPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 100

Table 91: Voice Interface – voicelfCodecTable (Continued)

Name	Access	Description
voicelfCodecG72624kbpsEnable	R/W	Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored. Note that if G.726 at 24 kbps is enabled, voice activity detection and comfort noise generation can be controlled via the <i>voicelfG711VoiceActivityDetectionEnable</i> and <i>voicelfG711ComfortNoiseGenerationEnable</i> variables. - disable: Disable G.726 at 24 kbps - enable: Enable G.726 at 24 kbps This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: disable
voicelfCodecG72624kbpsPayloadType	R/W	When enabling G.726 at 24 kbps for voice transmission, this variable determines the actual RTP dynamic payload type used in an initial offer. The payload types available are as per RFC 3551. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 98
voicelfCodecG72624kbpsMinPTime	R/W	Shortest packetization period allowed for the G.726-24kbps codec. Expressed in milliseconds. Authorized values start at 10 and come in discrete steps of 10 ms up to the one specified by variable <i>voicelfCodecG72624kbpsMaxPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 10
voicelfCodecG72624kbpsMaxPTime	R/W	Longest packetization period allowed for the G.726-24kbps codec. Expressed in milliseconds. Authorized values go up to 100, in discrete steps of 10 ms, and start at the one specified by variable <i>voicelfCodecG72624kbpsMinPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 100
voicelfCodecG72632kbpsEnable	R/W	Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored. Note that if G.726 at 32 kbps is enabled, voice activity detection and comfort noise generation can be controlled via the <i>voicelfG711VoiceActivityDetectionEnable</i> and <i>voicelfG711ComfortNoiseGenerationEnable</i> variables. - disable: Disable G.726 at 32 kbps - enable: Enable G.726 at 32 kbps This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: disable
voicelfCodecG72632kbpsPayloadType	R/W	When enabling G.726 at 32 kbps for voice transmission, this variable determines the actual RTP dynamic payload type used in an initial offer. The payload types available are as per RFC 3551. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 99
voicelfCodecG72632kbpsMinPTime	R/W	Shortest packetization period allowed for the G.726-32kbps codec. Expressed in milliseconds. Authorized values start at 10 and come in discrete steps of 10 ms up to the one specified by variable <i>voicelfCodecG72632kbpsMaxPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 10
voicelfCodecG72632kbpsMaxPTime	R/W	Longest packetization period allowed for the G.726-32kbps codec. Expressed in milliseconds. Authorized values go up to 100, in discrete steps of 10 ms, and start at the one specified by variable <i>voicelfCodecG72632kbpsMinPTime</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 100

Table 91: Voice Interface – voicelfCodecTable (Continued)

Name	Access	Description
voicelfCodecG72640kbpsEnable	R/W	Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored. Note that if G.726 at 40 kbps is enabled, voice activity detection and comfort noise generation can be controlled via the <i>voicelfG711VoiceActivityDetectionEnable</i> and <i>voicelfG711ComfortNoiseGenerationEnable</i> variables. - disable: Disable G.726 at 40 kbps - enable: Enable G.726 at 40 kbps This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: disable
voicelfCodecG72640kbpsPayloadType	R/W	When enabling G.726 at 40 kbps for voice transmission, this variable determines the actual RTP dynamic payload type used in an initial offer. The payload types available are as per RFC 3551. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 100
voicelfCodecG72640kbpsMinPTime	R/W	Shortest packetization period allowed for the G.726-40kbps codec. Expressed in milliseconds. Authorized values start at 10 and come in discrete steps of 10 ms up to the one specified by variable <i>voicelfCodecG72640kbpsMaxPTime</i> . This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 10
voicelfCodecG72640kbpsMaxPTime	R/W	Longest packetization period allowed for the G.726-40kbps codec. Expressed in milliseconds. Authorized values go up to 100, in discrete steps of 10 ms, and start at the one specified by variable <i>voicelfCodecG72640kbpsMinPTime</i> . This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 100

voicelfDtmfTransportTable

A table of configuration for each voice over IP interface. The parameters are defined in a table called *voicelfDtmfTransportTable*.

Table 92: Voice Interface – voicelfDtmfTransportTable

Name	Access	Description
voicelfDtmfTransport	R/W	Type of DTMF transport. If <i>signalingProtocolDependent</i> is selected, the signaling protocol has the control to select the DTMF transport mode. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. - inBand(0) - outOfBandUsingRtp(1) - outOfBandUsingSignalingProtocol(2) Default Value: inBand
voicelfDtmfPayloadType	R/W	When selecting <i>outOfBandUsingRtp(1)</i> as DTMF transport mode (see variable <i>voicelfDtmfTransport</i>), this variable determines the actual RTP dynamic payload type used for telephone-event in an initial offer. The payload types available are as per RFC 1890. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 96

Table 92: Voice Interface – voicelfDtmfTransportTable (Continued)

Name	Access	Description
voicelfDtmfEnforceDefaultEvents	R/W	This variable is used when a deliberate deviance to RFC 2833 is required. When enabled, conformance is enforced and support for RFC 2833 will imply the support of basic telephony-events. When setting the variable <i>voicelfDtmfTransport</i> to <i>outOfBandUsingRtp</i>, or the variable <i>telephonyAttributesHookFlashProcessing</i> to <i>outOfBandUsingRtp</i>, the unit will advertise the support for events 0-15; it will assume support for events 0-15 when support for RFC 2833 is received in an announcement. When disabled, support of basic events is not automatic. The variables <i>voicelfDtmfTransport</i> and <i>telephonyAttributesHookFlashProcessing</i> then act independently to specify which events will be relayed via RFC 2833. If Hook Flash relay is enabled by itself, support of event 16 alone will be advertised; if both Hook Flash and DTMF relay are activated, events 0-16 are supported. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: enable

voicelfDtmfDetectionTable

This table holds DTMF detection parameters indexed by endpoint number..

Table 93: Voice Interface – voicelfDtmfDetectionTable

Name	Access	Description
voicelfDtmfDetectionRiseTimeCriteria	R/W	Defines how the Rise Time criteria should be configured for DTMF detection. - checkSr: Enable the Step Rise criteria and disable the Confirm DTMF SNR criteria. - confirmSnr: Enable the Confirm DTMF SNR criteria and disable the Step Rise criteria. The Step Rise criteria compares the current frame energy to the high frequency power of the previous frame. If the current frame energy is high enough, then it passes the test, further validating the DTMF. Disabling the Step Rise criteria may result in deteriorated talk-off performance, but increases the detection of malformed DTMF. The Confirm DTMF SNR criteria is an additional Signal-to-noise ratio test performed before a confirmed DTMF report is sent to finally validate the DTMF. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: confirmSnr
voicelfDtmfDetectionMaxPowerThreshold	R/W	Maximum absolute power threshold (dBm0) for off-on transition of a DTMF. Raising this value increases the sensitivity of the DTMF detection. Raising this value too high may also cause false detections of DTMFs. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 1
voicelfDtmfDetectionMinPowerThreshold	R/W	Minimum absolute power threshold (dBm0) for off-on transition of a DTMF. Raising this value reduces the sensitivity to DTMF detection. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: -30
voicelfDtmfDetectionBreakPowerThreshold	R/W	Break absolute power threshold (dBm0) for on-off transition of a DTMF. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: -32
voicelfDtmfDetectionPositiveTwist	R/W	When the high-group frequency of a DTMF is more powerful than the low-group frequency, the difference between the high-group frequency absolute power and the low-group frequency absolute power must be smaller than or equal to the value set in this variable. Otherwise, the DTMF is not detected. Raising this value increases the sensitivity of DTMF detection. Raising this value too high may also cause false detections of DTMFs. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 6

Table 93: Voice Interface – voicelfDtmfDetectionTable (Continued)

Name	Access	Description
voicelfDtmfDetectionNegativeTwist	R/W	When the low-group frequency of a DTMF is more powerful than the high-group frequency, the difference between the low-group frequency absolute power and the high-group frequency absolute power must be smaller than or equal to the value set in this variable. Otherwise, the DTMF is not detected. Raising this value increases the sensitivity of DTMF detection. Raising this value too high may also cause false detections of DTMFs. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 9
voicelfDtmfDetectionMinDuration	R/W	Defines the minimum duration a DTMF must last to be detected. A DTMF whose duration is less than the configured value is not detected. A higher value may help prevent false DTMF detection. However, increasing the minimum duration can impact jitter if voicelfDtmfTransport is configured for out-of-band DTMF. This value is expressed in milliseconds. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 30

Configuration Parameters – dataIf MIB

This MIB provides information to configure data interface (such as T38, Fax, etc.) on a per interface basis.

dataIfMIBObjects

The following parameters allow you to define data information.

Table 94: T.38 Base Port Parameter

Name	Access	Description
dataIfT38BasePort	R/W	T.38 base port. The T.38 ports are allocated starting from this base port. The units use as many T.38 ports as the number of FXS/FXO interfaces. E.g.: let's say for instance that a unit has two FXS interfaces and the base port is defined on 6004: - if there is currently no ongoing call and FXS connector 1 has an incoming or outgoing call, it will use the T.38 port 6004. - if there is currently a call on FXS connector 1 and FXS connector 2 has an incoming or outgoing call, then FXS connector 2 will use the T.38 port 6005. Default Value: 6004
dataIfT38FinalFramesRedundancy	R/W	Defines the number of times T.38 packets will be retransmitted. This only applies to the T.38 packets where the PrimaryUDPTL contains the following T.38 data type: - HDLC_SIG_END, - HDLC_FCS_OK_SIG_END, - HDLC_FCS_BAD_SIG_END and - T4_NON_ECM_SIG_END Please see dataIfCodecT38ProtectionLevel for standard T.38 reliability options. Default Value: 0
dataIfT38NoSignalEnable	R/W	Enable/disable the sending of T.38 no-signal packets. When enabled, the unit will ensure that, during a T.38 fax transmission, data is sent out at least every time the <i>dataIfT38NoSignalTimeout</i> delay expires. In the absence of meaningful data to send, no-signal packets are output. Default Value: disable
dataIfT38NoSignalTimeout	R/W	The period, in seconds, at which no-signal packets are sent during a T.38 transmission, in the absence of valid data. The maximum value is 2147483647 seconds. Default Value: 1

dataIfTable

Table that contains data interface configuration parameters.

Table 95: Data Interface Parameters

Name	Access	Description
dataIfCngToneDetectionEnable	R/W	Enables fax calling tone (CNG tone) detection. - enable: Upon recognition of the CNG tone, the unit switches the communication from voice mode to fax mode and the CNG is transferred using the preferred fax codec. NOTE: This option allows for quicker fax detection, but it also increases the risk of false detection. - disable: The CNG tone does not trigger a transition from voice to data and the CNG is transferred in the voice channel. NOTE: With this option, faxes are detected later, but the risk of false detection is reduced. Default Value: enable
dataIfCedFaxToneEnable	R/W	Defines the behaviour of the unit upon reception of a CED fax tone from the network. - enable: Upon reception of a CED tone following a sent CNG tone, the unit switches the communication from voice mode to fax mode and the CED is transferred by using the preferred fax codec. - disable: The CED tone does not trigger a transition from voice to data and the CED is transferred in the voice channel. This configuration has no effect if the <i>dataIfCngToneDetectionEnable</i> variable is set to Enable. Default Value: disable
dataIfAnalogCedDetectionBehavior	R/W	Defines the behaviour of the unit upon reception of a CED fax tone from the analog port. - passthrough: In passthrough mode the CED tone does not trigger a transition from voice to data and is transferred in the voice channel. Use this setting when any kind of analog device (i.e.: telephone, fax or modem) can be connected to this port. - faxmode: In 'fax mode', upon reception of a CED tone the unit switches the communication from voice mode to fax mode and the CED is transferred by using the preferred fax codec. Only a fax can then be connected to this port. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: passthrough

dataIfCodecTable

Table that contains data interface configuration parameters.

Table 96: Data Interface Parameters

Name	Access	Description
dataIfCodecMediaTypeImageEnable	R/W	- disable: image media type is not present in the SDP. - pcmu: image media type is present in the SDP for PCMU only. - pcma: image media type is present in the SDP for PCMA only. - pcmu-pcma: image media type is present in the SDP for PCMU and PCMA. - g726: image media type is present in the SDP for G.726 only. - pcmu-g726: image media type is present in the SDP for PCMU and G.726. - pcma-g726: image media type is present in the SDP for PCMA and G.726. - pcmu-pcma-g726: image media type is present in the SDP for PCMU, PCMA and G.726. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Note: The G.726 flavours supported in the media type image are G.726-32 and G.726-40. G.726-16 and G.726-24 will not appear in the media type image. Default Value: pcmu-pcma

Table 96: Data Interface Parameters (Continued)

Name	Access	Description
dataIffClearChannelCodecPreferred	R/W	Indicates the preferred clear channel type of codec for fax transmission. This variable increases the relative priority of the selected codec vs other data-capable codecs. However, the priority of the preferred data codec remains lower than the preferred Voice codec. When no data-capable codec is part of the list of negotiated codecs, this variable indicates which codec to use when fax or modem tones are detected. If the negotiated voice codec is data-capable, it is be used for data instead of the preferred data codec. Note: When <i>noPreferredCodec</i> is selected and no data-capable codecs are negotiated, data transmission may fail. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. • pcmu(1) • pcma(2) • g726-32kbs(5) • g726-40kbs(6) • noPreferredCodec(7) Default Value: pcmu
dataIffCodecT38Enable	R/W	If enabled, T38 protocol will be used for Fax transmission. • disable(0) • enable(1) This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: enable
dataIffCodecT38ProtectionLevel	R/W	The number of redundancy packets. This is the standard redundancy offered by T.38. Please see dataIffT38FinalFramesRedundancy for additional reliability options for T.38. Available values are between 1 and 5. Default Value: 3

Configuration Parameters – fxs MIB

This MIB provides Foreign eXchange Station (FXS) parameters.

fxsMIBObjects

Use the following parameters to define how to use the FXS interfaces of the unit.

Table 97: FXS Parameters

Name	Access	Description
fxsByPassEnable	R/W	Enables the bypass service. - disable: The port with the bypass service is never redirected on the bypass line. - enable: When the port with the bypass service is unusable (<i>ifAdminUsageState</i> is idle-unusable), it will be redirected to the bypass line. When this port becomes usable again (<i>ifAdminUsageState</i> is idle), the redirection is stopped within 10 seconds if the bypass line is unused or 10 seconds after the termination of the call. NOTE: The control of the bypass service is only possible when the unit is powered on. When power is off, the bypass service is always enabled. Default Value: enable
fxsLoopCurrent	R/W	Current that flows through the current detector that permits the detection of the on-hook and off-hook states. The loop current is in mA. Some hardware platforms may support less than the available range. Please refer to the documentation shipped with your device for more details. Default Value: 30
fxsFlashHookDetectionDelayMin	R/W	Minimum time in ms the hook switch must remain pressed to perform a flash hook. Default Value: 100
fxsFlashHookDetectionDelayMax	R/W	Maximum time in ms the hook switch can remain pressed to perform a flash hook. Default Value: 1200
fxsLoopCurrentDropEnable	R/W	Instructs the FXS unit to suppress loop current on its ports when they cannot be used or when the IP connection is lost. - disable: Loop current is unaffected by the port usability. - enable: Loop current is interrupted on the port as soon as it enters an unusable state, or if the unit's IP network connection is lost. Default Value: disable
fxsCalleeHangupSupervision	R/W	Determines whether call clearing occurs as soon as the called user is the first to hang up a received call. This variable has no effect when the user acts as the calling party. - disable: The unit signals the end of the call as soon as the user hangs up. - enable: When the user is the first to hang up on a received call, the unit waits for the amount of time provisioned in the <i>fxsCalleeHangupDelay</i> variable before signaling the end of the call. Default Value: disable

Table 97: FXS Parameters (Continued)

Name	Access	Description
fxsCalleeHangupDelay	R/W	The amount of time, in seconds, the unit waits after the called user hangs up before signaling the end of the call. This delay is effective only when the <i>fxsCalleeHangupSupervision</i> variable is enabled and the user is the called party. When the user acts as the calling party, the call ends as soon as the user hangs up. Default Value: 60
fxsReversalOnIdleEnable	R/W	This object is deprecated. Therefore, agents may or may not implement it. Use <i>fxsPolarityAndDenialBehavior</i> instead. The Reversal on Idle feature is used because of an inability by some customer's CPE to react to busy tone. This problem can be overcome by applying polarity reversal when the circuit is not busy. The reversal allows the CPE to effect release of a circuit under line lockout conditions or the other party clearing. When a customer's line is in the idle, line lockout or blocked state, the polarity of the customer's line is reversed. When the customer's line is seized to originate a call, or ring current is applied to terminate a call, the line polarity is returned to normal. On release, line polarity is returned to the reversed condition. When activated, this feature replaces the default behaviour of the unit which is to briefly remove power from the line to signal that the remote party has hung up. • disable: Do not perform line reversal when the line enters the idle condition. • enable: Activates the Reversal on Idle feature as described above. Default Value: disable
fxsPolarityAndDenialBehavior	R/W	Determines how the line polarity is used to signal the beginning and end of a call. • noReversal: Polarity reversal is not used. A short power drop is made at the end of a call when the call is disconnected by the remote party. The drop duration can be configured in the variable <i>fxsPowerDropOnDisconnectDuration</i>. • reversalOnIdle: Activates the Reversal on Idle feature. When a customer's line is in the idle, line lockout or blocked state, the polarity of the customer's line is reversed. When the customer's line is seized to originate a call, or the ring current is applied to terminate a call, the line polarity is returned to normal. On release, the line polarity is returned to the reversed condition. • reversalOnEstablished: Activates the Reversal on Established option. The polarity remains normal (voltage on the phone line stays positive) when you pick up the phone, dial, and when the device is ringing. As soon as the other party picks up the phone, the unit reverses the line polarity. When the unit receives a hang-up signal or the caller hangs up the phone, the voltage returns to its positive state. Default Value: noReversal
fxsPowerDropOnDisconnectDuration	R/W	Determines the power drop duration that is made at the end of a call when the call is disconnected by the remote party. This value is expressed in milliseconds (ms). This variable only has an effect when the variable <i>fxsPolarityAndDenialBehavior</i> is set to 'noReversal'. Default Value: 1000
fxsBlankAnonymousCallerId	R/W	Instructs the FXS unit to blank out the name portion of the received caller ID whenever 'anonymous' (case insensitive) is used to identify the originator of the call. • disable: The anonymous string is passed on to the telephone and displayed to identify the calling party. • enable: The anonymous string is blanked out before caller ID data is sent to the telephone. Default Value: disable
fxsFskMarkoutBits	R/W	Determines the number of markout bits that are added after the checksum in FSK signals sent to the phone when it's on hook. The Bellcore 202 standard specifies that there can be up to 5280 bits. The ETSI doesn't specify any markout bits. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 200
fxsCallingNumberCriteria	R/W	Expression that the calling number must match in order to apply the transformation specified in <i>fxsCallingNumberTransformation</i>. The criteria must be a regular expression.

Table 97: FXS Parameters (Continued)

Name	Access	Description
fxsCallingNumberTransformation	R/W	Transformation applied on the calling number if it matches the expression specified in <i>fxsCallingNumberCriteria</i> . '\0' to '\9' are replaced by the corresponding group in the regular expression specified in <i>fxsCallingNumberCriteria</i> .

fxsEpSpecificLoopCurrentTable

Table that contains loop current configuration indexed by endpoint number..

Table 98: Specific Loop Current Parameters

Name	Access	Description
fxsEpSpecificLoopCurrentOverrideEnable	R/W	Defines whether or not a specific loop current configuration must be used for this endpoint. - disable: The endpoint loop current configuration is defined by the variable <i>fxsLoopCurrent</i>. - enable: The endpoint loop current configuration is defined by the variable <i>fxsEpSpecificLoopCurrentOverride</i> and the value in <i>fxsLoopCurrent</i> is ignored. Default Value: disable
fxsEpSpecificLoopCurrentOverride	R/W	Current flowing through the current detector that permits the detection of the on-hook and off-hook states. The loop current is in mA. Some hardware platforms may support less than the available range. Please refer to the documentation shipped with your device for more details. Default Value: 30

fxsEmergencyBypass

Use the following parameters to define how to use the FXS emergency bypass of the unit.

Table 99: FXS Parameters

Name	Access	Description
fxsEmergencyBypassEnable	R/W	Enables/Disables bypass for emergency calls. - disable: Bypass for emergency calls is disabled. - enable: Bypass for emergency calls is enabled. If dialed digits match those defined in the <i>fxsEmergencyBypassDialMap</i> variable, the unit switches to bypass mode and makes the call on the PSTN side. Note that the bypass functionality only applies for digits dialed on FXS port 1. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable
fxsEmergencyBypassTimeout	R/W	Indicates how long the unit will stay in bypass mode waiting for an incoming call after the outgoing call on the PSTN side is finished. This value is expressed in seconds (s). Default Value: 120
fxsEmergencyBypassDialMap	R/W	A string composing a digit map that will be considered valid to make the unit switch to bypass mode. The string must follow the syntax described in the <i>digitMapMIB</i> entry description.
fxsEmergencyBypassDialDelay	R/W	Indicates how long the unit will wait before playing emergency digits on the PSTN side once in bypass mode. This value is expressed in seconds (s). This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 3

Configuration Parameters – Digit Maps MIB

This MIB is used to configure digit maps for all endpoints of the unit. A digit map is a sequence of digits that is acceptable (or unacceptable) for calling. For instance, the digit map “xx” will accept any two dialed numbers as a valid digit map.

The permitted digit map syntax is taken from the core MGCP specification, RFC2705: <ftp://ftp.isi.edu/in-notes/rfc2705.txt>, section 3.4.

```
DigitMap = DigitString / '(' DigitStringList ')'
DigitStringList = DigitString 0* ( '|' DigitString )
DigitString = 1*(DigitStringElement)
DigitStringElement = DigitPosition ['.']
DigitPosition = DigitMapLetter / DigitMapRange
DigitMapLetter = DIGIT / '#' / '*' / 'A' / 'B' / 'C' / 'D' / 'T'
DigitMapRange = 'x' / '[' 1*DigitLetter ']'
DigitLetter ::= *(DIGIT '-' DIGIT) / DigitMapLetter
```

where “x” means “any digit” and “.” means “any number of”.

digitMapMIBObjects

The following parameters allow you to define SIP digit maps.

Table 100: Digit Maps Parameters

Name	Access	Description
digitMapProcessDigitsWhenPressed	R/W	Determines when a digit is processed through the digit maps. - disable: Digits are processed only when released. Disabling this feature increases the delay needed to match a dialed string to a digit map. There is also an impact on <i>digitMapTimeoutFirstDigit</i> and <i>digitMapTimeoutCompletion</i> since the timers are stopped at the end of a DTMF instead of the beginning. It can also lead to small DTMF leaks when using subscriber services if the variable <i>subscriberServicesProcessingTrigger</i> is set to flashHookAndDigits. - enable: Digits are processed as soon as they are pressed. This can lead to a DTMF leak in the RTP at the beginning of a call if the voice stream is established before the last DTMF is released. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details." Default Value: enable

digitMapAllowedTable

A table of the digit maps that are considered valid if dialed, indexed by the digit map entry number.

Table 101: Allowed Digit Maps Parameters

Name	Access	Description
digitMapAllowedEnable	R/W	If enabled, this digit map will be recognised and accepted only if it is also valid. If disabled, this digit map will not be recognised. Possible values are: - disable (0) - enable (1) Default Value: enable

Table 101: Allowed Digit Maps Parameters (Continued)

Name	Access	Description
digitMapAllowedDigitMap	R/W	A string composing a digit map that will be considered valid when dialed. The string must be declared with the syntax described in the <i>digitMapMIB</i> entry description. Default Value: x.T
digitMapAllowedIsValid	R-O	This object is deprecated. This means some agents may implement it and some agents may not implement it. Diagnosis of the string entered in <i>digitMapAllowedDigitMap</i> . Possible values are: - invalid (0) - valid (1) If the value is invalid, an error was found in the entered string, please make sure that the syntax respects that which is enumerated in the <i>digitMapMIB</i> entry description. Default Value: invalid
digitMapPrefixedDigitRemovalCount	R/W	Post-Dial number modification. This specifies the amount of digits to remove from the beginning of the dialed number, after dialing, but before starting the call. For instance, when dialing "1-819-xxx-xxxx", specifying a value of "4" would mean that the call is started using the number "xxx-xxxx". Also see <i>digitMapPrependedString</i> and <i>digitMapSuffixStringToRemove</i> . This rule is applied BEFORE applying both <i>digitMapSuffixStringToRemove</i> and <i>digitMapPrependedString</i> . Default Value: 0
digitMapPrependedString	R/W	Post-Dial number modification. This specifies a string to insert at the beginning of the dialed number before starting the call. This string is added after executing the operation required by the <i>digitMapPrefixedDigitRemovalCount</i> variable. For instance, let's say that you need to dial a special digit, "9", for all local calls. Dialing "xxx-xxxx" with a value of "9" would yield "9-xxx-xxxx" as the number with which to initiate the call. See also <i>digitMapPrefixedDigitRemovalCount</i> and <i>digitMapSuffixStringToRemove</i> . This rule is applied AFTER applying both <i>digitMapPrefixedDigitRemovalCount</i> and <i>digitMapSuffixStringToRemove</i> .
digitMapSuffixStringToRemove	R/W	Post-Dial number modification. This specifies a string to look for and remove, from the end of the dialed number. This can be especially helpful if one of your digit maps contains a terminating character that must not be dialed. For instance, let's take a digit map such as "25#" in which the "#" signals that the user has finished entering digits. If, for any reason, you wish to remove the "#", simply specify "#" in this variable and the resulting number will be "25". See also <i>digitMapPrefixedDigitRemovalCount</i> and <i>digitMapPrependedString</i> . This rule is applied AFTER applying <i>digitMapPrefixedDigitRemovalCount</i> but BEFORE applying <i>digitMapPrependedString</i> .
digitMapAllowedLineToApply	R/W	Specifies the line(s) on which to apply the digit map. The string has the following syntax: 'all': Applies to all lines. ',': Separator between non-consecutive lists of lines or single line. 'n': A single line, where n is the line number. 'm-n': List of lines where m is the start line number and n is the end line number. NOTE: Line duplication is not allowed. Lines must be specified in low to high order. Example: '1,3-6': Applies to lines 1, 3, 4, 5, and 6. Default Value: all

digitMapRefusedTable

A table of the digit maps that are considered invalid if dialed, indexed by the digit map entry number.

Table 102: Refused Digit Maps Parameters

Name	Access	Description
digitMapRefusedEnable	R/W	If enabled, this digit map will be recognised and refused only if it is also valid. If disabled, this digit map will not be recognised. Possible values are: • disable (0) • enable (1) Default Value: disable
digitMapRefusedDigitMap	R/W	A string making up a digit map that will be considered invalid when dialed. The string must be declared with the syntax described in the <i>digitMapMIB</i> entry description.
digitMapRefusedIsValid	R-O	This object is deprecated. This means some agents may implement it and some agents may not implement it. Diagnosis of the string entered in <i>digitMapRefusedDigitMap</i> . Possible values are: • invalid (0) • valid (1) If the value is invalid, an error was found in the entered string, please make sure that the syntax respects that which is enumerated in the <i>digitMapMIB</i> entry description. Default Value: valid
digitMapRefusedLineToApply	R/W	Specifies the line(s) on which to apply the digit map. The string has the following syntax: • 'all': Applies to all lines. • ',': Separator between non-consecutive lists of lines or single line. • 'n': A single line, where n is the line number. • 'm-n': List of lines where m is the start line number and n is the end line number. NOTE: Line duplication is not allowed. Lines must be specified in low to high order. Example: '1,3-6': Applies to lines 1, 3, 4, 5, and 6. Default Value: all

digitMapTimeouts

The following parameters define the timeouts you can configure for the digit maps.

Table 103: Digit Maps Timeouts Parameters

Name	Access	Description
digitMapTimeoutCompletion	R/W	Total time that the user has to dial the DTMF sequence. The timer starts when the dial tone is played. When the timer expires, the receiver off-hook tone will be played. This value is expressed in milliseconds (ms). Values range from 1000 ms to 180000 ms. Default Value: 60000
digitMapTimeoutFirstDigit	R/W	Time between the start of the dial tone and the receiver off-hook tone, if no DTMF is detected. This value is expressed in milliseconds (ms). Values range from 1000 ms to 180000 ms. Default Value: 20000
digitMapTimeoutInterDigit	R/W	Value of the "T" digit in the <i>digitMapAllowedDigitMap</i> strings. The "T" digit is used to express a time lapse between the detection of two DTMFs. This value is expressed in milliseconds (ms). Values range from 500 ms to 10000 ms. Default Value: 4000

Configuration Parameters – Telephony Attributes MIB

The Telephony attributes MIB is used to configure the characteristics of the telephony system being implemented.

telephonyAttributesMIBObjects

The following parameters allow you to define the telephony attributes information.

telephonyAttributesIfFeaturesTable

A table of the telephony features configuration for the interface, indexed by the interface number.

Table 104: Telephony Attributes Parameters

Name	Access	Description
telephonyAttributesAutomaticCallEnable	R/W	Enable/Disable the automatic call service. This service provides a 'redphone'-like experience. If enabled, the target address is automatically called when the user picks up the phone. When this service is enabled, the second line service will be disabled but the call waiting feature will still be functional. The user can still accept incoming calls. See <i>telephonyAttributesAutomaticCallTargetAddress</i> . Default Value: disable
telephonyAttributesAutomaticCallTargetAddress	R/W	A string that represents the address or telephone number that the user wants to automatically call. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
telephonyAttributesCallDirectionRestriction	R/W	Restriction on the direction of traffic on a specific line. - noRestriction : Allow incoming and outgoing calls. - scnToIpOnly : Allow only calls from the SCN to the IP network. For an FXS line, the unit allows making calls but not receiving calls. For an FXO line, the unit answers incoming calls but does not allow outgoing calls. - ipToScnOnly : Allow only calls from the IP network to the SCN. For an FXS line, the unit allows receiving calls but not making calls. For an FXO line, the unit allows outgoing calls but does not answer incoming calls. Default Value: NoRestriction

Table 104: Telephony Attributes Parameters (Continued)

Name	Access	Description
telephonyAttributesHookFlashProcessing	R/W	Select how hook-flash detection is processed. When a call is in progress and the "flash" button of the telephone is pressed, the user can normally put the call on hold, transfer the call or even initiate a conference call. <i>telephonyAttributesHookFlashProcessing</i> allows these subscriber services to be handled by the unit or to be delegated to a remote party. - processLocally: Hook-flash is processed locally. The actual behavior of the "flash" button depends on which subscriber services are enabled for this line. See <i>subscriberServicesIfEnablingTable</i>. - transmitUsingSignalingProtocol: Hook-flash is processed by a remote party. The hook-flash event is carried by a signaling protocol message. The actual behavior of the "flash" button depends on the remote party. - outOfBandUsingRtp : Hook-flash is processed by a remote party. The hook-flash event is relayed as telephone-event 16 via an RFC 2833 RTP packet. The actual behavior of the 'flash' button depends on the remote party. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: processLocally
telephonyAttributesDelayedHotLineEnable	R/W	Enables/Disables the Delayed Hot Line feature. This service places an automatic call whenever the <i>digitMapTimeoutFirstDigit</i> timer expires. When disabled, a user picking up the phone but not pressing any telephone keys hears the Receiver Off-Hook tone after the amount of time specified in the <i>digitMapTimeoutFirstDigit</i> variable. When enabled, the expiration of the above timeout rather results in an automatic call being placed to the destination specified by the <i>telephonyAttributesDelayedHotLineTargetAddress</i> variable. Default Value: disable
telephonyAttributesDelayedHotLineExtension	R/W	Enables/Disables the extended version of the Delayed Hot Line feature. With this extension, the automatic call mentioned in the basic feature is placed upon expiration of the <i>digitMapTimeoutCompletion</i> timer. When disabled, a user beginning to dial a telephone number but failing to complete the operation before the expiration of the <i>digitMapTimeoutCompletion</i> timeout, hears the Receiver Off-Hook tone. When enabled, the destination specified by the <i>telephonyAttributesDelayedHotLineTargetAddress</i> variable is called upon expiration of the timeout. See <i>telephonyAttributesDelayedHotLineEnable</i>. Default Value: disable
telephonyAttributesDelayedHotLineTargetAddress	R/W	The destination (address or telephone number) that is automatically called with both versions of the Delayed Hot Line feature. See <i>telephonyAttributesDelayedHotLineEnable</i> and <i>telephonyAttributesDelayedHotLineExtension</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
telephonyAttributesAutomaticRejection	R/W	The number of seconds a port is allowed to ring before automatically rejecting the call. A value of 0 means that there is no limit so the port rings until the caller hangs up. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: 0

telephonyAttributesIpAddressCallCustomization

The following parameters allow you to define the IP address call information.

Table 105: Telephony Attributes – IP Address Call

Name	Access	Description
telephonyAttributesIpAddressCallEnable	R/W	Enable/Disable the direct IP address call service. This service allows a user to make a call without the help of a server. When this service is enabled, the user can dial an IP address and enter an optional phone number. Note that the optional phone number will be matched by using the same digit maps as for a normal call. Using this method will bypass any server configuration found in your unit. To make an IP address call: 1. Dial '**' 2. Dial the numerical digits of the IP address. For the dot ".", use the star "*" sign. 3. Terminate the IP call without specifying a phone number by using the star "**". - or - Continue with a phone number by using the pound "#" sign. 4. Optionally, dial the phone number. Example IP calls to a unit at IP address "1.2.3.4": If the phone number is of no concern, the user dials the following digits: **1*2*3*4* To reach the phone number "3330001", the user dials the following digits: **1*2*3*4#3330001 Default Value: disable

Configuration Parameters – Emergency Call MIB

The Emergency Call MIB is used to configure the exceptional treatment of emergency calls.

emergencyCallMIBObjects

The following parameters allow you to define the emergency call information.

emergencyCallUrgentGatewayCustomization

The following parameters allow you to define the urgent gateway parameters.

Table 106: Emergency Call – Urgent Gateway

Name	Access	Description
emergencyCallUrgentGatewayEnable	R/W	Enable/Disable the urgent gateway service. This service allows a user to dial a special digit map resulting in a message being sent to a specified urgent gateway, bypassing any other intermediaries. If enabled, whenever the user dials the specified digit map, a message will be sent to the target address. See <i>emergencyCallUrgentGatewayDigitMap</i> and <i>emergencyCallUrgentGatewayTargetAddress</i> . Default Value: disable
emergencyCallUrgentGatewayDigitMap	R/W	Digit map the user must dial to initiate a call in urgent mode. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. Note: Dialing this digit map will not have any effect unless the service's status is "enabled". See <i>emergencyCallUrgentGatewayEnable</i> .
emergencyCallUrgentGatewayTargetAddress	R/W	A string that represents the address or telephone number that the user wants to automatically call when dialing the emergency number. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.

Configuration Parameters – Subscriber Services MIB

The Subscriber services MIB is used to configure the availability of the different basic subscriber services, such as call hold and conference, as well as more advanced services, such as call waiting and call forwarding preferences.

subscriberServicesMIBObjects

The following parameters allow you to define the subscriber services information.

subscriberServicesIfEnablingTable

A table of the basic subscriber services configuration for the interface, indexed by the interface number.

