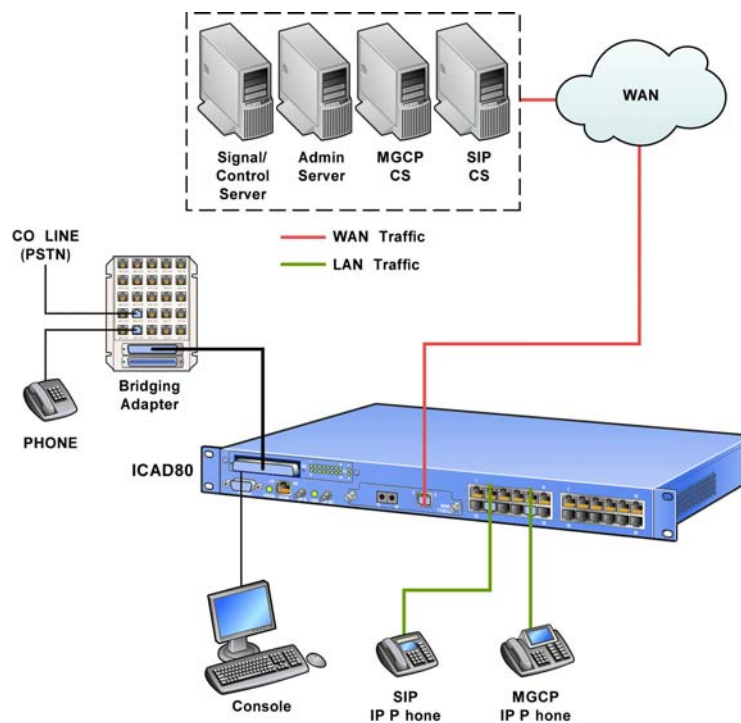

Business Gateway

User Guide

Release 1.1



CONTENTS

Copyright 2

Trademarks..... 2

Software Notice 2

Hardware Notice 2

CONTENTS

TABLES

FIGURES

ABOUT THIS GUIDE

Introduction 37

Organization..... 37

Typographical Conventions 38

Customer Support 39

1 STARTING WITH ICAD80

Introduction 41

Overview..... 42

 Feature Summary 42

 Session Controller..... 42

 User Agent 42

 Security..... 42

 Multi-Service QoS 42

 LAN Switch 42

 T1 Interface..... 42

 Monitoring..... 42

 Management 42

Connecting to ICAD80..... 43

Default Settings..... 43

 IP Interface 43

 default setting eth0 43

 default setting eth1 43

 User Groups 43

 User Accounts 43

 Voice Parameters 44

 Security Policies 44

 Security Policy 1 44

 Security Policy 2 44

 Security Policy 3 45

 Security Policy 4 45

 Security Policy 5 45

 Media Settings..... 45

 Voice ACL Policies 45

 Layer 2 QoS 46

 Services 46

 Telnet 46

 SSH/SFTP 46

Web Server Management Interface	46
Enabled by Default.....	46
Disabled by Default	46
2 USING COMMANDS	
Introduction.....	49
On-Line help	49
Help	49
General Information	49
Specific Information	52
Tab Key and ?	52
CLI Commands	53
Maintenance Commands.....	53
Debug Commands.....	53
Entering Commands	54
Syntax of CLI Commands	54
Syntax of Debug and Maintenance Commands.....	54
Interactive Mode	55
Command Keywords	55
NO	55
ALL.....	56
Showing Configuration.....	56
Saving Configuration.....	61
Auto Run Commands.....	61
3 USER MANAGEMENT	
Introduction.....	63
User Accounts, Groups and Rights.....	64
Configuration Main Menu.....	64
Adding a User Account	65
Configuration Requirements.....	65
Configuration Commands	65
Add User Account	65
Show User Account.....	66
Adding Group	66
Configuration Requirements.....	66
Configuration Commands	66
Add Group	66
Show Group	66
Configuring User Rights	67
Command Authority.....	67
Configuration Requirements.....	67
Configuration Commands	67
Configure User Rights.....	68
Show User Rights	68
Deleting a User Account	68
Configuration Requirements.....	68
Configuration Commands	68
Delete User Account Example	68
Deleting a User Group.....	69
Configuration Requirements.....	69
Configuration Commands	69
Delete Group Account Example	69
Deleting User Rights	69
Configuration Requirements.....	69
Configuration Commands	69
Delete User Rights Example	70

Password Entry	70
Failed Login Attempts	70
Change Password Example	70
Showing Active Users	70
RADIUS Client	71
Configuration Requirements	71
Configuration Commands	71
Configure RADIUS Authentication	71
Configure Radius Client	72
Show logs.....	73
4 INTERFACE CONFIGURATION	
Introduction	75
Configuring LAN Interface (eth1)	76
Configuration Requirements	76
Configuration Commands.....	76
Configure eth1 Interface	76
Show Configuration.....	76
Configuring WAN Interface (eth0)	77
Configuration Requirements	77
Configuration Commands.....	77
Configure eth0 Interface	77
Show Configuration.....	77
Configuring T1 Line	78
Configuration Requirements	78
Configuration Commands.....	78
Configuring T1 Line.....	79
Show Configuration.....	79
Configuration Status.....	79
Show T1 Alarms	80
Configuring PVC (Frame Relay).....	80
Configuration Requirements	80
Constraints.....	80
Configuration Commands.....	81
Configure PVC	81
Policing Traffic	81
Show PVC	81
PVC Statistics.....	82
PVC	82
Global Frame Relay.....	82
Clear Statistics	83
Configuring Local Management Interface.....	83
Configuration Requirements	83
Configuration Commands.....	83
Configure LMI.....	84
Show LMI	84
Statistics	84
Clear Statistics	85
Configure PVC Interface.....	85
Assigned IP Interface.....	85
Configuring PVC Interface	85
Show PVC Interface	85
Configuring VLAN	86
Configuring VLAN Interface	86
Configuration Requirements	87
Configuration Commands.....	87
VLAN Interface Configuration	87

VLAN IP Address Assignment	87
Configure VLAN Interface	87
Example 1	88
Show VLAN Interface	89
Modify VLAN Interface	89
Remove VLAN Interface	90

5 SYSTEM CONFIGURATION

Introduction.....	91
Time (SNTP Client)	91
Configuration Requirements	91
Configuration Commands	91
Configure Time	91
SNTP Time	92
Local Time	92
Modify SNTP Time	93
Show SNTP Time	93
DNS Client	93
Configuration Requirements	93
Configuration Commands	93
Configure DNS Client	94
Show DNS Client	94
Check DNS Client	94
Watchdog.....	95
Configuration Requirements	95
Configuration Commands	95
Configure Watchdog	95
Show Watchdog	95
Show System Exceptions	95
Show Exceptions Commands	95
Show Exceptions	96
Hardware	96

6 ROUTING CONFIGURATION

Introduction.....	99
Configuring ARP	99
Configuration Requirements	99
Configuration Commands	99
Configure ARP	100
Show ARP	100
Delete ARP	100
Flush ARP Table	101
Configuring Static Routing	101
Configuration Requirements	101
Configuration Commands	101
Add Static Route	101
Example 1	101
Example 2	101
Show Route Table	102
Delete Static Route	102
Configuration Commands	102
Configuring Dynamic Routing	102
Configuration Requirements	102
Configuration Commands	102
Configure Dynamic Routing	103
Show Dynamic Routing	103
Show Dynamic Route	103

7 SWITCHING CONFIGURATION

Introduction	105
Configuring LAN Ports	105
Speed	106
Duplex mode	106
Flow Control	106
Default Settings	106
Configuration Requirements	106
Configuration Commands	106
Configure LAN Ports	107
Example 1	107
Example 2	107
Example 3	107
Example 4	107
Show Configuration	107
Show Statistics	108
Clear Statistics	108
Configuring WAN Port	109
Speed	109
Duplex mode	109
Flow Control	109
Default Settings	109
Configuration Requirements	109
Configuration Commands	109
Configure WAN Port	110
Show Configuration	110
Show Statistics	110
Clear Statistics	111
Configuring ARL	111
Configuration Requirements	111
Constraints	111
Configuration Commands	111
Add ARL	113
Show configuration	113
Remove ARL	113
Flush ARL	113
Configuring Port Mirroring	114
Limitations and Recommendations	114
Configuration Requirements	114
Constraints	114
Configuration Commands	114
Configure Mirroring	114
Show Configuration	114
Remove Port Mirroring	115
Configuring Layer 2 QoS	115
Priority Queues	115
Configuration Requirements	116
Configuration Main Menu	116
Configure Layer 2 QoS	116
Configuration Commands	116
Configuring QoS Type	118
Configuring Priority	118
Show Configuration	118
Configuring VLAN	118
Configuration Requirements	119
Configuration Commands	119
Configure VLAN	120

Example 1	120
Example 2	120
Example 3	120
Show VLAN	120
Remove VLAN	121
Configuring STP	121
Spanning Tree Protocol (STP)	121
Configuration Requirements	122
Configuration Commands	122
STP Settings	122
STP Status	123
Configure STP	124
Show STP	124

8 SECURITY CONFIGURATION

Introduction	127
Traffic	127
VPN	128
SA	128
Configuring Firewall (Security Policies)	128
Configuration Requirements	128
Configuration Commands	128
Configure Firewall Rules	129
Show Firewall Rule	130
Remove Firewall Rule	130
Show Logs	130
Connection Timeout	131
Configuration Requirements	131
Configuration Commands	131
Show Timeout	131
Configuring IDS	131
IDS Anomaly	132
IDS Flood	132
IDS Scan	132
IDS Spoof	132
Configuration Parameters	132
Configuring IDS Anomaly	132
Configuring IDS Flood Activity	134
Configuring IDS Flood Settings	134
Configuring IDS Scan	136
Configuring IDS Spoof	136
Show IDS Statistics	137
Clear IDS Statistics	139
Show IDS Logs	139
Configuring NAT	140
Configuration Requirements	140
Configuration Main Menu	140
Configuring NAT Interface	141
Configuration Requirements	141
Configuration Commands – NAT Interface	141
Configure NAT Interface	141
Show Configuration	141
Configuring NAT Policy	141
Configuration Requirements	141
Configuration Commands	141
Configure NAT Policy	142
Configuring NAT Public	143

Configuring ALG	144
Configuration Requirements	144
Configuration Commands	144
Configure ALG	144
Show ALG	145
Security Configuration Using NAT	145
Port Forwarding	145
Address Forwarding	146
Configure Static NAT	147
Configuring IPsec	147
Configuration Main Menu	148
Configuring IPsec Policy	148
Configuration Requirements	148
Configuration Commands	148
Configure IPsec Proposal	149
Configuration Requirements	149
Configuration Commands	149
Configuring IPsec	149
Show IPsec Proposal	149
IPsec Statistics	150
Configuring IKE	150
Configuration Main Menu	150
Configuring IKE Policy	151
Configuration Requirements	151
Configuration Commands	151
Configure IKE Policy	151
Show IKE Policy	151
Show IKE SA	152
Configuring IKE Preshared	152
Configuration Requirements	152
Configuration Commands	153
Configure IKE Preshared	153
Show IKE Auto	153
Show IKE Task	153
..... VPN Configura-	
tions	154
Office to Office VPN	154
Local VPN Tunnel Interface	154
Tunnel Interface	154
Routing All Traffic	155
Show Configuration	156
 9 QoS CONFIGURATION	
Introduction	157
GoS	157
Configuring QoS	158
Configuring QoS Links	159
Configuration Requirements	159
Constraints and Recommendations	159
Configuration Commands	159
Configure QoS Link	159
Show QoS Link	159
Remove QoS Link	160
Configuring Quality Groups	160
Configuration Requirements	160
Configuration Commands	160
Quality Guaranteed Class	161

Configure Quality Group	161
Example 1	161
Example 2	162
Show Quality Group	162
Remove QoS Group	162
Configuring Traffic Classification	162
Configuration Requirements	162
Configuration Commands	163
Configure Traffic Classification	163
Example 1	163
Example 2	164
Show Traffic Classification	164
Remove Traffic Classification	164
QoS Statistics	164
Cumulative Statistics	164
Show Statistics	164
Clearing Counters	166
Instantaneous Statistics	166

10 SIP CONFIGURATION

Introduction	169
SIP Session Controller	170
SIP User Agent	170
SIP User Agent Features	170
Configuring SIP Server	171
Configuration Requirements	171
Configuration Commands	171
Configure SIP Server (Manual Mode)	172
Configure SIP Server (Automatic Mode)	172
Configure Failover Mode	172
Configure Load Balancing	173
Configure Additional SIP Servers	173
Show Configuration	174
Show Status	176
Configuring SIP Session Controller	176
SIP Signaling Proxy (SSP)	177
Configuration Requirements	177
Configuration Commands	177
Configure SIP Signaling Proxy (SSP)	177
Show Configuration	178
Show Status	178
Show Statistics	179
Media BRidge (MBR)	181
Configuration Requirements	181
Configuration Commands	181
Configure Media BRidge (MBR)	181
Show Configuration	182
Show Status	182
Show Statistics	182
Access Control List (ACL)	183
Configuration Requirements	183
Configuration Commands	183
Configure Access Control List (ACL)	184
Show Configuration	184
Endpoint Status Handling (ESH)	185
Configuration Requirements	185
Endpoint Status Handling (ESH)	185

Show Configuration	185
Show Statistics	185
Call Admission Control (CAC)	186
Configuration Requirements	186
Configuration Commands	186
Configure Call Admission Control (CAC)	186
Voice Quality Monitoring (VQM)	188
Configuration Requirements	188
Configuration Commands	188
Configure Voice Quality Monitoring (VQM)	189
Show Configuration	190
Show Statistics	190
Statistics Voice Quality	191
Alarm Logs	191
Alarms Statistics	192
Configuring SIP User Agent	192
Configuring SIP Protocol	193
Configuration Requirements	193
Configuration Commands	193
Show Configuration	194
Configuring FXS Port	194
Configuration Requirements	194
Configuration Commands	194
Show Configuration	195
Show Statistics	196
Configuring SIP UA	196
Configuration Requirements	197
Configuration Commands	197
Show Configuration	198
Show Status	198
Configure Numbering Plan	199
Configuration Requirements	200
Configuration Commands	200
Show Configuration	201
Show Call Statistics	201
Show Commands	201
Show Current calls	202
Show Call History	202
Configuring SIP Endpoints	203
Access Control List (ACL)	203
Registration	203

11 MGCP CONFIGURATION

Introduction	205
MGCP Session Controller	206
MGCP User Agent	206
Configuring MGCP Server	207
Configuration Requirements	207
Configuration Commands	207
Configure MGCP Server	207
Configure Failover Mode	208
Show Configuration	208
Show Status	209
Configuring MGCP Session Controller	209
MGCP Signaling Proxy (MSP)	210
Configuration Requirements	210
Configuration Commands	210