Table 107: Subscriber Services – Activation Parameters

Name	Access	Description
subscriberServicesHoldEnable	R/W	Enable/Disable the holding service. With this service enabled, an active call can be temporarily put on hold, usually by using the “flash” button of the telephone. The user can resume the call in the same way. This service has no dependencies on other services being enabled. Default Value: enable
subscriberServicesCallWaitingEnable	R/W	Enable/Disable the call waiting service. With this service enabled, new calls received by an endpoint during an already active call on that endpoint will result in the endpoint hearing a special tone indicating that a call is waiting on the second line. The user may then answer that call by using the “flash” button of the telephone. The user will be able to switch between the two active calls by using the “flash” button. For this service to be enabled, the call hold service must be enabled as well. The user cancels this service on a per-call basis when dialing a DTMF sequence matching the digit map stored in <i>subscriberServicesCallWaitingCancelDigitMap</i> . To disable or enable this service permanently, the <i>subscriberServicesCallWaitingPermanentDigitMapEnable</i> and <i>subscriberServicesCallWaitingPermanentDigitMapDisable</i> digit maps must be used. See <i>subscriberServicesHoldEnable</i> , <i>subscriberServicesCallWaitingCancelDigitMap</i> , <i>subscriberServicesCallWaitingPermanentDigitMapEnable</i> and <i>subscriberServicesCallWaitingPermanentDigitMapDisable</i> . Default Value: enable
subscriberServicesSecondCallEnable	R/W	Enable/Disable the second call service. With this service enabled, a user with an active call can put the call on hold and initiate a new call on the second line. This service is most useful in conjunction with the transfer and conference services. For this service to be enabled, the call hold service must be enabled as well. See <i>subscriberServicesHoldEnable</i> . Default Value: enable

Table 107: Subscriber Services – Activation Parameters (Continued)

Name	Access	Description
subscriberServicesBlindTransferEnable	R/W	Enable/Disable the blind call transfer service, sometimes called Transfer without Consultation, or Unattended Transfer. With this service enabled, a user can transfer a call on hold to a still ringing (unanswered) call. Starting with an active call, a user can put the call on hold, initiate a call to a third party, then transfer the participant that is currently on hold to the third party. This must be done before the third party has answered. In case the third party answers, the transfer becomes an Attended Transfer. The transfer is triggered by the user hanging up the handset. The remaining calls (held call and ringing call with third party) are then connected together. The held call will be automatically unheld and will hear the ringback tone provided by the third party's ringing. For this service to be enabled, the call hold AND second call services must be enabled as well. See <i>subscriberServicesHoldEnable</i> and <i>subscriberServicesSecondCallEnable</i>. Also see <i>subscriberServicesAttendedTransferEnable</i> for a variation of the transfer method. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: enable
subscriberServicesAttendedTransferEnable	R/W	Enable/Disable the attended call transfer service, sometimes called Transfer with Consultation. With this service enabled, a user can transfer a call on hold to an active call. Starting with an active call, a user can put the call on hold, initiate a call to a third party, wait for the third party to answer, then transfer the participant that is currently on hold to the third party. The transfer is triggered by the user hanging up the handset. The remaining calls (held call and active call with third party) are then connected together. For this service to be enabled, the call hold AND second call services must be enabled as well. See <i>subscriberServicesHoldEnable</i> and <i>subscriberServicesSecondCallEnable</i>. Default Value: enable
subscriberServicesConferenceEnable	R/W	Enable/Disable the call conference service. With this service enabled, a user can link two or more calls together to form a single conversation, called a conference. Starting with an active call, a user can put the call on hold, initiate a call to a third party, wait for the third party to answer, then use the 'flash' button of the telephone to start the conference with the call that is already on hold. - Supported conference type depends on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. - Currently, a participant of the conference can put the conference on hold and attempt other calls. This participant may then rejoin the conference at a later time by unholding it. The endpoint that has initiated the conference is NOT able to put the conference on hold. For this service to be enabled, the call hold AND second call services must be enabled as well. See <i>subscriberServicesHoldEnable</i> and <i>subscriberServicesSecondCallEnable</i>. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: enable
subscriberServicesCallForwardUnconditional Enable	R/W	Enable/Disable the unconditional call forward service. This service allows a user to forward ALL incoming calls to a specified target. A short ring will be emitted to alert the user that the call has been forwarded, but the user will not be able to pick up the call from that location. If enabled, the user can dial the digit maps for enabling and disabling this service. See <i>subscriberServicesCallForwardUnconditionalForwarding Address</i>. Default Value: disable
subscriberServicesCallForwardOnBusy Enable	R/W	Enable/Disable the call forward on busy service. This service allows a user to forward incoming calls to a specified target when the user is already participating in another call. The user will not have any feedback that a call was forwarded. If enabled, the user can dial the digit maps for enabling and disabling this service. See <i>subscriberServicesCallForwardOnBusyForwardingAddress</i>. Default Value: disable

Table 107: Subscriber Services – Activation Parameters (Continued)

Name	Access	Description
subscriberServicesCallForwardOnNoAnswerEnable	R/W	Enable/Disable the call forward on no answer service. This service allows a user to forward incoming calls to a specified target when the user is unable to pick up the call before the timeout, specified by <i>subscriberServicesCallForwardOnNoAnswerTimeout</i> expires. The user will not have any feedback that a call was forwarded. If enabled, the user can dial the digit maps for enabling and disabling this service. See <i>subscriberServicesCallForwardOnNoAnswerForwardingAddress</i> and <i>subscriberServicesCallForwardOnNoAnswerTimeout</i>. Default Value: disable

subscriberServicesIfStatusTable

A table of the basic subscriber services statuses for the interface, indexed by the interface number.

Table 108: Subscriber Services – Status Parameters

Name	Access	Description
subscriberServicesHoldStatus	R-O	Status of the holding service. See <i>subscriberServicesHoldEnable</i>. Default Value: active
subscriberServicesCallWaitingStatus	R-O	Status of the call waiting service. See <i>subscriberServicesCallWaitingEnable</i>. Default Value: active
subscriberServicesSecondCallStatus	R-O	Status of the second call service. See <i>subscriberServicesSecondCallEnable</i>. Default Value: active
subscriberServicesBlindTransferStatus	R-O	Status of the blind transfer service. See <i>subscriberServicesBlindTransferEnable</i>. Default Value: active
subscriberServicesAttendedTransferStatus	R-O	Status of the attended transfer service. See <i>subscriberServicesAttendedTransferEnable</i>. Default Value: active
subscriberServicesConferenceStatus	R-O	Status of the conference service. See <i>subscriberServicesConferenceEnable</i>. Default Value: active

subscriberServicesIfCallForwardActivationTable

A table of the call forward activation statuses for the interface, indexed by the interface number.

Table 109: Subscriber Services – Call Forward Activation

Name	Access	Description
subscriberServicesCallForwardUnconditionalActivation	R/W	Activation status of the unconditional call forward service. Using the digit maps configured for this service, the user can use his/her handset to activate or deactivate this service. In that case, the variable will be automatically updated to reflect the activation status. This service can also be activated or deactivated by setting the value of this variable. Default Value: inactive
subscriberServicesCallForwardUnconditionalForwardingAddress	R/W	A string that represents the address or telephone number to which the user wants to forward calls. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
subscriberServicesCallForwardOnBusyActivation	R/W	Activation status of the call forward on busy service. Using the digit maps configured for this service, the user can use his/her handset to activate or deactivate this service. In that case, the variable will be automatically updated to reflect the activation status. This service can also be activated or deactivated by setting the value of this variable. Default Value: inactive
subscriberServicesCallForwardOnBusyForwardingAddress	R/W	A string that represents the address or telephone number to which the user wants to forward calls. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.

Table 109: Subscriber Services – Call Forward Activation (Continued)

Name	Access	Description
subscriberServicesCallForwardOnNoAnswerActivation	R/W	Activation status of the call forward on no answer service. Using the digit maps configured for this service, the user can use his/her handset to activate or deactivate this service. In that case, the variable will be automatically updated to reflect the activation status. This service can also be activated or deactivated by setting the value of this variable. Default Value: inactive
subscriberServicesCallForwardOnNoAnswerForwardingAddress	R/W	A string that represents the address or telephone number to which the user wants to forward calls. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
subscriberServicesCallForwardOnNoAnswerTimeout	R/W	Time the telephone will keep ringing before the call forwarding activates, in milliseconds. Possible values range from 200 ms to 120000 ms. Default Value: 5000

subscriberServicesActivationDigitmaps

The following parameters allow you to define the information pertaining to the digits users will have to dial on their telephone keypad in order to enable/disable the call forward services.

Table 110: Subscriber Services – Call Forward Digit Maps

Name	Access	Description
subscriberServicesCallForwardUnconditionalEnableDigitMap	R/W	Digit map the user can dial to enable the application of the service. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. Note: Dialing this digit map will not have any effect unless the service's status is "enabled". See <i>subscriberServicesCallForwardUnconditional Enable</i> .
subscriberServicesCallForwardUnconditionalDisableDigitMap	R/W	Digit map the user can dial to disable the application of the service. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. Note: Dialing this digit map will not have any effect unless the service's status is "enabled". See <i>subscriberServicesCallForwardUnconditional Enable</i> .
subscriberServicesCallForwardOnBusyEnableDigitMap	R/W	Digit map the user can dial to enable the application of the service. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. Note: Dialing this digit map will not have any effect unless the service's status is "enabled". See <i>subscriberServicesCallForwardOnBusyEnable</i> .
subscriberServicesCallForwardOnBusyDisableDigitMap	R/W	Digit map the user can dial to disable the application of the service. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. Note: Dialing this digit map will not have any effect unless the service's status is "enabled". See <i>subscriberServicesCallForwardOnBusyEnable</i> .
subscriberServicesCallForwardOnNoAnswerEnableDigitMap	R/W	Digit map the user can dial to enable the application of the service. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. Note: Dialing this digit map will not have any effect unless the service's status is "enabled". See <i>subscriberServicesCallForwardOnNoAnswerEnable</i> .
subscriberServicesCallForwardOnNoAnswerDisableDigitMap	R/W	Digit map the user can dial to disable the application of the service. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. Note: Dialing this digit map will not have any effect unless the service's status is "enabled". See <i>subscriberServicesCallForwardOnNoAnswerEnable</i> .
subscriberServicesCallWaitingCancelDigitMap	R/W	Digit map the user can dial to disable the call waiting the service. This service is cancelled on a per-call basis. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. Note: Dialing this digit map will not have any effect unless the Call Waiting service's status is "enabled". See <i>subscriberServicesCallWaitingEnable</i> .
subscriberServicesCallWaitingPermanentDigitMapEnable	R/W	Digit map the user can dial to enable the call waiting service permanently. The <i>subscriberServicesCallWaitingEnable</i> variable for the line the user is currently using is set to 'enable' when this digit map is executed successfully. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. See <i>subscriberServicesCallWaitingEnable</i> .

Table 110: Subscriber Services – Call Forward Digit Maps (Continued)

Name	Access	Description
subscriberServicesCallWaitingPermanentDigitMapDisable	R/W	Digit map the user can dial to disable the call waiting service permanently. The <i>subscriberServicesCallWaitingEnable</i> variable for the line the user is currently using is set to 'disable' when this digit map is executed successfully. This digit map must follow the syntax for digit maps as declared in the digit maps MIB. See <i>subscriberServicesCallWaitingEnable</i> .

subscriberServicesProcessing

The following parameter allow you to select which action the user must perform to trigger a service change.

Table 111: Subscriber Services – Processing

Name	Access	Description
subscriberServicesProcessingTrigger	R/W	Selects which action the user must perform to trigger a service change. - flashHook: The user must perform a flash hook to activate a service. - flashHookAndDigits: The user must perform a flash hook and enter a digit to activate a service. The digit dialed has a different behavior depending on the current call context: One call active and one waiting call: Flash hook then dial the digit 2: Answer the waiting call. One call active and one call on hold: Flash hook then dial the digit 1: Terminate the active call and recover the call on hold. Flash hook then dial the digit 2: Hold the active call and recover the call on hold. Flash hook then dial the digit 3: Enter the conference mode. Flash hook then dial the digit 4: Transfer the call on hold to the active call. When hanging up in this context, the phone rings to notify the user there is still a call on hold. In conference mode: Flash hook then dial the digit 2: Return to one active call and one call on hold. Flash hook then dial the digit 4: Transfer the second active call to the first active call. When hanging up in this context, all calls are finished. As example, the following are the steps to perform a conference call: 1. Call the first attendee. 2. Flash hook to put the first attendee on hold. 3. Call the second attendee. The context is now one call active and one call on hold. 4. Flash hook then dial the digit 3 to start the conference call. Default Value: flashHook

Configuration Parameters – SNTP MIB

This MIB describes the parameters used by the Simple Network Time Protocol (SNTP).

sntpMIBObjects

The following parameters allow you to set the SNTP information.

Table 112: SNTP Parameters

Name	Access	Description
sntpEnable	R/W	Enable/Disable the SNTP client. • disable(0) • enable(1) Default Value: disable
sntpSynchronizationPeriod	R/W	Time interval (in minutes) between request made to the SNTP server. The result will be used to synchronize the unit with the time server. The maximum value is set to 1 440 minutes which corresponds to 24 hours. Default Value: 1440
sntpSynchronizationPeriodOnError	R/W	Time interval (in minutes) between retries after an unsuccessful attempt to reach the SNTP server. The maximum value is set to 1 440 minutes which corresponds to 24 hours. Default Value: 60

sntpTimeZoneConfig

The following parameters allow you to set the time zone information.

Table 113: SNTP Parameters – Time Zone

Name	Access	Description
sntpTimeZoneString	R/W	String describing the time zone to be used. This string MUST use the IEEE 1003.1 POSIX format as defined in <i>bootp-dhcp-option-88.txt</i>. The string format is validated upon entry. Invalid entries will be refused. The following are some example strings. - Pacific Time (Canada & US): PST8DST7,M3.2.0/02:00:00,M11.1.0/02:00:00 - Mountain Time (Canada & US): MST7DST6,M3.2.0/02:00:00,M11.1.0/02:00:00 - Central Time (Canada & US): CST6DST5,M3.2.0/02:00:00,M11.1.0/02:00:00 - Eastern Time (Canada & US): EST5DST4,M3.2.0/02:00:00,M11.1.0/02:00:00 - Atlantic Time (Canada): AST4DST3,M3.2.0/02:00:00,M11.1.0/02:00:00 - GMT Standard Time: GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00 W. Europe Standard Time: WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00 - China Standard Time: CST-8 - Tokyo Standard Time: TST-9 - Central Australia Standard Time: CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00 - Australia Eastern Standard Time: AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00 - UTC (Coordinated Universal Time) : UTC0 Default Value: EST5DST4,M3.2.0/02:00:00,M11.1.0/02:00:00
sntpTimeZoneStringsValid	R-O	This object is deprecated. This means some agents may implement it and some agents may not implement it. Diagnosis of the string entered in sntpPosixTimeZone. Possible values are: - invalid (0) - valid (1) If the value is invalid, an error is found in the entered string, please make sure that the syntax respects the POSIX string format. Default Value: invalid

Configuration Parameters – Line Grouping MIB

This MIB is used to customize the attributes related to groups of lines.

lineGroupingMIBObjects

The following parameters allow you to define the Line Grouping information.

Table 114: Line Grouping – Number of Group

Name	Access	Description
lineGroupingNbGroups	R/W	Indicates the number of groups of lines for this unit. The group indexes start at 1. For example, if the value is 3, the group indexes are 1, 2 and 3. When the number of groups is decreased, the higher group indexes are deleted. For example, if the value goes from 4 to 2, the group indexes 3 and 4 are deleted. When a group is deleted, its lines are associated with the default group index. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 0

lineGroupingIfAssociationTable

A table that optionally associates a group to each line.

Table 115: Line Grouping – Association

Name	Access	Description
lineGrpAssocIfType	R-O	The type of interface. - fxo: an FXO analog interface. - fxs: an FXS analog interface. Default Value: fxo
lineGrpAssocGroupIndex	R/W	The group index associated to this interface. A value of 0 means that the interface is not part of a group. Default Value: 0

lineGroupingGroupConfigTable

A table for configuring attributes for groups of lines, one row for each group.

Table 116: Line Grouping – Attributes

Name	Access	Description
lineGrpConfLineSelectionAlgorithm	R/W	The algorithm for selecting a line on an incoming IP to SCN call. - roundRobin: The unit starts from the interface following the interface used for the last IP to SCN call. Going toward the highest interface, the unit selects the first line available. If the highest interface is unavailable, the search continues from the lowest interface number to the interface used for the last IP to SCN call. - lowToHigh: Starting from the lowest interface number and going toward the highest interface number, the unit selects the first line available. - highToLow: Starting from the highest interface number and going toward the lowest interface number, the unit selects the first line available. Default Value: roundRobin
lineGrpConfCallForwardNoResourceEnable	R/W	Enables the call forward on no resource mechanism. When enabled, this mechanism reroutes an incoming IP to SCN call in the event that all the lines associated with the group are unavailable. The call is rerouted to the destination specified by <i>configCallForwardNoResourceAddress</i>. Default Value: disable
lineGrpConfCallForwardNoResourceAddress	R/W	A string that represents the address or telephone number that the user wants to call when all lines are unavailable. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.

Configuration Parameters – Line Selection MIB

This MIB is used to customize the properties of line port selection.

lineSelectionMIBObjects

The following parameters allow you to define the line selection information.

lineSelectionIfCustomizationTable

A table for customizing the line selection.

Table 117: Line Selection – Parameters

Name	Access	Description
lineSelectionEnable	R/W	Enable/Disable the source line selection feature. This feature provides a call line selection mechanism, based on the source of the call, and a per-port list of digit maps. When enabled, the source of the call is compared to all the line selection digit maps. The result of this comparison produces a list of lines that can take the call, but which are not necessarily available to do so. Once the match list has been created, there are two possibilities: 1. The list contains one or more lines. The port selection algorithm will then be used to select a line. If none of the lines in the list are available, the call is rejected. 2. The list is empty. The port selection algorithm will then cycle through all lines that do not use source line selection. If no available lines can be found, the call is rejected. See <i>lineSelectionDigitMap</i>. Default Value: disable
lineSelectionDigitMap	R/W	IP to SCN call sources that match this digit map will be permitted to use this line. See <i>digitMapMIB</i> for syntax. Note that this digit map will not have any effect unless the feature's status is "enabled". See <i>lineSelectionEnable</i>.

Configuration Parameters – Analog SCN Gateway MIB

This MIB is used to customize the properties of an analog SCN gateway.

analogScnGwMIBObjects

The following parameters allow you to define the analog SCN gateway information.

analogScnGwIfDialingTable

This table is used to customize the dialing options.

Table 118: Analog SCN Gateway Parameters – Dialing

Name	Access	Description
analogScnGwDialPrefix	R/W	A DTMF sequence to dial on the SCN before dialing the destination phone number. The dial prefix can be any combination of DTMFs or pause characters. "p", ",", and "." are accepted as pause characters. The pause duration is one second.
analogScnGwPreDialDelay	R/W	The delay between the time the line is successfully seized, or dial tone detected, and the moment the destination phone number is dialed. Some country specifications include a mandatory PreDialDelay. In that case, the highest between that and <i>analogScnGwPreDialDelay</i> is used. See <i>telephonyCountrySelection</i> . This value is expressed in milliseconds (ms). Default value: 0
analogScnGwInterDigitDialDelay	R/W	The delay between two DTMFs when dialing the destination phone number. This value is expressed in milliseconds (ms). Default value: 100
analogScnGwDtmfDuration	R/W	The duration of a DTMF when dialing the destination phone number. This value is expressed in milliseconds (ms). Default value: 100
analogScnGwDialEnable	R/W	Determines how the gateway behaves when it receives an IP call. This feature is useful in conjunction with the 'Remote Line Extension' service. • disable: The gateway picks up the SCN line and opens the audio channel with the peer. • enable: The gateway picks up the SCN line and dials the telephone number associated with the destination of the call before opening the audio channel with the peer. Default value: enable

Configuration Parameters – FXO MIB

This MIB is used to customize properties of FXO lines.

fxoMIBObjects

The following parameters allow you to define the FXO information.

fxoLinePropertiesCustomization

The following parameters are used to customize the line properties options.

Table 119: FXO Parameters – Line Properties

Name	Access	Description
fxoDialtoneDetectionMode	R/W	Enable the dial tone detection. When dial tone detection is enabled, the unit waits for a dial tone on the SCN before initiating the dialing sequence. If no dial tone is detected, the line is considered as busy with an incoming SCN call. This mechanism helps avoid collisions between incoming and outgoing SCN calls. - disable: Dial tone detection is disabled. - countryTone: The unit will try to detect the tone specified for this purpose in the current country's tone specification. Some country specifications omit this information. In that case, the unit behaves as if <i>fxoDialtoneDetectionMode</i> is "disable". See <i>telephonyCountrySelection</i>. Default value: countryTone
fxoDialtoneDetectionTimeout	R/W	Dial tone detection timeout. Indicates how long the unit waits for a dial tone before considering the line is busy with an incoming SCN call. This value is expressed in milliseconds (ms). Default value: 3000
fxoCallerIdDetectionRange	R/W	The range of caller ID signals that can be detected. - high: Between 30 and 530 mV RMS. - low: Between 7 and 110 mV RMS. Default value: high
fxoAnswerSupervisionMode	R/W	This feature configures when the IP call is established depending on the PSTN call state. - none: No answer supervision, the IP call is established immediately after signalling on the PSTN. - batteryReversal: The IP call is established after receiving a battery reversal from the PSTN. - billingTone: The IP call is established after receiving a billing tone from the PSTN. This variable's semantics are different depending on the software version. Please refer to the documentation shipped with your device for more details. Default value: none

fxoLineFaultDetection

The following parameters are used to customize the line fault detection options.

Table 120: FXO Parameters – Line Fault Detection

Name	Access	Description
fxoLineFaultDetectionEnable	R/W	Enable the line fault detection. The line fault detection mechanism allows the detection of defective or disconnected lines based on the absence of current when closing the loop. The line status is reported in the <i>fxoIfLineStatusTable</i> . Default value: enable
fxoLineSeizureTimeout	R/W	Indicates how long the unit waits before considering the seizure of an analog line failed. This value is expressed in milliseconds (ms). Default value: 5000

fxoIfLineStatusTable

A table of line statuses updated by the line fault detection mechanism.

Table 121: FXO Parameters – Line Status

Name	Access	Description
fxoLineStatus	R-O	Line status as reported by the line fault detection mechanism. The line fault detection can be enabled by using the <i>fxoLineFaultDetectionEnable</i> object. The unit does not automatically detect when a previously connected port has changed to the disconnected status. The unit only detects the change of status when it attempts to use the port or after a restart. The unit automatically detects within seconds when a disconnected port becomes connected. - unknown: The line fault detection is disabled. - connected: When last polled, the line was connected. - disconnected: When last polled, the line was disconnected. Default value: unknown

fxoIfAnsweringDelayTable

This table holds the answering delay configuration. Each row in this table configures the answering delay of a line.

Table 122: FXO Parameters – Answering Delay

Name	Access	Description
fxoPreAnswerDelay	R/W	The waiting period before answering an incoming SCN call. If this delay expires before the caller ID signal is decoded, the call will proceed without caller ID information. If a minimal waiting period is required for the selected country, the highest of both values is used. See <i>telephonyCountrySelection</i> . This value is expressed in milliseconds (ms). Default value: 8000
fxoAnswerOnCallerIdDetectionEnable	R/W	Enables answering on caller ID detection. When enabled, an incoming SCN call is answered on the first occurrence of either - the reception of the caller ID signal. - the expiration of the delay configured by <i>fxoPreAnswerDelay</i>. Default value: enable
fxoWaitForCalleeToAnswerEnable	R/W	When the line is set up for automatic call (see the <i>telephonyAttributesAutomaticCallEnable</i> variable), enabling this variable makes the FXO wait until the called party answers the phone before it picks up the PSTN line. When enabled, this feature renders the <i>fxoPreAnswerDelay</i> and <i>fxoAnswerOnCallerIdDetectionEnable</i> variables inoperative. Default value: disable

fxoForcedEndOfCallCustomization

The following parameters are used to customize the forced end of call options.

Table 123: FXO Parameters – Forced End of Call

Name	Access	Description
fxoFeocOnCallFailureEnable	R/W	Enables forced-end-of-call on call failure. This feature forcefully terminates a call that stayed in an error state for some time. When the line falls in an error state where a SIT, a ROH, a BUSY or any error tone is played, the unit waits for the timeout specified by <i>fxoFeocOnCallFailureTimeout</i> and then hangs up. Default value: enable
fxoFeocOnCallFailureTimeout	R/W	The waiting period before terminating a call in an error state. This value is expressed in seconds (sec). Default value: 30
fxoFeocOnSilenceDetectionMode	R/W	Enables forced-end-of-call on silence detection. This feature forcefully terminates a call that stayed silent for some time. When silence is detected on the IP and/or SCN side call for an amount of time specified by <i>fxoFeocOnSilenceDetectionTimeout</i> , the call is terminated. - disable: Forced-end-of-call on silence detection is disabled. - onScnSilent: The call is terminated if the SCN side is silent. - onIpSilent: The call is terminated if the IP side is silent. - onIpAndScnSilent: The call is terminated if both IP and SCN sides are silent at the same time. - onIpOrScnSilent: The call is terminated if either the IP or SCN side is silent. This feature is useful to free resources in the event of an IP network failure preventing the end-of-call to be detected or when SCN end-of-call tone was not detected. Default value: disable
fxoFeocOnSilenceDetectionTimeout	R/W	Maximum amount of time that a call can remain silent, as specified by <i>fxoForcedEndOfCallCustomization</i> , before it is terminated and the line is released. This value is expressed in seconds (sec). Default value: 300
fxoFeocOnToneDetectionMode	R/W	Enables forced-end-of-call on tone detection. This feature terminates a call on detection of an end-of-call tone on the SCN. - disable: Force-end-of-call on tone detection is disabled. - countryTone: The unit will try to detect the tone specified for this purpose in the current country's tone specification. Some country specifications omit this information. In that case, the unit behaves as if <i>fxoFeocOnToneDetectionMode</i> is "disable". See <i>telephonyCountrySelection</i>. - customTone: Terminates a call on detection of a custom tone. See <i>fxoEndOfCallToneCustomSettings</i>. Default value: countryTone

fxoEndOfCallToneCustomSettings

The following parameters are used to customize the custom tone settings.

Table 124: FXO Parameters – End of Call Custom Tone

Name	Access	Description
fxoEndOfCallToneCustomFrequency	R/W	Frequency to detect in the custom cadence. A customized tone detection can only detect a single frequency. To detect tones made of multiple frequencies, create the cadence for only one of the frequencies found in the tone. This value is expressed in hertz (Hz). Default value: 440

Table 124: FXO Parameters – End of Call Custom Tone (Continued)

Name	Access	Description
fxoEndOfCallToneCustomCadence	R/W	Custom cadence. A cadence is a series of frequencies that are played for a specified time, making up a tone. The format for a cadence is "on, off, on, off, ..." where "on" and "off", respectively are numerical values representing the time in milliseconds that the frequency can and can't be detected. Example: "2000, 1000, 2000, 0" is a cadence where the frequency will play for 2 seconds, stop for 1 second, and play for 2 more seconds. This example is also equivalent to setting the string "2000, 1000, 2000". Up to three "on, off" pairs can be specified. Specifying less than those six values will result in "0" values being added as necessary. Specifying more than six will only use the six first values. A cadence starting with a value of zero (0) is invalid. The first zero (0) found in the string signals the end of the cadence (i.e. "200, 0, 300" is the same as "200"). Allowed range for the "on" and "off" values are 0 to 32767. These values are expressed in milliseconds (ms).
fxoEndOfCallToneCustomRepetition	R/W	Repetition of the cadence. Number of times the custom cadence must be detected to consider the custom end-of-call tone has been detected. Default value: 3

fxolfAnalogLineTypeTable

Table that contains the type of analog lines used.

Table 125: FXO Parameters – Analog Line Type

Name	Access	Description
fxolfAnalogLineType	R/W	Analog line type based on the analog signaling method used. This method defines the way on-hook and off-hook conditions are detected in a voice network. - loopStart : A way of signaling that seizes a line by bridging both wires of the telephone line through a resistor. The average telephone line uses the loop start signaling method. - groundStart : A way of signaling on subscriber trunks in which one side of the two wire trunk is momentarily grounded to get dial tone. The ground start signaling method ensures proper Far End Disconnect between an FXO interface and the SCN. Default value: loopStart

fxolfIncomingCallNotAllowedBehaviorTable

Table that defines how each line behaves when an incoming call is not allowed.

Table 126: FXO Parameters – Incoming Call

Name	Access	Description
fxolfIncomingCallNotAllowedBehavior	R/W	Under certain circumstances (locked port, call direction set to 'IP to SCN only', etc...), incoming calls from the SCN are not allowed. When that is the case, the FXO line behaves in one of the manners below. - doNotAnswer: The incoming call is left unanswered. - playCongestionTone: The incoming call is answered, a congestion tone is played for 10 seconds, and then the call is terminated. Default value: playCongestionTone

Configuration Parameters – Message Waiting Indicator MIB

This MIB is used to configure the message waiting indicator service.

mwIMIBObjects

The following parameters allow you to define the unit-wide MWI configuration parameters.

Table 127: MWI Parameters – General

Name	Access	Description
mwIFetchDigitMap	R/W	Digit map that the user will dial to trigger a message fetch operation. Typically this will initiate a call to the voice-messaging system. <i>See mwIConfigFetchAddress.</i>
mwIExpirationTime	R/W	For signaling protocols that allow dynamic subscription to a messaging service, this value indicates the duration of such a subscription. This value is expressed in seconds (s). Default value: 3600
mwISubscriptionCmdRefresh	R/W	Command to refresh the subscriptions. - noOp: No operation. - refresh: Refresh message waiting subscriptions. All enabled endpoints unsubscribe themselves from the service and re-subscribe using the current provisioning. Default value: noOp

mwIIfConfigurationTable

A table of the configurable items relative to the message waiting indicator, indexed by the interface number.

Table 128: MWI Parameters – Configuration

Name	Access	Description
mwIConfigActivation	R/W	Enable/Disable the message waiting service. This service, used in conjunction with a voice-messaging system, will enable the user to be notified when new messages are awaiting attention on the messaging server. The user will be alerted by the blinking of the LED on the phone, and a different dial tone when picking up the handset (called the message waiting tone). This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default value: disable
mwIConfigUserSubscriptionAddress	R/W	Typically, the unit will need to subscribe to a notification mechanism that will notify it when new messages are available. This field contains the address of that entity. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
mwIConfigFetchAddress	R/W	The fetch operation typically consists in the user initiating a call to the voice-messaging system, then using an auto-attendant to get the messages. This field contains the destination to use in creating the call when the <i>mwIFetchDigitMap</i> is matched. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. <i>Also see mwIFetchDigitMap.</i>

Table 128: MWI Parameters – Configuration (Continued)

Name	Access	Description
mwiConfigVoltageEnable	R/W	Enable/Disable the voltage message waiting indicator. When new messages are awaiting attention on the messaging server, the unit uses the line voltage to power the LED on the telephone in addition to the default method. This variable is effective only if the endpoint is configured to use the visual message waiting indicator (<i>mwiConfigActivation</i>). This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details." Default value: disable

Configuration Parameters – PPPoE MIB

This MIB is used to customize properties of the PPPoE service.

pppoeMIBObjects

The following parameters allow you to define the PPPoE configuration parameters.

Table 129: PPPoE Parameters – General

Name	Access	Description
pppoeEnable	R/W	Enable/disable the PPPoE service. - enable: The PPPoE service is enabled. The unit tries to establish a PPPoE connection to the access concentrator (AC) and service specified in <i>pppoeAcName</i> and <i>pppoeServiceName</i>. - disable: The PPPoE service is disabled. Changes to this setting require a reboot to take effect. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable
pppoeAcName	R/W	The name of the access concentrator (AC) to connect to on the next PPPoE connection establishment. This name is matched against the <i>AC-Name</i> field of the PADO packet sent by the access concentrators. See RFC2516 section 5.2 for details. If empty, the unit accepts the first offer that it receives. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.
pppoeServiceName	R/W	The name of the service requested to the access concentrator (AC) on the next PPPoE connection establishment. This string is used as the <i>Service-Name</i> field of the PADL packet broadcasted to the access concentrators. See RFC2516 section 5.1 for details. If empty, the unit sends a null <i>Service-Name</i> field meaning that any service is acceptable. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details.

Configuration Parameters – IP Routing MIB

This MIB is used to customize IP routing properties.

ipRoutingMIBObjects

The following parameters allow you to define the IP Routing configuration parameters.

Table 130: IP Routing Parameters – General

Name	Access	Description
ipRoutingEnable	R/W	Indicates if the routing service is active. The <i>ipRoutingMode</i> variable indicates the behavior of the routing service. - enable: The routing service is activated. - disable: The routing service is deactivated. This variable's semantics are different depending on the protocol and the hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable
ipRoutingMode	R/W	Indicates what type of routing service is selected. It is only used if ipRoutingEnable is set to enable. - tas(0) : Indicates that the routing service is in TAS mode. Transparent Address Sharing assigns the WAN IP address to a computer or device on the LAN side. - nat(1) : Indicates that the routing service is in NAT mode. Network Address Translation makes it possible to share a single WAN IP address between multiple computers on the LAN. - normal(2) : Indicates that the routing service is in normal mode. In this mode, the computers on the LAN side use a public IP address. This variable's semantics are different depending on the hardware platform. Please refer to the documentation shipped with your device for more details. Default Value: tas

ipRoutingDhcp

The following parameter allows you to define the lease offered by the DHCP server.

Table 131: IP Routing Parameters – DHCP

Name	Access	Description
ipRoutingDhcpServerEnable	R/W	Indicates if the DHCP server service is active. The DHCP service allocates IP addresses to the PC or IP equipment located on the LAN. The DHCP server behavior depends on the routing mode (<i>ipRoutingMode</i>) selected. TAS routing mode: - The DHCP server is always enable, even if this variable is set to disable. - The DHCP server allocates only one lease and all other DHCP request are silently rejected. - The DHCP server allocates the value of <i>localHostWanAddress</i> as IP address. - The DHCP server allocates the value of <i>localHostDefaultRouter</i> as default router. - The DHCP server allocates the value of <i>localHostSubnetMask</i> as subnet mask. - The DHCP server allocates the value of <i>localHostPrimaryDns</i> and <i>localHostSecondaryDns</i> as DNS. NAT and Normal routing mode: - The DHCP server can allocate one lease for each IP address in the range. - The DHCP server allocates a free lease in the range defined by <i>ipRoutingDhcpIpLeaseRangeStart</i> to <i>ipRoutingDhcpIpLeaseRangeEnd</i> as IP address. - The DHCP server allocates the value of <i>lanStaticAddress</i> as default router. - The DHCP server allocates the value of <i>lanStaticNetworkMask</i> as subnet mask. - The DHCP server allocates the value of <i>localHostPrimaryDns</i> and <i>localHostSecondaryDns</i> as DNS. enable(1): The DHCP server service is activated. disable(0): The DHCP server service is deactivated. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: enable
ipRoutingDhcpServerLeaseTime	R/W	The duration, in seconds, of the lease offered by the DHCP server. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 30
ipRoutingDhcpIpLeaseRangeStart	R/W	The first address in the range of IP addresses offered by the DHCP server. This address cannot exceed the one entered into variable <i>ipRoutingDhcpIpLeaseRangeEnd</i>. It is not used when the IP routing mode (<i>ipRoutingMode</i>) is TAS. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 192.168.10.2
ipRoutingDhcpIpLeaseRangeEnd	R/W	The last address in the range of IP addresses offered by the DHCP server. This address cannot be lower than the one entered into variable <i>ipRoutingDhcpIpLeaseRangeStart</i>. It is not used when the IP routing mode (<i>ipRoutingMode</i>) is TAS. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 192.168.10.254

Table 131: IP Routing Parameters – DHCP

Name	Access	Description
ipRoutingDhcpServerDnsFallbackEnable	R/W	- enable: If the <i>ipRoutingDhcpServerDnsFallbackEnable</i> variable is enabled and the WAN link is down, the DHCP server will return <i>localHostStaticPrimaryDns</i> and <i>localHostStaticSecondaryDns</i> values as DNS server. - disable: If the <i>ipRoutingDhcpServerDnsFallbackEnable</i> is disabled, the variable <i>localHostSelectConfigSource</i> indicates the provisioning source for the localHost objects: <i>localHostPrimaryDns</i> and <i>localHostSecondaryDns</i>. The DNS fallback feature is only available in NAT and Normal IP routing mode (defined in the variable <i>ipRoutingMode</i>) and when DHCP server is enabled (defined in the variable <i>ipRoutingDhcpServerEnable</i>). This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable
ipRoutingDhcpServerNoWanLeaseEnable	R/W	- enable: The lease time used for DHCP server is the one defined in the variable <i>ipRoutingDhcpServerNoWanLeaseTime</i> when the WAN link is down. - disable: The lease time used is the one defined in the <i>ipRoutingDhcpServerLeaseTime</i> variable for the DHCP server. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable
ipRoutingDhcpServerNoWanLeaseTime	R/W	The duration, in seconds, of the lease offered by the DHCP server when the WAN link is down and the variable <i>ipRoutingDhcpServerNoWanLeaseEnable</i> is enabled. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 180

ipRoutingQos

The following parameters allow you to define the QoS substitution process.