Configure MGCP Signaling Proxy (MSP)	210
Show Configuration	211
Show Status	211
Show Statistics	211
Media BRidge (MBR)	213
Configuration Requirements	213
Configuration Commands	213
Configure Media BRidge (MBR)	214
Show Configuration	214
Show Status	214
Show Statistics	215
Access Control List (ACL)	215
Configuration Requirements	215
Configuration Commands	215
Configure Access Control List (ACL)	216
Show Configuration	216
Endpoint Status Handling (ESH)	217
Configuration Requirements	217
Configuration Commands	217
Configure Endpoint Status Handling (ESH)	217
Show Configuration	218
Show Statistics	218
Call Admission Control (CAC)	219
Configuration Requirements	219
Configuration Commands	219
Configure Call Admission Control (CAC)	219
Show Configuration	220
Show Status	220
Show Statistics	221
Voice Quality Monitoring (VQM)	221
Configuration Requirements	221
Configuration Commands	221
Configure Voice Quality Monitoring (VQM)	222
Show Configuration	223
Show Statistics	223
Configuring MGCP User Agent	225
MGCP Protocol	226
Configuration Requirements	226
Configuration Commands	226
Show Configuration	226
Configure FXS Port	226
Configuration Requirements	227
Configuration Commands	227
Configure FXS Port	227
Show Configuration	227
Show Status	228
Show Statistics	228
Configure MGCP UA	229
Configuration Requirements	230
Configuration Commands	230
Show Configuration	231
Show Status	231
Show Call Statistics	232
Show Commands	232
Show Current calls	233
Show Call History	233
Configuring MGCP Endpoints	234
Access Control List (ACL)	234

Registration.....	234
12 VOIP SURVIVABILITY	
Introduction	237
Local Call Routing	237
Lifeline Failover	238
Local Call Routing	238
Configuration Requirements	238
Configuration Main Menu	238
Configure LCR Accounts	239
Configure LCR Settings.....	239
Example 1	239
Example 2	240
Show Configuration.....	240
Show Status.....	240
Show Connections	241
Lifeline Failover	241
13 SERVICES CONFIGURATION	
Introduction	243
File System	244
File System Navigation.....	244
Configuration Requirements	244
Configuration Commands	244
Navigate Through File System	245
File System Management	245
Configuration Requirements	245
Configuration Commands	245
Manage File System.....	246
SFTP Server.....	247
Configuration Requirements	247
Configuration Commands	248
DSA Host Keys	248
Configure SFTP	248
Show Configuration	248
Regenerate SFTP keys.....	249
Upload Public Key.....	249
Remote Administration Services	250
Telnet Server	250
Configuration Requirements	250
Configuration Commands	250
Configure Telnet	250
Show Configuration	250
Show Connections.....	250
Telnet Client.....	250
Configuration Requirements	251
Configuration Commands	251
Open Telnet Session	251
SSH Server	251
Configuration Requirements	251
Configuration Commands	251
DSA Host Keys	252
Configure SSH.....	252
Show Configuration	252
Regenerate SSH keys	252
Upload Public Key.....	253
Show Connections.....	253

Web Server	253
SSL	253
Web Server	257
IP Connectivity Services	259
Ping	259
Ping Options	259
Ping	259
Traceroute	260
Configuration Requirements	260
Traceroute Options	260
Traceroute	260
Services To VoIP Phones	261
DHCP Server	261
Configuration Requirements	261
Configuration Commands	261
Configure DHCP Server	262
Show Configuration	263
Show DHCP Leases	263
DHCP Relay	264
Configuration Requirements	264
Configuration Commands	264
Configure DHCP Relay	264
Show Configuration	264
DNS Relay	264
Configuration Requirements	264
Configuration Commands	265
Configure DNS Relay	265
Show Configuration	265
Show Sessions	265
Show Cache	266
SNTP Relay	266
Configuration Requirements	266
Configuration Commands	266
Configure SNTP Relay	266
Show Configuration	266
Show Sessions	267
TFTP Relay	267
TFTP Relay	267
TFTP Cache	268

14 MONITORING

Introduction	271
System Status	271
System Hardware	271
System Information	272
System Exceptions	272
System Operations	273
Audit Logging	273
Configuration Requirements	273
Configuration Commands	273
Configure Audit Logging	273
Show Configuration	273
Show logs	274
Clear logs	274
Module Logging	274
Logging Level	275
Logging Map	276

Logging Destination.....	277
System Summary.....	279
Network Activity.....	280
Port Mirroring	280
Port Statistics	280
IP Stack Statistics.....	280
IP Statistics	280
ICMP Statistics.....	282
UDP Statistics.....	283
TCP Statistics	284
Protocol Monitoring (PMON).....	286
Configuration Requirements	287
Configuration Commands	287
Configure PMON	287
Show Configuration	288
Show Statistics	288
Clear Statistics	289
Netflow.....	289
Configuration Requirements	289
Configuration Commands	289
Configure Netflow	290
Show Configuration	291
Show Statistics	291
Clear Statistics	291
SNMP	292
SNMP Agent	292
SNMP Traps.....	295
trapmib.....	296
Configuration Requirements	296
Command	296
Example	296
TCPdump.....	297
Configuration Requirements	297
Start Capture	298
Stop Capture.....	299
Voice Quality Monitoring	300
Network Discovery	300
Cisco Discovery Protocol (CDP)	300
Configuration Requirements	300
Show Commands	300
Show CDP Entry	300
Show Neighbors	301
Show Statistics	302

A UPGRADE SOFTWARE

Introduction	303
Check Boot Code.....	303
Images.....	303
Upgrading Software Via Web UI.....	303
Requirements.....	303
Upgrade Software via Web UI.....	304
Verify Software Installation	306
Change Default Application Image.....	306
View Bootloader Code	306
Find IP Address via CLI.....	307

B	WEB UI	
	Introduction.....	311
	Web UI Features.....	312
	Browser Support.....	312
	User Interface	312
	Configuration	312
	Monitoring and Tracking.....	312
	Wizards	312
	WEB UI Navigation	313
	Buttons.....	313
	Additional Functions and User Modes	313
	i	313
	?	313
	S/A – User Modes	313
	Configuration Menu	315
	Operations.....	315
	Logout	315
	Save System	315
	Reset System	315
	Logging in to Web UI	316
	Login Requirements	316
	Login to Web UI.....	316
	Configuring ICAD80	317
	Configuring User Accounts	317
	Monitoring.....	320
	Using Wizards.....	321
	Configuring Interface	321
	Upgrading ICAD80 Software	325
	Exit Web UI	326
C	THIRD PARTY SOFTWARE	
	Software Applications	327
D	SSH FUNCTIONALITY	
	Introduction.....	329
	SSH Server Functionality.....	329
	SFTP	330
	Authentication.....	330
	Host Keys	330
	Remote Login	331
	Service Functions	331
	SSH Service.....	331
	SFTP Service	331
	SSH System Architecture.....	332
	SSH-TRANS.....	332
	SSH-AUTH.....	332
	SSH-CONNECTION.....	332
E	CLI COMMANDS	
	Introduction.....	333
	CLI Command Access	333
	CLI Configuration Commands.....	333
	audit.....	333
	calls analyser	333
	connection tcp.....	334
	dhcps pool.....	334

framer hw.....	335
ids.....	335
ids anomaly	336
ids flood activity	336
ids flood settingsj.....	336
ids scan	336
ids spoof.....	336
ike.....	337
ike policy.....	337
ike preshared	337
interface ip	337
int vlan	338
ipsec	338
ipsec policy	338
ipsec proposal	339
lcr	339
lcr accounts.....	339
lcr settings	339
logging.....	340
logging dest.....	340
logging map	340
logging modules.....	341
media settings	341
mgcp.....	341
mgcp sc settings	342
mgcp server settings	342
mgcp ua	342
mgcp ua port	342
mgcp ua settings	343
netflow	343
netflow agent.....	343
netflow filter	344
pmon.....	344
pmon agent	344
pmon trace.....	344
protocol	345
qos	345
qos group.....	345
qos link	346
radius client	346
relay	346
relay dns settings	347
relay sntp settings	347
relay tftp cache	347
relay tftp files	348
relay tftp settings.....	348
rip daemon	348
route.....	348
route arp	348
route table.....	349
security.....	349
security alg	349
security policy.....	350
service.....	351
service ssh	351
service telnet.....	351
service web	352
shell terminal	352

sip	352
sip gateway settings	352
sip sc settings	352
sip server settings	353
sip ua port	353
sip ua settings.....	354
snmp	354
snmp agent	355
snmp community	355
snmp traps.....	355
ssl.....	355
ssl cert	356
ssl csr.....	356
ssl key	356
switch	357
switch qos ieee	357
switch qos port	357
switch qos setting	357
switch qos tos.....	358
switch arl	358
switch mirror	358
switch port	358
vlan	359
system	359
system dns.....	359
system images.....	359
system info	360
system sntp.....	360
system startup	360
system watchdog	360
user.....	361
user accounts	361
user groups	361
voice	362
voice acl	362
voice np.....	363
voice parameters	363
Show CLI Commands.....	363
audit.....	363
audit log	363
audit status.....	364
calls	364
calls alarms.....	364
calls analyser.....	364
calls current.....	365
calls history.....	365
calls quality	366
calls statistics	366
cdp	367
cdp entry	367
cdp neighbors	368
cdp traffic	368
connection tcp.....	368
dhcps.....	368
dhcps lease	369
dhcps pool	369
fr.....	369
fr lmi	370

fr pvc	370
framer	370
show framer alarms	370
show framer hw	371
ids	371
ids anomaly	371
ids attacks	372
ids flood	372
ids scan	372
ids spoof	372
ike	373
ike policy	373
ike preshared	373
ike sa	373
ike task	374
interface	374
interface ip	374
interface vlan	375
ipsec	375
ipsec ap	375
ipsec policy	376
ipsec proposal	376
lcr	376
lcr accounts	377
lcr connection	377
lcr settings	377
logging	377
logging dest	378
logging file	378
logging internal	378
logging map	378
logging modules	379
media	379
media connection	379
media settings	380
media status	380
media stream	380
mgcp	381
mgcp sc calls	381
mgcp sc endpoints	381
mgcp sc settings	382
mgcp sc status	382
mgcp status settings	382
mgcp server settings	382
mgcp server status	383
mgcp ua port	383
mgcp ua status	384
netflow	384
netflow agent	384
netflow filter	384
netflow stats	385
pmon	385
pmon agent	385
pmon trace	385
protocol	386
protocol icmp	386
protocol ip	387
protocol tcp	388

protocol udp.....	390
qos.....	390
qos group	390
qos link.....	391
radius client.....	391
relay.....	391
relay dhcp settings	392
relay dns.....	392
relay dns cache	392
relay dns sessions.....	393
relay dns settings.....	393
relay sntp.....	393
relay sntp sessions.....	393
relay sntp settings.....	394
relay tftp	394
relay tftp cache.....	394
relay tftp sessions	394
relay tftp settings	395
rip.....	395
show rip daemon	395
rip routes	395
route	396
route arp.....	396
route table	396
security	396
security alg	397
security dynamic	397
security nat.....	398
security policy	398
service	399
service ssh	399
service telnet	399
service web.....	400
shell terminal	400
sip	400
sip gateway settings	401
sip sc calls	401
sip sc endpoints.....	401
sip sc settings	402
sip sc status	402
sip server settings	402
sip server status	403
sip ua port	403
sip ua settings.....	404
sip ua status	404
snmp.....	405
snmp agent	405
snmp community	405
snmp traps.....	406
ssl.....	406
ssl certificate	406
ssl csr.....	406
ssl key	407
switch	407
switch arl	407
switch mirror	408
switch port	408
switch qos ieee	408

switch qos port.....	409
switch qos setting.....	409
switch qos tos	409
switch status.....	409
switch vlan	409
system	410
system dns	410
system exceptions	410
system hardware.....	411
system info.....	411
system snmp	411
system startup.....	412
system watchdog.....	412
user	412
user accounts.....	412
user groups.....	413
user rights.....	413
voice	413
voice acl.....	414
voice jitterbuffer	414
voice np	414
voice parameters	415
Stats CLI Commands	415
calls quality.....	415
fr	416
fr global	416
fr lmi.....	416
fr pvc	417
framer	417
ike task	418
interface ip	418
ipsec ap	419
media status.....	420
mgcp sc	420
mgcp sc calls	420
mgcp sc status.....	421
netflow agent	422
clear netflow agent.....	422
pmon trace	422
protocol	423
protocol icmp.....	423
protocol ip	424
protocol tcp.....	425
protocol udp	426
qos	427
qos counters	427
stats qos day.....	427
qos group.....	428
qos link	428
service web.....	428
sip	429
sip sc calls.....	429
sip sc status.....	430
snmp agent	431
switch	432
switch port.....	432
switch summary	433

F	TCPDUMP EXPRESSIONS	
	Introduction.....	435
	Expressions.....	435
	Primitives	435
G	COUNTRY CODES	
	Introduction.....	439
	Configuration Commands	439
	Configure Country Code.....	440
	Show Configuration.....	440
H	COMPLIANCE	
	FCC Compliance (US)	441
	FCC Telecom Statement.....	441
	Declaration of Conformity	442
	Equipment Attachment Regulations (Canada)	442
	Canadian Department of Communications Statement.....	443
	Contact Information.....	443
	Supplementary Information.....	443
	Data Standards	443
	Switching	443
	Routing.....	443
	Security	444
	Quality of Service	444
	Services	444
	Monitoring	445
	Voice Standards	446
	SIP Session Controller.....	446
	MGCP Session Controller	446
	SIP User Agent	447
	MGCP User Agent	447
I	GoS FUNCTIONALITY	
	Introduction.....	449
	QoS for Converged Networks.....	449
	GoS Technology	450
	GoS in the Network	450
	GoS Features	450
	GoS Processing.....	451
	Advantages of GoS	451
	Principles	451
	Stages	451
	Stage 1 – Classification	452
	Stage 2 – Policing: Bandwidth Control.....	452
	Stage 3 – Multiplexing.....	453
	2-D QoS Model Matrix.....	453
	Predictable QoS.....	454
J	IMPORTANT INFORMATION	
	Copyright Information.....	455

K

GLOSSARY

Abbreviations and Definitions 461

L

INDEX

..... 465

ABOUT THIS GUIDE

This chapter provides information about the intended audience for this guide, how this guide is organized, typographical conventions, the use of notices, and related documentation.

Introduction

This document provides guidelines for configuring and monitoring the ICAD80. This guide is designed for network managers, administrators, and technicians who are responsible for the management of networking equipment in Enterprise and Service Provider environments. Knowledge of Telecom technologies and standards including telephony and internet protocols is assumed.

Organization

The following tables describe the content and organization of this guide.

Table 1 Document Organization

Chapter	Description
1	Starting With ICAD80 provides an overview of ICAD80 capabilities, default settings, and user interface.
2	Using Commands provides information about using CLI commands for online help, saving and showing configurations, and applying configurations in interactive mode.
3	User Management describes users, permissions, and groups, and provides guidelines to create, modify, and remove user access to the network.
4	Interface Configuration provides examples to configure the ICAD80 unit for ethernet access (LAN, WAN, VLAN).
5	System Configuration provides examples for system configuration (SNTP time, DNS client, watchdog).
6	Routing Configuration provides configuration examples for routing (ARP, static routing, dynamic, RIP).
7	Switching Configuration provides configuration examples for switch (port) configuration (LAN, WAN, ARL, port mirroring, VLAN, layer 2 QoS). configurations are related to <i>Chapter 4, Interface Configuration</i> .
8	Security Configuration provides examples for security configuration (Firewall, IDS, NAT, ALG).

Table 1 Document Organization (continued)

Chapter	Description
9	QoS Configuration provides configuration examples for layer 3 Quality of Service (links, quality service, security).
10	SIP Configuration provides examples to configure SIP devices (server, session controller, user agent).
11	MGCP Configuration provides configuration examples for MGCP devices (server, session controller, user agent).
12	VoIP Survivability provides configuration examples for local call routing.
13	Services Configuration provides configuration examples for services (file system, remote administration, connectivity, authentication).
14	Monitoring provides examples of tracking and monitoring system performance.
A	Upgrade Software provides examples of upgrading image and configuration software.
C	Third Party Software provides contact information for the third party software referred to in this document.
D	SSH Functionality provides information about SSH as related to user management.
B	Web UI provides examples of using the Web User Interface (monitor, configure, upgrade software).
E	CLI Commands lists the ICAD80 CLI commands for configuration, showing information, and statistics.
F	TCPdump Expressions provides detailed information about using specific tcpdump expressions (options).
G	Country Codes lists the ISO country codes.
H	Compliance lists the voice and data standards, and FCC compliance.
I	GoS Functionality provides details about <i>Guarantee of Service</i> (GoS).
J	Important Information lists copyright acknowledgements and restrictions.