Table 132: IP Routing Parameters – QoS

Name	Access	Description
ipRoutingQosDiffServSubstitutionEnable	R/W	Governs whether the content of the QoS Differentiated Services field of IP packets routed from the LAN to the WAN interface is replaced by the value assigned to the <i>ipRoutingQosDiffServSubstitution</i> variable. - enable: The <i>DiffServ</i> field of IP packets originating from the equipment connected to the LAN interface and routed to the WAN is modified as explained above. - disable: The <i>DiffServ</i> field of IP packets originating from the equipment connected to the LAN interface and routed to the WAN is left intact. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable
ipRoutingQosDiffServSubstitution	R/W	Substitution value used to fill the QoS Differentiated Services field of IP packets originating from the equipment connected to the LAN interface and routed to the WAN. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: 184

ipRoutingMacSpoof

The following parameters allow you to define the MAC address spoofing process.

Table 133: IP Routing Parameters – MAC Address Spoofing

Name	Access	Description
ipRoutingMacSpoofEnable	R/W	Indicates whether or not to spoof the unit's MAC address on the WAN side: - enable: The unit's MAC address used on the WAN side is the configured MAC address. - disable: The unit's MAC address used on the WAN side is the actual unit's MAC address. It is useful in the case of ISPs that use the MAC address of the device connected to the <i>Computer</i> interface of the unit (e.g. a PC) to identify the connection. When the ISP rather encounters the actual unit's MAC address, it refuses the connection. Spoofing the unit's MAC address with the one of the device connected to the <i>Computer</i> interface permits to be properly connected via the ISP. Default Value: disable
ipRoutingMacSpoofAddress	R/W	The MAC address used to spoof the unit's actual MAC address. An empty character string means that the spoofing is considered disabled, even though <i>ipRoutingMacSpoofEnable</i> is at enable . A valid MAC address is a series of 12 hexadecimal digits (without colons).

ipRoutingBandwidthControl

The following parameters allow you to define the WAN upstream bandwidth control.

Table 134: IP Routing Parameters – Bandwidth Control

Name	Access	Description
ipRoutingBandwidthControlEnable	R/W	Indicates whether the unit should limit the outgoing throughput on the WAN interface. The MIB variable <i>ipRoutingEnable</i> must be enabled for this feature to take effect. - enable: Packets, sent from the PC or IP equipment to the WAN, are limited in bandwidth. The maximum bandwidth is determined by the <i>ipRoutingWanUpstreamBandwidth</i> MIB variable. Excess packets coming from the LAN interface will be dropped. The unit uses the priorities set in the MIB folder <i>qosleee8021q</i> to determine which packets to drop first, even when 802.1q tagging is disabled. - disable: Bandwidth from the PC or IP equipment to the WAN, is not limited. Default Value: disable
ipRoutingWanUpstreamBandwidth	R/W	Maximum outgoing amount of data transferred (throughput) from the PC or IP equipment to the WAN interface. The value is expressed in kilobits per seconds. This variable applies only when the <i>ipRoutingBandwidthControlEnable</i> MIB variable is set to enable. Default Value: 512

ipRoutingStatus

The following parameter gives the current MAC address of the device connected to the *Computer* port.

Table 135: IP Routing Parameter – Status

Name	Access	Description
ipRoutingMacAddress	R-O	Current MAC address of the online device in the <i>Computer</i> port.

Configuration Parameters – HTTP Server MIB

This MIB is used to customize the properties of the web-based configuration service (HTTP).

httpServerMIBObjects

The following parameters allow you to define the web-based configuration service.

Table 136: Web-Based Service Parameters

Name	Access	Description
httpServerEnable	R/W	Enable or disable the web-based configuration service (HTTP). Default value: enable
httpServerAccess	R/W	Interface where the web-based configuration service can be accessed. - lanOnly(0), - wanOnly(1), - all(2) Default value: lanOnly
httpServerUsername	R/W	User name for the web-based configuration service access authentication. A user logging in with this user name has restricted configuration possibilities via the web interface. Default value: admin
httpServerDefaultPassword	R/W	Default password for the web-based configuration service access authentication. This password is only used when the user resets the password by using the httpServerResetToDefaultPwd variable. Default value: 1234
httpServerResetToDefaultPwd	R/W	Command to reset the web password to the default value specified by httpServerDefaultPassword. - noOp(0), - reset(1) Changing this variable requires a reboot of the unit in order to take effect. Default value: noOp
httpServerAdminAccess	R/W	Interface where the web-based configuration service can be accessed by administrator user. - lanOnly(0) - wanOnly(1) - all(2) Default value: wanOnly
httpServerAdminUsername	R/W	Administrator user name for the web-based configuration service access authentication. A user logging in with this user name has extended configuration possibilities via the web interface. Default value: root
httpServerDefaultAdminPassword	R/W	Administrator default password for the web-based configuration service access authentication. This password is only used when the user resets the password by using the httpServerResetToDefaultAdminPwd variable. Default value: 5678
httpServerResetToDefaultAdminPwd	R/W	Command to reset the administrator web password to the default value specified by httpServerDefaultAdminPassword. - noOp(0) - reset(1) Changing this variable requires a reboot of the unit in order to take effect. Default value: noOp

Table 136: Web-Based Service Parameters (Continued)

Name	Access	Description
httpServerAdminRealm	R/W	The realm identifies who requested the login information for the administrator web-based configuration service. The realm is usually presented by the user's browser when prompting for a user name and password. Default value: default
httpServerUserRealm	R/W	The realm identifies who requested the login information for the enduser web-based configuration service. The realm is usually presented by the user's browser when prompting for a user name and password. Default value: default

httpServerMIBCustomisation

The following parameters indicate if the web-based configuration service (HTTP) is customized.

Table 137: Web-Based Service Parameters – Customizing

Name	Access	Description
httpServerSipAuthenticationEnable	R-O	When this feature is enabled, it creates a new dynamic web page that allows the user to change the line-specific authentication information (the HTTP Server Service does not handle the unit authentication). The information that can be set is described below. - Port: The port selects the user names and passwords reserved for a specific line. The port is a read-only attribute and it communicates with the MIB variable <i>sipUAlfAuthenticationTable</i>. - Index: The Index selects one of the five possible passwords associated with a specific line. The index is a read-only attribute and it communicates with the MIB variable <i>sipUAAuthIndex</i>. - Username: The username is a unique identifier for the authentication process. It has a read-only attribute and it communicates with the MIB variable <i>sipUAAuthUsername</i>. - Password: The password is a unique identifier for the authentication process. It has a read-write attribute and it communicates with the MIB variable <i>sipUAAuthPassword</i>. Note: the variables 'username' and 'password' are accessed with two different indexes: port and index. If <i>httpServerSipAuthenticationEnable</i> is disabled, the user can't access SIP authentication through the HTTP Server Service. Default value: disable
httpServerBandwidthControlSectionEnable	R/W	When this feature is enabled, it creates a new dynamic web page that allows the user to: 1. Enable or disable the bandwidth management feature. 2. Set a limit to the outbound traffic on the WAN port. Please refer to the <i>ipRoutingBandwidthControlEnable</i> variable for more details on the bandwidth management feature. Default value: disable

Configuration Parameters – Configuration File Fetching MIB

This MIB describes the parameters to configure to fetch configuration files. The unit is the initiator of the TFTP sessions.

configFileFetchingMIBObjects

The following parameters allow you to define the configuration file fetching service.

Table 138: Configuration File Fetching Parameters

Name	Access	Description
configFileFetchingFileName	R/W	The name of the generic configuration file fetched by the unit (see <i>sysConfigDownloadConfigFile</i>). This file should be used to update a large number of units with the same configuration. If this field is empty, no generic configuration is fetched. Note that when both generic and specific configuration files are downloaded, settings from the specific file always override the settings from the generic file.
configFileFetchingSpecificFileName	R/W	The name of the specific configuration file fetched by the unit (see <i>sysConfigDownloadConfigFile</i>). This file should be used to update the configuration of a single unit. This field may contain macros that are substituted by actual values at the moment of fetching the configuration file. Supported macros are: %mac% - the mac address of the unit %% - the character '%' Note: When the character "%" is not part of a macro, it is not replaced. If this field is empty (after macro substitution), no specific configuration file is fetched. Note that when both generic and specific configuration files are downloaded, settings from the specific file always override the settings from the generic file. Default Value: %mac%.cfg
configFileFetchingFileLocation	R/W	The path of the configuration files (<i>configFileFetchingFileName</i>) location. The path is relative to the root of the transfer server (<i>configFileFetchingHost</i>). Use '/' to separate subdirectories.

configFileTransfer

The following parameters allow you to define the configuration file transfer.

Table 139: Configuration File Fetching Parameters – Transfer

Name	Access	Description
configFileTransferProtocol	R/W	The protocol to use for transferring the configuration files. - tftp: Trivial File Transfer Protocol. - http: Hypertext Transfer Protocol. - https: Hypertext Transfer Protocol over Transport Layer Security (HTTP over TLS). This option requires that the appropriate security certificate be installed on the unit. Furthermore, because HTTPS relies on the system clock for server authentication, the SNTP client (see <i>sntpMIB</i>) must be enabled and properly configured. Please refer to the documentation shipped with your device for more details. Default Value: tftp
configFileTransferUsername	R/W	The user name to use for authentication when transferring the configuration files. Only applies when using HTTP or HTTPS as the transfer protocol.

Table 139: Configuration File Fetching Parameters – Transfer (Continued)

Name	Access	Description
configFileTransferPassword	R/W	The password to use for authentication when transferring the configuration files. Only applies when using HTTP or HTTPS as the transfer protocol.

configFileAutomaticUpdate

The following parameters allow you to define the automatic update service.

Table 140: Configuration File Fetching Parameters – Automatic Update

Name	Access	Description
configFileAutoUpdateOnRestartEnable	R/W	Enables/Disables the automatic update of the unit configuration on restart. - disable: The unit configuration is not automatically updated at each restart. - enable: If <code>sysConfigDownloadConfigFile</code> is set to automaticInitiateFileDownload, the unit configuration is updated with fetched configuration files at each restart. The unit is automatically restarted after a successful unit configuration update. The update is only performed if at least one parameter value defined in the fetched configuration files is different from the actual unit configuration. Default Value: enable
configFileAutoUpdatePeriodicEnable	R/W	Enables/Disables the periodic update of the unit configuration. - disable: The unit configuration is not periodically updated. - enable: If <code>sysConfigDownloadConfigFile</code> is set to automaticInitiateFileDownload, the unit configuration is periodically updated with fetched configuration files. The unit is automatically restarted after a successful unit configuration update. The update is only performed if at least one parameter value defined in the fetched configuration files is different from the actual unit configuration. Default Value: disable
configFileAutoUpdateTimeUnit	R/W	The time base for periodic unit configuration updates. Modification to this setting resets the update timer. - minutes: The unit configuration is updated every x minutes. - hours: The unit configuration is updated every x hours. - days: The unit configuration is updated every x days. Note that x is defined by <code>configFileAutoUpdatePeriod</code> . Default Value: days
configFileAutoUpdatePeriod	R/W	The period at which the configuration files are automatically fetched by the unit in order to update the unit configuration. Modification to this setting resets the update timer. This value is expressed in units defined by <code>configFileAutoUpdateTimeUnit</code> . Default Value: 1
configFileAutoUpdateTimeOfDay	R/W	This object is deprecated. It is recommended to use the variable <code>configFileAutoUpdateTimeRange</code> because it has precedence over this variable. The time of the day, based on <code>sntpTimeZoneString</code> , when the unit periodically fetches the configuration files in order to update the unit configuration. Note that the SNTP server needs to be enabled (see <code>sntpEnable</code>). Modification to this setting resets the update timer. The configuration files are fetched at the first occurrence of this value and thereafter with a period defined by <code>configFileAutoUpdatePeriod</code> . Let's say for instance the automatic unit configuration update is set with the time of day at 14h00 and the update period at every 2 days. If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on. -1: The time of the day at which the unit first fetches the configuration files is randomly selected. Only applies when <code>configFileAutoUpdateTimeUnit</code> is set to days . Default Value: -1

Table 140: Configuration File Fetching Parameters – Automatic Update (Continued)

Name	Access	Description
configFileAutoUpdateTimeRange	R/W	The time of the day, based on <i>sntpTimeZoneString</i>, when the unit periodically fetches the configuration files in order to update the unit configuration. If a time range is specified, the unit will fetch the configuration files at a random time within the interval specified. The format should be one of the following: <pre>hh[:mm[:ss]] hh[:mm[:ss]] - hh[:mm[:ss]]</pre> Where: <pre>hh: Hours. mm: Minutes. ss: Seconds.</pre> The configuration files are fetched at the first occurrence of this value and thereafter with a period defined by <i>configFileAutoUpdatePeriod</i>. Let's say for instance the automatic unit configuration update is set with the time of day at 14h00 and the update period at every 2 days. If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, then the second update two days later at the same hour, and so on. If the time range is set to '14:00 - 15:00' and the automatic unit configuration update is enabled within those hours, the first update will take place the following day. This means that a range of '00:00:00 - 23:59:59' will always take place the next day. Note that the SNTP server needs to be enabled (see <i>sntpEnable</i>). Modification to this setting resets the update timer. It only applies when <i>configFileAutoUpdateTimeUnit</i> is set to days.

configFilePrivacy

The following parameters allow you to define the automatic update service.

Table 141: Configuration File Fetching Parameters – Automatic Update

Name	Access	Description
configFilePrivacyEnable	R/W	Enables/Disables the decryption of the configuration files. - enable : The configuration files are decrypted by the unit. - disable : The configuration file are not decrypted by the unit. When enabled, the configuration files must be encrypted with keys matching the secrets set in the variables <i>configFilePrivacyGenericSecret</i> and <i>configFilePrivacySpecificSecret</i>. Default Value: disable
configFilePrivacyGenericSecret	R/W	The secret key used to decrypt the generic configuration file. The key is encoded in hexadecimal notation, meaning only characters in the range 0-9,A-F can be used. Each character encodes 4 bits of the key. If too many bits are supplied for a given cipher algorithm, the key is truncated. If not enough bits are provided, the key is padded with zeros. For example, a 32 bits key could look like: A36CB299. This key must match the key used for encryption of the generic configuration file in order for the settings to be applied. The generic configuration file is decrypted only if <i>configFilePrivacyEnable</i> is enabled and this value is not empty.
configFilePrivacySpecificSecret	R/W	The secret key used to decrypt the specific configuration file. The key is encoded in hexadecimal notation, meaning only characters in the range 0-9,A-F can be used. Each character encodes 4 bits of the key. If too many bits are supplied for a given cipher algorithm, the key is truncated. If not enough bits are provided, the key is padded with zeros. For example, a 32 bits key could look like: A36CB299. This key must match the key used for encryption of the specific configuration file in order for the settings to be applied. The specific configuration file is decrypted only if <i>configFilePrivacyEnable</i> is enabled and this value is not empty.

Configuration Parameters – SNMP Agent MIB

This MIB is used to customize the properties of the SNMP agent.

snmpAgentMIBObjects

The following parameters allow you to define the SNMP agent configuration parameters.

Table 142: MWI Parameters – General

Name	Access	Description
snmpAgentEnable	R/W	Enable or disable the SNMP service agent. - enable: SNMP connections are allowed. - disable: SNMP connections are forbidden. Default Value: enable
snmpAgentAccess	R/W	Interface from which the unit can be accessed via SNMP: - lanOnly: SNMP connections are only permitted on the LAN side. - wanOnly: SNMP connections are only permitted on the WAN side. - all: SNMP connections are permitted on both LAN and WAN sides. Default Value: all

Configuration Parameters – Boot Behavior MIB

This MIB contains boot behavior related objects for Mediatrix products.

bootBehaviorMIBObjects

The following parameter allows you to define the boot behavior configuration parameters.

Table 143: Boot Behavior Parameters – General

Name	Access	Description
checkTcpIpStackForSuccessfulBoot	R/W	Enable the check of TCP/IP stack before declaring the boot successful. This variable affects the behavior of the unit when it reboots and a TCP/IP flood occurs. The flood prevents the TCP/IP stack from initializing properly, and the unit eventually reboots again. After three unsuccessful reboots, the unit falls into rescue mode. When <i>checkTcpIpStackForSuccessfulBoot</i> is enabled, the TCP/IP stack must initialize properly to consider the reboot a success. In a flood scenario, the unit may end up in the rescue mode. When <i>checkTcpIpStackForSuccessfulBoot</i> is disabled, during a TCP/IP flood, even if the TCP/IP stack fails to initialize, the reboot is considered successful, and thus, the unit never goes into rescue mode in this scenario. Default Value: enable

Configuration Parameters – PIN Dialing MIB

This MIB contains PIN dialing configuration objects for Mediatrix products.

pinDialingMIBObjects

The PIN Dialing Feature allows the administrator to configure a PIN (Personal Identification Number) that would be dialled in “n” milliseconds after an outgoing call was established.

pinDialingIfTable

This table holds the PIN Dialing Configuration of each line.

Table 144: PIN Dialing Parameters – General

Name	Access	Description
pinDialingEnable	R/W	Enables or disables the PIN Dialing Feature. Default Value: disable
pinDialingPin	R/W	The PIN to dial. The PIN contains the DTMFs to be dialed. The supported digits are "0123456789*#abcdABCD". Pause characters ",", ":", and "p" are also supported and represent 1 second.
pinDialingDelay	R/W	The delay prior to sending the PIN. This value is expressed in milliseconds (ms). Default Value: 1000

Configuration Parameters – STUN MIB

This MIB provides information to configure the STUN client of the Mediatrix unit.

stunMIBObjects

STUN is a simple client / server protocol that uses UDP packets to discover the configuration information of NATs and firewalls between a device and the public Internet.

Table 145: STUN Parameters – General

Name	Access	Description
stunEnable	R/W	Enables/Disables the STUN client. Default Value: disable
stunQueryCacheDuration	R/W	Indicates the amount of time the unit should keep a STUN query result in its internal cache. Keeping a query in a cache helps reduce the amount of unnecessary STUN queries. When set to 0, the cache is disabled. The unit will do a STUN query each time a socket needs to be used. This value is expressed in seconds (s). Default Value: 0
stunQueryTimeout	R/W	Indicates the maximum amount of time the unit should wait for an answer to a STUN query sent to a STUN server. This variable only applies when stunEnable is set to enable. Caution is advised in setting long timeouts. In the advent of an unresponsive STUN server, the unit may end up waiting a long time before it determines that a call cannot be made due to the STUN server failure. This value is expressed in milliseconds (ms). Default Value: 1000
stunKeepAliveInterval	R/W	Indicates the interval at which blank keepalive messages are sent by the unit to keep a firewall hole opened. Keepalive messages are used by both the signaling protocol socket and the RTP socket to keep those connections opened through a firewall. When set to 0, no keep alive packet is sent. This value is expressed in seconds (s). Default Value: 30
stunNatBindingQueryInterval	R/W	Indicates the frequency at which a unit should do NAT binding discovery for its signaling protocol socket. This is only used with units that do not register their ports. Units that register their ports do their NAT binding discovery just before registering. This value is expressed in seconds (s). Default Value: 300

Configuration Parameters – ATM MIB

This MIB is used to configure ATM/OAM/AAL5 layers and to provide statistics from those layers.



Note: This MIB is not used by the current version of the Mediatix products.

atmMIBObjects

atmStatus

The following are the parameters used to define the ATM interface.

atmVcTable

A table of supported virtual circuit (VC).

Table 146: ATM Parameters – VC Table

Name	Access	Description
atmVcName	R/W	Indicates a user-defined name for this VC.
atmVcEnable	R/W	Enable or disable the VC. Default Value: disable
atmVcType	R/W	Indicates the function for which this VC will be used. - bridge : If the IpRouting is disabled, the LAN port will use the first enabled bridge VC in order to act as a bridge for a IP device connected to the Computer port. In case that the IpRouting is enabled, all bridge VCs are ignored. - wan: This type of VC is used for WAN. The type of the first VC is set to WAN and it is always enabled since it is requested to have a valid configuration. This WAN VC is always the one used to operate/administrate and manage the unit. Default Value: bridge
atmVcInUse	R-O	VC usage state. - notUsed - inUse Default Value: notUsed
atmVpi	R/W	Sets the selected Virtual Path Indicator to use for the VC connection. Default Value: 0
atmVci	R/W	Sets the selected Virtual Channel Indicator to use for the VC connection. Default Value: 32
atmEncapsulation	R/W	Sets the encapsulation used. - llcBridged(0): LLC SNAP Encapsulation used with a bridged protocol. - vcMuxBridged(1): VC Mux encapsulation used with a bridged protocol. - llcRouted(3): LLC SNAP Encapsulation used with a routed protocol. - vcMuxRouted(4): VC Mux encapsulation used with a routed protocol. Default Value: llcBridged

Table 146: ATM Parameters – VC Table (Continued)

Name	Access	Description
atmTxTrafficClass	R/W	Traffic class value for VC. - ubr(1) : Undefined Bit Rate (best effort) - cbr(2) : Constant Bit Rate - vbr(3) : Variable Bit Rate Default Value: ubr
atmTxPeakCellRate	R/W	Sets the peak cell rate used by this VC (cells/seconds). Default Value: 0
atmTxSustainableCellRate	R/W	Sets the Sustainable Cell Rate used by this VC (cells/seconds). Only meaningful for <i>atmQos</i> = VBR. Default Value: 0
atmTxMaximumBurstSize	R/W	Sets the maximum burst size for this VC (cells/seconds). Only meaningful for a traffic class of VBR. Default Value: 0
atmTxCellDelayVariationTolerance	R/W	Sets the maximum Cell Delay Variation Tolerance for the VC connection in microseconds. Only meaningful for traffic class of VBR or CBR. Default Value: 0
atmTxMinimumCellRate	R/W	Sets the minimum cell rate size for this VC (cells/seconds). Default Value: 0
atmTxMaximumSdu	R/W	Sets the maximum size of payload for an ATM cell for the VC connection (bytes). Default Value: 1524
atmRxTrafficClass	R/W	Traffic class value for VC. - ubr(1) : Undefined Bit Rate (best effort) - cbr(2) : Constant Bit Rate - vbr(3) : Variable Bit Rate Default Value: ubr
atmRxPeakCellRate	R/W	Sets the peak cell rate used by this VC (cells/seconds). Default Value: 0
atmRxSustainableCellRate	R/W	Sets the Sustainable Cell Rate used by this VC (cells/seconds). Only meaningful for a traffic class of VBR. Default Value: 0
atmRxMaximumBurstSize	R/W	Sets the maximum burst size for this VC (cells/seconds). Only meaningful for a traffic class of VBR. Default Value: 0 }
atmRxCellDelayVariationTolerance	R/W	Sets the Cell Delay Variation Tolerance for the VC connection (microseconds). Only meaningful for a traffic class of VBR or CBR. Default Value: 0
atmRxMinimumCellRate	R/W	Sets the minimum cell rate size for this VC (cells/seconds). Default Value: 0
atmRxMaximumSdu	R/W	Sets the maximum size of payload for an ATM cell for the VC connection (bytes). Default Value: 1524

aal5Stats**Table 147:** ATM Parameters – AAL5 Statistics

Name	Access	Description
aal5TxPdu	R-O	Total number of AAL5 frames sent since last reset.
aal5RxPdu	R-O	Total number of AAL5 frames received since last reset.
aal5TxTotalBytes	R-O	Total bytes sent with AAL5 since last reset.
aal5RxTotalBytes	R-O	Total bytes received with AAL5 since last reset.
aal5TxTotalErrorCounts	R-O	Total error counts with AAL5 on cells sent since last reset.
aal5RxTotalErrorCounts	R-O	Total error counts with AAL5 on cells received since last reset.

oamStats

Table 148: ATM Parameters – OAM Statistics

Name	Access	Description
oamNearEndF5LoopBackCount	R-O	Counter indicating the number of segmented OAM F5 Ping since last reset.
oamNearEndF4LoopBackCount	R-O	Counter indicating the number of segmented OAM F4 Ping since last reset.
oamFarEndF5LoopBackCount	R-O	Counter indicating the number of end-to-end OAM F5 Ping since last reset.
oamFarEndF4LoopBackCount	R-O	Counter indicating the number of end-to-end OAM F4 Ping since last reset.

oamTools

OAM tools used in a ping command.

Table 149: ATM Parameters – OAM Tools

Name	Access	Description
oamResult	R-O	Holds the values of the last OAM operation performed. - failed(0): OAM test failed. - success(1): OAM test success. - pending(2): OAM test pending. - notStarted(3): OAM not started
generateOamPing	R/W	This command generates an OAM ping operation. This command has the following values: - noOp(0) : No operation. When read, this value is returned. - ping(1) : Perform the OAM ping. This command also uses the following variables: - oamPingType: F4 OAM ping or F5 OAM ping. - oamVpi : Value for the VPI. - oamVci : Value for the VCI (only used for f5OamPing commands). - oamMode: Value for the OAM mode (end-to-end or segment) - oamLimitTimeout: Timeout value in milliseconds Default Value: noOp

oamToolsParameters

OAM tools parameters used in a ping command..

Table 150: ATM Parameters – OAM Tools Parameters

Name	Access	Description
oamPingType	R/W	This command generates an OAM ping operation. This command has the following values: - f4OamPing(0): OAM ping on the VP. - f5OamPing(1): OAM ping on the VC. Default Value: f4OamPing
oamVpi	R/W	This variable indicates the VPI part of the PVC to be tested for an OAM ping command. Default Value: 0
oamVci	R/W	This variable indicates the VCI part of the PVC to be tested by an OAM ping command. Only used for F5 OAM ping. Default Value: 32
oamMode	R/W	This variable indicates what the target of the OAM ping command refers to. - segmented(0) : Middle man of VC - endToEnd(1): End point of VC Default Value: endToEnd
oamTimeOut	R/W	This variable indicates a timeout value in milliseconds to wait for the completion of the OAM ping. 0 means no limit. Otherwise the lower limit is 10 milliseconds. Default Value: 0

Configuration Parameters – DSL MIB

This MIB describes the parameters used by the DSL module.



Note: This MIB is not used by the current version of the Mediatrix products.

dsLMIBObjects

dslStatus

The following are the parameters used to define the DSL connection.

Table 151: DSL Parameters – General Parameters

Name	Access	Description
dslModulation	R/W	Sets the desired modulation for the DSL modem. The accepted values for the configuration are: - mMode(1): Autodetects the modulation of the DSLAM. - t1413(2): T1.413 modulation mode. Supports the T1.413 standard. - gDmt(3): G.DMT modulation mode. Supports the G992.1 standard. - gLite(4): G.Lite modulation mode. Supports the G992.2 standard. - adsl2(8): ADSL2 modulation mode. Supports the G992.3 standard. - adsl2Delt(9): ADSL2 DELT modulation mode. Supports the G992.3 DELT standard. - adsl2Plus(16): ADSL2+ modulation mode. Supports the G992.5 standard. - adsl2PlusDelt(17): ADSL2+ DELT modulation mode. Supports the G992.5 DELT standard. Default Value: mMode
dslModemState	R-O	Display sthe current state of the DSL modem. Correct values are: - unconnected(0): The modem is waiting for a connection or a modulation change. - connecting(1): The modem is connected and getting ready to perform with a specific modulation. Training between the modem and DSLAM is taking place. - connected(2): The modem is connected and ready to transmit and receive.
dslTrainedPath	R-O	Displays the trained path type of the DSL modem. The accepted values for the configuration are: - fast(0): Fast path - interleaved(1): Interleaved path

Table 151: DSL Parameters – General Parameters (Continued)

Name	Access	Description
dslTrainedModulation	R-O	Displays the trained modulation of the DSL modem. The values meaning are: - notTrained(0): The modem has not trained with the DSLAM. - t1413(2): T1.413 modulation mode. Supports the T1.413 standard. - gDmt(3): G.DMT modulation mode. Supports the G992.1 standard. - gLite(4): G.Lite modulation mode. Supports the G992.2 standard. - adsl2(*) : ADSL2 modulation mode. Supports the G992.3 standard. - adsl2Delt(9): ADSL2 DELT modulation mode. Supports the G992.3 DELT standard. - adsl2Plus(16) : ADSL2+ modulation mode. Supports the G992.5 standard. - adsl2PlusDelt(17): ADSL2+ DELT modulation mode. Supports the G992.5 DELT standard.

dslModemStats

Table 152: DSL Parameters – DSL Modem Statistics

Name	Access	Description
dslModemTxConnectionRate	R-O	Rate (KBps) of the upstream connection.
dslModemRxConnectionRate	R-O	Rate (KBps) of the downstream connection.
dslModemTxLineAttenuation	R-O	Upstream line attenuation (dB).
dslModemRxLineAttenuation	R-O	Downstream line attenuation (dB).
dslModemTxMargin	R-O	Upstream line margin (dB).
dslModemRxMargin	R-O	Downstream line margin (dB).
dslModemTxPayload	R-O	Upstream payload size (bytes).
dslModemRxPayload	R-O	Downstream payload size (bytes).
dslModemTxSuperframeCnt	R-O	Counter indicating the number of superframes sent since the last reset.
dslModemRxSuperframeCnt	R-O	Counter indicating the number of superframes received since the last reset.
dslModemLossOfSignalCount	R-O	Counts how many loss of signal occurred since the last reset.
dslModemSeverlyErroredFrameCount	R-O	Counts how many severely errored frames were received since the last reset.
dslModemTxPeakCellRate	R-O	Peak (ATM) cell rate observed by the modem. (cells per second).

interleavedPath

Table 153: DSL Parameters – Interleaved Path Statistics

Name	Access	Description
interleavedPathRxCrcError	R-O	Counter indicating the number of CRC errors received by the interleaved path since the last reset.
interleavedPathTxCrcError	R-O	Counter indicating the number of CRC errors caused by the modem interleaved path since the last reset.

fastPath

Table 154: DSL Parameters – Fast Path Statistics

Name	Access	Description
fastPathTxCrcError	R-O	Counter indicating the number of CRC errors caused by the modem fast path since the last reset.
fastPathRxCrcError	R-O	Counter indicating the number of CRC errors received by the fast path since the last reset.

Configuration Parameters – PPPoA MIB

This MIB is used to customize properties of the PPPoA service.



Note: This MIB is not used by the current version of the Mediatrix products.

pppoaMIBObjects

The following parameters allow you to define the PPPoA configuration parameters.

Table 155: PPPoA Parameters – General

Name	Access	Description
pppoaEnable	R/W	Enable/disable the PPPoA service. - enable: The PPPoA service is enabled. The unit tries to establish a PPPoA connection to the edge aggregation router. - disable: The PPPoA service is disabled. If both this variable and <i>pppoeEnable</i> from the <i>pppoeMIB</i> are set to enable, PPPoE has priority over PPPoA (PPPoA will not be enabled). This variable's semantics are different depending on the protocol and hardware platform. Please refer to the documentation shipped with your device for more details. Default Value: disable

Configuration Parameters – Security Certificates MIB

This MIB is used to manage the security certificates.

securityCertificatesMIBObjects

The following parameters allow you to define the security certificates configuration parameters.

certificateTable

A table of X.509 security certificates that are installed on this unit.

Table 156: Security Certificates Parameters

Name	Access	Description
certificateName	R-O	The name of the certificate. Displays the file name of the certificate, without the extension.
certificateSubjectCommonName	R-O	The certificate's subject name. If the certificate contains a subject field, displays the common name. Otherwise, displays the first non-empty subject alternative name from the following list: • Uniform Resource Identifier • DNS name • IP Address • RFC 822 name See RFC 3280 sections 4.1.2.6 and 4.2.1.7 for details.
certificateExpirationDate	R-O	The certificate's expiration date. Displays the date at which the certificate expires. The format is MM/DD/YYYY in universal time. See RFC 3280 section 4.1.2.5 for details.

Configuration Parameters – Interop MIB

This MIB contains Mediatrix unit interoperability configuration objects.

mxInteropMIBObjects

The following parameters allow you to define interop parameters.

Table 157: Interop Parameters

Name	Access	Description
mxInteropHttpUAHeaderConfig	R/W	Customize the HTTP User-Agent header value of HTTP request. The following macros are replaced by their representation: • %version%: Version of the application. • %mac%: Unit MAC address (lowercase). • %rev%: Hardware revision number. • %product%: Product name. • %%: A '%' sign." Default Value: %product%

Configuration Parameters – NAT MIB

This MIB provides information to configure the NAT module. This module configures the port forwarding, also known as virtual server or destination NAT (DNAT).

natMIBObjects

natPortForwarding

natPortForwardingTable

A table that contains the port forwarding rules. This table is enabled if the variable *ipRoutingEnable* is enabled and if the variable *ipRoutingMode* is set to NAT.

This table can contain up to 20 port forwarding rules.

These rules will be applied only on the incoming WAN traffic destined to the LAN.

This table's semantics are different depending on the hardware platform. Please refer to the documentation shipped with your device for more details.

Table 158: NAT Parameters – General

Name	Access	Description
natPortForwardingWanStartPort	R/W	The port on the unit's WAN side may be configured in two ways: - by identifying only one port or a port range. If the redirection affects only one port, the current variable represents this port and the variable <i>natPortForwardingWanFinishPort</i> must be the same. - In the case of a port range, the current variable represents the first port of the range, while the variable <i>natPortForwardingWanFinishPort</i> represents the last port of the range.
natPortForwardingWanFinishPort	R/W	If the redirection affects a port range, the current variable represents the last port of the range, while the variable <i>natPortForwardingWanStartPort</i> represents the first port of the range. In the case of a single port forwarding, this variable must be the same as <i>natPortForwardingWanStartPort</i> .
natPortForwardingProtocol	R/W	The protocol of the packets to forward. The specified protocol can be UDP, TCP or both. - udp: User Datagram Protocol - tcp: Transmission Control Protocol - all: UDP and TCP
natPortForwardingLanAddr	R/W	The new destination address on the unit's LAN side is configured by this variable.
natPortForwardingLanPort	R/W	The destination port on the unit's LAN side may be configured in two ways. - First, the WAN destination port or port range remains the same on the LAN side. For this configuration, the current variable must be set to 0. - Second, the traffic matching this rule is redirected to only one port on the LAN side. For this configuration, the current variable represents this port. Default Value: 0
natPortForwardingRuleLabel	R/W	Short description of the port forwarding rule.

Table 158: NAT Parameters – General (Continued)

Name	Access	Description
natPortForwardingRuleEnable	R/W	Indicates if the specific port forwarding rule of a row is used or not. This rule is enabled if the variable <i>ipRoutingEnable</i> is enabled and if the variable <i>ipRoutingMode</i> is set to NAT. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: disable

natSyslog

The following parameter allows you to enable or disable the syslog for NAT.

Table 159: NAT Parameters – Syslog

Name	Access	Description
natSyslogEnable	R/W	Enables/Disables the syslog for NAT notification messages. Default Value: disable

Configuration Parameters – Firewall MIB

This MIB provides information to configure the firewall module. This module is responsible to accept or drop packets intended for the unit and the clients on the LAN. The DROP action is done silently by default, without sending packets in answer. Otherwise, the specific action will be documented.

firewallMIBObjects

The following parameters allow you to configure the Firewall feature.