Typographical Conventions

This guide uses the following typographical conventions:

Table 2 Text Conventions

Font	Description
<i>NOTE:</i>	<i>Guidelines provided to use products more effectively.</i>
IMPORTANT:	Important information and/or instructions that must be followed.
CAUTION:	Guidelines provided to avoid equipment damage or faulty application.
WARNING:	Instructions provided to avoid personal injury.
<i>italic emphasis</i>	This font shows book titles, special terms, or emphasis.
bold emphasis	This font shows strong emphasis.
screen font	This font shows a screen capture: what is displayed on the monitor.
blue screen font	This font emphasizes selected items in a screen capture.

Table 2 Text Conventions (continued)

Font	Description
<i>italic screen font</i>	This font is used in command examples as a parameter placeholder – Replace the indicated text with the appropriate real name or value when using the command.
boldface screen font	This font shows commands that you enter or keyboard keys that you press.

Customer Support

For customer support, please contact your equipment supplier.

1 STARTING WITH ICAD80

This chapter provides introductory information about the ICAD80.

Introduction

This section summarizes ICAD80 capabilities, connecting to the unit, and factory default settings.

IMPORTANT: The software may need to be upgraded. For instructions, see Appendix A, “Upgrade Software”.

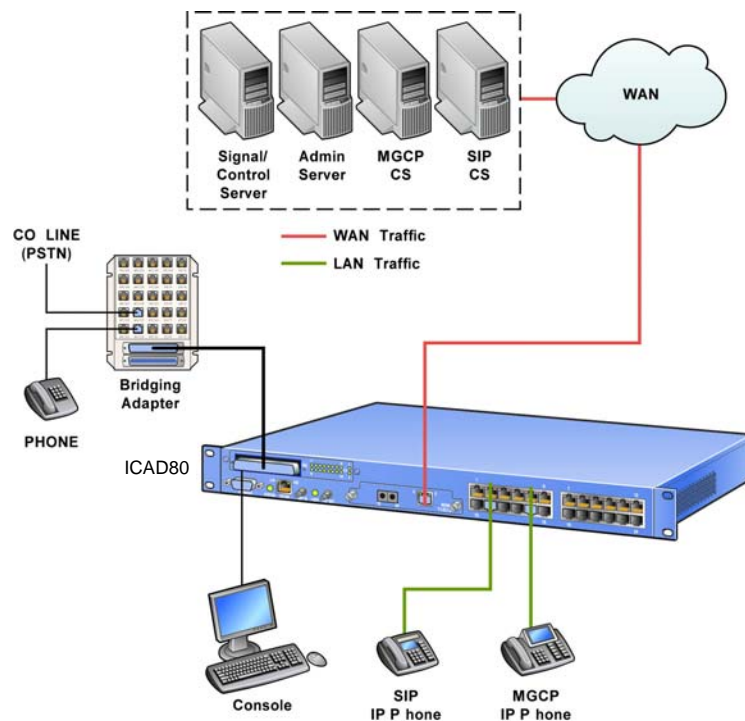


Figure 1 ICAD80 Connectivity

Overview

The ICAD80 is an integrated device, containing a broad set of networking functionality for voice and data in a single unit: a full featured router with VoIP, QoS and Security capabilities. It slots into the existing network, connected via Ethernet to the WAN access router, to enable the effective provisioning of converged VoIP and data services. It provides session control and service monitoring of VoIP devices on the company's LAN and protects against malicious packet attacks, assures bandwidth for calls and provides operator governed call admission control. The ICAD80 provides sixteen FXS and two FXO ports to provide legacy devices access to the IP network.

Feature Summary

ICAD80 provides the following services.

Session Controller

The ICAD80 has an MGCP and SIP Session Controller and can control up to 500 concurrent calls and 1000 registered devices. It provides VoIP survivability, switching local calls between LAN end points without the need for the proxy - when the WAN is down, calls around the office can still be made. This is coupled with an intelligent lifeline to switch calls to the PSTN via the emergency backup FXO line.

The ICAD80 is fully integrated with the multi-service QoS mechanism (GoS™), for delivery of carrier-class call quality and the firewall to allow reconfiguration and NAT traversal.

User Agent

The ICAD80 provides eighteen telephony interfaces, one FXO can act as a back-up lifeline, and sixteen FXS for connectivity of analog phones or fax machines (if power is down, only one FXO port is available; otherwise, two FXO ports are available). The User Agent (UA) acts as a VoIP endpoint within a network, performing signalling, media control and allowing the conversion from traditional interfaces to VoIP.

Security

The ICAD80 has a firewall, an advanced Intrusion Detection System (IDS), an Application Layer Gateway (ALG), and support for NAT.

Multi-Service QoS

The ICAD80 has an advanced, yet easy to configure QoS mechanism that ensures the optimal priority and bandwidth allocation for multiple classes of critical traffic. It is compatible with DiffServ with support for TOS bit re-marking.

LAN Switch

The ICAD80 has a 24-port switch, with support for Layer 2 QoS and VLAN.

T1 Interface

A T1 module is available to add to the ICAD80, providing T1 interface, supporting permanent virtual connectivity (PVC).

Monitoring

The ICAD80 dynamically monitors and provides statistics for both voice (statistics, such as MOS scores gathered per call) and data flows.

Management

The ICAD80 can be configured by both a CLI or web interface. The management system allows secure access and changes with SSH and HTTPS.

Connecting to ICAD80

This document assumes installing the ICAD80 and establishing connectivity have been completed. If necessary, refer to the *Business Gateway Installation Guide* that was provided on the CD that was included with the ICAD80.

For configuring the ICAD80 for Telnet access, see "Telnet Server" on page 250.

For information about Web UI, see Appendix B, "Web UI".

Default Settings

This section summarizes the factory default settings of the ICAD80. The following information is derived from the `dump` command, which was executed prior to configuration.

IP Interface

default setting eth0

```
config interface ip eth0
```

- IP address: 0.0.0.0
- No IP mask
- DHCP is on (enabled)

default setting eth1

```
config interface ip eth1
```

- IP address/IP mask 192.168.1.1/255.255.255.0
- No DHCP

User Groups

default setting admins

```
config user groups admins
```

- access ssh + web + cli + telnet + ftp
- All access rights are available

default setting users

```
config user groups users
```

- access web + cli

User Accounts

default setting System Access—admin

```
config user accounts admin
```

- access ssh + web + cli + telnet + ftp
- group1 admins
- group2 users
- group3 admins
- group4 admins
- group5 admins
- user ID admin

3

USER MANAGEMENT

This chapter describes the means provided to control access to the ICAD40 unit:

- Adding and removing users
- Setting up groups
- Assigning permission to users and to groups
- Authentication via Radius Client

Introduction

The user management functions control who can log in and whether they can change the ICAD40 configuration or just view information stored in the ICAD40. User access is controlled as follows:

- At login, by the user ID and password entered
Access methods for the user ID can be restricted (for example, permission to log in remotely could be denied).
the password must be authenticated (either internally or externally).
- After login, the user's access rights limit what the user can do.

IMPORTANT: The security of the ICAD40 depends on password security. To maintain access security to the ICAD40, passwords should be changed regularly and kept secure.

User Management supports user and group authentication, adding and removing users and groups to the network, and monitoring user activity. User Management can be accessed through CLI commands via console, telnet, and SSH, and through the Web user interface (Web UI).

Following is a summary of User Management functions.

- **Enforces access control by requiring login with a valid user ID and password**
 - Authenticates the entered password using either strong password hashing (SHA) or external authentication via a Radius client
 - Never stores passwords in clear text
 - Keeps a log of all failed login attempts and logouts
- **Limit login attempts**
 - A user can attempt to log in from the console port three times. If the user fails all three times, no one can log in to the console port for the next fifteen minutes.
- **Log failed login attempts and logouts**
- **Specified users can be locked out**
 - Users can be locked out from interface access methods such as Web and CLI

Adding a User Account

Before you add a new user account or change an existing user account, you should display the current user accounts and user groups by entering the commands: show user accounts and show user groups.

Configuration Requirements

There are no configuration requirements for adding a user account.

Configuration Commands

NPE> config user account

Table 4 describes the parameters for config user account.

Table 4 User Account Configuration Parameters

Parameter	Description
[name]	User name
access	Access mode for this user (all + ssh + web + cli + telnet + ftp + none)
auth	Whether internal or external authorization is required (SHA RADIUS)
group1	The first group the user belongs to (admins users -none-)
group2	The second group the user belongs to (admins users -none-)
group3	The third group the user belongs to (admins users -none-)
group4	The fourth group the user belongs to (admins users -none-)
group5	The fifth group the user belongs to (admins users -none-)
password	The password assigned to the user
inherit	Whether or not user inherits rights from groups
enabled	Whether or not user is enabled

Add User Account

This example assumes that the user should be given read and write access to the ICAD40, but only while connected directly to the console port: no remote access allowed.

name of user account: user1

access methods allowed: cli

group membership: admins

assigned password: test123

NOTE: This example is shown in interactive mode. For more information, see "Interactive Mode" on page 55.

1 Enter the following commands:

```
*NPE*> config user account user1 <enter>
  Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
  TAB to cycle parameter options
*user-accounts-user#*> access cli group1 admin password test123
*user-accounts-user#*> exit
```

2 To save the configuration, enter:

```
*NPE*> save
```

Show User Account

- To show the settings for account user1, enter the following command:

```
NPE*> show user account user1
```

- The display will be similar to the following:

```
Users:
Name          Access          Auth Group1 Group3 Group5 Password Inherit
              Group2 Group4              Enabled
-----
user1         cli          SHA  users              *****  yes
                                                    yes
```

NOTE: Password is encrypted; it is shown as asterisk characters.

Adding Group

This section provides examples for adding groups.

Configuration Requirements

There are no configuration requirements for adding a group.

Configuration Commands

```
NPE> config user groups
```

Table 5 describes the parameters for `config user groups`.

Table 5 User Groups Configuration Parameters

Parameter	Description
[name]	Group name
access	Access mode for this group (ssh web cli telnet ftp all none)
auth	Whether internal or external authorization is required (SHA RADIUS)
all	Whether or not access and auth should be allowed if not specified

Add Group

This example adds a new group as follows.

```
name: dev
access: all (ssh, web, cli, telnet, ftp)
unspecified access and authorizations: yes (allowed)
```

- 1 To add a group, enter the following command:

```
NPE> config user group dev access all all yes
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Group

- To show the settings for group dev, enter the following command:

```
*NPE*> show user group dev
```

- The display will be similar to the following:

Groups:			
Name	Access	Authorization	Allow All
dev	ssh + web + cli + telnet + ftp	SHA	yes

Configuring User Rights

This section describes how to configure a record that defines the access a group has to certain objects. The available access rights are read, write, and execute. Read allows the viewing of data; write allows the writing of data; execute is not currently used.

A group can have more than one rights record defined for it. For example, the default rights records `useradv` and `userbasic` are both defined for the same user group: the user group `users`. In this case, two rights records are defined so that the user group is granted different access to different objects in the system.

The `useradv` record applies to objects that belong to `Admins`; it grants only read access.

The `userbasic` record applies to objects that belong to `Users`; it grants both read and write access.

Command Authority

Commands are objects that belong to either `Admins` or `Users`. When you list the online help for a command (by entering the command followed by a `?` or tab key), you see a line for Authority (see page 51). If the Authority is `Admins`, the command is an object that belongs to `Admins` and the right to use that command is governed by the rights record that grants access to objects belonging to `Admins`.

In general, commands that require write access, such as `config` commands, have authority `Admins`. Commands that only display data, such as `show` and `stats`, have authority `Users`. Similarly, maintenance commands that require write access have authority `Admins`.

The notable exception is the `save` command that saves configuration changes; it has authority `Users` so it is available to all users belonging to groups `admins` or `users`.

Configuration Requirements

Setting user rights can only be applied to defined groups: those already added to the system. For more information, see "Adding Group" on page 66.

NOTE: In most cases, the default settings provide the appropriate permissions per user level. It is recommended to not change the settings unless deemed necessary, and the effects of authority and ownership are understood.

Configuration Commands

```
NPE> config user rights
```

Table 6 describes the parameters for configuring user permission.

Table 6 User Rights Parameters

Parameter	Description
[id]	Text identifier
access	Access mode for this rights record (read, write, execute) (read write execute all none)
gname	Group name for this rights record (admins users)
object	Object name for this rights record (Admins Users)

Configure User Rights

This example sets user rights as follows.

id: user (user being configured)
access modes allowed: read
group name: users
object name: Users

- 1 Enter the following command:

```
*NPE*> config user rights user access read gname users object Users
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show User Rights

- To show the current configuration of user rights enter the following command:

```
NPE> show user rights
```

- The display will be similar to the following:

Access Rights:

Identifier	Access mode	Group name	Object name
-----	-----	-----	-----
user	read	users	Users

Deleting a User Account

This section describes how to delete a user account.

Configuration Requirements

An user account must exist.

*NOTE: The user accounts **admin** and **user** cannot be removed or renamed.*

Configuration Commands

```
NPE> del user accounts
```

Table 7 describes the parameters for `del user accounts`.

Table 7 Delete User Account Parameters

Parameter	Description
[name]	User name

- name
Name of the user account to be deleted.

Delete User Account Example

- To remove an user account, enter the following command:

```
NPE> del user account user1
```

- To save the configuration, enter:

```
*NPE*> save
```

Deleting a User Group

This section describes how to delete a user group.

Configuration Requirements

NOTE: The default groups named `users` and `admins` cannot be deleted or renamed.

Configuration Commands

```
NPE> del user groups
```

Table 8 describes the parameters for `del user groups`.

Table 8 Delete Group Parameters

Parameter	Description
[name]	Group name

- `name`
Name of the user group to be deleted.

Delete Group Account Example

- To delete a user group named `dev`, enter the following command:

```
NPE> del user groups dev
```
- To save the configuration, enter:

```
*NPE*> save
```

Deleting User Rights

This section describes how to delete a user rights record.

Configuration Requirements

NOTE: The default right records named `admin`, `useradv`, and `userbasic` cannot be renamed or deleted.

Configuration Commands

```
NPE> del user rights
```

Table 9 describes the parameter for `del user rights`.

Table 9 Delete Rights Parameters

Parameter	Description
[name]	Right name

- `name`
Represents the name of an existing user rights record.

Delete User Rights Example

- To remove a user rights record named user, enter the following command:
NPE> `del user rights user`
- To save the configuration, enter:
NPE> `save`

Password Entry

All access to the ICAD80 requires entry of a valid user ID and password. The ICAD40 factory settings define two user IDs: admin with password admin; user with password netcat. The ICAD80 installation procedure recommends that these passwords be changed immediately.

NOTE: For security reasons, it is recommended that all passwords be changed on a regular basis.

Failed Login Attempts

A user can attempt to log in from the console port three times. If the user fails all three times, the console is locked out and no one can log in to the console port for the next fifteen minutes.

When attempting to log in remotely via Telnet or SSH, the user is given three login attempts and then the session is ended.

All invalid login attempts are recorded in the audit log. For more information about the audit log, see "Audit Logging" on page 273.

Change Password Example

The administrator, the user logged in with user ID admin, can change the password for any user account. This is done using the `config user account` command described on page 65. When logged on, all users can change their own passwords.