Table 160: Firewall Parameters – General

Name	Access	Description
firewallEnable	R/W	Enables/Disables the firewall. - enable: The traffic is analyzed and filtered by all the rules configured in this module. All the enabled security rules in this module apply immediately. - disable: No security rule is activated. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. This variable's semantics are different depending on the hardware platform. Please refer to the documentation shipped with your device for more details. Default Value: enable

firewallSecurity

The following parameter allows you to set the Firewall Security features.

Table 161: Firewall Parameters – Security

Name	Access	Description
firewallSecurityBadTcpPacketRule	R/W	Enables/Disables the behavior to drop the bad TCP packets from the WAN side. When enabled, this variable configures rules that check incoming TCP packets for malformed headers. If a bad TCP packet is found, the firewall drops it silently. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: enable
firewallSecurityTcpSynCookiesRule	R/W	Enables/Disables the behavior to protect the unit against the common 'syn flood attack'. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: enable
firewallSecuritySourceRoutedPacketRule	R/W	Enables/Disables the behavior to drop source routed packets (packets with SRR option) from the WAN side. When enabled, this variable configures rules that drop all packets with this option silently. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: disable

Table 161: Firewall Parameters – Security (Continued)

Name	Access	Description
firewallSecurityMulticastPacketRule	R/W	Enables/Disables the behavior to drop multicast packets from the WAN side. When enabled, this variable configures rules that drop incoming WAN multicast packets. If multicast packets are found, the firewall drops them silently. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: enable
firewallSecurityIdentRule	R/W	Enables/Disables the behavior to drop IDENT request packets from the WAN side. When enabled, this variable configures rules that drop incoming IDENT request packets and send back a TCP RST packet. This behavior is required because dropping silently on port 113 may cause connection problems. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: enable
firewallSecurityReversePathFilteringRule	R/W	Enables/Disables the behavior to filter packets by reverse path filtering. When enabled, this variable configures rules that silently drop packets received on one interface and answered on another interface. In this case, the packet is bogus and the firewall drops it. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: disable
firewallSecurityBlockWanEchoRequestRule	R/W	Enables/Disables the behavior to silently drop ICMP echo requests received from the WAN side. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: disable
firewallSecurityBlockLanEchoRequestRule	R/W	Enables/Disables the behavior to silently drop ICMP echo requests received on the LAN interface. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: disable
firewallSecurityBlockWanEchoBroadcastRule	R/W	Enables/Disables the behavior to silently drop incoming WAN ICMP echo requests sent to the broadcast address. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: enable
firewallSecurityBlockIcmpRedirectionInRule	R/W	Enables/Disables the behavior to silently drop the reception of ICMP redirect messages from the WAN side. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: enable
firewallSecurityBlockIcmpRedirectionOutRule	R/W	Enables/Disables the behavior to block sending of ICMP redirect messages. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: enable

firewallSecuritySpoof

This parameter allows you to enable or disable the Firewall Security Spoof feature.

Table 162: Firewall Parameters – Security Spoof

Name	Access	Description
firewallSecuritySpoofEnable	R/W	Enables/Disables the security rules against IP addresses spoofing contained in the table <i>firewallSecuritySpoofTable</i> . These rules can prevent reception of packets from the WAN side according to the source address of those packets. This variable applies only if the variable <i>firewallEnable</i> is enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: enable

firewallSecuritySpoofTable

A table that contains the static security rules against spoofing. Each one of these rules must be enabled by the variable *firewallSecuritySpoofRuleEnable*.

This table applies only if the variable *firewallSecuritySpoofEnable* is enabled and if the variable *firewallEnable* is also enabled.

The user cannot add rules in this table. The user can simply enable or disable the rules present.

Table 163: Firewall Parameters – Security Spoof Table

Name	Access	Description
firewallSecuritySpoofLabel	R-O	Short description of the anti-spoofing rule.
firewallSecuritySpoofAddress	R-O	Source IP address and mask of the packets this rule must drop silently.
firewallSecuritySpoofRuleEnable	R/W	Indicates if the specific anti-spoofing rule of a row is used or not. This variable applies only if both the variable <i>firewallEnable</i> and this table are enabled. Since the modification of this variable will be applied in real time, new settings can affect the current network connections. Default Value: disable

firewallSyslog

The following parameter allows you to enable or disable the syslog for Firewall.

Table 164: Firewall Parameters – Syslog

Name	Access	Description
firewallSyslogEnable	R/W	Enables/Disables the syslog for the firewall notification messages. Default Value: disable

IP Telephony Signalling

H.323 MIBs

Page Left Intentionally Blank

H.323 Protocol Parameters – Registration MIB

This MIB contains configuration objects for H.323 units registration.

h323RegistrationMIBObjects

The following parameter allows you to define the registration method used by the H.323 unit.

Table 165: H.323 Parameters – Registration Method

Name	Access	Description
h323RegMethod	R/W	The registration method used by the unit. Specifies how the unit registers its lines and groups of lines. The unit can register all its lines/groups together or it can register its lines/groups individually. • none: No gatekeeper registration. The unit does not register any line/group. • single: The unit registers all its lines and groups of lines together. The unit registers all the aliases of its lines/groups together. • multiple: the unit registers its lines/groups of lines individually. For each line/group, the unit local IP address is used. For each line/group, a unique RAS port and a unique call signaling port are used. Each line/group can be configured to register or not. Default Value: none

h323RegistrationSingleRegistration

The following parameters allow you to define the H.323 single registration information.

Table 166: H.323 Parameters – Single Registration

Name	Access	Description
h323SingleRegGkDiscoveryMode	R/W	The gatekeeper discovery method used by the unit. AUTOMATIC GATEKEEPER DISCOVERY METHOD The unit follows these steps until it registers successfully. 1. The unit sends a <i>gatekeeperRequest</i> message on the well-known Discovery Multicast Address. Every gatekeeper on the same network (as the unit) receives the <i>gatekeeperRequest</i> message. 2. A gatekeeper that accepts the gatekeeper request sends a <i>gatekeeperConfirm</i> message to the unit. The unit then sends a <i>registrationRequest</i> message to that gatekeeper. The gatekeeper responds with a <i>registrationConfirm</i> message. The unit is now registered. If several gatekeepers accept the gatekeeper request, the unit registers with the first gatekeeper that accepted the gatekeeper request (i.e. the gatekeeper that sent the first <i>gatekeeperConfirm</i> message received by the unit). 3. A gatekeeper that rejects the gatekeeper request sends a <i>gatekeeperReject</i> message to the unit. The unit does not initiate any action upon receipt of a <i>gatekeeperReject</i> message. 4. If no <i>gatekeeperConfirm</i> message is received within a time-out, the unit starts again at step 1. The calculation of the time-out starts as soon as the first <i>gatekeeperRequest</i> message is sent. Note: After sending a <i>gatekeeperRequest</i> message, the unit only considers the first answer (the first <i>gatekeeperConfirm</i> message or the first <i>gatekeeperReject</i> message). If the first answer to be received is a <i>gatekeeperReject</i> message, the unit sends another <i>gatekeeperRequest</i> message. MANUAL GATEKEEPER DISCOVERY METHOD The unit is configured with a list of gatekeeper IP addresses. The unit follows these steps until it registers successfully. 1. The unit sends a <i>registrationRequest</i> message to the first gatekeeper IP address of the list. 2. If the gatekeeper accepts the registration request, i.e. the gatekeeper sends a <i>registrationConfirm</i> message to the unit, the unit is now registered. 3. If the gatekeeper rejects the registration request, i.e. the gatekeeper sends a <i>registrationReject</i> message to the unit, the unit sends a <i>registrationRequest</i> message to the next gatekeeper IP address of the list. 4. If the registration request times-out, i.e. there is no answer from the gatekeeper, the unit sends a <i>registrationRequest</i> message to the next gatekeeper IP address of the list. 5. If the unit reaches the end of the list without registering successfully, the unit waits before starting again at step 1. During this waiting period, the unit does not send any <i>registrationRequest</i> message. Default Value: manual
h323SingleRegRetryTime	R/W	The waiting period, in seconds, between two gatekeeper registration attempts or two gatekeeper discovery attempts. After an unsuccessful gatekeeper registration (no answer from the gatekeeper), this waiting period specifies how long the terminal waits before trying to register again. After an unsuccessful gatekeeper discovery, this waiting period specifies how long the unit waits before starting a new gatekeeper discovery. Available values range from 30 seconds to 3600 seconds. Default Value: 60

Table 166: H.323 Parameters – Single Registration (Continued)

Name	Access	Description
h323SingleRegLightweightEnable	R/W	Indicates if the lightweight registration functionality is enabled. - disable: the unit does not use the lightweight registration functionality. The unit does not include the <i>timeToLive</i> field in the <i>registrationRequest</i> message. - enable: the unit uses the lightweight registration functionality. The unit includes the <i>timeToLive</i> field in the <i>registrationRequest</i> message. For the lightweight registration functionality, the following RAS message fields are used: <i>keepAlive</i> field of the <i>registrationRequest</i> message. The <i>keepAlive</i> field is either true or false. <i>timeToLive</i> field of the <i>registrationRequest</i> and <i>registrationConfirm</i> messages. The <i>timeToLive</i> field is a number of seconds. - A full <i>registrationRequest</i> message has the <i>keepAlive</i> field set to false. - A lightweight <i>registrationRequest</i> message has the <i>keepAlive</i> field set to true. When the lightweight registration functionality is enabled, the unit follows these steps: - The unit sends a first <i>registrationRequest</i> message to the gatekeeper. This <i>registrationRequest</i> message has the <i>keepAlive</i> field set to false and contains the <i>timeToLive</i> field. The value of the <i>timeToLive</i> field is configurable. - If the <i>registrationConfirm</i> message contains the <i>timeToLive</i> field, the unit sends lightweight <i>registrationRequest</i> messages. The interval between each lightweight <i>registrationRequest</i> message is one-third of the <i>timeToLive</i> value from the gatekeeper (from the <i>registrationConfirm</i> message). On a network with heavy traffic, a lightweight <i>registrationRequest</i> message could arrive a few seconds late at the gatekeeper. Furthermore, since the RAS channel between a unit and a gatekeeper is unreliable (UDP), a lightweight <i>registrationRequest</i> message may never arrive at the gatekeeper. These problems are avoided by using an interval equal to one-third the <i>timeToLive</i> value of the <i>registrationConfirm</i> message. - If the <i>registrationConfirm</i> message does not contain the <i>timeToLive</i> field, the unit does not send lightweight <i>registrationRequest</i> messages. Default Value: enable
h323SingleRegLightweightTimeToLive	R/W	The interval, in seconds, proposed to the gatekeeper for the lightweight registration functionality. When the lightweight registration functionality is enabled, the unit uses this value for the <i>timeToLive</i> field of the <i>registrationRequest</i> message. Available values range from 30 seconds to 3600 seconds. Default Value: 60
h323SingleRegRasPortSource	R/W	Indicates the source of the local RAS port. This applies only if the unit is configured to register. If the unit is not configured to register, it uses the well-known RAS port (1719) for its local RAS port. The local RAS port is used to exchange registration, admission and status messages with a gatekeeper. Examples of RAS messages sent by the unit are <i>registrationRequest</i>, <i>admissionRequest</i> and <i>disengageRequest</i>. Examples of RAS messages received by the unit are <i>registrationConfirm</i>, <i>admissionReject</i> and <i>disengageConfirm</i>. - dynamic: the unit chooses its local RAS port at run time. - static: the administrator sets the local RAS port. Default Value: dynamic
h323SingleRegStaticRasPort	R/W	The local static RAS port number. Available values range from 1719 to 1720 and from 7000 to 65535. Default Value: 7000
h323SingleRegCallSignalingPortSource	R/W	Indicates the source of the local call signaling port. Applies only if the unit is configured to register. If the unit is not configured to register, it uses the well-known call signaling port (1720) for its local call signaling port. The local call signaling port is used to exchange Q.931 messages with gatekeepers and other H.323 endpoints. Examples of Q.931 messages are SETUP, CONNECT and RELEASE COMPLETE. - dynamic: the unit chooses its local call signaling port at run time. - static: the administrator sets the local call signaling port. Default Value: dynamic

Table 166: H.323 Parameters – Single Registration (Continued)

Name	Access	Description
h323SingleRegStaticCallSignalingPort	R/W	The local static call signaling port number. Available values range from 1719 to 1720 and from 7000 to 65535. Default Value: 7000

h323RegistrationMultipleRegistrationIfTable

This table holds the multiple registration configuration. Each row is used to configure the gatekeeper registration of one line. This table only applies to unit of type terminal.

Table 167: H.323 Parameters – Multiple Registration

Name	Access	Description
h323MultipleRegGroupIndex	R-O	Indicates which group is associated with this line. This variable only applies to unit of type terminal. A value different than 0 indicates that the registration configuration for this line is superceded by the corresponding entry in the <i>h323RegistrationMultipleRegistrationGroupTable</i> . A value of 0 means this line is not part of a group and that it can be configured using this entry. Default Value: 0
h323MultipleRegEnable	R/W	Indicates if the line should register with a gatekeeper. This variable only applies to unit of type terminal. - disable: the line does not register with a gatekeeper. There is no gatekeeper registration for this line. - enable: the line registers with a gatekeeper. Default Value: enable

Table 167: H.323 Parameters – Multiple Registration (Continued)

Name	Access	Description
h323MultipleRegGkDiscoveryMode	R/W	The gatekeeper discovery method used by the line. This variable only applies to unit of type terminal. AUTOMATIC GATEKEEPER DISCOVERY METHOD The line follows these steps until it registers successfully. 1. The line sends a <i>gatekeeperRequest</i> message on the well-known Discovery Multicast Address. Every gatekeeper on the same network (as the line) receives the <i>gatekeeperRequest</i> message. 2. A gatekeeper that accepts the gatekeeper request sends a <i>gatekeeperConfirm</i> message to the line. The line then sends a <i>registrationRequest</i> message to that gatekeeper. The gatekeeper responds with a <i>registrationConfirm</i> message. The line is now registered. If several gatekeepers accept the gatekeeper request, the line registers with the first gatekeeper that accepted the gatekeeper request (i.e. the gatekeeper that sent the first <i>gatekeeperConfirm</i> message received by the line). 3. A gatekeeper that rejects the gatekeeper request sends a <i>gatekeeperReject</i> message to the line. The line does not initiate any action upon receipt of a <i>gatekeeperReject</i> message. 4. If no <i>gatekeeperConfirm</i> message is received within a time-out, the line starts again at step 1. The calculation of the time-out starts as soon as the first <i>gatekeeperRequest</i> message is sent. Note: After sending a <i>gatekeeperRequest</i> message, the line only considers the first answer (the first <i>gatekeeperConfirm</i> message or the first <i>gatekeeperReject</i> message). If the first answer to be received is a <i>gatekeeperReject</i> message, the line sends another <i>gatekeeperRequest</i> message. MANUAL GATEKEEPER DISCOVERY METHOD The unit is configured with a list of gatekeeper IP addresses. Each line uses the same list of gatekeeper IP addresses. The line follows these steps as long as it does not register successfully. 1. The line sends a <i>registrationRequest</i> message to the first gatekeeper IP address of the list. 2. If the gatekeeper accepts the registration request, i.e. the gatekeeper sends a <i>registrationConfirm</i> message to the line, the line is now registered. 3. If the gatekeeper rejects the registration request, i.e. the gatekeeper sends a <i>registrationReject</i> message to the line, the line sends a <i>registrationRequest</i> message to the next gatekeeper IP address of the list. 4. If the registration request times-out, i.e. there is no answer from the gatekeeper, the line sends a <i>registrationRequest</i> message to the next gatekeeper IP address of the list. 5. If the line reaches the end of the list without registering successfully, the line waits before starting again at step 1. During this waiting period, the line does not send any <i>registrationRequest</i> message. Default Value: manual
h323MultipleRegRetryTime	R/W	The waiting period, in seconds, between two gatekeeper registration attempts or two gatekeeper discovery attempts. This variable only applies to unit of type terminal. After an unsuccessful gatekeeper registration (no answer from the gatekeeper), this waiting period specifies how long the line waits before trying to register again. After an unsuccessful gatekeeper discovery (no answer from any gatekeeper or after receiving a <i>gatekeeperReject</i> message), this waiting period specifies how long the line waits before starting a new gatekeeper discovery. Available values range from 30 seconds to 3600 seconds. Default Value: 60

Table 167: H.323 Parameters – Multiple Registration (Continued)

Name	Access	Description
h323MultipleRegLightweightEnable	R/W	Indicates if the lightweight registration functionality is enabled. This variable only applies to unit of type terminal. • disable: the line does not use the lightweight registration functionality. The line does not include the <i>timeToLive</i> field in the <i>registrationRequest</i> message. • enable: the line uses the lightweight registration functionality. The line includes the <i>timeToLive</i> field in the <i>registrationRequest</i> message. For the lightweight registration functionality, the following RAS message fields are used: • <i>keepAlive</i> field of the <i>registrationRequest</i> message. The <i>keepAlive</i> field is either true or false. • <i>timeToLive</i> field of the <i>registrationRequest</i> and <i>registrationConfirm</i> messages. The <i>timeToLive</i> field is a number of seconds. • A full <i>registrationRequest</i> message has the <i>keepAlive</i> field set to false. • lightweight <i>registrationRequest</i> message has the <i>keepAlive</i> field set to true. When the lightweight registration functionality is enabled, the line follows these steps: 1. The line sends a first <i>registrationRequest</i> message to the gatekeeper. This <i>registrationRequest</i> message has the <i>keepAlive</i> field set to false and contains the <i>timeToLive</i> field. The value of the <i>timeToLive</i> field is configurable. 2. If the <i>registrationConfirm</i> message contains the <i>timeToLive</i> field, the line sends lightweight <i>registrationRequest</i> messages. The interval between each lightweight <i>registrationRequest</i> message is one-third of the <i>timeToLive</i> value from the gatekeeper (from the <i>registrationConfirm</i> message). On a network with heavy traffic, a lightweight <i>registrationRequest</i> message could arrive a few seconds late at the gatekeeper. Furthermore, since the RAS channel between a line and a gatekeeper is unreliable (UDP), a lightweight <i>registrationRequest</i> message may never arrive at the gatekeeper. These problems are avoided by using an interval equal to one-third the <i>timeToLive</i> value of the <i>registrationConfirm</i> message. 3. If the <i>registrationConfirm</i> message does not contain the <i>timeToLive</i> field, the line does not send lightweight <i>registrationRequest</i> messages. Default Value: enable
h323MultipleRegLightweightTimeToLive	R/W	The interval, in seconds, proposed to the gatekeeper for the lightweight registration functionality. When the lightweight registration functionality is enabled, the line uses this value for the <i>timeToLive</i> field of the <i>registrationRequest</i> message. Available values range from 30 seconds to 3600 seconds. Default Value: 60
h323MultipleRegRasPortSource	R/W	Indicates the source of the local RAS port. This applies only if the line is configured to register. If the line is not configured to register, it uses the well-known RAS port (1719) for its local RAS port. This variable only applies to unit of type terminal. The local RAS port is used to exchange registration, admission and status messages with a gatekeeper. Examples of RAS messages sent by the line are <i>registrationRequest</i>, <i>admissionRequest</i> and <i>disengageRequest</i>. Examples of RAS messages received by the line are <i>registrationConfirm</i>, <i>admissionReject</i> and <i>disengageConfirm</i>. • dynamic: the line chooses its local RAS port at run time. • static: the administrator sets the local RAS port. Default Value: dynamic
h323MultipleRegStaticRasPort	R/W	The local static RAS port number of the line. This variable only applies to unit of type terminal. Available values range from 1719 to 1720 and from 7000 to 65535. Default Value: 7000

Table 167: H.323 Parameters – Multiple Registration (Continued)

Name	Access	Description
h323MultipleRegCallSignalingPortSource	R/W	Indicates the source of the local call signaling port. This applies only if the line is configured to register. If the line is not configured to register, it uses the well-known call signaling port (1720) for its local call signaling port. This variable only applies to unit of type terminal. The local call signaling port is used to exchange Q.931 messages with gatekeepers and other H.323 endpoints. Examples of Q.931 messages are SETUP, CONNECT and RELEASE COMPLETE. - dynamic: the line chooses its local call signaling port at run time. - static: the administrator sets the local call signaling port. Default Value: dynamic
h323MultipleRegStaticCallSignalingPort	R/W	The local static call signaling port number of the line. This variable only applies to unit of type terminal. Values range from 1719 to 1720 and from 7000 to 65535. Default Value: 7000

h323RegistrationMultipleRegistrationGroupTable

This table holds the multiple registration configuration for group of lines. Each row is used to configure the gatekeeper registration of one group of lines.

Table 168: H.323 Parameters – Group Registration

Name	Access	Description
h323GroupMultipleRegEnable	R/W	Indicates if the group should register with a gatekeeper. - disable: the group does not register with a gatekeeper. There is no gatekeeper registration for this group. - enable: the group registers with a gatekeeper. Default Value: enable

Table 168: H.323 Parameters – Group Registration (Continued)

Name	Access	Description
h323GroupMultipleRegGkDiscoveryMode	R/W	The gatekeeper discovery method used by the group of lines. AUTOMATIC GATEKEEPER DISCOVERY METHOD The group follows these steps until it registers successfully. 1. The group sends a <i>gatekeeperRequest</i> message on the well-known Discovery Multicast Address. Every gatekeeper on the same network (as the unit) receives the <i>gatekeeperRequest</i> message. 2. A gatekeeper that accepts the gatekeeper request sends a <i>gatekeeperConfirm</i> message to the group. The group then sends a <i>registrationRequest</i> message to that gatekeeper. The gatekeeper responds with a <i>registrationConfirm</i> message. The group is now registered. If several gatekeepers accept the gatekeeper request, the group registers with the first gatekeeper that accepted the gatekeeper request (i.e. the gatekeeper that sent the first <i>gatekeeperConfirm</i> message received by the group). 3. A gatekeeper that rejects the gatekeeper request sends a <i>gatekeeperReject</i> message to the group. The group does not initiate any action upon receipt of a <i>gatekeeperReject</i> message. 4. If no <i>gatekeeperConfirm</i> message is received within a time-out, the group starts again at step 1. The calculation of the time-out starts as soon as the first <i>gatekeeperRequest</i> message is sent. Note: After sending a <i>gatekeeperRequest</i> message, the group only considers the first answer (the first <i>gatekeeperConfirm</i> message or the first <i>gatekeeperReject</i> message). If the first answer to be received is a <i>gatekeeperReject</i> message, the group sends another <i>gatekeeperRequest</i> message. MANUAL GATEKEEPER DISCOVERY METHOD The unit is configured with a list of gatekeeper IP addresses. Each group uses the same list of gatekeeper IP addresses. The group follows these steps as long as it does not register successfully. 1. The group sends a <i>registrationRequest</i> message to the first gatekeeper IP address of the list. 2. If the gatekeeper accepts the registration request, i.e. the gatekeeper sends a <i>registrationConfirm</i> message to the group, the group is now registered. 3. If the gatekeeper rejects the registration request, i.e. the gatekeeper sends a <i>registrationReject</i> message to the group, the group sends a <i>registrationRequest</i> message to the next gatekeeper IP address of the list. 4. If the registration request times-out, i.e. there is no answer from the gatekeeper, the group sends a <i>registrationRequest</i> message to the next gatekeeper IP address of the list. 5. If the group the end of the list without registering successfully, the group waits before starting again at step 1. During this waiting period, the group does not send any <i>registrationRequest</i> message. Default Value: manual
h323GroupMultipleRegRetryTime	R/W	The waiting period, in seconds, between two gatekeeper registration attempts or two gatekeeper discovery attempts. After an unsuccessful gatekeeper registration (no answer from the gatekeeper), this waiting period specifies how long the group of lines waits before trying to register again. After an unsuccessful gatekeeper discovery (no answer from any gatekeeper or after receiving a <i>gatekeeperReject</i> message), this waiting period specifies how long the group waits before starting a new gatekeeper discovery. Available values range from 30 seconds to 3600 seconds. Default Value: 60

Table 168: H.323 Parameters – Group Registration (Continued)

Name	Access	Description
h323GroupMultipleRegLightweightEnable	R/W	Indicates if the lightweight registration functionality is enabled. • disable: the group does not use the lightweight registration functionality. The group does not include the <i>timeToLive</i> field in the <i>registrationRequest</i> message. • enable: the group uses the lightweight registration functionality. The group includes the <i>timeToLive</i> field in the <i>registrationRequest</i> message. For the lightweight registration functionality, the following RAS message fields are used: • <i>keepAlive</i> field of the <i>registrationRequest</i> message. The <i>keepAlive</i> field is either true or false. • <i>timeToLive</i> field of the <i>registrationRequest</i> and <i>registrationConfirm</i> messages. The <i>timeToLive</i> field is a number of seconds. • A full <i>registrationRequest</i> message has the <i>keepAlive</i> field set to false. • lightweight <i>registrationRequest</i> message has the <i>keepAlive</i> field set to true. When the lightweight registration functionality is enabled, the group follows these steps: 1. The group sends a first <i>registrationRequest</i> message to the gatekeeper. This <i>registrationRequest</i> message has the <i>keepAlive</i> field set to false and contains the <i>timeToLive</i> field. The value of the <i>timeToLive</i> field is configurable. 2. If the <i>registrationConfirm</i> message contains the <i>timeToLive</i> field, the group sends lightweight <i>registrationRequest</i> messages. The interval between each lightweight <i>registrationRequest</i> message is one-third of the <i>timeToLive</i> value from the gatekeeper (from the <i>registrationConfirm</i> message). On a network with heavy traffic, a lightweight <i>registrationRequest</i> message could arrive a few seconds late at the gatekeeper. Furthermore, since the RAS channel between a group and a gatekeeper is unreliable (UDP), a lightweight <i>registrationRequest</i> message may never arrive at the gatekeeper. These problems are avoided by using an interval equal to one-third the <i>timeToLive</i> value of the <i>registrationConfirm</i> message. 3. If the <i>registrationConfirm</i> message does not contain the <i>timeToLive</i> field, the group does not send lightweight <i>registrationRequest</i> messages. Default Value: enable
h323GroupMultipleRegLightweightTimeToLive	R/W	The interval, in seconds, proposed to the gatekeeper for the lightweight registration functionality. When the lightweight registration functionality is enabled, the group uses this value for the <i>timeToLive</i> field of the <i>registrationRequest</i> message. Available values range from 30 seconds to 3600 seconds. Default Value: 60
h323GroupMultipleRegRasPortSource	R/W	Indicates the source of the local RAS port. This applies only if the group is configured to register. If the group is not configured to register, it uses the well-known RAS port (1719) for its local RAS port. The local RAS port is used to exchange registration, admission and status messages with a gatekeeper. Examples of RAS messages sent by the group are <i>registrationRequest</i>, <i>admissionRequest</i> and <i>disengageRequest</i>. Examples of RAS messages received by the group <i>registrationConfirm</i>, <i>admissionReject</i> and <i>disengageConfirm</i>. • dynamic: the group chooses its local RAS port at run time. • static: the administrator sets the local RAS port. Default Value: dynamic
h323GroupMultipleRegStaticRasPort	R/W	The local static RAS port number of the group. Values range from 1719 to 1720 and from 7000 to 65535. Default Value: 7000
h323GroupMultipleRegCallSignalingPort Source	R/W	Indicates the source of the local call signaling port. This applies only if the group is configured to register. If the group is not configured to register, it uses the well-known call signaling port (1720) for its local call signaling port. The local call signaling port is used to exchange Q.931 messages with gatekeepers and other H.323 endpoints. Examples of Q.931 messages are SETUP, CONNECT and RELEASE COMPLETE. • dynamic: the group chooses its local call signaling port at run time. • static: the administrator sets the local call signaling port. Default Value: dynamic

Table 168: H.323 Parameters – Group Registration (Continued)

Name	Access	Description
h323GroupMultipleRegStaticCallSignalingPort	R/W	The local static call signaling port number of the group. Values range from 1719 to 1720 and from 7000 to 65535. Default Value: 7000

h323RegistrationStatusIfTable

This table holds the IP addresses of the gatekeeper to which each line is actually registered.

Table 169: H.323 Parameters – Registration Status

Name	Access	Description
h323RegistrationGkHost	R-O	The gatekeeper IP address.
h323RegistrationGkPort	R-O	The gatekeeper RAS port (well-known gatekeeper RAS Channel TSAP Identifier). Default Value: 1719
h323RegistrationTimeToLive	R-O	The actual value, in seconds, of the optional time-to-live field sent back by the gatekeeper upon confirmation of the unit's registration. A blank field means that no time-to-live value has been received from the gatekeeper.

H.323 Protocol Parameters – Attributes MIB

This MIB contains signaling and telephony attributes of a H.323 unit.

h323AttributesMIBObjects

The following parameters allow you to define H.323 attributes settings.

h323AttributesQ931

This table holds Q931 attributes of a H.323 unit.

h323AttributesQ931BearerCapability

Table 170: H.323 Parameters – Q.931 Attributes

Name	Access	Description
h323AttributesInformationTransferCapability	R/W	Indicates the type of calls made by the H.323 unit. This value is used to set the information transfer capability field of the bearer capability element of the SETUP message (Q.931 header). This information may help the called endpoint to take actions based on the nature of the media stream to be established (voice-only call or data call or video call). This information may impact the called endpoint on its decision to accept the call. For example, a SCN gateway may not have access to enough bandwidth in order to accept a new IP to SCN data call. For calls between endpoints that are both on the IP network, this information may be ignored by the called endpoint. This information is mostly used by SCN gateways and ISDN gateways. The value of this variable should be changed only when necessary, in order to adapt to third-party systems. When receiving a call, this H.323 unit ignores the value of the information transfer capability field. - speech: Indicates a voice-only call. - unrestrictedDigitalInformation: Unrestricted Digital Information (64 kbps). Indicates an audiovisual call. - restrictedDigitalInformation: Restricted Digital Information (56 kbps). Indicates an audiovisual call. - audio31kHz: 3.1 kHz audio. Indicates a voice-only call. - udita: Unrestricted Digital Information with Tones/Announcements. Indicates an audiovisual call. - video: Indicates an audiovisual call. "speech" and "audio31kHz" are the choices that best represent the capabilities of this H.323 unit. Even though this H.323 unit does not support any video capability, "unrestrictedDigitalInformation", "restrictedDigitalInformation", "udita" and "video" are provided in order to increase interoperability with third-party systems. "unrestrictedDigitalInformation" is the default value for backward compatibility issues. Please refer to ITU-T Recommendation Q.931 and ITU-T Recommendation H.225.0 for more information on bearer capabilities. Default Value: unrestrictedDigitalInformation

h323AttributesQ931CalledPartyNumberTable

Table 171: H.323 Parameters – Q.931 Called Party Number

Name	Access	Description
h323AttributesCalledPartyNumberEnable	R/W	This variable is related to the 'called party number' information element (Q.931 header of the SETUP message). When all the digit maps are disabled, the 'type of number' field is set to 'National number' and the 'numbering plan identification' field is set to 'ISDN/telephony numbering plan'. When one or more digit maps are enabled but there is no match between the number dialed by the local user and the digit maps that are enabled, the 'type of number' and the 'numbering plan identification' fields are both set to 'Unknown'. - disable : the digit map is not used to set the value of the 'type of number' field. - enable : the digit map is used to set the value of the 'type of number' field. Default Value: disable
h323AttributesCalledPartyNumberDigitMap	R/W	This variable is related to the 'called party number' information element (Q.931 header of the SETUP message). This digit map is associated with a 'type of number' value. At the beginning of an outgoing call, the destination of the call is compared with the digit maps from this table. The destination of the call is the number dialed by the local user. If there is a match, the 'type of number' value (associated with the matching digit map) is used to set the 'type of number' field. Only the digit maps that are enabled are used in the comparison.
h323AttributesCalledPartyNumberTypeOfNumber	R/W	This variable is related to the 'called party number' information element (Q.931 header of the SETUP message). This variable indicates the 'type of number' value associated with a digit map. - internationalNumber: indicates that the call destination is an international number. An international number consists of a Country Code (CC), an optional National Destination Code (NDC) followed by a Subscriber Number (SN). For this value, the 'type of number' field is set to 'International number' and the 'numbering plan identification' field is set to 'ISDN/telephony numbering plan'. - nationalNumber: indicates that the call destination is a national number. A national number consists of a National Destination Code (NDC) followed by a Subscriber Number (SN). For this value, the 'type of number' field is set to 'National number' and the 'numbering plan identification' field is set to 'ISDN/telephony numbering plan'. - subscriberNumber: indicates that the call destination is a local number. A subscriber number identifies a unique subscriber in a network or a numbering area. For this value, the 'type of number' field is set to 'Subscriber number' and the 'numbering plan identification' field is set to 'ISDN/telephony numbering plan'. - privateNumber: indicates that the call destination is a private number. For this value, the 'type of number' field is set to 'Unknown' and the 'numbering plan identification' field is set to 'Private numbering plan'. - unknown: indicates that the call destination is a number specific to a network. The number is part of a dialing plan specific to some network. For this value, the 'type of number' and the 'numbering plan identification' fields are set to 'Unknown'. Please refer to ITU-T Recommendation E.164 for more information on international, national and subscriber numbers. Please refer to ITU-T Recommendation Q.931 for more information on the 'called party number' information element. Default Value: nationalNumber

h323IfSignalingAttributesTable

This table holds signaling attributes of a H.323 unit. This configuration applies to both terminal and gateway lines. Each row is used to configure the signaling attributes of one line.