- 1 Enter the command `password`.
NPE> `password`
- 2 Enter the old password.
Old Password: `*****`
- 3 Enter the new password.
New Password: `*****`
- 4 Re-enter the new password.
Verify Password: `*****`
- 5 To save the configuration, enter:
NPE> `save`

Showing Active Users

To see which users are currently connected to the ICAD80, use the maintenance command `whoison`; its display shows the source IP address of the user and type of access in effect. An example follows.

- Enter the following command:
NPE> `whoison`
- The display will be similar to the following:

User	Source IP	Type
-----	-----	-----
admin	Unknown	Terminal
user	10.0.1.2	Web

- **Type**
Indicates how the user is connected to the ICAD80: Terminal, SSH, Telnet, or Web.

RADIUS Client

Radius client provides an authentication service.

Users can be authenticated when logging in the system using the RADIUS protocol.

- Multiple Radius authentication records created by the Web UI and the CLI (maximum of 20)
- Legacy authentication, enabling ICAD80 to function as Network Access Server (NAS)
- User management authentication provides Radius authentication and Secure Hash Algorithm (SHA).
- Radius authentication records and users are mapped: keyed on the Primary Key user name
- Compatibility with standard Radius servers

Configuration Requirements

A user account must be created with authentication set to "RADIUS". For more information about user management, refer to "User Management" on page 63.

Configuration Commands

```
NPE> config radius client
```

Table 10 describes the parameters for `config radius client`.

Table 10 Radius Client Configuration Parameters

Parameter	Description
[user]	User name for the client (admin user)
enabled	Enable/Disable radius client
auto	Automatically bind to specified interface
authserver	Authorization server for the client
secret	Shared secret for the client
bindaddr	Binding IP address for the client
interface	If auto, the interface that Radius will run over (eth0 eth1 -none-)

Configure RADIUS Authentication

This example configures a user with authentication set to Radius.

- 1 Enter the following command:

```
NPE> conf user account user16
```

CLI enters interactive mode.

```
Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
TAB to cycle parameter options
```

- 2 Enter the following commands:

```

user-accounts-user#> access web + ssh + cli
user-accounts-user#> auth radius
user-accounts-user#> group1 users
user-accounts-user#> password test123
user-accounts-user#> exit

```

3 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the current Radius Client configuration, enter:

```
NPE> show user account user16
```

- The display will be similar to the following:

Radius Client:

User Interface	Enabled	Automatic Auth	Secret	Bind

user16	yes	yes	radius-usa	testing123 0.0.0.0

Configure Radius Client

This example configures Radius Client as follows:

User account name: RadiusUser

Radius server: radius.wan.com

Shared secret: secret

Interface: eth0

1 Enter the following command:

```
NPE> conf radius client RadiusUser
```

CLI enters interactive mode.

Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
TAB to cycle parameter options

2 Enter the following commands:

```

radius-cl-user#> enabled yes
radius-cl-user#> authserver radius.wan.com
radius-cl-user#> secret secret
radius-cl-user#> interface eth0
radius-cl-user#> exit

```

3 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the current Radius configuration, enter:

```
NPE> show user account RadiusUser
```

- The display will be similar to the following:

Radius Client:

User	Enabled	Automatic Auth	Secret	Bind	Interface

RadiusUser	yes	no	radius.wan.com	secret 0.0.0.0	eth0

Show logs

Radius activity is reported in the system logging.

- To show the Radius logs, enter the following command:

```
NPE> show logging internal
```

- The display will be similar to the following:

```
(E)02:36:31: rc_send_server: bind: radius.wan.com: errno = 0x31
(C)02:36:31: RADIUS Authentication failure
(E)02:36:31: Cannot authenticate Radius!
(C)02:36:31: Cannot initialize Radius user: RadiusUser
(E)02:36:31: Cannot authenticate RADIUS user RadiusUser
(W)02:36:31: RadiusUser INVALID LOGON at TUE MAR 06 02:34:45 2007
```

4

INTERFACE CONFIGURATION

This chapter provides information and configuration examples for the interfaces for routing traffic:

- LAN
- WAN
- T1/Frame Relay
- VLAN

Introduction

A single Ethernet interface, eth1, represents the LAN ports. The Ethernet interface eth0 represents the WAN port. VLAN interfaces, Vif, can be added to either LAN or WAN ports.

ICAD80 routes traffic between the following interfaces:

- **LAN**
eth1 provides LAN ports to connect to the Corporate Network.
- **WAN (ethernet)**
eth0 can be used as a WAN port to connect to the external Internet.
- **T1/Frame Relay**

Frame Relay is a link layer that can be run over T1, and can provide the logical connection of a permanent virtual circuit (PVC), and support security and guaranteed bandwidth.

T1 provides 1.544 Mbps bandwidth on a WAN port.

NOTE: T1/Frame relay is only available when the T1 module is installed in the ICAD80. When installed, the ethernet (10/100) port is not available for use as a WAN port; however, the ethernet port can be used as a management port.

- **VLAN**

A virtual LAN (VLAN) is a logically independent network, a logical subcomponent of a physical network. Each VLAN functions as a separate network, which isolates internet multicasts and broadcasts to and from other groups.

The ICAD80 supports IEEE 801.Q VLAN: up to 512 VLANs on the switch and up to 16 VLAN interfaces (Vif) in the IP stack. VLANs are integrated into the host IP stack as separate layer 2 ethernet interfaces.

By default, VLAN is not configured; traffic is routed between eth1 and eth0.

VLAN can be configured through eth0 or eth1, but not the frame relay (fr0, fr1, etc).

ICAD80 provides 24 physical LAN ports and one physical WAN port. For information about port configuration, see Chapter 7, “Switching Configuration”.

Configuring LAN Interface (eth1)

This section provides configuration examples for the LAN interface.

Configuration Requirements

The eth1 ports should be configured. See “Configuring LAN Ports” on page 105.

Configuration Commands

```
NPE> config interface ip eth1
```

Table 11 describes the configuration parameters for `config interface ip eth1`.

Table 11 LAN Interface Parameters

Parameter	Description
[if]	Interface to change behavior of (eth0 eth1 vif0 vif1 ppp0 ppp1 ppp2 ppp3)
ip	IP address and mask of interface
mtu	The Maximum Transmission Unit (MTU) of the interface
dhcp	Whether or not DHCP is enabled for the interface
status	Configuration status of the interface (up down)
speed	Speed/Duplex of eth0 (Auto 10Half 10Full 100Half 100Full)

NOTE: Speed only applies to the WAN interface (eth0); it does not apply to the LAN interface (eth1).

Configure eth1 Interface

The following example sets the eth1 interface as follows:

IP address: 192.168.1.1

IP mask: 255.255.255.0

- 1 Enter the following command:

```
NPE> config interface ip eth1 ip 192.168.1.1/24
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the current configuration, enter the following command:

```
NPE> show interface ip eth1
```

- The display will be similar to the following:

```
"eth1" info:
```

```
Interface          eth1
Flags              (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP
```

```

MULTICAST >
  IP Address/Mask      192.168.1.1/255.255.255.0
  MTU                  1500
  DHCP                 off
  MAC Address          00:15:93:FE:00:CD
  Speed                N/A

```

Configuring WAN Interface (eth0)

This section provides configuration examples for the WAN interface.

Configuration Requirements

The eth0 port should be configured. See "Configuring WAN Port" on page 109.

Configuration Commands

```
NPE> config interface ip eth0
```

Table 12 describes the parameters for `config interface ip eth0`.

Table 12 WAN Interface Parameters

Parameter	Description
[if]	Interface to change behavior of (eth0 eth1 vif0 vif1 ppp0 ppp1 ppp2 ppp3)
ip	IP address and mask of interface
mtu	The Maximum Transmission Unit (MTU) of the interface
dhcp	Whether or not DHCP is enabled for the interface
status	Configuration status of the interface (up down)
Speed	Speed/Duplex of eth0 (Auto 10Half 10Full 100Half 100Full)

NOTE: Speed applies only to the eth0 port; it does not apply to the T1 interface.

Configure eth0 Interface

The port will be configured as follows:

DHCP: enabled

- 1 Enter the following command:

```
NPE> config interface ip eth0 dhcp on
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the current configuration of interface eth0, enter the following:

```
NPE> show interface ip eth0
```

- The display will be similar to the following:

```
"eth0" info:
```

```

Interface          eth0
Flags              (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP
MULTICAST >
IP Address/Mask    66.206.164.212/255.255.255.224
MTU                1500
DHCP               on
MAC Address        00:E0:45:10:00:90
Speed              FULL100(AUTONEG)

```

Configuring T1 Line

This section provides information and configuration examples about the T1 WAN line. This feature is available when the optional T1 module is installed in the ICAD80.

Configuration Requirements

The T1 module is installed in the ICAD80.

Configuration Commands

NPE> config framer hw

Table 13 describes the parameters for config framer hw.

Table 13 Frame Relay Configuration Parameters

Parameter	Description
type	Line type (T1)
mode	Layer 2 protocol (FR)
framing	Framing protocol (ESF, D4)
code	Line coding: B8ZS, HDB3, AMI
clock	Clock mode
loop	Loopback type
lbo	T1: Short Haul (ft): 0-655, Long Haul: -1 (0dB), -2 (-7.5dB), -3 (-15dB), -4 (-22.5dB)
mask	Timeslot mask for fractional connection (e.g. 1,2,3,4-32)

Additional information follows.

- type
At the release of this document, only T1 is supported; E1 is not available.
 - mode
In this release, only Frame Relay is supported
 - framing
T1 is typically setup for ESF (extend super frame).
 - code
T1 is typically setup for B8ZS (bipolar with 8-zero substitution). This setup allows 64 kbps per channel.
 - clock
8 kHz network clock
master: ICAD80 provides the network system clock
slave: ICAD80 follows the network system clock
-

The default value is `slave`.

- `mask`

T1 mode can provide 24 slots for fractional services: set to enable timeslots in a fractional connection. 24 timeslots are available in a T1 line which can be specified individually (separated by commas, such as 1, 2, 3, etc.) or as ranges (hyphenated, such as 1–24).

- `lbo`

Modifies the line build out of the interface: compensates for signal attenuation from the source (such as a repeater) direct to the ICAD80.

A positive value denotes short haul LBO; the units are in feet. A negative value specifies a long haul LBO; the units are in decibels.

For most configurations, this parameter should be used at its default value: -2 (-7.5 dB)

When used as a smart jack, `lbo` should be set to 0.

- `loop`

Enables loopbacks in the framer: remote Tx to remote Rx, or local Tx to local Rx. Used for debug. Default value is off.

This parameter should only be used for debug. When debug is complete, disable `loop`.

Configuring T1 Line

This example configures the T1 line as follows:

Type: T1 (default value)

Mode: Frame relay (default value)

Framing type: ESF

code: B8ZS

clock: slave (ICAD80 retrieves clocking information from the T1 line)

- 1 Enter the following command:

```
NPE> config framer hw type t1 mode fr framing esf code b8zs clock
      slave
```

- 2 To save the command, enter:

```
*NPE*> save
```

Show Configuration

- To show the current configuration, enter the following command:

```
NPE> show framer hw
```

- The display will be similar to the following:

```
Framer Settings:
```

Type	Mode	Framing	Code	Clock	Loop	LBO	Mask
T1	FR	ESF	B8ZS	SLAVE	OFF	-2	1-24

Configuration Status

Assuming the data communications equipment (DCE) at the other end is configured correctly, the line should be functional. The frame relay configuration can be verified as follows:

- LEDs

Check the LEDs on the T1 WAN module (see Figure 2). They should both be off; on indicates failure, as described below.

- Red LED indicates loss of carrier
- Amber LED indicates loss of synchronization

- Loopback, Slave Mode

When the ICAD80 is configured as a slave, inserting a loopback plug in the WAN interface should cause the red (carrier) LED to turn off; the amber LED should remain on.

- Loopback, Master Mode

When the ICAD80 is configured as a master, inserting a loopback plug into the interface should cause both LEDs to turn off.

If the NP80 is connected to a DCE and the amber LED flashes rapidly, check the configuration. This may indicate two masters are connected to the same link.

If any of the above problems occur and cannot be resolved, contact Customer Support.

To view the frame relay status remotely, see "Show T1 Alarms" on page 80.

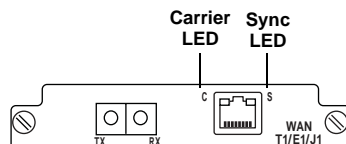


Figure 2 ICAD80 WAN Module

Show T1 Alarms

The T1 alarm status can be viewed with the command `show framer alarms`. For viewing the alarm status on the LEDs of the T1 module, see "Configuration Status" on page 79.

- To show the T1 alarm status, enter the following command:

```
NPE> show framer alarms
```

- The display will be similar to the following:

Framer Alarms:

Loss of carrier	inactive
Loss of synchronization	inactive
Alarm Indication Signal	inactive
Remote alarm indication	inactive
Loss of carrier count	0
Loss of synchronization count	0
Alarm Indication Signal count	0
Remote Alarm Indication count	0

NOTE: It may take several seconds after the fault condition is corrected before the alarm turns off (returns to inactive).

Configuring PVC (Frame Relay)

This section provides information and an example of configuring Permanent Virtual Circuits (PVC).

Configuration Requirements

There are no configuration requirements.

Constraints

Traffic is not sent unless the T1 line is up.

Up to 5 PVCs can be supported.

Up to five DLCIs (IP) can be configured per PVC.

PVC can be setup without T1; however, if setup with T1 and T1 goes down, data sent over the PVC line will be discarded.

Configuration Commands

NPE> `config fr pvc`

Table 14 describes the parameters for `config framer pvc`.

Table 14 Frame Relay PVC Configuration Parameters

Parameter	Description
[dlci]	The data link connection identifier
interface	IP interface that this PVC is bound to

- [dlci]
DLCI identification number: determines who (which other PVC in the network) the ICAD80 can talk to. The range of numbers is 16–1022. The assigned number must match the identification number of the DLCI at the remote. The default value is 16.
- interface
This parameter is non-configurable; it displays which IP interface the system has allocated to the PVC.

Configure PVC

The following example creates a new PVC as follows:

DLCI: 100

- 1 Enter the following command.

NPE> `config fr pvc new dlci 100`

- 2 To save the command, enter:

NPE> `save`

Policing Traffic

The following example sets the bandwidth to 1.544 Mbps. It is assumed only one PVC exists and that fr0 was assigned as the IP interface. For more

- 1 Enter the following command.

NPE> `config qos link fr0 max 154400`

- 2 To save the command, enter:

NPE> `save`

For more information about QoS, see "QoS Configuration" on page 157 and "GoS Functionality" on page 449

Show PVC

- To show the current PCV configuration, enter the following command.

NPE> `show fr pvc`

- The display will be similar to the following:

Frame Relay PVCs:

DLCI	Committed burst	IP Interface
CIR	Excess burst	LMI Status

```

-----
100          0          fr0
0           0          Down - invalid

```

- IP interface `fr0` is bound to the PVC.
- The PVC is down, according to LMI.
Packets sent to or received from a PVC that is down are marked as invalid and discarded in the Frame Relay AP.

PVC Statistics

This section provides information and examples of PVC and global frame relay statistics.

```
NPE> stats fr
```

Table 15 describes the parameters for `stats fr`.

Table 15 FR Statistics

Parameter	Description
<code>pvc <dlci></code>	PVC statistics
<code>global</code>	Global frame relay statistics

PVC

```
NPE> stats framer pvc <dlci>
```

If DLCI is not provided, stats for all currently configured PVCs will be displayed. An example follows.