Table 172: H.323 Parameters – Signaling Attributes

Name	Access	Description
h323AttributesEarlyH245Enable	R/W	With the early H.245 procedure, the line includes its H.245 address in the SETUP message (when making a call) or in the CONNECT message (when receiving a call). This H.245 address may be used by the remote endpoint to open a H.245 connection. The H.245 connection may be opened before the call is connected, thus the qualification of “early” H.245. - disable: the line does not use the early H.245 procedure. - enable: the line uses the early H.245 procedure. Default Value: enable
h323AttributesH245TunnelingEnable	R/W	When tunneling is enabled, the line sends H.245 messages within Q.931 messages. When H.245 is enabled and the line is the calling endpoint: - The line offers the use of H.245 tunneling by setting the <i>h245Tunneling</i> field to true in the SETUP message. - If the called endpoint accepts the use of H.245 tunneling, the line sets the <i>h245Tunneling</i> field to true in every subsequent Q.931 messages. - If the called endpoint refuses the use of H.245 tunneling, the line stops using H.245 tunneling. The line considers the H.245 messages sent in the SETUP message as ignored by the called endpoint. When H.245 is disabled and the line is the calling endpoint: - The line does not offer the use of H.245 tunneling. The line sets the <i>h245Tunneling</i> field to false in every Q.931 messages. When H.245 is enabled and the line is the called endpoint: - When offered, the line accepts the use of H.245 tunneling. The line sets the <i>h245Tunneling</i> field to true in the first Q.931 message sent as response to the SETUP message. The line sets the <i>h245Tunneling</i> field to true in every subsequent Q.931 messages. When H.245 is disabled and the line is the called endpoint: - When offered, the line refuses the use of H.245 tunneling. The line sets the <i>h245Tunneling</i> field to false in every Q.931 messages. When the line is the called endpoint, it does not use H.245 tunneling if it was not offered by the calling endpoint. - disable: the line does not use H.245 tunneling. - enable: the line uses H.245 tunneling. Default Value: disable
h323AttributesFastConnectEnable	R/W	The Fast Connect procedure allows two H.323 endpoints to establish a call with as few as one round-trip message exchange, enabling immediate media stream delivery upon call connection. When making a call, the line includes the fastStart element in the SETUP message. When receiving a call, the line includes the fastStart element in the ALERTING message. The fastStart element contains the voice and data capabilities supported by the line. - disable: the line does not use the Fast Connect procedure. - enable: the line uses the Fast Connect procedure. Default Value: enable

Table 172: H.323 Parameters – Signaling Attributes (Continued)

Name	Access	Description
h323AttributesParallelH245Enable	R/W	The parallel H.245 procedure allows a line to include all the following elements in the SETUP message: • <i>fastStart</i> channels • <i>terminalCapabilitySet</i> message • <i>masterSlaveDetermination</i> message The <i>terminalCapabilitySet</i> and <i>masterSlaveDetermination</i> messages are included in the <i>parallelH245Control</i> field of the SETUP message. At the same time as sending <i>fastStart</i> channels, the parallel H.245 procedure is useful to send capabilities that can't be described in a <i>fastStart</i> channel. Examples of such capabilities are the <i>UserInputIndication</i> capability and the RTP payload types. Also, the parallel H.245 procedure accelerates the call establishment when the called endpoint doesn't support the Fast Connect procedure. In order to include a <i>parallelH245Control</i> field in the SETUP message, the Fast Connect procedure must be enabled. See the <i>h323AttributesFastConnectEnable</i> variable. • disable: the line does not use the parallel H.245 procedure. • enable : the line uses the parallel H.245 procedure. Default Value: disable }

Table 172: H.323 Parameters – Signaling Attributes (Continued)

Name	Access	Description										
h323AttributesVoiceCapabilitySendingMethod	R/W	Indicates how the line constructs the <i>fastStart</i> element and the <i>terminalCapabilitySet</i> message. This variable applies only to the <i>fastStart</i> element of the SETUP message. This applies to all the <i>terminalCapabilitySet</i> messages. This variable applies only to voice capabilities. abbreviated: In the <i>fastStart</i> element, for each voice capability enabled, the line sends a forward <i>OpenLogicalChannel</i> structure with the minimum packetization period and a reverse <i>OpenLogicalChannel</i> structure with the maximum packetization period. - In the <i>terminalCapabilitySet</i> message, for each voice capability enabled, the line sends a "transmit and receive" <i>AudioCapability</i> structure with the maximum packetization period. detailed: In the <i>fastStart</i> element, for each voice capability enabled, the line sends a forward and a reverse <i>OpenLogicalChannel</i> structure for each packetization period step. - In the <i>terminalCapabilitySet</i> message, for each voice capability enabled, the line sends a "transmit and receive" <i>AudioCapability</i> structure for each packetization period step. Each voice capability is configured with a minimum packetization period and a maximum packetization period. The following table explains the concept of packetization period step. <table><tr><th>Voice capability family</th><th>Packetization period step</th></tr><tr><td>=====</td><td>=====</td></tr><tr><td>G.711</td><td>One packetization period step at every 10 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 10 ms and the maximum packetization period is 30 ms, the steps are 10, 20 and 30.</td></tr><tr><td>G.729</td><td>One packetization period step at every 10 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 40 ms and the maximum packetization period is 50 ms, the steps are 40 and 50.</td></tr><tr><td>G.723</td><td>One packetization period step at every 30 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 60 ms and the maximum packetization period is 120 ms, the steps are 60, 90 and 120.</td></tr></table> The line can send a maximum of 20 voice capabilities: <i>fastStart</i> element: a maximum of 40 <i>openLogicalChannel</i> structures can be sent in the <i>fastStart</i> element (20 forward <i>openLogicalChannel</i> structures and 20 reverse <i>openLogicalChannel</i> structures). Each voice capability is described by one forward and one reverse <i>openLogicalChannel</i> structure. <i>terminalCapabilitySet</i> message: a maximum of 20 <i>AudioCapability</i> structures can be sent in the <i>terminalCapabilitySet</i> message. Each voice capability is described by one <i>AudioCapability</i> structure. If more than 20 voice capabilities are enabled by the configuration, only the first 20 voice capabilities are sent. This restriction only applies to voice capabilities and it has no impact on the non-voice capabilities. Default Value: detailed	Voice capability family	Packetization period step	=====	=====	G.711	One packetization period step at every 10 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 10 ms and the maximum packetization period is 30 ms, the steps are 10, 20 and 30.	G.729	One packetization period step at every 10 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 40 ms and the maximum packetization period is 50 ms, the steps are 40 and 50.	G.723	One packetization period step at every 30 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 60 ms and the maximum packetization period is 120 ms, the steps are 60, 90 and 120.
Voice capability family	Packetization period step											
=====	=====											
G.711	One packetization period step at every 10 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 10 ms and the maximum packetization period is 30 ms, the steps are 10, 20 and 30.											
G.729	One packetization period step at every 10 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 40 ms and the maximum packetization period is 50 ms, the steps are 40 and 50.											
G.723	One packetization period step at every 30 ms between the minimum and the maximum packetization periods. For example, if the minimum packetization period is 60 ms and the maximum packetization period is 120 ms, the steps are 60, 90 and 120.											

h323IfTelephonyAttributesTable

This table holds telephony attributes of a H.323 unit. This configuration applies to both terminal and gateway lines. Each row is used to configure the telephony attributes of one line.

Table 173: H.323 Parameters – Telephony Attributes

Name	Access	Description
h323AttributesDirectGatewayCallEnable	R/W	The "Direct Gateway Call" is a Media5 Corporation proprietary procedure. The line is configured with the IP address of a gateway. This procedure applies only to lines that are not configured to register: - The unit is configured with the multiple registration method and the registration for the line is disabled. OR - The unit is configured with the none registration method. This procedure allows the use of a gateway without the presence of a gatekeeper. The user simply dials a telephone number. The new outgoing call goes directly to the gateway. The telephone number is the call destination on the SCN side. This procedure is not used if the user dials an IP address before dialing a telephone number. - disable: the line does not use the "Direct Gateway Call" procedure. - enable: the line uses the "Direct Gateway Call" procedure. Default Value: disable
h323AttributesDirectGatewayCallHost	R/W	The IP address of the gateway used in the "Direct Gateway Call" procedure. The "Direct Gateway Call" is a Media5 Corporation proprietary procedure. It allows the use of a gateway without the presence of a gatekeeper. The user simply dials a telephone number. The new outgoing call goes directly to the gateway. The telephone number is the call destination on the SCN side. This procedure is not used if the user dials an IP address before dialing a telephone number. This procedure applies only to lines with the following configuration: - Multiple registration method - Registration disabled

H.323 Protocol Parameters – Aliases MIB

This MIB contains the alias configuration of a H.323 unit.

h323AliasesMIBObjects

The following parameters allow you to define the H.323 aliases information.

h323AliasesIfAliasesTable

This table holds the aliases of the H.323 unit. Each row is used to configure the aliases of one line.

Table 174: H.323 Parameters – Aliases

Name	Access	Description
h323AliasesGroupIndex	R-O	Indicates which group is associated with this line. A value different than 0 indicates that the aliases configuration for this line is superceded by the corresponding entry in the <i>h323AliasesGroupAliases Table</i> . A value of 0 means this line is not part of a group and that it can be configured by using this entry. Default Value: 0
h323AliasesConfigured	R/W	The aliases that uniquely identify the line. These are the configured aliases. This variable only applies to unit of type terminal. Each line must be configured with unique aliases. A line can be configured with zero, one or two aliases. A line can be configured with two aliases of the same type or two aliases of different types. A line can be configured with E.164 aliases, H.323 ID aliases and party number aliases. Transport ID aliases (IP addresses) are not allowed. The local IP address of the unit is configured through <i>ipAddressConfigLocalHost</i> . The configured aliases are included in the <i>terminalAlias</i> field of the <i>gatekeeperRequest</i> and <i>registrationRequest</i> messages. As an example, a line is configured with two aliases, "3460707" as E.164 alias and "user1" as H.323 ID alias. The following string is used to describe these aliases: E164=3460707;H323ID=user1 Each line must have at least one current alias (either configured or confirmed). If a line has no alias, the unit locks this line. When a line is locked, no call can be made/received from/to this line. Refer to the administrator documentation for the description of the aliases syntax. Refer to the administrator documentation for the description of the configured, confirmed and current aliases.
h323AliasesCurrent	R-O	The aliases currently used by the line. This variable only applies to unit of type terminal. Each line must have at least one current alias (either configured or confirmed). If a line has no alias, the unit locks this line. When a line is locked, no call can be made/received from/to this line. Refer to the administrator documentation for the description of the aliases syntax. Refer to the administrator documentation for the description of the configured, confirmed and current aliases.

h323AliasesGroupAliasesTable

This table holds the aliases of the unit. Each row is used to configure the aliases of one group of lines.

Table 175: H.323 Parameters – Group Aliases

Name	Access	Description
h323GroupAliasesConfigured	R/W	The aliases that uniquely identify a group of lines. These are the configured aliases. Each group must be configured with unique aliases. A group can be configured with zero, one or two aliases. A group can be configured with two aliases of the same type or two aliases of different types. A group can be configured with E.164 aliases, H.323 ID aliases and party number aliases. Transport ID aliases (IP addresses) are not allowed. The local IP address of the unit is configured through <i>ipAddressConfigLocalHost</i>. The configured aliases are included in the <i>terminalAlias</i> field of the <i>gatekeeperRequest</i> and <i>registrationRequest</i> messages. If the unit is a H.323 gateway, the E.164 aliases (considered as voice supported prefixes) are also included in the <i>supportedPrefixes</i> field of the <i>gatekeeperRequest</i> and <i>registrationRequest</i> messages. As an example, a group is configured with two aliases, "3460707" as E.164 alias and "user1" as H.323 ID alias. The following string is used to describe these aliases: E164=3460707;H323ID=user1 Each group must have at least one current alias (either configured or confirmed). If a group has no alias, the unit locks the lines associated with that group. When a line is locked, no call can be made/received from/to this line. Refer to the administrator documentation for the description of the aliases syntax. Refer to the administrator documentation for the description of the configured, confirmed and current aliases.
h323GroupAliasesCurrent	R-O	The aliases currently used by the group of lines. Each group must have at least one current alias (either configured or confirmed). If a group has no alias, the unit locks the lines associated with this group. When a line is locked, no call can be made/received from/to this line. Refer to the administrator documentation for the description of the aliases syntax. Refer to the administrator documentation for the description of the configured, confirmed and current aliases.

H.323 Protocol Parameters – Experimental MIB

This MIB contains H.323 experimental and interoperability configuration objects.

h323ExperimentalMIBObjects

The following parameters allow you to define the H.323 experimental information.

h323Interop

This parameter indicates if the unit registers as a gateway.

Table 176: H.323 Parameters – Interop

Name	Access	Description
h323RegAsGateway	R/W	Indicates if the unit registers as a gateway. This variable applies only to H.323 terminal. A H.323 terminal is an H.323 unit with only FXS ports. - disable: the unit registers as a H.323 terminal. - enable: the unit registers as a gateway. The unit registers with an empty supported voice prefix (gateway field of the <i>registrationRequest</i> message). Certain gatekeepers require this distinctive feature. From the user point of view, this behavior is transparent and has no impact on the use of the unit. Default Value: disable
h323AliasTypeRestriction	R/W	This configuration compares the aliases from the unit with the destination aliases of the incoming call. This configuration applies only to: - units with FXS ports - units with no group of lines - aliases of type E.164 and party number. When the unit receives an incoming IP call, it compares the aliases from its configuration with the destination aliases of the incoming call. There must be at least one common alias in the destination of the call and the configuration of the unit. This comparison is used to select the line that will handle the incoming call. There are two levels of comparison: 1. Type of the aliases. 2. Value of the aliases. - enable: Both the type and the value of the aliases are compared. This applies to all aliases of all types. - disable: For the aliases of type E.164 or party number, only the value of the aliases is compared. For the aliases of other types, both the type and value of the aliases are compared. For instance, a unit with two FXS ports is configured with the following aliases: - FXS port 1: alias of type E.164 defined as "1111". - FXS port 2: alias of type E.164 defined as "2222". The unit receives an incoming IP call with a public subscriber number alias (party number) as its destination. The public subscriber number is "1111". If <i>h323AliasTypeRestriction</i> is enabled, the call is rejected because the unit is not configured with a public subscriber number equal to "1111". Both the type and the value of the alias are compared. If <i>h323AliasTypeRestriction</i> is disabled, the call is accepted because the unit is configured with an E.164 alias equal to "1111". Only the value of the alias is compared. Default Value: enable

Table 176: H.323 Parameters – Interop (Continued)

Name	Access	Description
h323AcceleratedRequestedLogicalChannel	R/W	Modifies the H.245 <i>OpenLogicalChannel</i> timing during the Request Mode negotiation. If <i>h323AcceleratedRequestedLogicalChannel</i> is enabled, the application immediately opens its new logical channel when receiving the H.245 <i>RequestMode</i> or <i>RequestModeAck</i>. If <i>h323AcceleratedRequestedLogicalChannel</i> is disabled, even if the H.245 <i>RequestMode</i> or <i>RequestModeAck</i> is received, the application opens its new logical channel only when the H.323 stack definitively closes the last channel used. This mechanism ensures to have only one logical channel opened at any given time. Default Value: disable
h323AddT38MediaControlChannel	R/W	Enables or disables the <i>mediaControlChannel</i> address in the H.245 <i>openLogicalChannelAck</i> message. - disable: Remove the <i>mediaControlChannel</i> address in the H.245 <i>openLogicalChannelAck</i> message. - enable: Add the <i>mediaControlChannel</i> address in the H.245 <i>openLogicalChannelAck</i> message. Default Value: disable
h323UseEvenT38Port	R/W	Defines if the odd lines use an even T.38 port. - disable: The unit uses both even and odd T.38 ports. For example, line 1 uses T.38 port 6001 and line 2 uses T.38 port 6002. - enable: The unit uses only even T.38 ports. For example, line 1 uses T.38 port 6002 and line 2 uses T.38 port 6004. Default Value: disable

h323VoicelfCodecTable

This table holds codec parameters specific to the H.323 protocol..

Table 177: H.323 Parameters – Interop, G.729

Name	Access	Description																																				
h323VoicelfCodecG729Enable	R/W	Indicates if the g729 audio capability is enabled. This variable is used in conjunction with the following variables (from voicelfMIB): <i>voicelfCodecG729Enable</i>: Indicates if the g729AnnexA audio capability is enabled. <i>voicelfG729VoiceActivityDetectionEnable</i>: Indicates if the Voice Activity Detection (VAD, silence suppression in Annex B) is enabled for the G.729 audio capabilities. <i>voicelfCodecG729MinPTime</i>: Minimum packetization period for the G.729 audio capabilities (expressed in milliseconds). <i>voicelfCodecG729MaxPTime</i>: Maximum packetization period for the G.729 audio capabilities (expressed in milliseconds). The values of <i>voicelfCodecG729MinPTime</i> and <i>voicelfCodecG729MaxPTime</i> are used for all the G.729 audio capabilities. The following table shows the possible sets of G.729 audio capabilities. <table><tr><th>g729AnnexA</th><th>g729</th><th>VAD</th><th>capability set</th></tr><tr><td>-----</td><td>----</td><td>---</td><td>-----</td></tr><tr><td>disable</td><td>disable</td><td>disable</td><td>no G.729 audio codec</td></tr><tr><td>enable</td><td>disable</td><td>disable</td><td>g729AnnexA</td></tr><tr><td>disable</td><td>enable</td><td>disable</td><td>g729</td></tr><tr><td>enable</td><td>enable</td><td>disable</td><td>g729AnnexA, g729</td></tr><tr><td>enable</td><td>disable</td><td>enable</td><td>g729AnnexAwAnnexB, g729AnnexA</td></tr><tr><td>disable</td><td>enable</td><td>enable</td><td>g729wAnnexB, g729</td></tr><tr><td>enable</td><td>enable</td><td>enable</td><td>g729AnnexAwAnnexB, g729AnnexA, g729wAnnexB, g729</td></tr></table> Default Value: disable	g729AnnexA	g729	VAD	capability set	-----	----	---	-----	disable	disable	disable	no G.729 audio codec	enable	disable	disable	g729AnnexA	disable	enable	disable	g729	enable	enable	disable	g729AnnexA, g729	enable	disable	enable	g729AnnexAwAnnexB, g729AnnexA	disable	enable	enable	g729wAnnexB, g729	enable	enable	enable	g729AnnexAwAnnexB, g729AnnexA, g729wAnnexB, g729
g729AnnexA	g729	VAD	capability set																																			
-----	----	---	-----																																			
disable	disable	disable	no G.729 audio codec																																			
enable	disable	disable	g729AnnexA																																			
disable	enable	disable	g729																																			
enable	enable	disable	g729AnnexA, g729																																			
enable	disable	enable	g729AnnexAwAnnexB, g729AnnexA																																			
disable	enable	enable	g729wAnnexB, g729																																			
enable	enable	enable	g729AnnexAwAnnexB, g729AnnexA, g729wAnnexB, g729																																			

IP Telephony Signalling

MGCP MIBs

Page Left Intentionally Blank

MGCP Protocol Parameters – MGCP MIB

This MIB contains MGCP configuration objects.

mgcpMIBObjects

The following parameters allow you to define general MGCP information.

Table 178: MGCP Parameters

Name	Access	Description
mgcpPort	R/W	MGCP IP port number. This is the UDP port number on which the gateway is listening for any MGCP request. Default Value: 2427
mgcpDefaultDigitMap	R/W	Default digit map for all the endpoints. Default Value: x.T
mgcpDefaultPackage	R/W	Default package for all the endpoints. - linePackage(0) - dtmfPackage(1) - genericPackage(2) Default Value: linePackage
mgcpRestartLevel	R/W	Level of restart for initial RSIP. - gateway(0) - group(1) - endpoint(2) Default Value: gateway
mgcpEndpointIdListIncludeNotStarted	R/W	Indicates if the EndpointIdList returned by a wildcarded AUEP will include or not endpoints that are not started. - excludeNotStarted(0) - includeNotStarted(1) Default Value: excludeNotStarted
mgcpPiggyBackingEnable	R/W	Indicates if piggy-backing can be used to send several MGCP messages in the same UDP packet. If enabled, piggy-backing can be used. Otherwise, no piggy-backing is used. - disable(0) - enable(1) Default Value: enable
mgcpAddPtimeIfPresentInLCO	R/W	If includePtime is selected, the ptime will be included in the SDP packets whenever the ptime is provided in the <i>LocalConnectionOptions(LCO)</i> parameters. Otherwise the ptime is never provided in SDP. - excludePtime(0) - includePtime(1) Default Value: excludePtime

mgcpEndpointId

mgcpEndpointIdTable

The *mgcpEndpointIdTable* contains the local endpoint name. The endpoint name is created as follows: *term2/term1@localHostFqdn*. Endpoints are originating or terminating devices such as phones or faxes.

Table 179: MGCP Parameters – Endpoint

Name	Access	Description
mgcpEndpointIdTerm1	R/W	The right most term, of the local endpoint name.
mgcpEndpointIdTerm2	R/W	Second term from the right of the local endpoint name. Default Value: aaln

mgcpRetransmission

The following parameters allow you to define Retransmission information. Retransmission is a method of error control in which hosts receiving messages acknowledge the receipt of correct messages and do not acknowledge the receipt of incorrect messages. The lack of acknowledgement is an indication to the sending host that it should transmit the failed message again.

Table 180: MGCP Parameters – Retransmission

Name	Access	Description
mgcpRetransmissionAlgorithm	R/W	Retransmission algorithm used. - static(0) - exponential(1) - exponentialWithJitter(2) Default Value: exponentialWithJitter
mgcpRetransmissionInitialPeriod	R/W	Retransmission initial period in ms. Default Value: 200
mgcpRetransmissionMaxPeriod	R/W	Retransmission maximum period in ms. Must be greater than or equal to the retransmission initial period. Default Value: 30000
mgcpRetransmissionDisconnectTimeout	R/W	Time elapsed (in ms) at which an endpoint will become disconnected. Default Value: 20000
mgcpRetransmissionSuspicionThreshold	R/W	Number of retransmissions at which an endpoint may actively query the name server to detect the possible change of the Call Agent's interfaces. Default Value: 7
mgcpRetransmissionSuspicionThresholdDnsQuery	R/W	Indicates whether a DNS query will be performed or not when the number of retransmissions is equal to the suspicion threshold. - noDnsQuery(0) - performDnsQuery(1) Default Value: noDnsQuery
mgcpRetransmissionDisconnectThreshold	R/W	Number of retransmissions at which an endpoint should contact the DNS one more time to see if any other interfaces have become available. When the number of retransmissions is greater than this value the endpoint will become disconnected. Default Value: 7
mgcpRetransmissionDisconnectThresholdDnsQuery	R/W	Indicates whether a DNS query will be performed or not when the number of retransmissions is equal to the disconnect threshold. - noDnsQuery(0) - performDnsQuery(1) Default Value: noDnsQuery
mgcpRetransmissionHistoryTimeout	R/W	Number of milliseconds for which responses to old transactions must be kept. Default Value: 20000
mgcpRetransmissionMaxWaitingDelay	R/W	Maximum waiting delay (in ms) an endpoint can wait before sending an RSIP. Default Value: 600000
mgcpRetransmissionDisconnectInitialWaitingPeriod	R/W	Initial waiting delay (in ms) an endpoint must wait before starting the disconnect procedure. Default Value: 15000

Table 180: MGCP Parameters – Retransmission (Continued)

Name	Access	Description
mgcpRetransmissionDisconnectMinWaitingPeriod	R/W	Minimum waiting delay (in ms) that must have elapsed since the gateway became initially disconnected, and before reinitiating the disconnect procedure. If the endpoint remains disconnected after the "disconnected" procedure, the minimum waiting delay is doubled up to a maximum value. Default Value: 15000
mgcpRetransmissionDisconnectMaxWaitingPeriod	R/W	Disconnected maximum waiting delay (in ms) since the gateway became disconnected that an endpoint can wait before starting the disconnect procedure. Default Value: 600000

mgcpDtmfPackage

The following parameters allow you to define the MGCP DTMF Package. The DTMF package groups variables pertaining to the DTMFs.

Table 181: MGCP Parameters – DTMF Package

Name	Access	Description
mgcpDtmfPackageLDuration	R/W	DTMF long duration time out value in ms. Default Value: 2000
mgcpDtmfPackageTCriticalDuration	R/W	Interdigit time out value in msec when a timer is all that is required for the digit string to match a pattern in the digit map. Default Value: 4000
mgcpDtmfPackageTPartialDuration	R/W	Interdigit time out value in msec when at least one more digit is required for the digit string to match any of the patterns in the digit map. Default Value: 16000

mgcpGenericMediaPackage

The following parameters allow you to define the Generic Media Package, which groups the events and signals that can be observed on several types of endpoints, such as trunking gateways, access gateways or residential gateways.

Table 182: MGCP Parameters – Generic Media Package

Name	Access	Description
mgcpGenericMediaPackageRbkDuration	R/W	Ring back on connection tone timeout value in ms. Default Value: 180000
mgcpGenericMediaPackageRtDuration	R/W	Ring back tone timeout value in ms. Default Value: 180000

mgcpLinePackage

The following parameters allow you to define the Line Package, which groups variables that determine tone time outs of the MGCP protocol Line Package.

Table 183: MGCP Parameters – Line Package

Name	Access	Description
mgcpLinePackageBzDuration	R/W	Busy tone timeout value in ms. Default Value: 30000
mgcpLinePackageDIDuration	R/W	Dial tone timeout value in ms. Default Value: 16000
mgcpLinePackageMwiDuration	R/W	Message waiting indicator tone timeout value in ms. Default Value: 16000
mgcpLinePackageOtDuration	R/W	Off hook warning tone timeout value in ms. Default Value: 65535000
mgcpLinePackageRgDuration	R/W	Ring tone timeout value in ms. Default Value: 180000

Table 183: MGCP Parameters – Line Package (Continued)

Name	Access	Description
mgcpLinePackageRoDuration	R/W	Reorder tone timeout value in ms. Default Value: 30000
mgcpLinePackageSIDuration	R/W	Stutter dial tone timeout value in ms. Default Value: 16000
mgcpLinePackageWtDuration	R/W	Call waiting tone timeout value in ms. Default Value: 30000
mgcpLinePackageOsiDuration	R/W	Network disconnect timeout value in ms. Default Value: 900
mgcpLinePackageHdPersistent	R/W	Indicates whether the off-hook event is persistent or not. Persistent events in a given package are always detected on an endpoint that implements that package. If a persistent event is not included in the list of RequestedEvents, and the event occurs, the event will be detected anyway, and processed like all other events, as if the persistent event had been requested with a Notify action. • disable(0) • enable(1) Default Value: disable
mgcpLinePackageHfPersistent	R/W	Indicates whether the flash hook event is persistent or not. Persistent events in a given package are always detected on an endpoint that implements that package. If a persistent event is not included in the list of RequestedEvents, and the event occurs, the event will be detected anyway, and processed like all other events, as if the persistent event had been requested with a Notify action. • disable(0) • enable(1) Default Value: disable
mgcpLinePackageHuPersistent	R/W	Indicates whether the on hook event is persistent or not. Persistent events in a given package are always detected on an endpoint that implements that package. If a persistent event is not included in the list of RequestedEvents, and the event occurs, the event will be detected anyway, and processed like all other events, as if the persistent event had been requested with a Notify action. • disable(0) • enable(1) Default Value: disable

mgcpStats

The following parameters allow you to define statistics pertaining to the MGCP signalling protocol.

Table 184: MGCP Parameters – Statistics

Name	Access	Description
mgcpStatsCurrentNumberOfActiveConnections	R-O	Number of active connections which are currently conducted by the gateway.

mgcpStatsCurrentStatistics

Table 185: MGCP Parameters – Current Statistics

Name	Access	Description
mgcpStatsCurrentTotalNumberOfConnections	R-O	Total number of connections conducted by the gateway so far in the current statistics period.
mgcpStatsCurrentAvgConnectionTime	R-O	Average connection time (in second) so far in the current statistics period.

mgcpStatsCumulatedStatistics

Table 186: MGCP Parameters – Cumulated Statistics

Name	Access	Description
mgcpStatsCumulatedTotalNumberOfConnections	R-O	Cumulated number of connections conducted by the gateway.
mgcpStatsCumulatedAvgConnectionTime	R-O	Cumulated average connection time (in second).

mgcpFirewall

The following parameter allow you to define the firewall keep-alive feature.

Table 187: MGCP Parameters – Firewall Keep-Alive

Name	Access	Description
mgcpFwKeepAliveEnable	R/W	Enable/disable the Firewall keep-alive timeout mechanism. When Media Gateways (MGW) controlled with the MGCP protocol are deployed behind firewalls, the Media Gateway Controller (MGC) should be allowed to control the MGW. To keep the firewall and NAT connection alive, signalling packets must be exchanged between the MGW and MGC within a specified period of time called the keep-alive timeout. If no packets are exchanged for the specified period, then the connection will be closed. To keep the connection alive, the gateway uses the RSIP RM : x-keepalive command to indicate that the gateway inactivity timer has timed-out. The RSIP keep-alive command is sent from a provisionable virtual endpoint. The RSIP keep-alive command does not require any 200 OK from the Media Gateway controller (MGC). The RSIP keep-alive is launched immediately after the activation of the MGCP stack. It is then possible to see RSIP keep-alive command preceeding the initial RSIP restart if the registration initial delay period is larger than the inactivity timer. Also, the RSIP keep-alive is not submitted to the disconnection procedure. Note that voice packets cannot be used to keep the connection opened because they are transmitted on another channel. Default Value: disable
mgcpFwKeepAliveTimeout	R/W	Keep-alive timeout value in sec. The range varies from 10 sec to 24 hrs. The default value is set to 5 min. Default Value: 300

MGCP Protocol Parameters – FXS Meter Pulse MIB

This MIB contains meter pulse configuration objects.

fxsMeterPulseMIBObjects

The following parameter allows you to define the FXS Meter Pulse frequency information.

Table 188: FXS Meter Pulse Frequency Parameter

Name	Access	Description
fxsMeterPulseFreq	R/W	Meter pulse may use different frequencies. The selected frequency applies to ALL FXS ports. - freq-12-kHz(1) - freq-16-kHz(2) Default Value: freq-12-kHz

fxsMeterPulseTable

The *fxsMeterPulseTable* parameters allow you to define the pulse duration information.

Table 189: FXS Meter Pulse Duration Parameters

Name	Access	Description
fxsMeterPulseDuration	R/W	This is the pulse duration (voltage is ON) in ms. The clock precision is 10 ms, i.e. you can request 213 ms, but the system will play each pulse 213 +/- 10 ms. Values range from 120 ms to 220 ms. Default Value: 160
fxsMeterPauseDuration	R/W	This is the pause duration (voltage is OFF) in ms. The clock precision is 10 ms, i.e. you can request 327 ms, but the system will pause for 327 +/- 10 ms. Values range from 100 ms to 600 ms. Default Value: 360

MGCP/NCS Protocol Parameters – Experimental MIB

This MIB contains MGCP/NCS experimental and interoperability configuration objects.

mgcpncsExperimentalMIBObjects

mgcpncsInterop

The following parameters allow you to define experimental MGCP/NCS information.

Table 190: MGCP/NCS Experimental Parameters

Name	Access	Description
mgcpncsAnswerStreamFormat	R/W	The answer to an offered session description is based on the offered session description. RFC 3264 stipulates that to reject an offered stream, the port number in the corresponding stream in the answer MUST be set to zero. However, some gateways prefer to remove the unwanted stream from the answer. • zeroAnswerStream: The port number is set to zero if the corresponding stream in the answer is unwanted. This behaviour follows the RFC 3264 best practice. • removeAnswerStream: The unwanted stream is removed from the answer and returned to the offerer. This behaviour is kept for backward compatibility issue. Default Value: zeroAnswerStream
mgcpncsOriginLineSessionIDAndVersionMaxLength	R/W	The maximum length of the session ID and the session version number in the origin line (o=) of the SDP. • none: The session ID and the session version number are represented by the 0 value. • max-32bits: The session ID and the session version number are represented with a 32-bit integer. They have a maximum length of 10 digits. • max-64bits: The session ID and the session version number are represented with a 64-bit integer. They have a maximum length of 20 digits. Default Value: none

Table 190: MGCP/NCS Experimental Parameters (Continued)

Name	Access	Description
mgcpncsG729AnnexBNegotiation	R/W	Indicates if the G.729 Annex B is negotiated through the session description protocol. RFC 3555 (MIME Type Registration of RTP Payload Formats), July 2003 explains how the Annex B can be negotiated by using the session description protocol. The Annex B indicates that Annex B, voice activity detection, is used or preferred. Permissible values are 'yes' and 'no' (without the quotes); 'yes' is implied if this parameter is omitted. <pre>m=audio 5004 RTP/AVP 0 18 13 a=fmtp:18 annexb=yes</pre> - disable: The G.729 Annex B is NOT negotiated through the session description protocol. In that case, the G.729 Annex B is based on the MIB variable <i>voiceIfG729VoiceActivityDetectionEnable</i>. When this variable is set to enable, the G.729 codec negotiated as payload number 18 (G729) supports the Annex B implicitly. However, when the <i>voiceIfG729VoiceActivityDetectionEnable</i> variable is set to disable, the G.729 codec negotiated as payload number 18 (G729) does NOT support the Annex B implicitly. - enable: The G.729 Annex B is negotiated through the session description protocol. In that case, the G.729 Annex B is advertised in the offer. The value depends on the MIB variable <i>voiceIfG729VoiceActivityDetectionEnable</i>. If this variable is set to enable, then the Annex B is set to 'yes'; otherwise, the value 'no' is advertised. The answerer MAY not be able to support the Annex B. In that case, the answer to the Annex B can be set to 'no'. This forces the offerer not to use the Annex B in G.729. However, the opposite is not possible. The answerer can NOT force the offerer to use the Annex B if this one does not bear such capability. Default Value: disable
mgcpncsValidateOfferAnswerModel	R/W	Determines whether the unit requires strict adherence to RFC 3264 from the peer when negotiating capabilities for the establishment of a media session. When enabled, the following guidelines from the Offer-Answer Model must be strictly followed. An answer must: - Include at least one codec from the list that the unit sent in the offer; - Avoid adding extra codecs that were not present in the offer; - Contain the same number of media lines that the unit put in its offer. Otherwise, the answer is rejected and the unit ends the call. When disabled, then the peer can freely: - Send back a brand new list of codecs or add new ones to the offered list; - Add media lines AFTER the ones found in the offer. As long as at least one codec sent back is supported by the unit, the call is allowed to go on. Any media lines added by the peer is simply ignored. Default Value: enable
mgcpncsMultipleFaxToneDetection	R/W	Controls whether the unit reports more than one occurrence of the fax tone during the negotiation phase. This when event notification requests can be received after the fax tone. - disable: when establishing a fax call, the unit only reports the first occurrence of the fax tone event. - enable: the unit will report every occurrence of the fax tone event. Default Value: disable
mgcpncsConnectRtpSockets	R/W	Determines whether the endpoints will listen to RTP sources other than the one to which they are sending packets. - disable: use unconnected sockets. Endpoints will play any RTP packets addressed to them. - enable: use connected sockets. Endpoints will only play packets coming from the address to which they are sending. Default Value: disable

Table 190: MGCP/NCS Experimental Parameters (Continued)

Name	Access	Description
mgcpncsRtpUdpChecksumEnable	R/W	Enables/disables the UDP checksum for RTP packets. UDP checksum is disabled by default to gain performance. - Enable: UDP checksum will be calculated for each RTP packet. This may affect performance. - Disable: UDP checksum will not be calculated. The value 0 will be written in the checksum field of each RTP packet header. Default Value: disable
mgcpncsT38CapabilitiesUsingAudioCodec98	R/W	Enables or disables parsing of remote SDP in order to extract remote T.38 capabilities from an audio stream. This variable is useful when a call-agent is re-using the audio stream to advertise the remote T.38 capabilities instead of creating a new image stream. - Enable: Verifies the remote SDP audio stream for the T.38 port number. The remote SDP must meet the following conditions in order to detect T.38 capabilities from the audio stream: - Single audio stream - Single media format 98 - No rtpmaps - Disable: The call-agent never uses the audio stream to advertise the remote T.38 port number. Default Value: disable
mgcpncsImmediateModemToneReporting	R/W	Controls whether the early detection of a modem tone by the unit is immediately reported to the call agent (when requested) or delayed until the exact nature of the transmission has been determined. Some fax transmissions begin by exchanging modem tones in their setup stage; therefore, a little time is needed before the unit is able to discriminate between a fax or a modem transmission. - enable: The unit will report a modem tone to the call agent (assuming the call agent has requested it) as soon as it detects one. - disable: The unit will wait until it has determined the exact nature of a data transmission and then report either a fax or a modem tone to the call agent (always assuming the call agent has requested it). Default Value: disable
mgcpncsMakeOsiSignalBrief	R/W	For legacy reasons, this variable makes it possible to change the behaviour of the Network Disconnect signal (L/osi) by changing its type from time-out to brief (see RFC 3435 for a description of the various signal types). - enable: The L/osi signal will behave like a brief signal. - disable: The L/osi signal will conform to its standard definition and behave like a time-out signal. Default Value: disable
mgcpncsFakeRfc3407Recognition	R/W	Allows recognition of a remote endpoint's T.38 capabilities when they are advertised using the notation recommended in RFC 3407. More precisely, when enabled, the unit will recognize the line 'a=cdsc: 1 image udptl t38' in the following SDP: <pre>v=0 c=IN IP4 47.47.47.47 a=sqn: 0 a=cdsc: 1 image udptl t38 m=audio 1234 RTP/AVP 18 a=ptime:20</pre> as valid T.38 support advertisement. No other part of the RFC is supported and the unit itself never uses this syntax. - enable: T.38 advertisement as described above will be recognized. - disable: RFC 3407 syntax will be ignored. Default Value: disable

Table 190: MGCP/NCS Experimental Parameters (Continued)

Name	Access	Description
mgcpncsUseT38Format	R/W	Determines the format used, in the SDP portion of packets, to advertise the unit's T.38 capabilities. - disable: Support for the boolean T.38 parameters T38FaxFillBitRemoval, T38FaxTranscodingMMR and T38FaxTranscodingJBIG is advertised by associating a value of 0 (unsupported) or 1 (supported) with the parameter in the following manner: - a=T38FaxFillBitRemoval:0 - a=T38FaxTranscodingMMR:0 - a=T38FaxTranscodingJBIG:0 - enable: Support for the above T.38 parameters is advertised in conformance with ITU-T Recommendation T.38, section D.2.3. The presence of the parameter in the SDP indicates support for it (without the need for an associated value), while its absence means that it is not supported. Default Value: disable
mgcpncsBracketsAroundIpAddressInDomainNameEnable	R/W	Defines when brackets are added around the endpoint's domain name only when the configured domain name is an IP address. disable : Brackets are not added around the IP address. e.g.: aaln/1@192.168.0.1 enable : Brackets are added around the IP address. e.g.: aaln/1@[192.168.0.1]" Default Value: enable
mgcpncsPolarityReversalOnCallingCardServiceToneEnable	RW	Defines if a polarity reversal must be performed before playing the calling card service tone when receiving the S:L/z signal request. - disable: Calling card service tone signal request is handled normally. - enable: A polarity reversal is performed before handling the calling card service tone signal request. Default Value: disable

IP Telephony Signalling NCS MIBs

Page Left Intentionally Blank

NCS Protocol Parameters – NCS MIB

This MIB contains NCS configuration objects.

ncsMIBObjects

The following parameters allow you to define general NCS information.

Table 191: NCS Parameters

Name	Access	Description
ncsPort	R/W	NCS IP port number. This is the UDP port number on which the gateway is listening for any NCS request. Default Value: 2427
ncsDefaultDigitMap	R/W	Default digit map for all the endpoints. Default Value: x.T
ncsRestartLevel	R/W	Level of restart for initial RSIP. - gateway(0) - group(1) - endpoint(2) Default Value: gateway
ncsEndpointIdListIncludeNotStarted	R/W	Indicates if the EndpointIdList returned by a wildcarded AUEP will include or not endpoints that are not started. - excludeNotStarted(0) - includeNotStarted(1) Default Value: excludeNotStarted
ncsPiggyBackingEnable	R/W	Indicates if piggy-backing can be used to send several NCS messages in the same UDP packet. If enabled, piggy-backing can be used. Otherwise, no piggy-backing is used. - disable(0) - enable(1) Default Value: enable

ncsEndpointId

ncsEndpointIfTable

The *ncsEndpointIfTable* contains NCS endpoint interface parameters. It contains the local endpoint name. The endpoint name is created as follows: *term2/term1@localHostFqdn*. Endpoints are originating or terminating devices such as phones or faxes.

Table 192: NCS Parameters – Endpoint

Name	Access	Description
ncsEndpointIdTerm1	R/W	The right most term, of the local endpoint name.
ncsEndpointIdTerm2	R/W	Second term from the right of the local endpoint name. Default Value: aaln

ncsRetransmission

The following parameters allow you to define Retransmission information. Retransmission is a method of error control in which hosts receiving messages acknowledge the receipt of correct messages and do not acknowledge the receipt of incorrect messages. The lack of acknowledgement is an indication to the sending host that it should transmit the failed message again.

Table 193: NCS Parameters – Retransmission

Name	Access	Description
ncsRetransmissionAlgorithm	R/W	Retransmission algorithm used. - static(0) - exponential(1) - exponentialWithJitter(2) Default Value: exponentialWithJitter
ncsRetransmissionInitialPeriod	R/W	Retransmission initial period in ms. Default Value: 200
ncsRetransmissionMaxPeriod	R/W	Retransmission maximum period in ms. Must be greater than or equal to the retransmission initial period. Default Value: 30000
ncsRetransmissionDisconnectTimeout	R/W	Time elapsed (in ms) at which an endpoint will become disconnected. Default Value: 20000
ncsRetransmissionSuspicionThreshold	R/W	Number of retransmissions at which an endpoint may actively query the name server to detect the possible change of the Call Agent's interfaces. Default Value: 7
ncsRetransmissionSuspicionThresholdDnsQuery	R/W	Indicates whether a DNS query will be performed or not when the number of retransmissions is equal to the suspicion threshold. - oDnsQuery(0) - performDnsQuery(1) Default Value: noDnsQuery
ncsRetransmissionDisconnectThreshold	R/W	Number of retransmissions at which an endpoint should contact the DNS one more time to see if any other interfaces have become available. When the number of retransmissions is greater than this value the endpoint will become disconnected. Default Value: 7
ncsRetransmissionDisconnectThresholdDnsQuery	R/W	Indicates whether a DNS query will be performed or not when the number of retransmissions is equal to the disconnect threshold. - noDnsQuery(0) - performDnsQuery(1) Default Value: noDnsQuery
ncsRetransmissionHistoryTimeout	R/W	Number of milliseconds for which the responses to old transactions must be kept. Default Value: 5000
ncsRetransmissionMaxWaitingDelay	R/W	Maximum waiting delay (in ms) an endpoint can wait before sending an RSIP. Default Value: 600000
ncsRetransmissionDisconnectInitialWaitingPeriod	R/W	Initial waiting delay (in ms) an endpoint must wait before starting the disconnect procedure. Default Value: 15000
ncsRetransmissionDisconnectMinWaitingPeriod	R/W	Disconnected minimum waiting delay (in ms) that must have elapsed since the gateway became disconnected before entering the disconnect procedure. Default Value: 15000
ncsRetransmissionDisconnectMaxWaitingPeriod	R/W	Disconnected maximum waiting delay (in ms) since the gateway became disconnected that an endpoint can wait before starting the disconnect procedure. Default Value: 600000

ncsLinePackage

The following parameters allow you to define the Line Package, which groups variables that determine tone time outs of the NCS protocol Line Package.

Table 194: NCS Parameters – Line Package

Name	Access	Description
ncsLinePackageBzDuration	R/W	Busy tone timeout value in ms. Default Value: 30000
ncsLinePackageDIDuration	R/W	Dial tone timeout value in ms. Default Value: 16000
ncsLinePackageLDuration	R/W	DTMF long duration timeout value in ms. Default Value: 2000
ncsLinePackageMwiDuration	R/W	Message waiting indicator tone timeout value in ms. Default Value: 16000
ncsLinePackageOtDuration	R/W	Off hook warning tone timeout value in ms. Default Value: 65535000
ncsLinePackageRbkDuration	R/W	Ring back on connection tone timeout value in ms. Default Value: 180000
ncsLinePackageRgDuration	R/W	Ring tone timeout value in ms. Default Value: 180000
ncsLinePackageRoDuration	R/W	Reorder tone timeout value in ms. Default Value: 30000
ncsLinePackageRtDuration	R/W	Ring back tone timeout value in ms. Default Value: 180000
ncsLinePackageSIDuration	R/W	Stutter dial tone timeout value in ms. Default Value: 16000
ncsLinePackageTCriticalDuration	R/W	Interdigit timeout value in ms when a timer is all that is required for the digit string to match a pattern in the digit map. Default Value: 4000
ncsLinePackageTPartialDuration	R/W	Interdigit timeout value in ms when at least one more digit is required for the digit string to match any of the patterns in the digit map. Default Value: 16000

ncsStats

The following parameters allow you to define statistics pertaining to the NCS signalling protocol.

Table 195: NCS Parameters – Statistics

Name	Access	Description
ncsStatsCurrentNumberOfActiveConnections	R-O	Number of active connections which are currently conducted by the gateway.

ncsStatsCurrentStatistics

Table 196: NCS Parameters – Current Statistics

Name	Access	Description
ncsStatsCurrentTotalNumberOfConnections	R-O	Total number of connections conducted by the gateway so far in the current statistics period.
ncsStatsCurrentAvgConnectionTime	R-O	Average connection time (in second) so far in the current statistics period.

ncsStatsCumulatedStatistics

Table 197: NCS Parameters – Cumulated Statistics

Name	Access	Description
ncsStatsCumulatedTotalNumberOfConnections	R-O	Cumulated number of connections conducted by the gateway.

Table 197: NCS Parameters – Cumulated Statistics (Continued)

Name	Access	Description
ncsStatsCumulatedAvgConnectionTime	R-O	Cumulated average connection time (in second).

NCS Protocol Parameters – NCS Compatibility MIB

This MIB contains objects for NCS compatibility of the Mediatrix products.

ncsCompatibilityMIBObjects

The following parameters allow you to define general NCS information.

Table 198: NCS Compatibility Parameters

Name	Access	Description
ncsCompatibilityRtpPayloadType18Encoding Name	R/W	Literal name of the compression algorithm corresponding to the RTP payload type 18. Available values are: - g729(0) - g729A(1) Default Value: g729
ncsCompatibilityVersion	R/W	Defines the content of the protocol header. - mgcp01Ncs10: Protocol header is set to 'MGCP 0.1 NCS 1.0'. This protocol is fully supported. - fakeMgcp10Ncs10: Protocol header is set to 'MGCP 1.0 NCS 1.0'. This protocol is not supported and the behavior of the unit is the same as for MGCP 0.1 NCS 1.0. This is a fake support to allow communication with a call agent that supports it. This configuration only has an effect if the <i>telephonyIpSignalingProtocolSelection</i> variable is set to ncs. Default Value: mgcp01Ncs10

IP Telephony Signalling SIP MIBs

Page Left Intentionally Blank

SIP Protocol Parameters – SIP MIB

This MIB contains SIP configuration objects.

sipMIBObjects

The following parameters allow you to set the SIP information.

Table 199: SIP Parameters – Basic

Name	Access	Description
sipPort	R/W	Port on which the SIP user agent server (UAS) will be listening for incoming SIP traffic. This value applies to all transports (e.g. UDP, TCP, etc.). Note: If set to 0, the default SIP port, 5060, will be used. This variable's semantics are different depending on the software version. Please refer to the documentation shipped with your device for more details. Default Value: 0
sipDomain	R/W	SIP domain name. If not empty, the address of record uses this string instead of the home domain proxy host (refer to the variable 'sipHomeDomainProxyStaticHost').

sipUAlfTable

This table holds the user agent configuration variables. A user agent is a logical entity that can act as both client and server for the duration of a dialog. The informations contained in this table will be used to dynamically create the To, From and Contact headers used in the request sent by the UAC.

Table 200: SIP Parameters – SIP User Agents

Name	Access	Description
sipUAMainUsername	R/W	A string that uniquely identifies this endpoint in the domain. For example, a telephone number. This string is used in the creation of the Contact and From headers. The SIP From header carries the permanent location (IP address, home domain) where the endpoint is. The SIP Contact header carries the CURRENT location (IP address) where the endpoint can be reached. Contact headers are used in two ways: - First, contacts are registered to the SIP registrar. This enables callers to be redirected to the endpoint's current location. - Second, a contact header is sent along with any request the UA sends (e.g.: INVITE), and will be used by the target UA as a return address for later requests sent by the target to this endpoint. This variable cannot be set to an empty value and is reset to 333000X during a factory reset, the X digit being the port number.
sipUADisplayName	R/W	Friendly name for the SIP User Agent. A friendly name or display name is meant to contain a descriptive version of the URI, and is intended to be displayed to a user interface.

Table 200: SIP Parameters – SIP User Agents (Continued)

Name	Access	Description
sipUAOtherAcceptedUsernames	R/W	A comma-separated list of user names that the endpoint will recognise as its own, but will NOT register in contacts sent to the registrar. Only the username in <i>sipUAMainUsername</i> is registered. This variable can be used to add variations on the main user name. For instance, let's say that the main user name is a telephone number, 555-1111. Variations could be to prefix the local area or country code, such as 819-555-1111. This value can contain multiple user names. These must be separated by a ',' character, such as: user1, user2, 5552222, 18195552222.
sipUAMaximumSessionExpirationDelay	R/W	Suggested maximum time, in seconds, for the periodical session refreshes. This value will be reflected in the Session-Expires header. Increasing the maximum will help to reduce network traffic, but will also make 'dead' calls longer to detect. This value is expressed in seconds (s). To disable the session timer service, set the maximum session timer expiration value to 0. However, this is not recommended since it will make 'dead' calls impossible to detect. Questions & Answers: - What is the session timer extension? The session timer extension allows the detection of the premature end of a call caused by a network problem or a peer's failure. The session timer mechanism simply resends an INVITE every <i>n</i> seconds. A successful response (200 OK) to this INVITE will indicate that the peer is still alive and reachable. A timeout to this INVITE may mean that there are problems in the signaling path, or that the peer is simply not there anymore. In that case the call will be shut down using normal SIP means. - SDP in Session Timer reINVITEs: The reINVITE is sent with the last SDP that was negotiated. Reception of a session timer reinvite should not modify the connection characteristics. - Relation between minimum and maximum values: A UA that receives a Session-Expires header whose value is smaller than the minimum it is willing to accept will reply a 422 Timer too low to the INVITE and terminate the call. The phone will not ring. It is up to the caller to decide what to do when it receives a 422 to its INVITE. Mediatix units will automatically retry the INVITE, with a Session-Expires value equal to the minimum value that the UAS was ready to accept (found in the Min-SE header). This means that the maximum value as set in the Mediatix unit might not be respected. This has the advantageous effect of establishing the call even if the two endpoints have conflicting values. Mediatix units will also keep retrying as long as they get 422 answers with different Min-SE values. - Who refreshes? Re-sending a session timer INVITE is referred to as refreshing the session. Normally, the UAS that receives the INVITE will have the last word on who refreshes. Mediatix units will always let the UAC (caller) do the refreshes if the caller supports session timers. In the case the caller does not support session timers, the Mediatix unit will assume the role of the refresher. Also see <i>sipUAMinimumSessionExpirationDelay</i>. Default Value: 3600
sipUAMinimumSessionExpirationDelay	R/W	Minimum value for the periodical session refreshes. This value will be reflected in the Min-SE header. The Min-SE value is a threshold that proxies and/or UAs on the signaling path are not allowed to go under. Increasing the minimum will help to reduce network traffic, but will also make 'dead' calls longer to detect. This value is expressed in seconds (s). Also see <i>sipUAMaximumSessionExpirationDelay</i>. Default Value: 1800

sipUAlfAuthenticationTable

This table holds the user agent authentication configuration variables. Authentication information adds some level of security.

Table 201: SIP Parameters – User Agent Authentication

Name	Access	Description
sipUAAuthIndex	R-O	Authentication index for this row.
sipUAAuthRealm	R/W	When authentication informations are required from users, the realm identifies who requested the information.
sipUAAuthUsername	R/W	A string that uniquely identifies this endpoint in the realm, used for authentication purposes. The user name always maps to a password.
sipUAAuthPassword	R/W	User password.
sipUAAuthValidateRealm	R/W	When set to disable, the current user credentials are valid for any realm. When set to enable, the user credentials are used only for a specific realm set in the <i>sipUAAuthRealm</i> variable. Default Value: enable

sipUnitAuthenticationTable

This table holds the unit authentication configuration variables. Authentication information adds some level of security..

Table 202: SIP Parameters – Unit Authentication

Name	Access	Description
sipUnitAuthIndex	R-O	Authentication index for this row.
sipUnitAuthRealm	R/W	When authentication informations are required from users, the realm identifies who requested the information.
sipUnitAuthUsername	R/W	A string that uniquely identifies this endpoint in the realm, used for authentication purposes. The user name always maps to a password.
sipUnitAuthPassword	R/W	User password.
sipUnitAuthValidateRealm	R/W	When set to disable, the current unit credentials are valid for any realm. When set to enable, the unit credentials are used only for a specific realm set in the <i>sipUnitAuthRealm</i> variable. Default Value: enable

sipRegistration

The following parameter defines the SIP registration..

Table 203: SIP Parameters – Registration

Name	Access	Description
sipRegistrationCmdRefresh	R/W	Command to refresh the registrations. - noOp: No operation. - refresh: Refresh registrations. All enabled endpoints unregister themselves from the previous registrar and send a new registration to the current registrar with the current parameters. Default Value: noOp
sipReRegistrationTime	R/W	In SIP, a registration is valid for a period of time decided by the registrar. Once a unit is registered, the SIP protocol requires the User Agent to refresh this registration before the registration expires. Typically, this re-registration must be completed before the ongoing registration expires, so that the User Agent's registration state will not change (i.e. will remain 'registered'). This variable defines the time, relative to the end of the registration, at which a registered unit will begin updating its registration. For example, if the registration lasts 60 minutes, and <i>sipReRegistrationTime</i> is set to 43, the unit will send new REGISTER requests 59 minutes and 17 seconds after the reception of the registration acknowledgement (43 seconds before the end of the registration period). Setting <i>sipReRegistrationTime</i> to 0 will have for effect that the User Agent will fall into the 'unregistered' state BEFORE sending the re-REGISTER requests. This value is expressed in seconds (s) and MUST be lower than the value of the Expires header of the contact in the 200 OK response to the REGISTER, otherwise the unit rapidly sends REGISTER requests continuously. Default Value: 60
sipRegistrationProposedExpirationValue	R/W	Configures the suggested expiration delay of a contact in the SIP REGISTER. Set the value to 0 to disable the expiration proposition. This value does not modify the delay before a re-REGISTER. The delay is the expires of the contact in the 200 OK response to the REGISTER minus the value set in the <i>sipReRegistrationTime</i> variable. If the expires of the contact in the 200 OK response to the REGISTER is not present or badly formatted, then the delay is the default registration expires minus the value set in the <i>sipReRegistrationTime</i> variable. See also the <i>sipReRegistrationTime</i> variable. This value is expressed in seconds (s). Default Value: 0

sipTransport

The following parameter defines the SIP transport..

Table 204: SIP Parameters – Transport

Name	Access	Description
sipTransportRegistrationEnable	R/W	Indicates whether the unit must include its supported transports in its registrations. If enabled, then the unit will register with one contact for each transport that is currently enabled. Each of these contacts will contain a "transport" parameter. Default Value: disable
sipTransportContactEnable	R/W	Indicates whether the unit must include its supported transport in all SIP messages that have the contact header, except for the REGISTER message (see the <i>sipTransportRegistrationEnable</i> variable). If enabled, then the unit will send SIP messages with the 'transport' parameter in the contact header It is either set to transport=tcp when TCP is enabled and UDP is disabled, transport=udp when UDP is enabled and TCP disabled or no transport parameter when both TCP and UDP are enabled. Default Value: disable

sipTransportConfigTablet

This table contains the informations pertaining to the supported transports. It is indexed by transport number (udp, tcp)..

Table 205: SIP Parameters – Transport Configuration

Name	Access	Description
sipTransportIndex	R-O	Transport index for this row. • udp: Index for the UDP transport • tcp: Index for the TCP transport
sipTransportEnable	R/W	Enables or disables the transport in question. This variable's semantics are different depending on the software version. Please refer to the documentation shipped with your device for more details. Default Value: enable
sipTransportQValue	R/W	Indicates the priority of the transport in question. A qvalue parameter will be added to each contact. This only applies if the transport-specific registration is enabled (see <i>sipTransportRegistration Enable</i>). Qvalues give each transport a weight, indicating the degree of preference for that transport. A higher value means higher preference. The format of the qvalue string must follow the RFC3261 ABNF (a floating point value between 0.000 and 1.000). If an empty string is specified, no qvalue will be set in the contacts.

sipPenaltyBox

The following parameters define the SIP penalty box feature..

Table 206: SIP Parameters – Penalty Box

Name	Access	Description
sipPenaltyBoxEnable	R/W	Indicates whether the unit uses the penalty box feature. The penalty box feature is used when a given host address times out. When the address times out, it is put into the penalty box for a given amount of time. During that time, the address in question is considered as "non-responding" for all requests. This feature is most useful when using multiple servers and some of them are down. It makes sure that users wait a minimal period of time before trying a secondary host. The penalty box is always "active". This means that even if the feature is disabled, IP addresses are marked as invalid, but they are still tried. The advantage is that when the feature is enabled, IP addresses that were already marked as invalid are instantly put into the penalty box. Also see <i>sipPenaltyBoxTime</i> . Default Value: disable
sipPenaltyBoxTime	R/W	Amount of time that a host spends in the penalty box. This value is expressed in seconds (s). An IP address is put into the penalty box for the current <i>sipPenaltyBoxTime</i> . Changing the <i>sipPenaltyBoxTime</i> does not affect IP addresses that are already in the penalty box. In other words, the <i>sipPenaltyBoxTime</i> only affects new entries in the penalty box. Also see <i>sipPenaltyBoxEnable</i> . Default Value: 300

sipGrouping

The following parameters define the SIP grouping feature.

sipUAGroupConfigTable

This table holds the user agent configuration variables. A user agent is a logical entity that can act as both client and server for the duration of a dialog. The informations contained in this table will be used to dynamically create the *To*, *From* and *Contact* headers used in the request sent by the UAC.

Table 207: SIP Parameters – User Agent Group

Name	Access	Description
sipUAGroupMaximumSessionExpirationDelay	R/W	Suggested maximum time for the periodical session refreshes. This value will be reflected in the Session-Expires header. Increasing the maximum will help to reduce network traffic, but will also make "dead" calls longer to detect. This value is expressed in seconds (s). To disable the session timer service, set the maximum session timer expiration value to 0. However, this is not recommended since it will make "dead" calls impossible to detect. Questions & Answers - Q - What is the session timer extension? A - The session timer extension allows the detection of the premature end of a call caused by a network problem or a peer's failure. The session timer mechanism simply resends an INVITE every <i>n</i> seconds. A successful response (200 OK) to this INVITE will signify that the peer is still alive and reachable. A timeout to this INVITE may mean that there are problems in the signaling path, or that the peer is simply not there anymore. In that case the call will be shut down using normal SIP means. - Q - SDP in Session Timer reINVITEs: A - The reINVITE is sent with the last SDP that was negotiated. Reception of a session timer reinvite should not modify the connection characteristics. - Q - Relation between minimum and maximum values: A - A UA that receives a Session-Expires header whose value is smaller than the minimum it is willing to accept will reply a 422 Timer too low to the INVITE and terminate the call. The phone will not ring. It is up to the caller to decide what to do when it receives a 422 to its INVITE. Mediatix units will automatically retry the INVITE, with a Session-Expires value equal to the minimum value that the UAS was ready to accept (found in the Min-SE header). This means that the maximum value as set in the Mediatix unit might not be respected. This has the advantageous effect of establishing the call even if the two endpoints have conflicting values. Mediatix units will also keep retrying as long as they get 422 answers with different Min-SE values. - Q - Who refreshes? A - Re-sending a session timer INVITE is referred to as refreshing the session. Normally, the UAS that receives the INVITE will have the last word on who refreshes. Mediatix units will always let the UAC (caller) do the refreshes if the caller supports session timers. In the case the caller does not support session timers, the Mediatix unit will assume the role of the refresher. Also see <i>sipUAGroupMinimumSessionExpirationDelay</i>. Default Value: 3600
sipUAGroupMinimumSessionExpirationDelay	R/W	Minimum value for the periodical session refreshes. This value will be reflected in the Min-SE header. The Min-SE value is a threshold that proxies and/or UAs on the signaling path are not allowed to go under. Increasing the minimum will help to reduce network traffic, but will also make "dead" calls longer to detect. This value is expressed in seconds (s). Also see <i>sipUAGroupMaximumSessionExpirationDelay</i>. Default Value: 1800

Table 207: SIP Parameters – User Agent Group (Continued)

Name	Access	Description
sipUAGroupRegistrationUsername	R/W	Used to enable the SIP registration of an FXO unit. When empty, the FXO unit does not register with the SIP registrar. This is the standard behaviour. When a name is configured, the unit sends a single REGISTER request to the SIP Registrar, using this identification, in order to make its presence known. When a previously configured name is set to empty, the unit unregisters itself from the SIP Registrar.

sipUAGroupAuthenticationTable

This table holds the user agent authentication configuration variables. Authentication information adds some level of security.

Table 208: SIP Parameters – Authentication per Group

Name	Access	Description
sipUAGroupAuthIndex	R-O	Authentication index for this row.
sipUAGroupAuthRealm	R/W	When authentication informations are required from users, the realm identifies who requested the information.
sipUAGroupAuthUsername	R/W	A string that will uniquely identify this endpoint in the realm, used for authentication purposes. The username always maps to a password.
sipUAGroupAuthPassword	R/W	User password.
sipUAGroupAuthValidateRealm	R/W	When set to disable, the current group credentials are valid for any realm. When set to enable, the group credentials are used only for a specific realm set in the sipUAGroupAuthRealm variable. Default Value: enable

sipPublication

The following parameter defines the SIP publication..

Table 209: SIP Parameters – Publication

Name	Access	Description
sipPublicationCmdRefresh	R/W	Command to refresh the publications. - noOp: No operation. - refresh: Refresh publications. All enabled endpoints unpublish themselves from the previous Presence Compositor and send a new publication to the current Presence Compositor with the current parameters. Default Value: noOp
sipPublicationRefreshTime	R/W	A publication is valid for a period of time specified by the Presence Compositor. The User Agent is then responsible for refreshing its previously established publications before their expiration interval has elapsed. This variable defines the time, relative to the end of the publication, at which the User Agent will begin refreshing its publication. This value is expressed in seconds (s). For example, if the publication lasts 60 minutes and sipPublicationRefreshTime is set to 43, the unit will send new PUBLISH requests 59 minutes and 17 seconds after the reception of the publication acknowledgement (43 seconds before the end of the publication period). Setting <i>sipPublicationRefreshTime</i> to 0 means that the User Agent will fall into the 'unpublished' state BEFORE sending the refreshing PUBLISH request. Default Value: 60

Table 209: SIP Parameters – Publication (Continued)

Name	Access	Description
sipPublicationProposedExpirationValue	R/W	Configures the suggested expiration delay of a publication. Keep in mind that this is only a suggestion and that servers will decide the publication time following local policy. Set the value to 0 to disable the expiration proposition. This value is expressed in seconds (s). This value does not modify the delay before a re-PUBLISH. The delay is the value of the Expires header in the 200 OK response to the PUBLISH minus the value set in the <i>sipPublicationRefreshTime</i> variable. If the Expires header in the 200 OK response to the PUBLISH is not present or badly formatted, then the delay is the value of the variable <i>sipInteropDefaultPublicationExpiration</i> minus the value set in the <i>sipPublicationRefreshTime</i> variable. See also the <i>sipPublicationRefreshTime</i> variable. Default Value: 0

sipConference

The following parameter defines the SIP conference..

Table 210: SIP Parameters – Conference

Name	Access	Description
sipConferenceType	R/W	Specifies how to manage a SIP conference. This configuration only applies to a conference initiated by one of the unit's endpoint. - local: The conference is managed locally by the unit. - conferenceServer: The conference is managed by a remote SIP conference server. This variable only has an effect when <i>subscriberServicesConferenceEnable</i> is set to enable. Default Value: local
sipConferenceServerURI	R/W	A string that represents the address of a conference server. This variable only has an effect when <i>sipConferenceType</i> is set to conferenceServer. Please refer to the documentation shipped with your device for more details regarding this variable's semantics.

sipTrustedSources

The following parameters define the SIP trusted sources feature..

Table 211: SIP Parameters – Trusted Sources

Name	Access	Description
sipTrustedSourcesEnable	R/W	Enables the SIP trusted sources feature. - enable: The unit only accepts SIP messages from the trusted addresses listed in <i>sipTrustedSourcesTable</i>. All other SIP messages are ignored. This source address validation takes place at the IP level and does not depend on the SIP header or body. - disable: The unit does not validate the source address of SIP messages at the IP level. Default Value: disable

sipTrustedSourcesTable

Table that lists up to 6 trusted sources of SIP messages..

Table 212: SIP Parameters – Trusted Sources Table

Name	Access	Description
sipTrustedSourcesIpAddress	R/W	IP address of a trusted source of SIP messages.

SIP Protocol Parameters – Experimental MIB

This MIB contains SIP experimental (NAT traversal and others) configuration objects.

sipExperimentalMIBObjects

The following parameters allow you to set various experimental configuration objects.

Table 213: SIP Parameters – Experimental

Name	Access	Description
sipUnregisteredPortBehavior	R/W	This variable specifies whether a port should remain enabled or not when not registered. • disablePort: When an endpoint is not registered, it is disabled. This prevents the user from making or receiving calls. Picking up the handset will yield a fast busy tone, and incoming INVITEs will receive a "403 Forbidden" response. Ports that have a physical bypass will enable the bypass in this case. • enablePort: When an endpoint is not registered, it is still enabled. The user will be able to receive and initiate outgoing calls. Note that since the endpoint is not registered to a registrar, the public address of the endpoint is not available to the outside world, so the endpoint will most likely be unreachable except through direct IP calling. Default Value: disablePort
sipOutboundProxyConfig	R/W	This variable provisions the type of routing that the configured outbound proxy does. • looseRouter: This is the most current method for SIP routing, as per RFC3261, and will become the standard behavior once RFC3261 compliance is achieved. See sipOutboundProxyHost in the SIP MIB for a description. • strictRouter: Pre-RFC3261, RFC2543 compatible SIP routing. The initial route for all SIP requests will contain the home domain proxy address (the Request-URI). Requests will be directed to the outbound proxy. In other words, the Request-URI is constructed as usual, using the home domain proxy and the username, but is used in the route set. The Request-URI is filled by the outbound proxy address. Also see <i>sipHomeDomainProxyHost</i>. Default Value: looseRouter

Table 213: SIP Parameters – Experimental (Continued)

Name	Access	Description
sipEnforceOfferAnswerModel	R/W	Determines whether the unit requires strict adherence to RFC 3264 from the peer when negotiating capabilities for the establishment of a media session. When enabled, the following guidelines from the Offer-Answer Model must be strictly followed. An answer must: • Include at least one codec from the list that the unit sent in the offer; • Avoid adding extra codecs that were not present in the offer; • Contain the same number of media lines that the unit put in its offer. Otherwise, the answer is rejected and the unit ends the call. When disabled, then the peer can freely: • Send back a brand new list of codecs or add new ones to the offered list; • Add media lines AFTER the ones found in the offer. As long as at least one codec sent back is supported by the unit, the call is allowed to go on. Any media lines added by the peer is simply ignored. The <i>sipAllowMediaReactivationInAnswerEnable</i> and <i>sipAllowAudioAndImageNegotiationEnable</i> variables allow to enable or disable other deviations from the Offer/Answer model. Default Value: enable
sipAllowMediaReactivationInAnswerEnable	R/W	Determines the unit behaviour when receiving a SDP answer activating a media that had been previously deactivated in the offer. • Enable: A media reactivated in an incoming answer is ignored. This behaviour goes against the SDP Offer/Answer model described by IETF RFC 3264. • Disable: A media reactivated in an incoming answer ends the current media negotiation and the call. This behaviour follows the SDP Offer/Answer model described by IETF RFC 3264. The <i>sipEnforceOfferAnswerModel</i> and <i>sipAllowAudioAndImageNegotiationEnable</i> variables allow to enable or disable other deviations from the Offer/Answer model. Default Value: disable
sipAllowAudioAndImageNegotiationEnable	R/W	Determines the unit behaviour when offering media or answering to a media offer with audio and image negotiation. • Enable: The unit offers audio and image media simultaneously in outgoing SDP offers and transits to T.38 mode upon reception of a T.38 packet. Also, when the unit answers positively to a SDP offer with audio and image, it transits to T.38 mode upon reception of a T.38 packet. • Disable: Outgoing offers never include image and audio simultaneously. Incoming offers with audio and image medias with a non-zero port are considered as offering only audio. The <i>sipEnforceOfferAnswerModel</i> and <i>sipAllowMediaReactivationInAnswerEnable</i> variables allow to enable or disable other deviations from the Offer/Answer model. Default Value: disable
sipCodecOrderInAnswer	R/W	Determines the unit behaviour when answering to a media offer. • localOrder: The codecs contained in the answer are prioritized according to the configured preferred codec. This means that the codecs in the answer may have a different order than in the received offer. • offerOrder: The codecs contained in the answer have the same order as the received offer. This means that the preferred codec configured has no effect on the codec order of the answer. Default Value: localOrder
sipRtpUdpChecksumEnable	R/W	Enables/disables the UDP checksum for RTP packets. UDP checksum is disabled by default to gain performance. • Enable: UDP checksum will be calculated for each RTP packet. This may affect performance. • Disable: UDP checksum will not be calculated. The value 0 will be written in the checksum field of each RTP packet header. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation shipped with your device for more details. Default Value: disable

sipNatCustom

The following parameters allow you to set the SIP NAT Custom information.

Table 214: SIP Parameters – SIP NAT

Name	Access	Description
sipNatCustomEnable	R/W	Enable/disable the NAT traversal scheme. • disable(0) • enable(1) Default Value: disable
sipNatCustomPublicAddress	R/W	The public IP address used as Contact address by outgoing SIP packets crossing a NAT system. Default Value: 0.0.0.0

SIP Protocol Parameters – Interop MIB

This MIB contains SIP interoperability configuration objects.

sipInteropMIBObjects

The following parameters allow you to set the SIP Interop information.