- Enter the following command:
`NPE> stats fr pvc`
- The display will be similar to the following:

```

DLCI      RxPackets  RxBytes  TxPackets  TxBytes
-----
100        0          0          0          0

```

Global Frame Relay

```
NPE> stats fr global
```

- To view the global frame relay statistics, enter the following command:
`NPE> stats framer global`
- The display will be similar to the following:
Global frame relay statistics:

```

Received packets      429
Received bytes        8929 bytes
Transmitted packets    8
Transmitted bytes      704 bytes

Valid packets received 0
Invalid packets received 30
Valid packets transmitted 0
Invalid transmit packets 8

```

CRC Errors	8
Aborts	1
Overruns	0
In progress errors	0
Input queue full count	0

Clear Statistics

To clear the statistics for PVC and Global Frame Relay, enter the following command:

```
NPE> clear fr pvc | global
```

Configuring Local Management Interface

The Local Management Interface (LMI) provides a series of network management features for Frame Relay. The NP80 supports three types of LMI: ANSI Annex D, ITU Q933A and Cisco Gang of Four.

LMI is only supported in DTE mode. The ICAD80 initiates requests; it does not respond.

Configuration Requirements

The T1 must be up and running. See "Configuring T1 Line" on page 78.

The framer must be configured. See "Configuring PVC (Frame Relay)" on page 80.

Configuration Commands

```
NPE> config fr lmi
```

Table 16 describes the parameters of `config fr lmi`.

Table 16 Frame Relay LMI Parameters

Parameter	Description
type	LMI Type (none autodetect ansi q933A gfour)
t391	The Link Integrity Verification Timer (5–30)
n391	Threshold to send full status enquiry messages (1–255)
n392	Number of errors in window before link is declared down(1–10)
n393	Monitored events count(1–10)

- **type**
Specifies which LMI to use. `none` turns off LMI; only use this when LMI is not needed. The default setting is `autodetect`: which type of LMI.
`none` turns off LMI
NOTE: If the LMI type is set to autodetect the LMI type, the result of the auto detection is shown with the command `show framer lmi`. See "Show LMI" on page 84.
- **t391**
The Link Integrity Verification Timer is the duration between link integrity messages. `t391` is typically set to 10 seconds (default value). The timer units are seconds.
- **n391**
Specifies the number of `t391` messages (partial enquiries) that should be sent before sending a full status enquiry.
Example: if `n391` is set to 6 (default value), after 5 partial enquiries, the next (6th) will be a full enquiry.

-
- **n392**
Specifies the required number of error events in the event window to declare the link down.
Default value: 4.
LMI uses this value with n393 to determine if the PVCs should be declared as down: the number of errors exceeds the allotted number within the event window (n393). Should thresholds exceed in both n392 and n393, all PVCs will be marked as down.
 - **n393**
Specifies the size of the LMI event window: an internal buffer. Default value: 3.
LMI uses this value with n392 to determine if the PVCs should be declared as down: the number of errors exceeds the allotted number (n392) within the event window. Should thresholds exceed in both n392 and n393, all PVCs will be marked as down.

Configure LMI

This example configures the LMI as follows:

type: LMI autodetect

- 1 **Enter the following command:**
NPE> **config fr lmi type auto**
- 2 **To save the configuration, enter:**
NPE> **save**

Show LMI

- **To show the current LMI configuration, enter the following command:**
NPE> **show fr lmi**
- **The display will be similar to the following:**

LMI Status:

Type	autodetect
Discovered	gfour
T391	10 seconds
N391	6
N392	3
N393	4

Statistics

- **To view the frame relay LMI statistics, enter the following command:**
NPE> **stats fr lmi**
- **The display will be similar to the following:**

LMI Statistics:

Host interrupts	363
Received packets	363
Received bytes	4425 bytes
Transmitted packets	372
Transmitted bytes	4425 bytes

```

Local sequence number          109
Remote sequence number         108
Retransmits                    0
Packets rejected by LMI stack  0

```

Clear Statistics

- To clear the statistics, enter the following command:

```
NPE> clear fr lmi
```

NOTE: The local sequence number, remote sequence number and number of retransmits are private to the LMI stack; they cannot be cleared with this command.

Configure PVC Interface

This section provides information and an example of configuring the PVC interface.

When a PVC interface is configured, the system binds in IP interface to it. The IP interface can be accessed by other aspects of the system, such as firewall, GoS configuration, etc.

Assigned IP Interface

- To determine which IP interface the system has assigned to a particular PVC, enter the following command:

```
NPE> show fr pvc
```

- The display will be similar to the following:

Frame Relay PVCs:

DLCI	IP Interface	LMI Status
16	fr0	Up - valid

- The example above indicates PVC 100 is bound to fr0 (the PVC interface).
- The range of values of the PVC interface is fr0 – fr4

Configuring PVC Interface

The PVC interface is configured with the command `config interface ip`.

This example configures the PVC interface as follows:

Assigned IP address to fr0: 1.2.3.7/8

- 1 Enter the following command:

```
NPE> config interface ip fr0 ip 1.2.3.7/8
```

- 2 To save the command, enter:

```
*NPE*> save
```

Show PVC Interface

- To show the PVC interface, enter the following command:

```
NPE> show interface ip
```

- The display will be similar to the following:

```
"eth0" info:
```

```
Interface          eth0
Flags              (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP
MULTICAST >
IP Address/Mask    192.168.134.214/255.255.255.0
MTU                1500
DHCP               off
MAC Address        00:12:52:73:ED:B3
Speed              AUTONEG
```

"eth1" info:

```
Interface          eth1
Flags              (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP
MULTICAST >
IP Address/Mask    10.0.1.1/255.255.255.0
MTU                1500
DHCP               off
MAC Address        00:12:52:73:ED:B4
Speed              N/A
```

"fr0" info:

```
Interface          fr0
Flags              (20C1) < UP RUNNING NOARP LINKUP >
IP Address/Mask    1.2.3.7/255.0.0.0
MTU                4096
DHCP               off
MAC Address        00:00:00:00:00:00
Speed              N/A
```

Configuring VLAN

The following sections provide information and examples for configuring VLAN Interface. For information about VLAN switch configuration, see "Configuring VLAN" on page 118.

Configuring VLAN Interface

This section provides information and examples for configuring VLAN interfaces.

VLAN enables logically independent networks within a physical network, which can be used to isolate specified groups from other groups: isolate multicasts, protect data, etc.

By default, VLAN is not configured; traffic is routed between eth1 and eth0.

VLAN can be configured through eth0 or eth1, but not the frame relay (fr0, fr1, etc).

An IP address is assigned to a VLAN interface, which enables the ICAD80 to route traffic between this VLAN and other networks.

NOTE: When an IP address is assigned to a VLAN interface, the Firewall, by default, is closed for this interface. Rules need to be added to use the IP address. See "Configuring Firewall (Security Policies)" on page 128.

Configuration Requirements

VLAN must exist on the switch. See "Configuring VLAN" on page 118.

The maximum number of VLAN interfaces is 16.

Configuration Commands

This section describes the CLI commands for configuring VLAN interface.

VLAN Interface Configuration

```
NPE> config interface vlan
```

Table 17 describes the parameters for `config interface VLAN`.

Table 17 VLAN Interface Parameters (VLAN)

Parameter	Description
[vid]	VLAN ID for VLAN Range: 1 – 4095.
interface	Local interface to use for VLAN eth1 for VLAN configured on LAN. eth0 for VLAN configured on WAN.
status	VLAN on/off
comment	VLAN Comment (if any) Maximum length 256 characters. Special CLI characters are not allowed.

VLAN IP Address Assignment

```
NPE> config interface ip
```

Table 18 describes the parameters for `config interface ip`.

Table 18 VLAN Interface Parameters (IP)

Parameter	Description
[if]	Interface to change behavior of (eth0 eth1 vif0)
ip	IP address and mask of interface
mtu	The Maximum Transmission Unit (MTU) of the interface
vid	VLAN ID for interface
dhcp	Whether or not DHCP is enabled for the interface
status	Configuration status of the interface (up down)
speed	Speed/Duplex of eth0 (Auto 10Half 10Full 100Half 100Full)

NOTE: Speed applies only to the eth0 port; it does not apply to VLAN interfaces.

Configure VLAN Interface

This section provides two examples of configuring VLAN interface.

Example 1

The following example shows VLAN 1 configured with LAN port 4.

- Enter the following command:

```
NPE> show switch vlan
```

- The display will be similar to the following:

```
Switch VLAN:
VID    VLAN Name                WAN P1 P2 P3 P4 . . . P24
-----
1      MyLANVLAN                 *   *   *   *   U
2      MyWANVLAN                 T   *   *   *   *
```

The following example assigns an IP address to the VLAN interface:

```
VLAN ID: 1
IP address: 192.168.135.1
IP mask: 255.255.255.0
```

- 1 Create the VLAN interface for VLAN 1. Enter the following command:

```
NPE> config interface vlan 1 interface eth1
```

NOTE: The system automatically create the virtual interface, vif0.

- 2 Assign an IP address to the VLAN interface. Enter the following command:

```
*NPE*> config interface ip vif0 ip 192.168.135.1/24
```

- 3 To save the configuration, enter:

```
*NPE*> save
```

Example 2

The following example shows VLAN 2 configured with WAN port.

- Enter the following command:

```
NPE> show switch vlan
```

- The display will be similar to the following:

```
Switch VLAN:
VID    VLAN Name                WAN P1 P2 P3 P4 . . . P24
-----
1      MyWANVLAN                 T   *   *   *   *
2      MyWANVLAN                 T   *   *   *   *
```

The following example assigns an IP address to the VLAN interface:

```
VLAN ID: 2
IP address: 192.168.136.1
IP mask: 255.255.255.0
```

- 1 Create the VLAN interface for VLAN 1. Enter the following command:

```
NPE> config interface vlan 2 interface eth0
```

NOTE: The system automatically create the virtual interface, vif1

- 2 Assign an IP address to the VLAN interface:

```
*NPE*> config interface ip vif1 ip 192.168.136.1/24
```

- 3 To save the configuration, enter:

```
*NPE*> save
```

Show VLAN Interface

- To view the VLAN interface configuration, enter the following commands:

```
NPE> show interface vlan
```

- The display will be similar to the following:

Interfaces:

VID	Interface	Status	VIF	Comment
1	eth1	on	vif0	
2	eth0	on	vif1	

- To view the IP address assigned to VLAN interface, enter the following command:

```
NPE> show interface ip
```

- The display will be similar to the following:

"vif0" info:

```

Interface          vif0
Flags              (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP
MULTICAST >
IP Address/Mask    192.168.135.1/255.255.255.0
MTU                1500
DHCP               off
MAC Address        00:19:09:74:00:01
Speed              N/A
```

"vif1" info:

```

Interface          vif1
Flags              (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP
MULTICAST >
IP Address/Mask    192.168.136.1/255.255.255.0
MTU                1500
DHCP               off
MAC Address        00:19:09:74:00:00
Speed              N/A
```

Modify VLAN Interface

After a VLAN is created, it can only be turned on or off.

Also, the VLAN interface can be configured as a normal interface, as described below.

This example modifies VLAN as follows:

VLAN 1: activate

IP address: modify and modify its IP address.

- 1 Enter the following command to activate VLAN 1.
NPE> `config interface vlan 1 status on`
- 2 Enter the following command to modify the IP address of vif0.
NPE> `config interface ip vif0 ip 1.2.3.4/24`
- 3 To save the configuration, enter:
NPE> `save`

Remove VLAN Interface

To remove a VLAN, both the IP address assigned to the VLAN interface and the VLAN interface need to be removed.

When a VLAN is removed, the devices attached to that VLAN will no longer be able to communicate with the ICAD80.

The following examples remove VLANs:

VLAN 1
IP interface: delete vif0
VLAN interface: delete VLAN 1
VLAN 2
IP interface: delete vif1
VLAN interface: delete VLAN 2

- 1 To remove the VLAN 1, enter the following:
NPE> `del interface ip vif0`
NPE> `del interface vlan 1`
- 2 To remove VLAN 2, enter the following:
NPE> `del interface ip vif1`
NPE> `del interface vlan 2`
- 3 To save the configuration, enter:
NPE> `save`

9

QoS CONFIGURATION

This chapter provides guidelines and examples for configuring Quality of Service, which is based on Guarantee of Service™.

Introduction

The ICAD80 incorporates a sophisticated Quality of Service architecture known as Guarantee of Service™ (GoS). This chapter provides examples of configuring Guarantee of Service™ (GoS). For details of how GoS operates, see "GoS" on page 157 and Appendix I, "GoS Functionality".

The ICAD80 uses our patented QoS technology, GoS™, which delivers reliable Quality of Service. GoS is an advanced QoS solution designed for the convergence of voice and other real-time services with data traffic. Configuring GoS on the ICAD80 ensures optimum control and performance of your applications.

GoS

GoS is based on network layers 3 and above. ICAD80 also supports Layer 2 QoS, which allows the user to prioritize LAN traffic as it enters the device. For Layer 2 information, see "Configuring Layer 2 QoS" on page 115.

GoS can be configured for the following:

- **Manage Contention**

In typical installations the ICAD80 is deployed at the customer premises, at the boundary between the high bandwidth LAN and the lower bandwidth WAN. Network contention occurs at this point, where traffic traverses from Fast Ethernet to the WAN connection.

- **Voice Traffic Protection**

Voice streams in particular are sensitive to quality degradation. Real-time calls cannot tolerate high packet delay (and to a lesser extent high packet loss) and must therefore be appropriately prioritized as they are forwarded onto the WAN. GoS is integrated with the Session Controller for automatic control of the QoS allocation for voice traffic as calls are established.

For information about Session Controllers, see "Configuring SIP Session Controller" on page 176 and "Configuring MGCP Session Controller" on page 209.

Configuring QoS

Configuring QoS requires three steps:

1 Configuring QoS Links

A QoS link defines the portion of bandwidth managed by GoS for a specified interface. For example, to manage all of the bandwidth for a Fast Ethernet link, a QoS link would be configured for the maximum rate of 100Mbps.

2 Configuring Quality Groups

Within a Quality Group, traffic is managed as a single unit. No distinction is made between packets, streams, or flows within a Quality Group; all traffic in a Quality Group must share the Group's allocated bandwidth and quality. This can allow one, ill-behaved, out-of-contract stream to adversely affect the throughput of all other streams within that group.

When necessary, different streams can be isolated from each other: contained in separate Quality Groups. Quality Groups are used to group traffic streams with similar quality requirements and to apply the appropriate quality treatment to them.

A Quality Group is an aggregate of one or more traffic types that have similar quality requirements. Quality Groups have parameters to assign the quality treatment. These involve the allocation of loss and delay priorities (through 10 GoS Classes) and the allocation of bandwidth (using two types of policers,):

GoS Classes

A1, A2, A3, B1, B2, B3, C1, C2, C3 and BE allow the independent specification of loss and delay priorities to Quality Groups to be assigned different priorities relative to one another. See Figure 3 on page 161.

A1 represents minimum loss of packets and minimum delay: highest priority. To ensure guarantee of service can be provided, this class should only be assigned to the most critical data.

1–3 represent packet delay; typically, this is more acceptable for data than voice. The importance of each data stream must be considered; it may be necessary to minimize delay.

A–C represent the packet loss; typically, this is more acceptable for voice than data. The importance of each voice stream must be considered; it may be necessary to minimize loss.

BE represents best effort, a default setting that provides the lowest priority of all traffic. Within the BE group, all packet streams are given equal weight, with full access to the bandwidth the prioritized groups are not using. A BE group has the lowest priority.