Table 215: SIP Interop Parameters

Name	Access	Description
sipInteropReplacesConfig	R/W	Configures usage of the Replaces header mechanism used in a transfer. When supported by the target of the transfer, Replaces ensures a more seamless transfer by permitting the initiating party to effectively replace a current call by another instead of disconnecting the call to be replaced and creating a second call. <i>doNotUseReplaces</i>: The Replaces header is not used. <i>useReplacesWithRequire</i>: The Replaces header is used. It can be seen in the Refer-To header found in the REFER request sent by the transferor. It can also be seen in the INVITE sent by the transferee. The target that supports Replaces will use its information to merge the new INVITE with an existing call specified in the Replaces header. The transferee will require the use of the replaces extension for proper completion of the transfer. If the replaces extension is not supported by the target of the transfer, the unit will go into a fallback algorithm to retry the transfer using replaces, by reversing the roles of the target and the transferee (by resending the REFER to the initial target instead of the initial transferee). As a last resort (if none of the participants supports replaces), the transfer will be carried out without using the replaces extension. <i>useReplacesNoRequire</i>: The Replaces header is used. It can be seen in the Refer-To header found in the REFER request sent by the transferor. It can also be seen in the INVITE sent by the transferee. The target that supports Replaces will use its information to merge the new INVITE with an existing call specified in the Replaces header. This will disable the transfer fallback. The replaces information will still be present, but no check will be made that it is effectively used to complete the transfer. Default Value: useReplacesWithRequire

Table 215: SIP Interop Parameters (Continued)

Name	Access	Description
siplInteropTransferVersion	R/W	Selects the version of the transfer draft that the unit will use. The provisioned version is used for initiating transfers, and receiving them. Transfer versions other than those provisioned will not work. - transfer02: The unit will execute transfers using the methods described in the now expired <i>draft-ietf-sip-cc-transfer-02.txt</i>. This draft was obsoleted. Its use is deprecated and this setting should be used for backward compatibility issues only. - transfer05UsingRefer02: The unit will execute transfers using the methods described in the more recent <i>draft-ietf-sip-cc-transfer-05.txt</i>. This draft version contains several enhancements over the previous ones. Among others, it is possible to use the replaces header to provide a more seamless attended transfer to the user. This method also uses <i>draft-ietf-sip-refer-02.txt</i>. This setting should be used if you don't need to interop with transfer02-enabled parties. - sippingTransfer01UsingReferRfc3515 The unit executes transfers by using the methods described in <i>draft-ietf-sipping-cc-transfer-01.txt</i>. This draft version is more recent than Transfer02 and Transfer05UsingRefer02. This method also uses RFC 3515 - The Session Initiation Protocol (SIP) Refer Method. Default Value: transfer05UsingRefer02
siplInteropSessionTimerVersion	R/W	Selects the version of the session timer draft that the unit will use. Session timer versions other than those provisioned may not work because of backward compatibility issues between the versions. - sessionTimer04: The unit will use the session timer extension as described in the now expired <i>draft-ietf-sip-session-timer-04.txt</i>. This draft was obsoleted. Its use is deprecated and this setting should be used for backward compatibility issues only. - sessionTimer08: The unit will use the session timer extension as described in the more recent <i>draft-ietf-sip-session-timer-08.txt</i>. This draft version contains several enhancements over the previous ones, including the use of the Min-SE header. This setting should be used if you don't need to interoperate with session timer v4-enabled parties. Default Value: sessionTimer08
siplInteropTransmissionTimeout	R/W	Changes the time to wait for a response or an ACK before considering a transaction timed out. This corresponds to timers B, F and H for all transport protocols and timer J for UDP. These timers are defined in section A of RFC3261. This timeout will affect the number of retransmissions. Retransmissions continue to follow the timing guidelines found in RFC3261. For example, if using DNS SRV and multiple entries are present, this value will be the time spent waiting for answers from each entry. This value is expressed in seconds (s). Default Value: 32
siplInteropReplacesVersion	R/W	Selects the version of the ietf-sip-replaces draft to conform to. The provisioned version affects the way blind transfers are executed. - replaces01: When following the sip-replaces-01 draft, the Transferor is allowed to use a REFER with Replaces when proceeding to initiate a blind transfer. This, in turn, results in the Transferee including a Replaces header in its INVITE to the Transfer Target. - replaces03: The sip-replaces-03 draft forbids the use of Replaces in the case of a blind transfer. When initiating one, the Transferor first CANCELS its call with the Target and then issues a REFER without Replaces to the Transferee. Default Value: replaces01

Table 215: SIP Interop Parameters (Continued)

Name	Access	Description
sipInteropSymmetricUdpSourcePortEnable	R/W	Indicates whether the unit always uses the same local port when sending SIP traffic over UDP. Symmetric UDP ports are sometimes needed to traverse NAT/Firewall devices. Note that when changing this setting, all destinations are automatically thrown out of the penalty box, when applicable. - enable: SIP signaling sent over UDP originates from the same port as the port on which the user agent is listening. This is configured in MX-SIP-MIB's <i>sipPort</i> variable. When enabled, ICMP messages are not processed, which means that unreachable targets will take longer to detect. - disable: SIP signaling over UDP uses a randomly-generated originating port. ICMP errors are processed correctly. This variable's semantics are different depending on the software version. Please refer to the documentation shipped with your device for more details. Default Value: enable
sipInteropMaxForwardsValue	R/W	Sets the value that will be used in the <i>Max-Forwards</i> header. To disable inclusion of this header in SIP requests, set the value to -1. This variable's semantics are different depending on the software version. Please refer to the documentation shipped with your device for more details. Default Value: 70
sipInteropAutomaticRejectionCode	R/W	Configures the SIP code to use when rejecting a call once the timer specified in <i>telephonyAttributesCallDirectionRestriction</i> elapses. Examples of possible SIP code: 400: Bad Request 401: Unauthorized 402: Payment required 403: Forbidden 404: Not found 405: Method not allowed 406: Not acceptable 407: Proxy authentication required 408: Request timeout 410: Gone 413: Request Entity too long 414: Request-URI too long 415: Unsupported media type 416: Unsupported URI Scheme 420: Bad extension 421: Extension Required 423: Interval Too Brief 480: Temporarily unavailable 481: Call/Transaction Does not Exist 482: Loop Detected 483: Too many hops 484: Address incomplete 485: Ambiguous 486: Busy here 500: Server internal error 501: Not implemented 502: Bad gateway 503: Service unavailable 504: Server time-out 504: Version Not Supported 513: Message Too Large 600: Busy everywhere 603: Decline 604: Does not exist anywhere Default Value: 480
sipInteropSendUAHeaderEnable	R/W	Enables/Disables sending of the SIP User-Agent header. Note: The unit must be rebooted to apply the modification. Default Value: enable

Table 215: SIP Interop Parameters (Continued)

Name	Access	Description
sipInteropUAHeaderConfig	R/W	Customize the SIP User-Agent header value. The following macros are replaced by their representation: • %version%: Version of the application. • %mac%: Unit MAC address (lowercase). • %rev%: Hardware revision number. • %product%: Product name. • %%: A '%' sign. Note: The unit must be rebooted to apply the modification. Default Value: MxSipApp/%version%
sipInteropSdpDirectionAttributeEnable	R/W	Indicates if the SDP direction attribute is present in the initial INVITE sent by the unit and if the direction attribute present in the SDP received from the peer is ignored or not. disable: • No direction attribute is present in the SDP sent by the unit. • Any direction attribute found in the SDP received from the peer is ignored by the unit. • To put an endpoint on hold, a SDP containing a connection address of "0.0.0.0" is sent. The method to put a session on hold is in conformance with RFC 2543. enable: • The unit always sends the direction attribute in the SDP of the initial INVITE. • The initial handshake determines if the peer supports the direction attribute or not. • If present in the SDP, the direction attribute is preferred over the connection address to transmit session modification information. This method is in conformance with RFC 3264. Default Value: enable
sipInteropAllowMultipleActiveMediaInAnswer	R/W	Determines the behaviour of the device when answering a request offering more than one active media. • disable : The answer contains only one active media. The media specified as active in the answer is the top-most matching one in the offer. Other medias are set to inactive. • enable : Each matching active media in the offer is specified as active in the answer. Other medias are set to inactive. Default Value: enable
sipInteropOnHoldSdpStreamDirection	R/W	Indicates the direction attribute and the meaning of the connection address "0.0.0.0" sent in the SDP when putting an endpoint on hold. • inactive: The stream is put on hold by marking it as inactive. • sendonly: The stream is put on hold by marking it as sendonly. This method is in conformance with RFC 3264. This configuration has no effect if the <i>sipInteropSdpDirectionAttributeEnable</i> variable is set to 'Disable'." Default Value: inactive
sipInteropOnHoldAnswerSdpStreamDirection	R/W	Indicates how to set the direction attribute and the connection address in the SDP when answering a hold offer with the direction attribute 'sendonly'. • inactive: The stream is marked as inactive and the connection address is set to '0.0.0.0'. • revconly: If the stream is currently active or receive only, the stream is marked as revconly and the connection address is set to the IP address of the unit. If the stream is currently send only or inactive, the stream is marked as inactive and the connection address is set to '0.0.0.0'. This method is in conformance with RFC 3264. In both cases, no direction attribute is present in the SDP if the <i>sipInteropSdpDirectionAttributeEnable</i> variable is set to 'Disable'." Default Value: revconly

Table 215: SIP Interop Parameters (Continued)

Name	Access	Description
siplInteropIgnoreMediaRenegotiationAfterCngDetection	R/W	Configures the behaviour of the unit when being re-invited after a CNG detection. - disable: Re-invites are processed normally; they are replied positively or negatively depending on the unit's codec configuration. - enable: Re-invites are replied positively but the resulting negotiated codecs are ignored. When a CED is detected, the data codec selection procedure is applied using the initial negotiated codecs. This configuration has no effect if the <i>dataIfCngToneDetectionEnable</i> variable is set to Enable. This variable's semantics are different depending on protocol and/or hardware platforms. Please refer to the documentation for more details. Default Value: disable
siplInteropMwiMessageSummaryValidation	R/W	Indicates how Message Waiting Indicator notifications must be validated. - enable: In order to have the Message Waiting Indicator activated, the SIP notification must meet all of the following requirements: a. 'Messages-Waiting' must be set to yes. b. The message waiting media type must contain 'voice-message'. c. The number of new messages must be greater than or equal to 1. - disable: In order to have the Message Waiting Indicator activated, the SIP notification must meet the following requirement: a. 'Messages-Waiting' must be set to yes. Note that only Message Waiting notifications for an established subscription are affected. Message Waiting notifications without subscription always behaves as described in 'disable'. Default Value: enable
siplInteropSipOptionsMethodSupport	R/W	Determines the behaviour of the device when answering a SIP OPTIONS request. - none: The unit responds with an error 405 Method not allowed. - alwaysOk: The unit responds with a 200 OK regardless of the content of the OPTIONS request. Default Value: none
siplInteropLocalRingOnProvisionalResponse	R/W	Specifies if the local ring should be started on reception of a "18x Provisional" response without SDP. Note that this variable does not affect the behavior in case where the "18x Provisional" response contains SDP. - disable: The local ring will not be started on a "18x Provisional" response without SDP, except for a "180 Ringing" message. - enable: The local ring will be started on any "18x Provisional" response without SDP. Default Value: disable
siplInteropCallWaitingToneControlViaSipInfo	R/W	Indicates if the call waiting tone can be controlled via the SIP INFO method with the content type 'application/broadsoft'. The controlled call waiting tone is played through the telephony interface. - disable: The application rejects the SIP INFO with the content type 'application/broadsoft'. - enable: SIP INFO with the content type 'application/broadsoft' is accepted and the call waiting tone is started or stopped according to the body. The INFO method is also included in the 'Allow' SIP header. Default Value: disable
siplInteropSdpOriginLineSessionIDAndVersionMaxLength	R/W	The maximum length of the session ID and the session version number in the origin line (o=) of the SDP. - max-32bits: The session ID and the session version number are represented with a 32 bit integer. They have a maximum length of 10 digits. - max-64bits: The session ID and the session version number are represented with a 64 bit integer. They have a maximum length of 20 digits. Default Value: max-64bits

Table 215: SIP Interop Parameters (Continued)

Name	Access	Description
sipInteropIgnoreUsernameParam	R/W	Controls whether or not the username parameter is ignored when routing an incoming SIP call to a line. - disable: The username parameter is not ignored when routing an incoming SIP call to a line. The parameter is considered as part of the username. - enable: The username parameter is ignored when routing an incoming SIP call to a line. Default Value: disable
sipInteropEscapePoundInSipUriUsername	R/W	Determines whether or not the pound character (#) must be escaped in the username part of a SIP URI. - disable: Pound character (#) is not escaped in the username part of a SIP URI. - enable: Pound character (#) is escaped in the username part of a SIP URI. Note: RFC 3261 specifies that the pound character (#) needs to be escaped in the username part of a SIP URI. Default Value: enable
sipInteropRegisterHomeDomainHostOverride	R/W	Home domain override configuration. If not empty, the address of record in the REGISTER uses this string instead of the SIP domain or home domain proxy host (refer to the variables 'sipDomain' and 'sipHomeDomainProxyStaticHost').
sipInteropRetryFailedRegistration	R/W	Controls whether or not failed registration attempts are retried periodically. - disable: No retries are performed following a failed registration attempt. Manual intervention is required for the port to attempt registration again. - enable: A failure to register a port to the SIP Registrar triggers an automatic retry every 2 minutes. Default Value: enable
sipInteropUseSipDomainInRequestURI	R/W	Controls whether or not the request URI is built using the SIP Domain. - disable: The request URI is built using the home domain proxy host. (refer to the variable 'sipHomeDomainProxyStaticHost') - enable: The request URI is built using the sipDomain, if one is specified, for all SIP methods with the exception of REGISTER and PUBLISH. The parameter maddr is also added to the Request URI with the value of the home domain proxy host. (refer to the variable 'sipDomain' and 'sipHomeDomainProxyStaticHost') Default Value: disable
sipInteropReferredByConfig	R/W	Configures usage of the Referred-By field used in a SIP REFER message. - useSipStackDefault: Let the SIP stack populate the Referred-By header field. - useLocalUrl: Use the local URL to populate the Referred-By header field. Default Value: useSipStackDefault
sipInteropConferenceServerMechanism	R/W	Determines the mechanism used to establish a conference and how the participants are connected to the conference server. rfc4579WithoutErrorRecovery: The connection with the conference server is made as defined in RFC 4579. The participants are connected to the conference server by sending the REFERs simultaneously. The connection with the participant is terminated if the participant fails to complete the REFER. rfc4579WithErrorRecovery: The connection with the conference server is made as defined in RFC 4579. The participants are connected to the conference server by sending the REFERs sequentially. The REFER is not sent to the second participant and the call stays in the same state if the first participant fails to complete the REFER. This variable only has an effect when sipConferenceType is set to conferenceServer. Default Value: rfc4579WithErrorRecovery

Table 215: SIP Interop Parameters (Continued)

Name	Access	Description
sipInteropUseT38Format	R/W	Determines the format used, in the SDP portion of SIP packets, to advertise the unit's T.38 capabilities. - disable: Support for the boolean T.38 parameters T38FaxFillBitRemoval, T38FaxTranscodingMMR and T38FaxTranscodingJBIG is advertised by associating a value of 0 (unsupported) or 1 (supported) with the parameter in the following manner: <pre> a=T38FaxFillBitRemoval:0 a=T38FaxTranscodingMMR:0 a=T38FaxTranscodingJBIG:0 </pre> - enable: Support for the above T.38 parameters is advertised in conformance with ITU-T Recommendation T.38, section D.2.3. The presence of the parameter in the SDP indicates support for it (without the need for an associated value), while its absence means that it is not supported. Default Value: disable
sipInteropT38NoSignalBehavior	R/W	Determines when the unit starts sending T.38 no-signal packets when being Re-Invited to switch from voice to T.38. - receivingReInvite: The unit starts sending T.38 no-signal packets when receiving the Re-Invite. - receivingAck: The unit waits until the ACK to its 200 OK has been received before sending T.38 no-signal packets. This configuration has no effect if the <i>dataT38NoSignalEnable</i> variable is set to 'Disable.' Default Value: receivingReInvite
sipInteropBehaviorOnT38InviteRejectedWith606	R/W	Behavior of the device when receiving a 606 SIP error response to an INVITE for T.38 fax. - dropCall: The call is dropped by sending a BYE. - usePreviousMediaNegotiation: No re-INVITE is sent and the audio codec from the last successful negotiation is used. For the remainder of the call, T.38 is disabled and fax detection may trigger a switch to a clear channel codec that was available in the last successful negotiation. Default Value: dropCall
sipInteropLockDnsSrvRecordPerCallEnable	R/W	Configures the behavior of the DNS SRV feature. - disable: The behavior follows RFC 3263. - enable: All messages during a call or registration use the same SRV record. Default Value: disable
sipInteropRemoveOutboundProxyRouteHeader	R/W	Determines whether or not SIP requests sent to the proxy contain a Route header displaying the proxy's address. It is only effective when an outbound proxy host is configured (see sipOutboundProxyStaticHost or sipOutboundProxyDhcpSiteSpecificCode). It is useful when interoperating with SIP servers that do not conform to RFC 3261's recommended practice concerning outbound proxy usage. - disable: Default behaviour. SIP requests sent to the outbound proxy contain a Route header, as per RFC 3261's recommendation. - enable: SIP requests are routed to the outbound proxy without inserting a Route header in the SIP packet. Default Value: disable
sipInteropReuseCredentialEnable	R/W	Configures how to reuse the credential in different transactions of the same call or registration. - disable: Do not reuse the credential negotiated in previous transactions. - enable: Reuse the credential negotiated in previous transactions. Default Value: enable
sipInteropUsePAssertedHeader	R/W	Enables the extraction of caller ID information from the P-Asserted-Identity header (a SIP extension described in RFC 3325). - disable: Caller ID data is based on the value assigned to the From header of the incoming SIP request. - enable: The unit first attempts to get the caller ID information from the P-Asserted-Identity header, if present. In case of failure, it falls back to the content of the From header. Default Value: disable

Table 215: SIP Interop Parameters (Continued)

Name	Access	Description
siplInteropRingingResponseCode	R/W	Configures the response code sent back when the endpoint starts ringing. - send180Ringing: Send out a '180 Ringing' response without a body. - send183WithSdp: Return a '183 Session Progress' packet with SDP (needed if the endpoint is required to generate ringback on connection). Default Value: send180Ringing
siplInteropRejectCodeForNoResource	R/W	Configures the rejection code used when all lines of the group are unavailable. - temporarilyUnavailable: The '480 Temporarily Unavailable' rejection code is used. - busyHere: The '486 Busy Here' rejection code is used." Default Value: temporarilyUnavailable
siplInteropAckUnsupportedInfoRequests	R/W	Determines the unit's behavior upon reception of an unknown type of INFO request. - disable: Unknown INFO requests trigger a 415 Unsupported Media Type response. - enable: Reception of unknown INFO requests is acknowledged with a 200 OK response. Default Value: disable
siplInteropBranchMatchingMethod	R/W	Configures the method used to match incoming SIP packets with a branch. - rfc2543: Follows the method described in RFC 2543 (section 10.1.2). - rfc3261: Follows the method described in RFC 3261 (section 8.1.1.7). Default Value: rfc3261
siplInteropIgnoreViaBranchIdInCancelEnable	R/W	Specifies whether the SIP stack's transaction matching procedure ignores the Via header field's branch parameter in CANCEL requests with no To tag. - disable: The transaction matching procedure behaves according to section 17.2.3 of RFC3261. - enable: The branch parameter is not used as a transaction matching criterion for CANCEL requests with no To tag." Default Value: disable
siplInteropDefaultRegistrationExpiration	R/W	Configures the default registration expiration. This value is used when the contact in a registration response contains no expires or the expires is badly formatted. In this case, the delay before a re-REGISTER is the value set in the <i>siplInteropDefaultRegistrationExpiration</i> variable minus the value set in the <i>sipReRegistrationTime</i> variable. The recommended value in RFC 3261 (section 10.2) is 3600. This value is expressed in seconds (s). Default Value: 3600
siplInteropDefaultPublicationExpiration	R/W	Configures the default publication expiration. This value is used when a publication response contains no or a badly formatted Expires header. In this case, the delay before a re-PUBLISH is the value set in the <i>siplInteropDefaultPublicationExpiration</i> variable minus the value set in the <i>sipPublicationRefreshTime</i> variable. This value is expressed in seconds (s). Default Value: 3600
siplInteropAuthenticationQop	R/W	Specifies the quality of protection the SIP User Agent should apply to its authentication request. - auth: The SIP User Agent applies authentication only. - auth-int: The SIP User Agent applies authentication with integrity protection (see RFC 2617). Default Value: auth
siplInteropProxyAuthenticationUriParametersEnable	R/W	Indicates if the uri-parameters are copied from the Request-URI to the level of proxy authentication. - enable: Copy uri-parameters to the level of proxy authentication. - disable: Do not copy uri-parameters to the level of proxy authentication. This allows reducing the SIP packet size but it does not follow the recommendations of RFC 3261. Default Value: enable

Table 215: SIP Interop Parameters (Continued)

Name	Access	Description
sipInteropUseDtmfPayloadTypeFoundInAnswer	R/W	The default behavior when sending an initial offer that contains an RFC 2833 payload type is to keep using that payload type even if the response comes back with a different one. When this variable is enabled, the unit rather uses the payload type found in the answer. The variable does not affect the behaviour when receiving an offer. The payload type is used symmetrically meaning that it's used to send and receive the DTMF. Use the variable <i>sipInteropAllowAsymmetricDtmfPayloadType</i> to allow asymmetric payload type. - disable: Keep using the initial payload type. - enable: Use the RFC 2833 payload type found in the received answer. This variable only has an effect when <i>voicelfDtmfTransport</i> is set to <i>outOfBandUsingRtp</i>. Default Value: disable
sipInteropAllowAsymmetricDtmfPayloadType	R/W	The default behaviour when receiving an answer to an offer that contained an RFC 2833 payload type is to use that payload type symmetrically (to send and receive DTMF). When this variable is enabled, the unit rather uses the payload type that was placed in the initial offer to receive DTMF but still uses the one in the response to send them. The variable does not affect the behaviour when receiving an offer. - disable: Use the RFC 2833 payload type found in the received answer to receive DTMF. - enable: Keep using the initial payload type to receive DTMF. This variable only has an effect when <i>sipInteropUseDtmfPayloadTypeFoundInAnswer</i> is set to enable. Default Value: disable
sipInteropFromUriDomainSelection	R/W	Specifies the composition of the domain used in the from:URI of SIP requests sent by the unit. - sipDomain: The domain of from:URI is built from the <i>sipDomain</i> variable. If <i>sipDomain</i> is empty, <i>sipHomeDomainProxyHost</i> is used instead. - localHostWanAddress: The domain of from:URI is built from the unit address taken from the <i>localHostWanAddress</i> variable. - localHostFqdn: The domain of from:URI is built from the unit's FQDN taken from the <i>localHostFqdn</i> variable. If <i>localHostFqdn</i> is empty, <i>localHostWanAddress</i> is used instead. Default Value: sipDomain

sipInteropDtmfTransportBySipProtocol

The following parameters allow you to set the DTMF transport by SIP information.

Table 216: SIP Interop Parameters – DTMF Transport

Name	Access	Description
sipInteropDtmfTransportMethod	R/W	Configures the method used to transmit DTMFs over the SIP protocol. This variable is effective only if the endpoint is configured to use the DTMF out-of-band by protocol transport method (<i>outOfBandUsingSignalingProtocol</i>; refer to the variable '<i>voicelfDtmfTransport</i>'). - draftChoudhuriSipInfoDigit00: Transmits DTMFs by using the method defined in the draft '<i>draft-choudhuri-sip-info-digit-00</i>'. - infoDtmfRelay: Transmits DTMFs by using a custom method. This custom method requires no SDP negotiation and uses a SIP INFO message with a content of type '<i>application/dtmf-relay</i>'. Default Value: draftChoudhuriSipInfoDigit00
sipInteropDtmfTransportDuration	R/W	Configures the DTMF duration sent in the INFO message when using the 'infoDtmfRelay' method (refer to the variable 'sipInteropDtmfTransportMethod'). This value is expressed in milliseconds (ms). Default Value: 100

sipInteropInternationalCodeMapping

The following parameters allow you to set the international code mapping information.

Table 217: SIP Interop Parameters – International Code Mapping

Name	Access	Description
sipInteropInternationalCodeMappingEnable	R/W	Instructs the FXS unit to substitute the content of the variable <code>sipInteropInternationalCodeMappingString</code> to the '+' character that prepends the caller ID of some international calling parties. • disable: The default value. No substitution is performed. The '+' character is simply removed. • enable: The substitution takes place. Default Value: disable
sipInteropInternationalCodeMappingString	R/W	The character string that is substituted to the '+' character that prepends some international caller IDs when the variable <code>sipInteropInternationalCodeMappingEnable</code> is enabled.

Appendices

Page Left Intentionally Blank

List of MIB Parameters

A

aal5RxPdu	132
aal5RxTotalBytes	132
aal5RxTotalErrorCounts	132
aal5TxPdu	132
aal5TxTotalBytes	132
aal5TxTotalErrorCounts	132
analogScnGwDialEnable	103
analogScnGwDialPrefix	103
analogScnGwDtmfDuration	103
analogScnGwInterDigitDialDelay	103
analogScnGwPreDialDelay	103
atmEncapsulation	131
atmRxCellDelayVariationTolerance	132
atmRxMaximumBurstSize	132
atmRxMaximumSdu	132
atmRxMinimumCellRate	132
atmRxPeakCellRate	132
atmRxSustainableCellRate	132
atmRxTrafficClass	132
atmTxCellDelayVariationTolerance	132
atmTxMaximumBurstSize	132
atmTxMaximumSdu	132
atmTxMinimumCellRate	132
atmTxPeakCellRate	132
atmTxSustainableCellRate	132
atmTxTrafficClass	132
atmVcEnable	131
atmVci	131
atmVcInUse	131
atmVcName	131
atmVcType	131
atmVpi	131

C

certificateExpirationDate	139
certificateName	139
certificateSubjectCommonName	139
checkTcpIpStackForSuccessfulBoot	125
configFileAutoUpdateOnRestartEnable	120
configFileAutoUpdatePeriod	120
configFileAutoUpdatePeriodicEnable	120
configFileAutoUpdateTimeOfDay	120
configFileAutoUpdateTimeRange	121
configFileAutoUpdateTimeUnit	120
configFileFetchingConfigSource	19
configFileFetchingDhcpSiteSpecificCode	32
configFileFetchingFileLocation	119
configFileFetchingFileName	119
configFileFetchingHost	19
configFileFetchingPort	19
configFileFetchingSelectConfigSource	32

configFileFetchingSpecificFileName	119
configFileFetchingStaticHost	32
configFileFetchingStaticPort	32
configFilePrivacyEnable	121
configFilePrivacyGenericSecret	121
configFilePrivacySpecificSecret	121
configFileTransferPassword	120
configFileTransferProtocol	119
configFileTransferUsername	119
countryCustomizationToneOverride	61
countryCustomizationTonePattern	61
countryCustomizationToneTone	61

D

dataIcfAnalogCedDetectionBehavior	74
dataIcfCedFaxToneEnable	74
dataIcfClearChannelCodecPreferred	75
dataIcfCngToneDetectionEnable	74
dataIcfCodecMediaTypeImageEnable	74
dataIcfCodecT38Enable	75
dataIcfT38BasePort	73
dataIcfT38FinalFramesRedundancy	73
dataIcfT38NoSignalEnable	73
dataIcfT38NoSignalTimeout	73
digitMapAllowedDigitMap	82
digitMapAllowedEnable	81
digitMapAllowedIsValid	82
digitMapAllowedLineToApply	82
digitMapPrefixedDigitRemovalCount	82
digitMapPrependedString	82
digitMapProcessDigitsWhenPressed	81
digitMapRefusedDigitMap	83
digitMapRefusedEnable	83
digitMapRefusedIsValid	83
digitMapRefusedLineToApply	83
digitMapSuffixStringToRemove	82
digitMapTimeoutCompletion	83
digitMapTimeoutFirstDigit	83
digitMapTimeoutInterDigit	83
dsIcfModemLossOfSignalCount	136
dsIcfModemRxConnectionRate	136
dsIcfModemRxLineAttenuation	136
dsIcfModemRxMargin	136
dsIcfModemRxPayload	136
dsIcfModemRxSuperframeCnt	136
dsIcfModemSeverlyErroredFrameCount	136
dsIcfModemState	135
dsIcfModemTxConnectionRate	136
dsIcfModemTxLineAttenuation	136
dsIcfModemTxMargin	136
dsIcfModemTxPayload	136
dsIcfModemTxPeakCellRate	136
dsIcfModemTxSuperframeCnt	136
dsIcfModulation	135
dsIcfTrainedModulation	136
dsIcfTrainedPath	135

E

emergencyCallUrgentGatewayDigitMap	89
emergencyCallUrgentGatewayEnable	89
emergencyCallUrgentGatewayTargetAddress	89

F

fastPathRxCrcError	136
fastPathTxCrcError	136
firewallEnable	145
firewallSecurityBadTcpPacketRule	145
firewallSecurityBlockIcmpRedirectionInRule	146
firewallSecurityBlockIcmpRedirectionOutRule	146
firewallSecurityBlockLanEchoRequestRule	146
firewallSecurityBlockWanEchoBroadcastRule	146
firewallSecurityBlockWanEchoRequestRule	146
firewallSecurityIdentRule	146
firewallSecurityMulticastPacketRule	146
firewallSecurityReversePathFilteringRule	146
firewallSecuritySourceRoutedPacketRule	145
firewallSecuritySpoofAddress	147
firewallSecuritySpoofEnable	147
firewallSecuritySpoofLabel	147
firewallSecuritySpoofRuleEnable	147
firewallSecurityTcpSynCookiesRule	145
firewallSyslogEnable	147
fxoAnswerOnCallerIdDetectionEnable	106
fxoAnswerSupervisionMode	105
fxoCallerIdDetectionRange	105
fxoDialtoneDetectionMode	105
fxoDialtoneDetectionTimeout	105
fxoEndOfCallToneCustomCadence	108
fxoEndOfCallToneCustomFrequency	107
fxoFeocOnCallFailureEnable	107
fxoFeocOnCallFailureTimeout	107
fxoFeocOnSilenceDetectionMode	107
fxoFeocOnSilenceDetectionTimeout	107
fxoFeocOnToneDetectionMode	107
fxoIfAnalogLineType	108
fxoIfIncomingCallNotAllowedBehavior	108
fxoLineFaultDetectionEnable	106
fxoLineSeizureTimeout	106
fxoLineStatus	106
fxoPreAnswerDelay	106
fxoWaitForCalleeToAnswerEnable	106
fxsBlankAnonymousCallerId	78
fxsByPassEnable	77
fxsCalleeHangupDelay	78
fxsCalleeHangupSupervision	77
fxsCallingNumberCriteria	78
fxsCallingNumberTransformation	79
fxsEmergencyBypassDialDelay	79
fxsEmergencyBypassDialMap	79
fxsEmergencyBypassEnable	79
fxsEmergencyBypassTimeout	79
fxsEpSpecificLoopCurrentOverride	79
fxsEpSpecificLoopCurrentOverrideEnable	79
fxsFlashHookDetectionDelayMax	77
fxsFlashHookDetectionDelayMin	77
fxsFskMarkoutBits	78

fxsLoopCurrent	77
fxsLoopCurrentDropEnable	77
fxsMeterPauseDuration	179
fxsMeterPulseDuration	179
fxsMeterPulseFreq	179
fxsPolarityAndDenialBehavior	78
fxsPowerDropOnDisconnectDuration	78
fxsReversalOnIdleEnable	78

G

generateOamPing	133
groupAdminDescription	7
groupAdminIndex	7
groupAdminParentGroup	8
groupAdminState	7
groupAdminType	7
groupOpState	7
groupReset	7
groupSetAdmin	7
groupUsageState	7

H

h323AcceleratedRequestedLogicalChannel	170
h323AddT38MediaControlChannel	170
h323AliasesConfigured	167
h323AliasesCurrent	167
h323AliasesGroupIndex	167
h323AliasTypeRestriction	169
h323AttributesCalledPartyNumberDigitMap	162
h323AttributesCalledPartyNumberEnable	162
h323AttributesCalledPartyNumberTypeOfNumber	162
h323AttributesDirectGatewayCallEnable	166
h323AttributesDirectGatewayCallHost	166
h323AttributesEarlyH245Enable	163
h323AttributesFastConnectEnable	163
h323AttributesH245TunnelingEnable	163
h323AttributesInformationTransferCapability	161
h323AttributesParallelH245Enable	164
h323AttributesVoiceCapabilitySendingMethod	165
h323GkDhcpSiteSpecificCode	40
h323GroupAliasesConfigured	168
h323GroupAliasesCurrent	168
h323GroupMultipleRegCallSignalingPortSource	159
h323GroupMultipleRegEnable	157
h323GroupMultipleRegGkDiscoveryMode	158
h323GroupMultipleRegLightweightEnable	159
h323GroupMultipleRegLightweightTimeToLive	159
h323GroupMultipleRegRasPortSource	159
h323GroupMultipleRegRetryTime	158
h323GroupMultipleRegStaticCallSignalingPort	160
h323GroupMultipleRegStaticRasPort	159
h323MultipleRegCallSignalingPortSource	157
h323MultipleRegEnable	154
h323MultipleRegGkDiscoveryMode	155
h323MultipleRegGroupIndex	154
h323MultipleRegLightweightEnable	156
h323MultipleRegLightweightTimeToLive	156
h323MultipleRegRasPortSource	156

h323MultipleRegRetryTime	155
h323MultipleRegStaticCallSignalingPort	157
h323MultipleRegStaticRasPort	156
h323RegAsGateway	169
h323RegistrationGkHost	160
h323RegistrationGkPort	160
h323RegistrationTimeToLive	160
h323RegMethod	151
h323SelectConfigSource	39
h323SingleRegCallSignalingPortSource	153
h323SingleRegGkDiscoveryMode	152
h323SingleRegLightweightEnable	153
h323SingleRegLightweightTimeToLive	153
h323SingleRegRasPortSource	153
h323SingleRegRetryTime	152
h323SingleRegStaticCallSignalingPort	154
h323SingleRegStaticRasPort	153
h323UseEvenT38Port	170
h323VoicelfCodecG729Enable	170
httpServerAccess	117
httpServerAdminAccess	117
httpServerAdminPort	41
httpServerAdminRealm	118
httpServerAdminUsername	117
httpServerBandwidthControlSectionEnable	118
httpServerDefaultAdminPassword	117
httpServerDefaultPassword	117
httpServerEnable	117
httpServerPort	41
httpServerResetToDefaultAdminPwd	117
httpServerResetToDefaultPwd	117
httpServerSipAuthenticationEnable	118
httpServerUsername	117
httpServerUserRealm	118

I

ifAdminAdminState	11
ifAdminOpState	11
ifAdminParent	12
ifAdminParentType	12
ifAdminSetAdmin	11
ifAdminUsageState	11
imageAutoUpdateOnRestartEnable	48
imageAutoUpdatePeriod	48
imageAutoUpdatePeriodicEnable	48
imageAutoUpdateTimeOfDay	48
imageAutoUpdateTimeRange	48
imageAutoUpdateTimeUnit	48
imageCompletion	49
imageCompletionControl	49
imageConfigSource	16
imageDhcpPrimarySiteSpecificCode	31
imageDhcpSecondarySiteSpecificCode	31
imageLocation	47
imageLocationProvisionSource	47
imageLocationStatus	49
imageLocationUsed	49
imagePrimaryHost	16
imagePrimaryPort	16

imageSecondaryHost	16
imageSecondaryPort	16
imageSelectConfigSource	31
imageSelectionFileLocation	47
imageStaticPrimaryHost	31
imageStaticPrimaryPort	31
imageStaticSecondaryHost	31
imageStaticSecondaryPort	31
imageTransferPassword	47
imageTransferProtocol	47
imageTransferUsername	47
interleavedPathRxCrcError	136
interleavedPathTxCrcError	136
ipAddressConfigH323GkStaticHost	39
ipAddressConfigH323GkStaticPort	39
ipRoutingBandwidthControlEnable	116
ipRoutingDhcpIpLeaseRangeEnd	114
ipRoutingDhcpIpLeaseRangeStart	114
ipRoutingDhcpServerDnsFallbackEnable	115
ipRoutingDhcpServerEnable	114
ipRoutingDhcpServerLeaseTime	114
ipRoutingDhcpServerNoWanLeaseEnable	115
ipRoutingDhcpServerNoWanLeaseTime	115
ipRoutingEnable	113
ipRoutingMacAddress	116
ipRoutingMacSpoofAddress	116
ipRoutingMacSpoofEnable	116
ipRoutingQosDiffServSubstitution	115
ipRoutingQosDiffServSubstitutionEnable	115
ipRoutingWanUpstreamBandwidth	116

L

lanStaticAddress	40
lanStaticNetworkMask	41
lineGroupingNbGroups	99
lineGrpAssocGroupIndex	99
lineGrpAssocIfType	99
lineGrpConfCallForwardNoRessourceAddress	100
lineGrpConfCallForwardNoRessourceEnable	100
lineGrpConfLineSelectionAlgorithm	100
lineSelectionDigitMap	101
lineSelectionEnable	101
localHostAddress	15
localHostConfigSource	15
localHostDefaultRouter	15
localHostDhcpServer	15
localHostDnsOverrideEnable	30
localHostFqdn	15
localHostFqdnConfigSource	15
localHostFqdnSelectConfigSource	29
localHostPrimaryDns	15
localHostSecondaryDns	15
localHostSelectConfigSource	29
localHostSnmpPort	15
localHostStaticAddress	30
localHostStaticDefaultRouter	30
localHostStaticFqdn	30
localHostStaticPrimaryDns	30
localHostStaticSecondaryDns	30

localHostStaticSnmpPort	30
localHostStaticSubnetMask	30
localHostStaticWanAddress	30
localHostSubnetMask	15
localHostWanAddress	16
localHostWanAddressConfigSource	15
localHostWanAddressSelectConfigSource	29

M

mgcpAddPtimeIfPresentInLCO	173
mgcpCAConfigSource	17
mgcpCADhcpSiteSpecificCode	35
mgcpCAHost	17
mgcpCAPort	17
mgcpCAsSelectConfigSource	35
mgcpCAsStaticHost	35
mgcpCAsStaticPort	35
mgcpDefaultDigitMap	173
mgcpDefaultPackage	173
mgcpDtmfPackageLDuration	175
mgcpDtmfPackageTCriticalDuration	175
mgcpDtmfPackageTPartialDuration	175
mgcpEndpointIdListIncludeNotStarted	173
mgcpEndpointIdTerm1	174
mgcpEndpointIdTerm2	174
mgcpFwKeepAliveEnable	177
mgcpFwKeepAliveTimeout	177
mgcpGenericMediaPackageRbkDuration	175
mgcpGenericMediaPackageRtDuration	175
mgcpLinePackageBzDuration	175
mgcpLinePackageDIDuration	175
mgcpLinePackageHdPersistent	176
mgcpLinePackageHfPersistent	176
mgcpLinePackageHuPersistent	176
mgcpLinePackageMwiDuration	175
mgcpLinePackageOsiDuration	176
mgcpLinePackageOtDuration	175
mgcpLinePackageRgDuration	175
mgcpLinePackageRoDuration	176
mgcpLinePackageSIIDuration	176
mgcpLinePackageWtDuration	176
mgcpnacsAnswerStreamFormat	181
mgcpnacsBracketsAroundIpAddressInDomainNameEnable	184
mgcpnacsConnectRtpSockets	182
mgcpnacsFakeRfc3407Recognition	183
mgcpnacsG729AnnexBNegotiation	182
mgcpnacsImmediateModemToneReporting	183
mgcpnacsMakeOsiSignalBrief	183
mgcpnacsMultipleFaxToneDetection	182
mgcpnacsOriginLineSessionIDAndVersionMaxLength	181
mgcpnacsPolarityReversalOnCallingCardServiceToneEnable	184
mgcpnacsRtpUdpChecksumEnable	183
mgcpnacsT38CapabilitiesUsingAudioCodec98	183
mgcpnacsUseIuT38Format	184
mgcpnacsValidateOfferAnswerModel	182
mgcpPiggyBackingEnable	173
mgcpPort	173
mgcpRestartLevel	173
mgcpRetransmissionAlgorithm	174

mgcpRetransmissionDisconnectInitialWaitingPeriod	174
mgcpRetransmissionDisconnectMaxWaitingPeriod	175
mgcpRetransmissionDisconnectMinWaitingPeriod	175
mgcpRetransmissionDisconnectThreshold	174
mgcpRetransmissionDisconnectThresholdDnsQuery	174
mgcpRetransmissionDisconnectTimeout	174
mgcpRetransmissionHistoryTimeout	174
mgcpRetransmissionInitialPeriod	174
mgcpRetransmissionMaxPeriod	174
mgcpRetransmissionMaxWaitingDelay	174
mgcpRetransmissionSuspicionThreshold	174
mgcpRetransmissionSuspicionThresholdDnsQuery	174
mgcpStatsCumulatedAvgConnectionTime	176
mgcpStatsCumulatedTotalNumberOfConnections	176
mgcpStatsCurrentAvgConnectionTime	176
mgcpStatsCurrentNumberOfActiveConnections	176
mgcpStatsCurrentTotalNumberOfConnections	176
msConfigSource	16
msDhcpSiteSpecificCode	33
msEnable	51
msHost	16
msSelectConfigSource	33
msStaticHost	33
msStaticTrapPort	33
msTrapConfigInformation	51
msTrapPort	16
msTrapRetransmissionPeriod	51
msTrapRetransmissionRetryCount	51
msTrapStatusConfigFile	51
msTrapStatusInformation	51
mwiconfigActivation	109
mwiconfigFetchAddress	109
mwiconfigUserSubscriptionAddress	109
mwiconfigVoltageEnable	110
mwiconfigExpirationTime	109
mwiconfigFetchDigitMap	109
mwiconfigSubscriptionCmdRefresh	109
mxInteropHttpUAHeaderConfig	141

N

natPortForwardingLanAddr	143
natPortForwardingLanPort	143
natPortForwardingProtocol	143
natPortForwardingRuleEnable	144
natPortForwardingRuleLabel	143
natPortForwardingWanFinishPort	143
natPortForwardingWanStartPort	143
natSyslogEnable	144
ncsCAConfigSource	17
ncsCADhcpSiteSpecificCode	36
ncsCAHost	17
ncsCAPort	17
ncsCAsSelectConfigSource	36
ncsCAStaticHost	36
ncsCAStaticPort	36
ncsCompatibilityRtpPayloadType18EncodingName	191
ncsCompatibilityVersion	191
ncsDefaultDigitMap	187
ncsEndpointIdListIncludeNotStarted	187

ncsEndpointIdTerm1	187
ncsEndpointIdTerm2	187
ncsLinePackageBzDuration	189
ncsLinePackageDIDuration	189
ncsLinePackageLDuration	189
ncsLinePackageMwiDuration	189
ncsLinePackageOtDuration	189
ncsLinePackageRbkDuration	189
ncsLinePackageRgDuration	189
ncsLinePackageRoDuration	189
ncsLinePackageRtDuration	189
ncsLinePackageSIDuration	189
ncsLinePackageTCriticalDuration	189
ncsLinePackageTPartialDuration	189
ncsPiggyBackingEnable	187
ncsPort	187
ncsRestartLevel	187
ncsRetransmissionAlgorithm	188
ncsRetransmissionDisconnectInitialWaitingPeriod	188
ncsRetransmissionDisconnectMaxWaitingPeriod	188
ncsRetransmissionDisconnectMinWaitingPeriod	188
ncsRetransmissionDisconnectThreshold	188
ncsRetransmissionDisconnectThresholdDnsQuery	188
ncsRetransmissionDisconnectTimeout	188
ncsRetransmissionHistoryTimeout	188
ncsRetransmissionInitialPeriod	188
ncsRetransmissionMaxPeriod	188
ncsRetransmissionMaxWaitingDelay	188
ncsRetransmissionSuspicionThreshold	188
ncsRetransmissionSuspicionThresholdDnsQuery	188
ncsStatsCumulatedAvgConnectionTime	190
ncsStatsCumulatedTotalNumberOfConnections	189
ncsStatsCurrentAvgConnectionTime	189
ncsStatsCurrentNumberOfActiveConnections	189
ncsStatsCurrentTotalNumberOfConnections	189

O

oamFarEndF4LoopBackCount	133
oamFarEndF5LoopBackCount	133
oamMode	133
oamNearEndF4LoopBackCount	133
oamNearEndF5LoopBackCount	133
oamPingType	133
oamResult	133
oamTimeOut	133
oamVci	133
oamVpi	133

P

pinDialingDelay	127
pinDialingEnable	127
pinDialingPin	127
pppoaEnable	137
pppoeAcName	111
pppoeEnable	111
pppoeServiceName	111

Q

qosInteropUseVoiceQoSForRtcpEnable	58
qosSignalingDiffServ	55
qosSignalingIeee8021qEnable	55
qosSignalingIeee8021qUserPriority	56
qosT38FaxDiffServ	55
qosT38FaxIeee8021qEnable	56
qosT38FaxIeee8021qUserPriority	56
qosVbdDiffServ	55
qosVbdIeee8021qEnable	56
qosVbdIeee8021qUserPriority	56
qosVlanIeee8021qDefaultUserPriority	57
qosVlanIeee8021qSubstitutionEnable	57
qosVlanIeee8021qSubstitutionFiltering	58
qosVlanIeee8021qSubstitutionUserPriority	57
qosVlanIeee8021qSubstitutionVlanID	57
qosVlanIeee8021qTaggingEnable	57
qosVlanIeee8021qVirtualLanID	57
qosVoiceDiffServ	55
qosVoiceIeee8021qEnable	56
qosVoiceIeee8021qUserPriority	56

R

rtpConfigBasePort	25
rtpStatsCumulatedTotalInterarrivalJitterAvg	24
rtpStatsCumulatedTotalInterarrivalJitterMax	24
rtpStatsCumulatedTotalInterarrivalJitterMin	24
rtpStatsCumulatedTotalLatencyAvg	24
rtpStatsCumulatedTotalLatencyMax	24
rtpStatsCumulatedTotalLatencyMin	24
rtpStatsCumulatedTotalOctetsReceived	24
rtpStatsCumulatedTotalOctetsTransmitted	24
rtpStatsCumulatedTotalPacketsLost	24
rtpStatsCumulatedTotalPacketsReceived	24
rtpStatsCumulatedTotalPacketsTransmitted	24
rtpStatsCumulatedTotalPercentPacketsLost	24
rtpStatsCurrentTotalInterarrivalJitterAvg	24
rtpStatsCurrentTotalInterarrivalJitterMax	24
rtpStatsCurrentTotalInterarrivalJitterMin	24
rtpStatsCurrentTotalLatencyAvg	24
rtpStatsCurrentTotalLatencyMax	24
rtpStatsCurrentTotalLatencyMin	24
rtpStatsCurrentTotalOctetsReceived	24
rtpStatsCurrentTotalOctetsTransmitted	24
rtpStatsCurrentTotalPacketsLost	24
rtpStatsCurrentTotalPacketsReceived	24
rtpStatsCurrentTotalPacketsTransmitted	24
rtpStatsCurrentTotalPercentPacketsLost	24
rtpStatsLastConnInterarrivalJitterAvg	23
rtpStatsLastConnInterarrivalJitterMax	23
rtpStatsLastConnInterarrivalJitterMin	23
rtpStatsLastConnLatencyAvg	23
rtpStatsLastConnLatencyMax	23
rtpStatsLastConnLatencyMin	23
rtpStatsLastConnNumberOctetsReceived	23
rtpStatsLastConnNumberOctetsTransmitted	23
rtpStatsLastConnNumberPacketsLost	23
rtpStatsLastConnNumberPacketsReceived	23
rtpStatsLastConnNumberPacketsTransmitted	23

rtpStatsLastConnPercentPacketsLost	23
--	----

S

sipAllowAudioAndImageNegotiationEnable	204
sipAllowMediaReactivationInAnswerEnable	204
sipCodecOrderInAnswer	204
sipConferenceServerURI	202
sipConferenceType	202
sipDomain	195
sipEnforceOfferAnswerModel	204
sipHomeDomainProxyDhcpSiteSpecificCode	38
sipHomeDomainProxyHost	18
sipHomeDomainProxyPort	18
sipHomeDomainProxyStaticHost	37
sipHomeDomainProxyStaticPort	37
sipInteropAckUnsupportedInfoRequests	214
sipInteropAllowAsymmetricDtmfPayloadType	215
sipInteropAllowMultipleActiveMediaInAnswer	210
sipInteropAuthenticationQop	214
sipInteropAutomaticRejectionCode	209
sipInteropBehaviorOnT38InviteRejectedWith606	213
sipInteropBranchMatchingMethod	214
sipInteropConferenceServerMechanism	212
sipInteropDefaultPublicationExpiration	214
sipInteropDefaultRegistrationExpiration	214
sipInteropDtmfTransportDuration	215
sipInteropDtmfTransportMethod	215
sipInteropEscapePoundInSipUriUsername	212
sipInteropFromUriDomainSelection	215
sipInteropIgnoreMediaRenegotiationAfterCngDetection	211
sipInteropIgnoreUsernameParam	212
sipInteropIgnoreViaBranchIdInCancelEnable	214
sipInteropInternationalCodeMappingEnable	216
sipInteropInternationalCodeMappingString	216
sipInteropLocalRingOnProvisionalResponse	211
sipInteropLockDnsSrvRecordPerCallEnable	213
sipInteropMaxForwardsValue	209
sipInteropMwiMessageSummaryValidation	211
sipInteropOnHoldAnswerSdpStreamDirection	210
sipInteropOnHoldSdpStreamDirection	210
sipInteropProxyAuthenticationUriParametersEnable	214
sipInteropReferredByConfig	212
sipInteropRegisterHomeDomainHostOverride	212
sipInteropRejectCodeForNoResource	214
sipInteropRemoveOutboundProxyRouteHeader	213
sipInteropReplacesConfig	207
sipInteropReplacesVersion	208
sipInteropRetryFailedRegistration	212
sipInteropReuseCredentialEnable	213
sipInteropRingingResponseCode	214
sipInteropSdpOriginLineSessionIDAndVersionMaxLength	211
sipInteropSendUAHeaderEnable	209
sipInteropSessionTimerVersion	208
sipInteropSipOptionsMethodSupport	211
sipInteropSymmetricUdpSourcePortEnable	209
sipInteropT38NoSignalBehavior	213
sipInteropTransferVersion	208
sipInteropTransmissionTimeout	208
sipInteropUAHeaderConfig	210

sipInteropUseDtmfPayloadTypeFoundInAnswer	215
sipInteropUseIuT38Format	213
sipInteropUsePAssertedHeader	213
sipInteropUseSipDomainInRequestURI	212
sipNatCustomEnable	205
sipNatCustomPublicAddress	205
sipOutboundProxyConfig	203
sipOutboundProxyDhcpSiteSpecificCode	38
sipOutboundProxyHost	18
sipOutboundProxyPort	18
sipOutboundProxyStaticHost	37
sipOutboundProxyStaticPort	37
sipPenaltyBoxEnable	199
sipPenaltyBoxTime	199
sipPort	195
sipPresenceCompositorDhcpSiteSpecificCode	38
sipPresenceCompositorHost	18
sipPresenceCompositorPort	19
sipPresenceCompositorStaticHost	38
sipPresenceCompositorStaticPort	38
sipPublicationCmdRefresh	201
sipPublicationProposedExpirationValue	202
sipPublicationRefreshTime	201
sipRegistrarDhcpSiteSpecificCode	38
sipRegistrarHost	18
sipRegistrarPort	18
sipRegistrarStaticHost	37
sipRegistrarStaticPort	37
sipRegistrationCmdRefresh	198
sipRegistrationProposedExpirationValue	198
sipReRegistrationTime	198
sipRtpUdpChecksumEnable	204
sipServerConfigSource	18
sipServerSelectConfigSource	37
sipTransportContactEnable	198
sipTransportEnable	199
sipTransportIndex	199
sipTransportQValue	199
sipTransportRegistrationEnable	198
sipTrustedSourcesEnable	202
sipTrustedSourcesIpAddress	202
sipUAAuthIndex	197
sipUAAuthPassword	197
sipUAAuthRealm	197
sipUAAuthUsername	197
sipUAAuthValidateRealm	197
sipUADisplayName	195
sipUAGroupAuthIndex	201
sipUAGroupAuthPassword	201
sipUAGroupAuthRealm	201
sipUAGroupAuthUsername	201
sipUAGroupAuthValidateRealm	201
sipUAGroupMaximumSessionExpirationDelay	200
sipUAGroupMinimumSessionExpirationDelay	200
sipUAGroupRegistrationUsername	201
sipUAMainUsername	195
sipUAMaximumSessionExpirationDelay	196
sipUAMinimumSessionExpirationDelay	196
sipUAOtherAcceptedUsernames	196
sipUnitAuthIndex	197

sipUnitAuthPassword	197
sipUnitAuthRealm	197
sipUnitAuthUsername	197
sipUnitAuthValidateRealm	197
sipUnregisteredPortBehavior	203
snmpAgentAccess	123
snmpAgentEnable	123
sntpConfigSource	19
sntpEnable	97
sntpHost	19
sntpPort	19
sntpSelectConfigSource	38
sntpStaticHost	38
sntpStaticPort	39
sntpSynchronizationPeriod	97
sntpSynchronizationPeriodOnError	97
sntpTimeZoneString	98
sntpTimeZoneStringIsValid	98
stunEnable	129
stunKeepAliveInterval	129
stunNatBindingQueryInterval	129
stunQueryCacheDuration	129
stunQueryTimeout	129
stunStaticHost	42
stunStaticPort	42
subscriberServicesAttendedTransferEnable	92
subscriberServicesAttendedTransferStatus	93
subscriberServicesBlindTransferEnable	92
subscriberServicesBlindTransferStatus	93
subscriberServicesCallForwardOnBusyActivation	93
subscriberServicesCallForwardOnBusyDisableDigitMap	94
subscriberServicesCallForwardOnBusyEnable	92
subscriberServicesCallForwardOnBusyEnableDigitMap	94
subscriberServicesCallForwardOnBusyForwardingAddress	93
subscriberServicesCallForwardOnNoAnswerActivation	94
subscriberServicesCallForwardOnNoAnswerDisableDigitMap	94
subscriberServicesCallForwardOnNoAnswerEnable	93
subscriberServicesCallForwardOnNoAnswerEnableDigitMap	94
subscriberServicesCallForwardOnNoAnswerForwardingAddress	94
subscriberServicesCallForwardOnNoAnswerTimeout	94
subscriberServicesCallForwardUnconditionalActivation	93
subscriberServicesCallForwardUnconditionalDisableDigitMap	94
subscriberServicesCallForwardUnconditionalEnable	92
subscriberServicesCallForwardUnconditionalEnableDigitMap	94
subscriberServicesCallForwardUnconditionalForwardingAddress	93
subscriberServicesCallWaitingCancelDigitMap	94
subscriberServicesCallWaitingEnable	91
subscriberServicesCallWaitingPermanentDigitMapDisable	95
subscriberServicesCallWaitingPermanentDigitMapEnable	94
subscriberServicesCallWaitingStatus	93
subscriberServicesConferenceEnable	92
subscriberServicesConferenceStatus	93
subscriberServicesHoldEnable	91
subscriberServicesHoldStatus	93
subscriberServicesProcessingTrigger	95
subscriberServicesSecondCallEnable	91
subscriberServicesSecondCallStatus	93
sysAdminAppMode	4
sysAdminCommand	3
sysAdminDefaultSettingsEnable	3

sysAdminDownloadConfigFileStatus	4
sysAdminLastCheckRam	4
sysAdminLastCheckRom	4
sysAdminLastDownloadSoftware	4
sysConfigBootpFlags	44
sysConfigComputerEthernetSpeed	43
sysConfigDhcpWait	44
sysConfigDhcpWaitDelay	44
sysConfigDownloadConfigFile	45
sysConfigDownloadConfigMode	45
sysConfigDownloadConfigPathname	46
sysConfigMaxDynamicPort	44
sysConfigMinDynamicPort	43
sysConfigNetworkEthernetSpeed	43
sysConfigProductNamePadding	44
sysConfigStatsBySyslogEnable	45
sysConfigStatsNumberPeriods	45
sysConfigStatsPeriodLength	45
sysHardwareVersion	21
syslogConfigSource	17
syslogDhcpSiteSpecificCode	34
syslogHost	17
syslogMsgDisplayLocalHost	54
syslogMsgDisplayMacAddress	54
syslogMsgDisplayTime	54
syslogMsgDisplayTimeFormat	54
syslogMsgLocalMaxNbr	53
syslogMsgLocalMaxSeverity	53
syslogMsgLocalModule	53
syslogMsgLocalMsg	53
syslogMsgLocalSeverity	53
syslogMsgLocalTime	53
syslogMsgMaxSeverity	53
syslogPort	17
syslogSelectConfigSource	34
syslogStaticHost	34
syslogStaticPort	34
sysMacAddress	21
sysMibVersion	21
sysSerialNumber	21
sysSoftwareVersion	21

T

telephonyAttributesAutomaticCallEnable	85
telephonyAttributesAutomaticCallTargetAddress	85
telephonyAttributesAutomaticRejection	86
telephonyAttributesCallDirectionRestriction	85
telephonyAttributesDelayedHotLineEnable	86
telephonyAttributesDelayedHotLineExtension	86
telephonyAttributesDelayedHotLineTargetAddress	86
telephonyAttributesHookFlashProcessing	86
telephonyAttributesIpAddressCallEnable	87
telephonyCountrySelection	60
telephonyDnsOverrideEnable	41
telephonyDnsPrimaryDns	19
telephonyDnsSecondaryDns	20
telephonyDnsStaticPrimaryDns	41
telephonyDnsStaticSecondaryDns	41
telephonyIpSignalingProtocolProprietary	59

telephonyIpSignalingProtocolSelection	59
---	----

V

voicelfAdaptativeJitterBufferEnable	63
voicelfAllowDtmfOobRecovery	63
voicelfBaseGainConfigurationSource	64
voicelfBaseInputGain	64
voicelfBaseInputGainOffset	65
voicelfBaseOutputGain	64
voicelfBaseOutputGainOffset	65
voicelfCodecG723Enable	66
voicelfCodecG723MaxPTime	67
voicelfCodecG723MinPTime	67
voicelfCodecG72616kbpsEnable	67
voicelfCodecG72616kbpsMaxPTime	67
voicelfCodecG72616kbpsMinPTime	67
voicelfCodecG72616kbpsPayloadType	67
voicelfCodecG72624kbpsEnable	68
voicelfCodecG72624kbpsMaxPTime	68
voicelfCodecG72624kbpsMinPTime	68
voicelfCodecG72624kbpsPayloadType	68
voicelfCodecG72632kbpsEnable	68
voicelfCodecG72632kbpsMaxPTime	68
voicelfCodecG72632kbpsMinPTime	68
voicelfCodecG72632kbpsPayloadType	68
voicelfCodecG72640kbpsEnable	69
voicelfCodecG72640kbpsMaxPTime	69
voicelfCodecG72640kbpsMinPTime	69
voicelfCodecG72640kbpsPayloadType	69
voicelfCodecG729Enable	67
voicelfCodecG729MaxPTime	67
voicelfCodecG729MinPTime	67
voicelfCodecPcmaEnable	66
voicelfCodecPcmaMaxPTime	66
voicelfCodecPcmaMinPTime	66
voicelfCodecPcmuEnable	66
voicelfCodecPcmuMaxPTime	66
voicelfCodecPcmuMinPTime	66
voicelfCodecPreferred	66
voicelfDtmfDetectionBreakPowerThreshold	70
voicelfDtmfDetectionMaxPowerThreshold	70
voicelfDtmfDetectionMinDuration	71
voicelfDtmfDetectionMinPowerThreshold	70
voicelfDtmfDetectionNegativeTwist	71
voicelfDtmfDetectionPositiveTwist	70
voicelfDtmfDetectionRiseTimeCriteria	70
voicelfDtmfEnforceDefaultEvents	70
voicelfDtmfPayloadType	69
voicelfDtmfTransport	69
voicelfEchoCancellationEnable	64
voicelfG711ComfortNoiseGenerationEnable	64
voicelfG711VoiceActivityDetectionEnable	64
voicelfG723VoiceActivityDetectionEnable	65
voicelfG729VoiceActivityDetectionEnable	65
voicelfMaxJitterBufferLength	63
voicelfNlpThresholdLevel	65
voicelfSignalLimiterLevel	65
voicelfTargetJitterBufferLength	63
voicelfUserInputGainOffset	64

voicelfUserOutputGainOffset 64

Index

A

- aliases, H.323
 - configuration [167](#)
 - groups [168](#)
- analog SCN gateway, configuration [103](#)
- answering delay (FXO), configuration [106](#)
- ATM configuration
 - AAL5 statistics [132](#)
 - general parameters [131](#)
 - OAM statistics [133](#)
 - OAM tools [133](#)
 - OAM tools parameters [133](#)
- attended call transfer, enabling [92](#)
- attributes, H.323 configuration [161](#)
 - Q931 [161](#)
 - signaling [163](#)
 - telephony [166](#)

B

- bandwidth control [116](#)
- blind call transfer, enabling [92](#)
- boot behavior configuration, general parameters [125](#)
- bypass, configuration of emergency [79](#)

C

- call forward
 - on busy
 - activating [93](#)
 - enabling [92](#)
 - on no answer
 - activating [94](#)
 - enabling [93](#)
 - unconditional
 - activating [93](#)
 - enabling [92](#)
- call on hold, enabling [91](#)
- call transfer
 - attended transfer, enabling [92](#)
 - blind transfer, enabling [92](#)
- call waiting, enabling [91](#)
- certificates, security configuration, general parameters [139](#)
- clear channel, data codec [74](#)
- codecs
 - data configuration
 - clear channel [74](#)
 - T.38 [73](#), [74](#)
 - tone detection [74](#)
 - voice interface configuration [66](#)
 - G.723 [66](#)
 - G.729 [67](#)
 - PCMA [66](#)
 - PCMU [66](#)
- comfort noise, enabling [64](#)
- conference, enabling [92](#)
- configuration file fetching
 - automatic update [120](#)
 - IP addresses
 - setting [32](#)
 - status [19](#)
 - privacy [121](#)
 - service configuration [119](#)

- configuration file fetching (continued)
 - transfer [119](#)

D

- data interface configuration
 - codecs
 - clear channel [74](#)
 - T.38 [73](#), [74](#)
 - tone detection [74](#)
- DHCP IP addresses, configuring
 - configuration file fetching [32](#)
 - H.323 gatekeepers [40](#)
 - image [31](#)
 - management server [33](#)
 - MGCP Call Agent [35](#)
 - NCS Call Agent [36](#)
 - SIP Servers [38](#)
 - syslog [34](#)
- digit maps configuration
 - activating for calls [94](#)
 - allowed [81](#)
 - enabling [81](#)
 - refused [83](#)
 - timeouts [83](#)
- DNS, telephony
 - IP addresses, setting [41](#)
- download
 - configuration file [45](#)
 - image [47](#)
 - automatic update [48](#)
 - status [49](#)
 - transfer [47](#)
- DSL configuration
 - general parameters [135](#)
 - modem statistics [136](#)
- DTMF transport interop by SIP [215](#)

E

- emergency bypass, configuration [79](#)
- emergency call, urgent gateway [89](#)
- events
 - image configuration [49](#)
 - management server [51](#)
- experimental, H.323
 - interop
 - G.729 codec [170](#)
 - H.323 gateway [169](#)

F

- Firewall configuration
 - general parameters [145](#)
 - security [145](#)
 - syslog [147](#)
- forced end of call
 - configuration [107](#)
 - custom tone setting, configuration [107](#)
- FXO configuration
 - analog line type [108](#)
 - analog SCN gateway [103](#)
 - answering delay [106](#)

- FXO configuration (continued)
 - forced end of call [107](#)
 - custom tone setting [107](#)
 - line fault detection [106](#)
 - line properties [105](#)
 - line status [106](#)
- fxs configuration
 - emergency bypass [79](#)
 - loop current, specific [79](#)
 - objects [77](#)

G

- G.723, voice codec [66](#)
- G.729, voice codec [67](#)
- ground start line type [108](#)
- group administration
 - introduction [5](#)
 - objects [7](#)
- grouping, line [99](#)

H

- H.323 configuration
 - aliases [167](#)
 - group [168](#)
 - attributes [161](#)
 - Q931 [161](#)
 - signaling [163](#)
 - telephony [166](#)
 - experimental, interop [169](#)
 - IP addresses, setting [39](#)
 - registration method [151](#)
 - multiple [154](#)
 - group [157](#)
 - single [152](#)
 - status [160](#)
- HTTP server
 - IP addresses, setting [41](#)

I

- ifAdminInitialAdminState [12](#)
- image
 - configuration
 - automatic update [48](#)
 - events [49](#)
 - objects [47](#)
 - status [49](#)
 - transfer [47](#)
 - IP addresses
 - setting [31](#)
 - status [16](#)
- interface administration
 - introduction [9](#)
 - objects [11](#)
- international code mapping interop [216](#)
- interop
 - G.720 codec, in H.323 [170](#)
 - H.323 gateway [169](#)
- interop configuration, general parameters [141](#)
- interop, SIP
 - DTMF transport [215](#)
 - general [207](#)
 - international code mapping [216](#)
 - Replaces config [207](#)

- interop, SIP (continued)
 - session timer version [208](#)
 - transfer version [208](#)
 - transmission timeout [208](#)
- IP address call, enabling [87](#)
- IP addresses
 - configuring [xxv](#)
 - configuration file fetching [32](#)
 - H.323 gatekeepers [39](#)
 - HTTP server [41](#)
 - image [31](#)
 - LAN interface [40](#)
 - local host [29](#)
 - management server [33](#)
 - MGCP Call Agent [35](#)
 - NCS Call Agent [36](#)
 - SIP Servers [37](#)
 - SNTP [38](#)
 - STUN [42](#)
 - syslog [34](#)
 - telephony DNS [41](#)
 - defining
 - decimal [xxv](#)
 - hexadecimal [xxv](#)
 - octal [xxv](#)
 - DHCP, setting
 - configuration file fetching [32](#)
 - H.323 gatekeepers [40](#)
 - image [31](#)
 - management server [33](#)
 - MGCP Call Agent [35](#)
 - NCS Call Agent [36](#)
 - SIP Servers [38](#)
 - syslog [34](#)
 - static, setting
 - configuration file fetching [32](#)
 - H.323 gatekeepers [39](#)
 - image [31](#)
 - local host [30](#)
 - management server [33](#)
 - MGCP Call Agent [35](#)
 - NCS Call Agent [36](#)
 - SIP Servers [37](#)
 - SNTP [38](#)
 - STUN [42](#)
 - syslog [34](#)
 - telephony DNS [41](#)
 - status [xxv](#)
 - configuration file fetching [19](#)
 - image [16](#)
 - local host [15](#)
 - management server [16](#)
 - MGCP Call Agent [17](#)
 - NCS Call Agent [17](#)
 - SIP Servers [18](#)
 - SNTP [19](#)
 - STUN [20](#)
 - syslog [17](#)
 - telephony DNS [19](#)
- IP routing configuration
 - bandwidth control [116](#)
 - DHCP parameters [114](#)
 - general parameters [113](#)
 - MAC address spoofing [116](#)
 - QoS parameters [115](#)

IP telephony signaling
 see *H.323 configuration*
 see *MGCP configuration*
 see *NCS configuration*
 see *SIP configuration*
 ipRoutingMode [113](#)

J

jitter buffer, setting [63](#)

L

LAN interface
 IP addresses, setting [40](#)
 line fault detection (FXO), configuration [106](#)
 line grouping configuration
 association [99](#)
 attributes [100](#)
 number of [99](#)
 line properties (FXO), configuration [105](#)
 line selection configuration, general parameters [101](#)
 line status (FXO) [106](#)
 local host
 IP addresses
 setting [29](#)
 status [15](#)
 loop current, specific [79](#)
 loop start line type [108](#)

M

MAC address, spoofing [116](#)
 management server
 events [51](#)
 IP addresses
 setting [33](#)
 status [16](#)
 objects [51](#)
 manual conventions [xxix](#)
 meter pulse
 basic parameters [179](#)
 duration parameters [179](#)
 MGCP Call Agent
 IP addresses
 setting [35](#)
 status [17](#)
 MGCP configuration
 basic parameters [173](#)
 endpoints [174](#)
 experimental [181](#)
 firewall [177](#)
 meter pulse
 basic parameters [179](#)
 duration parameters [179](#)
 packages
 DTMF [175](#)
 Generic Media [175](#)
 Line [175](#)
 retransmission [174](#)
 statistics [176](#)
 cumulated [176](#)
 current [176](#)
 MIB structure
 changing a parameter value [xxvi](#)
 conformance [xxv](#)

MIB structure (continued)
 description
 mediatrixAdmin [xxiii](#)
 mediatrixConfig [xxiii](#)
 mediatrixExperimental [xxiii](#)
 mediatrixIpTelephonySignaling [xxiii](#)
 mediatrixMgmt [xxiii](#)
 mediatrixModules [xxiii](#)
 mediatrixProducts [xxiii](#)
 events [xxv](#)
 introduction [xix](#)
 MIB, defined [xix](#)
 objects [xxv](#)
 OID, defined [xix](#)
 persistent parameters [xxvi](#)
 SMI, defined [xix](#)
 SNMP messages. see *SNMP*
 switching protocol [xxvi](#)
 tables
 defined [xxvii](#)
 generic [xxvii](#)
 groupAdmin [xxviii](#)
 ifAdmin [xxviii](#)
 textual conventions [xxiv](#)
 volatile parameters [xxvi](#)
 MIB, defined [xix](#)
 MWI configuration
 general parameters [109](#)
 specific parameters [109](#)

N

NAT configuration
 general parameters [143](#)
 syslog [144](#)
 NCS Call Agent
 IP addresses
 setting [36](#)
 status [17](#)
 NCS compatibility, basic parameters [191](#)
 NCS configuration
 basic parameters [187](#)
 endpoints [187](#)
 experimental [181](#)
 packages, Line [189](#)
 retransmission [188](#)
 statistics [189](#)
 cumulated [189](#)
 current [189](#)

O

OID, defined [xix](#)

P

parameter, changing its value [xxvi](#)
 PCMA, voice codec [66](#)
 PCMU, voice codec [66](#)
 persistent parameters, defined [xxvi](#)
 PIN dialing configuration, general parameters [127](#)
 PPPoA configuration, general parameters [137](#)
 PPPoE configuration, general parameters [111](#)
 protocol, switching [xxvi](#)

Q

- Q931 attributes, in H.323 [161](#)
- qos configuration
 - diffserv [55](#)
 - IEEE 802.1q [55](#)
 - interop [58](#)
 - VLAN [57](#)
 - VLAN substitution [57](#)

R

- registration method, H.323
 - configuration [151](#)
 - multiple [154](#)
 - group [157](#)
 - single [152](#)
 - status [160](#)
- Replaces config, in SIP [207](#)
- rtp management
 - configuration [25](#)
 - statistics
 - cumulated [24](#)
 - current [24](#)
 - last connection [23](#)

S

- second call, enabling [91](#)
- security certificates configuration, general parameters [139](#)
- session timer version, in SIP [208](#)
- SIP configuration
 - basic parameters [195](#)
 - conference [202](#)
 - Experimental, NAT custom [205](#)
 - grouping [200](#)
 - interop
 - DTMF transport [215](#)
 - general [207](#)
 - international code mapping [216](#)
 - Replaces config [207](#)
 - session timer version [208](#)
 - transfer version [208](#)
 - transmission timeout [208](#)
 - penalty box [199](#)
 - publication [201](#)
 - registration [198](#)
 - SIP User Agents [195](#)
 - transport [198](#)
 - TCP [199](#)
 - UDP [199](#)
 - trusted sources [202](#)
 - User Agents
 - Authentication (agent) [197](#)
 - Authentication (unit) [197](#)
- SIP Servers
 - IP addresses
 - setting [37](#)
 - status [18](#)
- siplInteropSdpDirectionAttributeEnable [210](#)
- SMI, defined [xix](#)
- SNMP
 - behaviour [xxi](#)
 - non-secure management mode [xxii](#)
 - secure management mode [xxii](#)
 - messages [xx](#)

- SNMP agent configuration, general parameters [123](#)
- SNTP
 - general [97](#)
 - IP addresses
 - setting [38](#)
 - status [19](#)
 - time zone config [98](#)
- static IP addresses, configuring
 - configuration file fetching [32](#)
 - H.323 gatekeepers [39](#)
 - image [31](#)
 - local host [30](#)
 - management server [33](#)
 - MGCP Call Agent [35](#)
 - NCS Call Agent [36](#)
 - SIP Servers [37](#)
 - SNTP [38](#)
 - STUN [42](#)
 - syslog [34](#)
 - telephony DNS [41](#)
- statistics
 - cumulated rtp [24](#)
 - current rtp connection [24](#)
 - last rtp connection [23](#)
 - setting
 - MGCP [176](#)
 - NCS [189](#)
 - system configuration [45](#)
- STUN
 - IP addresses
 - setting [42](#)
 - status [20](#)
- STUN configuration, general parameters [129](#)
- subscriber services
 - call forward
 - on busy [93](#)
 - on no answer [94](#)
 - unconditional [93](#)
 - call forward activation [93](#)
 - digit maps activation [94](#)
 - enabling [91](#)
 - interface status [93](#)
 - processing [95](#)
- syslog
 - configuration
 - local message table [53](#)
 - message customization [54](#)
 - objects [53](#)
 - IP addresses
 - setting [34](#)
 - status [17](#)
- system
 - administration, objects [3](#)
 - configuration [43](#)
 - download [45](#)
 - statistics [45](#)
 - management, objects [21](#)

T

- T.38, data codec [73](#), [74](#)
- tables
 - defined [xxvii](#)
 - generic [xxvii](#)
 - groupAdmin [xxviii](#)
 - ifAdmin [xxviii](#)

- TCP, SIP transport [199](#)
- telephony attributes
 - enabling [85](#)
 - IP address call [87](#)
- telephony configuration
 - country selection [59](#)
 - custom tone configuration [61](#)
 - signalling protocol [59](#)
- telephony DNS
 - IP addresses, status [19](#)
- textual conventions, in MIB structure [xxiv](#)
- tone detection, [74](#)
- transfer version, in SIP [208](#)
- transmission timeout, in SIP [208](#)

U

- UDP, SIP transport [199](#)
- Unit Manager Network product, using [xxvi](#)
- urgent gateway, setting [89](#)
- user gain, setting [64](#)

V

- voice activity detection, enabling [64](#)
- voice interface configuration
 - codecs [66](#)
 - G.723 [66](#)
 - G.729 [67](#)
 - PCMA [66](#)
 - PCMU [66](#)
 - DTMF detection [70](#)
 - DTMF transport [69](#)
 - IfTable [63](#)
 - comfort noise [64](#)
 - jitter buffer [63](#)
 - user gain [64](#)
 - voice activity detection [64](#)
- volatile parameters, defined [xxvi](#)

W

- web-based service configuration [117](#)
 - customizing [118](#)