Policing

(CAR and Policed) allows the allocation of bandwidth either to a strictly enforced limit (policed), or with an additional burst parameter (randomised gaps between packets), permitting available bandwidth to be taken to an upper limit (CAR).

Strict policing allows the network administrator to set an absolute limit for traffic in this Quality Group (its rate). Traffic arriving at a rate below this level is allowed through, and receives the loss and delay priority treatment assigned to the QG. Traffic arriving above the configured rate is discarded. This bandwidth is guaranteed to be available to the QG whenever it is demanded.

CAR (committed access rate) policing provides a way for traffic in this Quality Group to “reuse” bandwidth that is assigned to other Quality Groups but is currently not in use. This bandwidth is made available on a best-effort basis; it is not regulated, and is treated with the lowest loss and delay priority.

3 Configuring Traffic Classification (security policy)

Security Policies are used to identify incoming traffic, map the traffic to Quality Groups, and activate the QoS configuration.

Configuring QoS Links

This section provides guidelines to configure QoS links. A QoS link specifies on which interface traffic management is required.

Configuration Requirements

Rates take into account the Ethernet header without FCS.

Constraints and Recommendations

Apply QoS links only to WAN interfaces (eth0, vif, or fr); although this can be done, QoS is typically used to manage high bandwidth links.

See "Constraints and Limitations" on page 165.

Configuration Commands

```
NPE> config qos link
```

Table 63 describes the parameters for `config qos link`.

Table 63 QoS Link Configuration Parameters

Parameters	Description
[if]	The egress interface that this link applies to (eth0 eth1 vif0)
max	The speed of the link in bps
comment	An optional comment for this link

Configure QoS Link

This example configures the QoS link as follows:

Output interface (WAN): eth0

Maximum speed (Ethernet bandwidth, Mbps): 1.5

Comment (description of link): "office link"

- 1 Enter the following command:

```
NPE> config qos link eth0 max 1500000 comment "Office link"
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show QoS Link

- To show the results of the configuration, enter the following:

```
NPE> show qos link
```

- The display will be similar to the following:

QoS Links:

Interface	Max	Comment
-----------	-----	---------

eth0	1500000	Office link
------	---------	-------------

Remove QoS Link

NOTE: To remove a QoS link, all Quality Groups must be removed.

This example removes QoS link eth0.

- 1 Enter the following command:

```
NPE> del qos link eth0
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Configuring Quality Groups

This section provides guidelines to configure Quality Groups. A Quality Group is the definition of a QoS treatment, including bandwidth, loss, and delay parameters.

Configuration Requirements

A QoS link must exist.

When a QoS link is created, a default Quality Group assigned to BE (best effort) is automatically set up; traffic is not prioritized. This Quality Group is not displayed; however it always exists and manages the traffic flows which are not assigned to any Quality Groups.

A Quality Group can be explicitly assigned to BE, in which case it replaces the hidden BE. Functionally, nothing has changed, other than the BE Quality Group become visible.

The sum of the specified committed rates for all the Quality Groups must total no more than 90% of the link rate. 10% of link capacity is reserved for Best Effort traffic.

Configuration Commands

```
NPE> config qos group
```

Table 64 describes the parameters for `config qos group`.

Table 64 QoS Group Configuration Parameters

Parameter	Description
[name]	The name of the quality group
link	The interface of the link
qg	The GoS™ 2.0 class (A1 A2 A3 B1 B2 B3 C1 C2 C3 BE) Refer to "Quality Guaranteed Class" on page 161.
type	The type of the policer (car policed besteffort)
committed	The committed rate for a Quality Group The maximum rate setting is 90% of the total link rate
burst	The burst rate (ignored when Type = police) The burst rate should be greater than the committed rate and less than or equal to the link rate.
ipToS	Decimal IP ToS value to write into packets in this quality group (no to disable) Allowed values are 0–255 none

Table 64 QoS Group Configuration Parameters (continued)

Parameter	Description
cos	IEEE 802.1p value to write into packets in this quality group if VLAN ("no" to disable). Allowed values are no 0 1 2 3 4 5 6 7

NPE> config protocol arp qg

protocol arp qg is used to protect ARP traffic from self to WAN.

Table 65 describes the parameter for protocol arp qg.

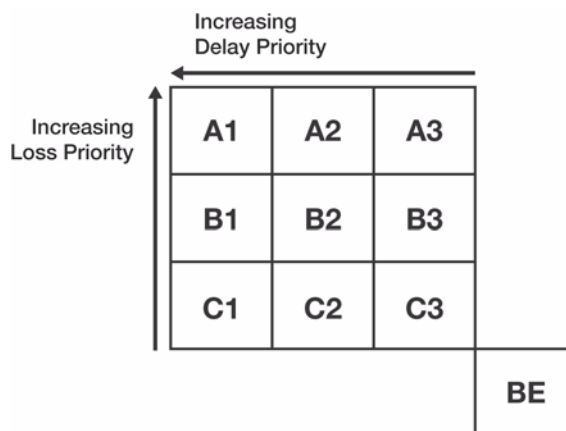
Table 65 Protocol ARP Parameter

Parameter	Description
qg	The GoS 2.0 Quality Group

Quality Guaranteed Class

Figure 3 summarizes the class values that can be allocated to quality groups. A1 indicates the highest class that can be allocated: low loss and low delay. BE indicates Best Effort; the best available resources will be utilized. With BE, there is no prioritization for a guaranteed level of quality.

For more information about *guaranteed class*, see Appendix I, "GoS Functionality".

**Figure 3 Quality Guaranteed Class**

Configure Quality Group

Example 1

This example configures a Quality Group for handling high priority VoIP traffic:

Name of group: VoIP
Quality group class: A1
Type of policer: policed
Commitment rate: 500000 (500 kbps)

1 Enter the following command:

```
NPE> config qos group VoIP qg A1 type policed committed 500000
```

-
- 2 To save the configuration, enter:

```
*NPE*> save
```

Example 2

This example configures a Quality Group for handling low priority data traffic:

```
Name of group: Data
Quality group class: A3
Type of policer: CAR
Committed rate: 850 000 (850 kbps)
Burst rate: 1500000 (1.5 Mbps)
```

- 1 Enter the following command:

```
NPE> config qos group Data qg A3 type CAR committed 850000 burst
1500000
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Quality Group

- To show the results of the configuration, enter the following command:

```
NPE> show qos group
```

- The display will be similar to the following:

QoS Quality Groups:

Name	Link	QG	Type	Committed	Burst	IPToS	COS
VoIP	eth0	A1	policed	500000	0	no	no
Data	eth0	A3	car	1000000	1500000	no	no

Remove QoS Group

To remove a QoS group, all the traffic flows assigned to it must be removed.

The following example removes the QoS group Data:

- 1 Enter the following command:

```
NPE> del qos group Data
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Configuring Traffic Classification

This section provides guidelines to configure the traffic classification to assign traffic flows to Quality Groups.

If the incoming traffic does not match any entry of the classifier, it is managed by the default Quality Group assigned to BE (Best Effort).

Configuration Requirements

At least one Quality Group must exist.

Traffic classification is accomplished by re-using the command of the security policies; the traffic classification for QoS and Security is the same.

Configuration Commands

NPE> config security policy

Table 66 describes the parameters for config security policy.

Table 66 Traffic Classification Policy Parameters

Parameter	Description
[index]	Unique numeric identifier, accepts 'new' for new policy creation
from	Where the packet originated from (self eth0 eth1)
to	Where the packet is destined to (i.e.: interface) (self eth0 eth1)
sip	The source IP or range of IP addresses
dip	The destination IP or range of IP addresses
sport	The source port or range of ports
dport	The destination port or range of ports
proto	The protocol to which the policy applies (udp tcp icmp any)
nat	NAT Policy to apply
qosg	The GoS 2.0 quality group
iptos	IP ToS value (decimal byte) to match ("any" to disable)
seq	Sequence of the policy (Begin End Position)
action	Whether to allow or deny traffic or disabled policy (allow deny)

Additional information follows:

- from, to, sip, dip, sport, dport, proto, iptos
These parameters configure traffic classification.
- qosg
Assigns traffic to a Quality Group.
- [index], nat, ipsec, seq, action
These parameters do not affect QoS functions.

Configure Traffic Classification

Example 1

This example configures VoIP traffic sent from LAN IP address 10.0.1.100 to WAN IP address 192.168.134.100 to be protected by the Quality Group VoIP:

- 1 Enter the following command:

```
NPE> config security policy new from eth1 to eth0 sip 10.0.1.100 dip
192.168.134.100 proto udp qosg VoIP
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Example 2

This example configures SNMP traffic sent from the SNMP agent of the ICAD80 to a SNMP client located in WAN IP address 192.168.134.101, to be managed by the Quality Group Data.

- 1 Enter the following command:

```
NPE> config security policy new from self to eth0 sport 161 dip
192.168.134.101 proto udp qosgp Data
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Traffic Classification

- To show the results of the configuration, enter the following:

```
NPE> show security policy
```

- The display will be similar to the following:

Security Policies:

Id	Seq	From To	Source IP	Dest IP	Source	Dest	Proto	NAT	QoS
							Action		ToS
1	1	eth1 eth0	10.0.1.100	192.168.134.100	any	any	udp allow	0	VoIP any
2	1	self eth0	any	192.168.134.101	161	any	udp allow	0	Data any

Remove Traffic Classification

This configuration removes traffic classification (security policy) 1.

- 1 Enter the following command:

```
NPE> del security policy 1
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

QoS Statistics

This section provides examples to monitor the QoS mechanisms. Two types of statistics are available:

- Cumulative statistic, incremented over time since the last clearing.
- Instantaneous statistics, calculated over one second.

Cumulative Statistics

Following are examples to display and clear cumulative counters.

Show Statistics

- To show counters for the Quality Group VoIP, enter:

```
NPE> stats qos counters VoIP
```

- The display will be similar to the following:

Name	VoIP
Link	eth0

```

Packets in:                2572
Primary packets out:       2572
Downgraded packets:        0
Packets dropped:           0
Bytes in:                  278950 bytes
Primary bytes out:         278950 bytes
Bytes dropped:              0 bytes
Bytes downgraded:          0 bytes

```

Table 67 describes the parameters of `stats qos` counters.

Table 67 QoS Cumulative Statistics

Parameter	Description
Packets in	The total number of packets received n This is the number of packets offered to the Quality Group.
Primary packets out	The total number of packets forwarded on the primary output n This is the number of packets protected forwarded by the Quality Group. n This represents what has been committed.
Downgraded packets	The total number of packets downgraded n This is the number of packets non protected forwarded by the Quality Group. This only applies to Quality Groups defined as CAR. n This represents bursts over commitments.
Packets dropped	The total number of packets dropped n In the case of a Quality Group defined as POLICED this is the number of packets dropped because they have been received at a speed over what is committed. n In the case of a Quality Group defined as CAR this is the number of packets dropped because they have been received at a speed over the burst rate.
Bytes in	The total number of bytes received n This is the number of bytes offered to the Quality Group
Primary bytes out	The total number of bytes forwarded on the primary output n This is the number of bytes protected forwarded by the Quality Group. n It represents what has been committed.
Bytes downgraded	The total number of bytes downgraded n This is the number of bytes non protected forwarded by the Quality Group. n This only applies to Quality Groups defined as CAR. This represents bursts over commitments.
Bytes dropped	The total number of bytes dropped n In the case of a Quality Group defined as POLICED, this is the number of bytes dropped because they have been received at a speed over what is committed. n In the case of a Quality Group defined as CAR, this is the number of bytes dropped because they have been received at a speed over the burst rate.

Constraints and Limitations

The following should be considered when configuring QoS contracts.

- For a Quality Group defined as CAR, the traffic received between the committed rate and the burst rate is downgraded; traffic is forwarded by the Quality Group to the Quality Group assigned to BE. Assigned to BE, traffic is forwarded if bandwidth is available. If bandwidth is in full use, the traffic is discarded; forwarding downgraded traffic is not guaranteed.
- Dropping packets/bytes indicates the offered load is out of contract. Traffic received over the committed rate for a Quality Group defined as POLICED or over the burst rate for a Quality Group defined as CAR is discarded. This ensures *not* forwarding more than what is guaranteed.
- Dropping packets is typically due to peak traffic; however, it may also occur due to an incorrect estimate, such as offered loads. For example, a Quality Group can be sized to protect 10 VoIP calls, when in actuality, up to 15 VoIP calls can be setup simultaneously. In this case, the size of the Quality Group should be updated accordingly.
- In some scenarios, GoS may drop packets when the average theoretical throughput of the flow is within contract. This is because the traffic source is bursting and packets are being deterministically dropped.
- Bytes take into account the Ethernet header without FCS.

Clearing Counters

Example 1

- 1 To clear the QoS statistics of the Quality Group VoIP, enter the following command:

```
NPE> clear qos counters VoIP
```
- 2 To save the configuration, enter:

```
*NPE*> save
```

Example 2

- 1 To clear the QoS statistics of all Quality Groups, enter the following command:

```
NPE> clear qos counters all
```
- 2 To save the configuration, enter:

```
*NPE*> save
```

Instantaneous Statistics

Following are examples to display instantaneous counters.

- To show counters for the Quality Group VoIP, enter the following command:

```
NPE> stats qos group VoIP
```
- The display will be similar to the following:

Name	VoIP
Link	eth0
Input rate:	448 bps
Output rate:	448 bps
Primary output rate:	448 bps
Downgrade output rate:	0 bps
Packet loss rate:	0 pps
Data loss rate:	0 bps
Packet loss ratio:	0 % packets lost
Data loss ratio:	0 % bytes lost
Average packet size:	56 bytes

Statistics are provided over one second.

Rates and bytes take into account the Ethernet header without FCS.

Table 68 describes the statistics of `stats qos group`.

Table 68 QoS Instantaneous Statistics

Parameter	Description
Input rate	The input rate <ul style="list-style-type: none"> This is the offered rate to the Quality Group.
Output rate	The output rate <ul style="list-style-type: none"> This is the total output rate of the Quality Group.
Primary output rate	Primary output rate <ul style="list-style-type: none"> This is the output rate of the protected traffic.
Downgrade output rate	Downgrade output rate <ul style="list-style-type: none"> This is the output rate of the non-protected traffic. This only applies to a Quality Group defined as CAR.
Packet loss rate	Packet loss rate <ul style="list-style-type: none"> This is the rate of packets dropped by the Quality Group. In the case of a Quality Group defined as POLICED this concerns packets dropped because they have been received at a speed over what is committed. In the case of a Quality Group defined as CAR this concerns packets dropped because they have been received at a speed over the burst rate.
Data loss rate	Data loss rate <ul style="list-style-type: none"> This is the rate of bytes dropped by the Quality Group. In the case of a Quality Group defined as POLICED this concerns bytes dropped because they have been received at a speed over what is committed. In the case of a Quality Group defined as CAR this concerns bytes dropped because they have been received at a speed over the burst rate.
Packet loss ratio	Packet loss ratio <ul style="list-style-type: none"> This is the ratio of packets dropped by the Quality Group.
Data loss ratio	Data loss ratio <ul style="list-style-type: none"> This is the ratio of bytes dropped by the Quality Group.
Average packet size	Average packet size <ul style="list-style-type: none"> This is the average size of the packets handled by the Quality Group.

11

MGCP CONFIGURATION

This chapter provides configuration examples for the MGCP Session Controller and the MGCP User Agent.

Introduction

The ICAD80 can be configured as both VoIP Session Controller and User Agent. The Media Gateway Control Protocol (MGCP) Session Controller controls logical links—requests from endpoint devices. The MGCP User Agent, which operates behind the Session Controller, interfaces the VoIP Gateway and analog terminals. In use, many of the endpoints (terminals) are IP telephones controlled through the Session Controller.

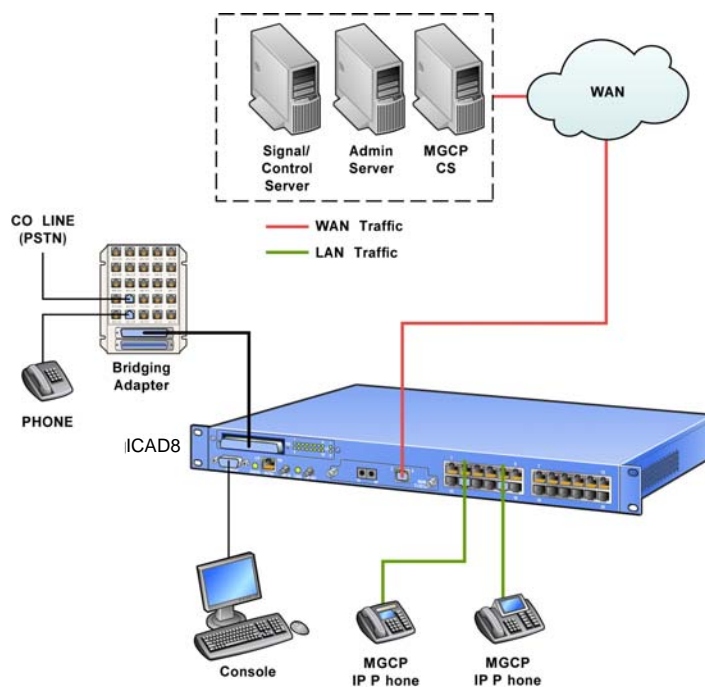


Figure 5 MGCP Network

MGCP Session Controller

The MGCP Session Controller can handle 1000 VoIP terminal accounts and 500 concurrent calls. Traffic can be directed through the Session Controller, allowing all VoIP calls to be controlled. All VoIP devices on the local internal network, LAN, are isolated from the external network, WAN. The following services are available:

- Relay the allowed MGCP messages to the proper destination. It relays incoming messages from the Media Gateway Controller (MGC) in WAN to Media Gateway (MG) or MGCP phone, or vice versa. All the relayed messages have the source address and port as the IP address and port of the Session Controller. The MGCP SC has a transparency behavior.
- Perform the following “Keep-alive” functions:
 - If the Call Server should not receive “Keep-alive” messages, the Session Controller filters out those messages.
 - If the Call Server requires “Keep-alive” messages but a LAN endpoint does not do so, Session Controller generates those packets for the endpoint device.
- Overwrite the media session information in SDP so that media streams go through the ICAD80 or avoid it (direct media connection, for LAN to LAN calls only).
- Track device status on the LAN to know when a LAN endpoint goes down (using AUPE requests). If the Session Controller is rebooted, maintain information of the device; re-registration is not necessary.
- Reject call requests if a LAN endpoint is not allowed to make calls according to Access List Control (ACL) rules.
- Reject call requests if a LAN endpoint is not registered (RSIP).
- Reject call requests from either a LAN endpoint or the MGC, if the Session Controller fails to allocate bandwidth for the call, according to the Call Admission Control (CAC).
- Monitor voice quality.

The MGCP Session Controller supports the local call routing: when all MGCP servers are down, the MGCP SC still routes local calls and optionally routes calls to the PSTN network. For more information about local call routing, see Chapter 12, “VoIP Survivability”.

MGCP User Agent

The FXS port of ICAD80 can be configured as a MGCP User Agent (MGCP UA) port, enabling VoIP communication with analog and IP terminals.

The MGCP User Agent (MGCP UA) interfaces VoIP to POTS (Plain Old Telephone System—analog), and functions as a VoIP Gateway, connecting an analog phone, modem or FAX machine to the MGCP network.

MGCP User Agent Features

MGCP UA supports the following features.

- MGCP User Agent functions as an MGCP integrated access device (IAD).
- Digit Maps

MGCP UA works with Call Server’s digit maps to initiate calls after enough digits have been received from the analog interface, instead of waiting for timeout.
- Analog telephone features are supported—MGCP UA detects hook flash in FXS and reports the event to Call Agent (CA). The features include:
 - Call onhold / retrieve
 - Make /receive second call
 - Call transfer
 - 3-way conference
 - Call Waiting notification

Configuring MGCP Server

This section provides guidelines to configure the MGCP servers.

Up to 3 MGCP servers can be configured. They must be set manually.

Each MGCP server has a priority. When the manual mode is selected, the priorities are as follows:

- mgc1: highest priority 0
- mgc2: priority 1
- mgc3: lowest priority 2

The MGCP SC uses priorities to implement a failover mode; when the current MGCP server goes down, the MGCP SC tries to use the alternative servers.

When MGCP servers are configured, the Firewall is automatically updated to accept MGCP messages from those MGCP servers.

To configure the MGCP features of the ICAD80, the following steps are required:

- 1 Configuring MGCP servers
- 2 Configuring MGCP Session Controller
- 3 Configuring MGCP User Agent and other LAN MGCP phones

Configuration Requirements

The MGCP servers should be reachable.

Configuration Commands

```
NPE> config mgcp server settings
```

Table 83 describes the parameters for `config mgcp server settings`.

Table 83 MGCP Server Configuration Parameters

Parameter	Description
[name]	Name of the settings profile
mgc1	The 1st media gateway controller (Name IP)
port1	The 1st media gateway controller's port
mgc2	The 2nd media gateway controller (Name IP)
port2	The 2nd media gateway controller's port
mgc3	The 3rd media gateway controller (Name IP)
port3	The 3rd media gateway controller's port
retries	Number of retries before blacklisting MGC (0 to disable)
blacklist	Blacklist timer in seconds

Configure MGCP Server

This example configures a single MGCP server as follows:

Name: Sylantro
MGC server: 206.229.26.51
MGC server port: 2727

- 1 Enter the following command:

```
NPE> config mgcp server settings Sylantro mgc1 206.229.26.51 port1 2727
```

-
- 2 To save the configuration, enter the following:

```
*NPE*> save
```

Configure Failover Mode

The failover mode is available when two or more MGCP servers are configured; the MGCP servers must be synchronized.

When the failover mode is not activated, the MGCP SC communicates with the MGCP server of highest priority. If the MGCP server goes down, the MGCP SC continuously retries to contact it. In this scenario, to establish calls, the MGCP SC must wait until the server recovers.

When the failover mode is activated, the MGCP SC automatically detects that a MGCP server is down: if it does not have IP connectivity with it (WAN interface unplugged, no IP route, etc.) or if it receives no MGCP replies from it.

The latter case can be configured with the parameter `retries`. It configures the number of retries before considering the MGCP server down. If this occurs, the MGCP server is marked as down by the MGCP SC for the duration configured by the parameter `blacklist`; the MGCP SC will not retry to contact it during this period of time. Instead the MGCP SC tries to communicate with the next MGCP server of highest priority. When the period of time expires for a MGCP server marked as down, the MGCP SC tries to resume the MGCP communications with it.

NOTE: The period of time during which a MGCP server is considered down starts when the MGCP SC detects it. This period of time is independent for each MGCP server marked as down.

This example configures the failover mode as follows:

```
Name: Sylantro_FailOverMode
Mgc1: primary.sylantro.com
Port1: 2727
Mgc2: secondary.sylantro.com
Port2: 2727
Retries: 10
Blacklist: 300
```

- 1 Enter the following command:

```
NPE> config mgcp server settings Sylantro_FailOverMode mgc1
primary.sylantro.com port1 2727 mgc2 secondary.sylantro.com port2 2727
retries 10 blacklist 300
```

- 2 To save the configuration, enter the following:

```
*NPE*> save
```

Show Configuration

- To show the results of the configuration, enter the following:

```
NPE> show mgcp server settings
```

- The display will be similar to the following:

```
MGCP Server "Sylantro":
```

Name	Sylantro
MGC1	206.229.26.51
Port1	2727
MGC2	
Port2	2727
MGC3	
Port3	2727

```

Retries      7
Blacklist    600 sec

MGCP Server "Sylantro_FailOverMode":

Name          Sylantro_FailOverMode
MGC1          primary.sylantro.com
Port1         2727
MGC2          secondary.sylantro.com
Port2         2727
MGC3
Port3         2727
Retries      10
Blacklist    300 sec

```

Show Status

The following example shows the status of the MGCP server.

- To show the status of the MGCP server, enter the following:

```
NPE> show mgcp server status
```

- The display will be similar to the following:

```

MGCP Server "Sylantro_FailOverMode":

Name          Sylantro_FailOverMode
Active        Yes
MGC1          primary.sylantro.com (In-use)
Port1         2727
MGC2          secondary.sylantro.com (Ready)
Port2         2727
MGC3
Port3         2727

```

Following are descriptions of the information fields:

- Active
 - Reports if at least one MGCP server is active:
 - Yes: the status is active, the MGCP SC normally communicates with a MGCP server.
 - No: the status is down, the MGCP SC does not communicate with any MGCP server.
- MGC1, MGC2, MGC3
 - Report which MGCP server is currently used is the field Active is Yes.
 - In-use: the MGCP server is currently active and used.
 - Ready: the MGCP server is not used.

The remaining information is extracted from the configuration (manual or automatic).

Configuring MGCP Session Controller

This section provides guidelines to configure the MGCP Session Controller (MGCP SC).

The MGCP Session Controller provides the following features:

- Relays MGCP messages between MGCP endpoints and MGCP servers (MGCP Signaling Proxy or MSP).

NOTE: The MGCP SC only supports endpoint identification endpoint@domain-name in which domain-name is a MAC address. It does not support identification per IP address.

- Controls how VoIP media traffic is established (Media BRidge: MBR)
- Controls which LAN endpoints can place/receive calls (Access Control List: ACL)
- Controls the status (i.e. up or down) of LAN endpoints (Endpoint Status Handling: ESH)
- Controls if LAN endpoints can place/receive calls (Call Admission Control: CAC).
- Reports the quality of calls (Voice Quality Monitoring: VQM).

MGCP Signaling Proxy (MSP)

Configuration Requirements

A MGCP server must be configured. See "Configuring MGCP Server" on page 207.

A QoS Quality Group must be configured to protect the MGCP signaling traffic. See "Configuring Quality Groups" on page 160.

Configuration Commands

```
NPE> config mgcp sc settings
```

Table 84 describes the parameters for `config mgcp sc settings`.

Table 84 MGCP Session Controller Configuration Parameters

Parameter	Description
server	Profile name of the MGCP call server
wanrxport	Signaling Rx port on WAN side
lanrxport	Signaling Rx port on LAN side
keepalive	Time period sending keep-alive to MGC -- 0 means no sending
eptimeout	Timeout of an active LAN endpoint -- time for keep-alive checking
maxcalls	Call Admission Control, maximum calls allowed
sigqos	GoS 2.0 quality group for signaling

Configure MGCP Signaling Proxy (MSP)

The MGCP Signaling Proxy (MSP) is configured with the command `config mgcp sc settings`, which specifies how the MGCP signaling is relayed.

- `server`
How to modify MGCP headers to be relayed.
- `wanrxport`, `lanrxport`
On which ports to listen MGCP signaling messages on LAN and WAN.
- `sigqos`
Which QoS Quality Group to protect MGCP signaling from other traffic. MGCP signaling is sensitive traffic. If MGCP packets are dropped, calls can fail.
- `keepalive`
If the MGCP server requires "Keep-alive" messages to be sent from LAN endpoints, the MGCP SC can still send those messages if they are not supported

This example configures the MGCP Signaling Proxy as follows:

MGCP server: Sylantro

WAN RX port: 2427
 LAN RX port: 2427
 Signaling QoS: VoIP

- 1 Enter the following command:

```
NPE> config mgcp sc settings server Sylantro wanrxport 2427 lanrxport
2427 sigqos VoIP
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the results of the configuration, enter the following command:

```
NPE> show mgcp sc settings
```

- The display will be similar to the following:

MGCP Session Controller settings:

Server	Sylantro
Wan Rx Port	2427
Lan Rx Port	2427
Keep Alive	0 sec
EP Timeout	3600 sec
Max Calls	500
Signaling QoS Group	VoIP

Show Status

- To show the status of the MGCP Signaling Proxy, enter the following command:

```
NPE> show mgcp sc status
```

- The display will be similar to the following:

MGCP Session Controller status:

MSC Started	Yes
MSC Server Ready	Yes
My Wan IpAddr	192.168.134.217
Wan Rx Port	2427
Lan Rx Port	2427
CAC Max Calls	500

Following are descriptions of the information fields:

- MSC Server Ready
 - Yes: MGCP server is active
 - No MGCP: server is not active

The remaining information is extracted from the configuration.

Show Statistics

Example 1

The following example displays the statistics of the MGCP signaling packets relayed.

- To show the statistics of the MGCP signaling relayed, enter the following command:

```
NPE> stats mgcp sc status
```

- The display will be similar to the following:

MGCP Session Controller message stats:

```

Msg per sec. (current/highest):      0/0

TotalMsgRxCount                      0

RxMsgDropSrcErr                     0
RxMsgDropIntErr                     0
RxMsgDropNoBufErr                   0
RxMsgDropWanCsErr                   0
RxMsgDropWanIfErr                   0
TxMsgDropNoBufErr                   0
TxMsgDropIntErr                     0

WanMsgRecvCount                     0
WanMsgProcCount                     0

WanMsgDropDataErr                   0
WanMsgDropNoBufErr                   0
WanCmdCacRejErr                     0
WanCmdDropSecFail                   0
WanCmdDropDataErr                   0
WanRspDropDataErr                   0
WanRspDropStateErr                  0

LanMsgRecvCount                     0
LanMsgProcCount                     0

LanMsgDropDataErr                   0
LanMsgDropSecErr                     0
LanMsgDropNoBufErr                   0
LanCmdEacRejErr                     0
LanCmdCacRejErr                     0
LanCmdDropSecFail                   0
LanCmdDropDataErr                   0
LanRspDropDataErr                   0
LanRspDropStateErr                  0

```

Following are descriptions of the information fields:

- WanMsgRecvCount, WanMsgProcCount, LanMsgRecvCount, LanMsgProcCount
Report normal relaying.

All other fields report errors.

Example 2

The following example displays the statistics of MGCP calls.

- To show the statistics of the MGCP calls, enter the following command:

```
NPE> stats mgcp sc calls
```

- The display will be similar to the following:

MGCP Session Controller call stats:

```

Call per sec. (current/highest):          0/0

Active calls (current/highest):           0/0

Total calls attempted:                    0

    Total outbound calls from LAN:         0
        Calls on going:                   0
        Calls succeeded:                   0
        Calls failed:                     0
        - Call rejected no bandwidth:     0
        - Call cancelled:                 0
        - Called dest busy:               0
        - Others causes:                  0

    Total inbound calls from WAN:          0
        Calls on going:                   0
        Calls succeeded:                   0
        Calls failed:                     0
        - Call rejected no bandwidth:     0
        - Call cancelled:                 0
        - Called dest busy:               0
        - Others causes:                  0

```

The calls from LAN are the calls originated from LAN endpoints. The calls from WAN are the calls originated from the MGCP server.

NOTE: A LAN to LAN call is both a call originated from a LAN endpoint and a call originated from the MGCP server.

Media BRidge (MBR)

Configuration Requirements

A QoS Quality Group must be configured to protect the VoIP media traffic. For more information about QoS refer to "Configuring Quality Groups" on page 160.

The RTP range must contain at least 1000 values and must not overlap any existing services of the ICAD80.

Configuration Commands

```
NPE> config media settings
```

Table 85 describes the parameters for config media settings.

Table 85 Media Configuration Parameters

Parameter	Description
dm	Enable use of direct media/RTP between 2 endpoints
rtp	Range of RTP ports to use (syntax: 'RTP low#-high#')
medqos	GoS 2.0 quality group for media streams
maxqos	Max number of media connection (streams) allow

Configure Media BRidge (MBR)

Media BRidge specifies how the VoIP media traffic is established:

- If LAN to LAN communications must be bridged by the ICAD80, or must be established directly between the parties.
 - `dm`
- Which values to use as destination and source UDP ports, respectively for the LAN and WAN side of the ICAD80. These values can be used by ISP access routers as criteria to classify media traffic in order to apply QoS actions.
 - `rtp`
- Which QoS Quality Group to protect VoIP media traffic. VoIP media traffic is very sensitive. If VoIP media packets are dropped or are delayed, voice quality can be poor.
 - `medqos`

This example configures the Media BRidge as follows:

Direct Media: `yes`
RTP range: `10000-12000`
Media QoS: `VoIP`

- 1 Enter the following command:

```
NPE> config media settings dm yes rtp 10000-12000 medqos VoIP
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the results of the configuration, enter the following command:

```
NPE> show media settings
```

- The display will be similar to the following:

Media config:

DM Enabled	Yes
RTP Ports	10000 - 12000
MedQoS	VoIP
MaxConn	500

Show Status

- To show the status of the Media BRidge, enter the following command:

```
NPE> show media status
```

- The display will be similar to the following:

Media status:

Max. cap (max_conn/qos_bps):	500/89000000
Port usage (current/highest):	0/0
Conn usage (current/highest):	0/0
Rate usage (current/highest):	0/0

Following are descriptions of the information fields:

- `port usage`
Reports the current number of ports used and the highest port.
- `conn usage`
Reports the current number of VoIP connections and the highest connection.
- `rate usage`

Reports the current VoIP media rate and the highest media rate.

Show Statistics

The following command displays the list of MGCP calls established by the Media BRidge.

- To show the list of MGCP calls established by the Media BRidge, enter the following command:

```
NPE> show mgcp sc calls
```

- The display will be similar to the following:

MGCP Session Controller detailed call entries:

```
EP Call Info          Call to:  6019
  EP Info             4083747001@001122334455, 127.0.0.1:0
  Line Number         1
  Line State          CALL_CONNECTED
  Media Conn Mode     NORMAL
  Media Type          AUDIO
  Media Conn_b        66.206.164.199:32046--66.206.164.203:13024<==
  Media Conn_a        ==>127.0.0.1:13024--127.0.0.1:32100
```

The following command displays the list of VoIP media connections established by the Media BRidge.

- To show the list of VoIP media connections established by the Media BRidge, enter the following command:

```
NPE> show media connection
```

- The display will be similar to the following:

SMedia Connections:

From IP (In) Port	To IP (In) Port	From IP (Out) Port	To IP (Out) Port	Mode
10.0.20.2 29268	10.0.1.1 13006	172.29.250.5 13006	172.29.250.30 29490	Bridge
10.0.20.2 29269	10.0.1.1 13007	172.29.250.5 13007	172.29.250.30 29491	Bridge

Access Control List (ACL)

Configuration Requirements

CDP must run on the ICAD80.

Configuration Commands

```
NPE> config voice acl
```

Table 86 describes the parameters for `config voice acl`.

Table 86 Voice ACL Configuration Parameters

Parameter	Description
[id]	Unique numeric identifier, accepts 'new' for new policy creation
mac	MAC address of the endpoint
epid	ID of the endpoint

Table 86 Voice ACL Configuration Parameters (continued)

Parameter	Description
softversion	Software Version of the endpoint
platform	Platform type of the endpoint
deviceid	Device Id of the endpoint
seq	Sequence number of the policy (begin end position)
ip	Single or a range of addresses of the endpoints
type	Signalling type for the endpoint (any mgcp sip)
action	Access (Deny or Allow)

Configure Access Control List (ACL)

The Access Control List (ACL) is configured with the command `config voice acl`. It specifies which LAN endpoints are allowed to place/receive calls. Authentication is based on the following information:

- MAC address
- IP address
- Signaling Type
- Device ID
- Endpoint ID
- Platform
- Software version

The MAC address, IP address, and Signaling Type are discovered by the MGCP SC; the other information is discovered by the Cisco Discovery Protocol (CDP). For information about CDP, see "Cisco Discovery Protocol (CDP)" on page 300.

By default, Access Control List allows all LAN endpoints to place/receive calls. If omitted parameters for classification are set to "any", which means that all values match. If omitted the action is "allow".

This example configures the Access Control List as follows:

IP address: 10.0.1.100
Signaling type: MGCP
Device ID: MGC000F8F073088
Action: deny

- 1 Enter the following command:

```
NPE> config voice acl new ip 10.0.1.100 type mgcp deviceid
MGC000F8F073088 action deny
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the results of the configuration, enter the following command:

```
NPE> show voice acl
```

- The display will be similar to the following:

Id	Seq	EpId	Platform	IP	MAC Address	Action
		Software	DeviceId		Type	Stats
1	1	any	any	10.0.1.100	any	deny
		any	MGC000F*		mgcp	0

- `stats`
Reports the number of times the policy matched.

Endpoint Status Handling (ESH)

Configuration Requirements

There are no requirements to configure Endpoint Status Handling.

Configuration Commands

NPE> `config mgcp sc settings`

Table 87 describes the parameters for `config mgcp sc settings`.

Table 87 MGCP Session Controller (ESH) Configuration Parameters

Parameter	Description
<code>server</code>	Profile name of the MGCP call server
<code>wanrxport</code>	Signaling Rx port on WAN side
<code>lanrxport</code>	Signaling Rx port on LAN side
<code>keepalive</code>	Time period sending keep-alive to MGC -- 0 means no sending
<code>eptimeout</code>	Timeout of an active LAN endpoint -- time for keep-alive checking
<code>maxcalls</code>	Call Admission Control, maximum calls allowed
<code>sigqos</code>	GoS 2.0 quality group for signaling

Configure Endpoint Status Handling (ESH)

The Endpoint Status Handling (ESH) saves information about LAN endpoints in non-volatile memory, which can be retrieved when the ICAD80 is rebooted. This information is saved during the MGCP registration process (RSIP) of the LAN endpoints to the MGCP servers. Following is a list of the information that is stored:

- MGCP Endpoint ID
- Name
- Telephone number
- IP address
- MGCP port
- MGCP Call Agent port
- Remaining active time (based on the parameter `eptimeout`)

The MGCP SC rejects calls terminating LAN endpoints that are not registered to the MGCP server; these calls do not need to be re-registered should the ICAD80 reboot.

ICAD80 periodically checks the status of each LAN endpoint using the MGCP method AUER. When a LAN endpoint answers, the timer (remaining active time) is reset to the value `eptimeout`. If the endpoint does not answer, the MGCP SC marks it as down and rejects all calls terminating it.

The following example configures the Endpoint Status Handling:

Active time: 1800 seconds

- 1 Enter the following command:

```
NPE> config mgcp sc settings server Sylantro eptimeout 1800
```

2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the results of the configuration, enter the following command:

```
NPE> show mgcp sc settings
```

- The display will be similar to the following:

MGCP Session Controller settings:

Server	Sylantro
Wan Rx Port	2427
Lan Rx Port	2427
Keep Alive	0 sec
EP Timeout	1800 sec
Max Calls	500
Signaling QoS Group	VoIP

Show Statistics

The following command displays the list of LAN endpoints registered to the MGCP server through the MGCP SC. This list can be retrieved should the ICAD80 be re-booted.

- To show the list of the LAN endpoints registered, enter the following command:

```
NPE> stats mgcp sc status
```

- The display will be similar to the following:

MGCP Session Controller endpoints:

Endpoint ID	EP Addr	EP Port	Act Calls
Endpoint Name	TelNo	CA Port	Timeout
4083746017@00152b177677	10.0.1.57	2427	0
Sophia 6017	6017	2432	1500
4083747001@001111111111	127.0.0.1	0	0
	7000	2429	1011

Following are descriptions of the information fields:

- Endpoint ID, Endpoint Name, IP Addr, TelNo, EP Port
Extracted from the MGCP registration process (RSIP) of the LAN endpoints to the MGCP server.
- CA Port
Extracted from the last MGCP message received from the MGCP server including a Notified Entity.
- Timeout
Initialized with the value `eptimeout`: decremented over time.
- Act Calls i
Incremented when the LAN endpoint places or receives a call.
Decrementd when the call is torn down.

Call Admission Control (CAC)

This section provides information and configuration examples for CAC.

Configuration Requirements

A QoS Quality Group must be configured to protect the VoIP media traffic in the case Call Admission Control is set-up based on QoS. For more information about QoS refer to "QoS Configuration" on page 157.

Configuration Commands

```
NPE> config mgcp sc settings
```

Table 88 describes the parameters for `config mgcp sc settings`.

Table 88 MGCP Session Controller (CAC) Configuration Parameters

Parameter	Description
<code>server</code>	Profile name of the MGCP call server
<code>wanrxport</code>	Signaling Rx port on WAN side
<code>lanrxport</code>	Signaling Rx port on LAN side
<code>keepalive</code>	Time period sending keep-alive to MGC -- 0 means no sending
<code>eptimeout</code>	Timeout of an active LAN endpoint -- time for keep-alive checking
<code>maxcalls</code>	Call Admission Control, maximum calls allowed
<code>sigqos</code>	GoS 2.0 quality group for signaling

```
NPE> config media settings
```

Table 89 describes the parameters for `config media settings`.

Table 89 Media Configuration Parameters

Parameter	Description
<code>dm</code>	Enable use of direct media/RTP between 2 endpoints
<code>rtp</code>	Range of RTP ports to use (syntax: 'RTP low#-high#')
<code>medqos</code>	GoS 2.0 quality group for media streams
<code>maxqos</code>	Max number of media connection (streams) allow

Configure Call Admission Control (CAC)

Call Admission Control (CAC) is configured with the commands `config mgcp sc settings` and `config media settings`. They specify if a LAN endpoint can place/receive a call, as described below.

- The maximum number of MGCP calls can be established through the ICAD80.
 - `maxcalls` (`config mgcp sc settings`)
- The maximum number of VoIP media streams can be established through the ICAD80.
 - `maxqos` (`config media settings`)
 - `medqos` (`config media settings`)

A MGCP call can be rejected for three reasons:

- The maximum number of MGCP calls `maxcalls` is exceeded.
- The maximum number of streams `maxqos` is exceeded.

-
- The `medqos` refers to a QoS Quality Group and there is no more bandwidth available.

For performance, the following considerations are recommended:

- The parameter `sigqos` should be configured to administratively limit the number of calls. It is typically defined by an ISP based on a number of users.
- The parameters `maxqos` and `medqos` should be configured to prevent call quality from deteriorating.

Calls are rejected when the WAN bandwidth dedicated to VoIP traffic is not available. In that circumstance, if all calls were accepted, exceeding the committed load for VoIP traffic, would cause VoIP packets to be dropped. As a result, the quality of all calls would be impacted. The parameters `maxqos` and `medqos` are typically based on the WAN bandwidth that is dedicated to VoIP traffic.

The parameter `maxqos` does not differentiate between VoIP media streams of different CODECs (so of different rates); however, the parameter `medqos` does.

Based on the CODEC negotiation, the MGCP SC derives how much bandwidth is required to establish the call, and checks if there is sufficient bandwidth remaining in the QoS Quality Group. Based on that information, the SC decides whether to accept or reject the call.

- When the Call Admission Control is configured based on QoS, it is strongly recommended to select a Quality Group assigned to A1; this selection guarantee the lowest delays and the lowest percentage of packets dropped. It is strongly recommended to select a Quality Group defined as POLICED to strictly enforce the rate of the incoming traffic, which protects the calls.

For information about QoS groups, refer to Chapter 9, “QoS Configuration” and Appendix I, “GoS Functionality”.

The following example configures the Call Admission Control based on QoS:

QoS Quality Group: VoIP

- 1 Enter the following command:

```
NPE> config media settings medqos VoIP
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the results of the configuration, enter the following command:

```
NPE> show media settings
```

- The display will be similar to the following:

Media config:

DM Enabled	No
RTP Ports	13000 - 14999
MedQoS	VoIP
MaxConn	500

Show Status

The following command shows the status of maxcalls.

- To show the status of the Call Admission Control for maxcalls, enter the following command:

```
NPE> show mgcp sc status
```

- The display will be similar to the following:

MGCP Session Controller status:

MSC Started	Yes
-------------	-----

```

MSC Server Ready      Yes
My Wan IpAddr         192.168.134.217
Wan Rx Port           2427
Lan Rx Port           2427
CAC Max Calls         500

```

The field `CAC Max Calls` reports the maximum number of MGCP calls allowed.

The following command shows the status of `maxqos` and `medqos`.

- To show the status of the Call Admission Control for `maxqos` and `medqos`, enter the following command:

```
NPE> show media status
```

- The display will be similar to the following:

Media status:

```

Max. cap (max_conn/qos_bps):    500/1000000
Port usage (current/highest):    0/0
Conn usage (current/highest):    0/0
Rate usage (current/highest):    0/0

```

- maximum capacity

Reports the maximum number of streams (extracted from the configuration), and the maximum available bandwidth of the QoS Quality Group managing the VoIP media traffic.

Show Statistics

The commands `stats mgcp sc status` and `stats mgcp sc calls`, described in "Show Statistics" on page 211, report statistics about the number of calls rejected because of the Call Admission Control.

For the command `stats mgcp sc status`, statistics are reported by through counters `WanReqCacRejErr` and `LanReqCacRejErr`.

For the command `stats mgcp sc calls`, statistics are reported by the counter `Call rejected no bandwidth`.

Voice Quality Monitoring (VQM)

Configuration Requirements

There are no requirements to configure Voice Quality Monitoring.

Configuration Commands

```
NPE> config calls analyzer
```

Table 90 describes the parameters for `config calls analyzer`.

Table 90 Call Analyzer Configuration Parameters

Parameter	Description
<code>jb</code>	Whether emulate a static or adaptive jitter buffer (static adaptive)
<code>min</code>	Minimum for the simulated JB
<code>max</code>	Maximum for the simulated JB

Table 90 Call Analyzer Configuration Parameters (continued)

Parameter	Description
nom	Nominal level for simulated JB
rtdelay	Estimate of Round Trip delay if no RTCP records detected
quality	Whether the low quality alarms are enabled
burst	Whether the excessive bursting alarms are enabled
delay	Whether the excessive delay alarms are enabled
rquality	The low quality R Factor trigger
rburst	The excessive bursting R Factor trigger
minburst	The excessive bursting minimum trigger
maxdelay	The excessive delay maximum delay trigger
galertclear	The minimum duration for the low listening quality alarm clear trigger
balertclear	The minimum duration for the excessive bursting alarm clear trigger
dalertclear	The minimum duration for the excessive delay alarm clear trigger

Configure Voice Quality Monitoring (VQM)

The Voice Quality Monitoring (VQM) specifies how to measure call quality.

The Voice Quality Monitoring simulates a Jitter Buffer to analyze VoIP media streams, then deduce information such as packet loss, delay, jitter, etc. Based on these parameters, it calculates R-Factors/Mean Opinion Scores updated in real-time over the duration of calls.

Related parameters are `jb`, `min`, `max`, `nom` and `rtdelay`.

- VQM specifies if alarms must be triggered for a low quality R-Factor, an excessive bursting R-factor (low quality R-factor lasting a certain period of time) and an excessive delay.

Related parameters are respectively `quality`, `burst` and `delay`.

- VQM also specifies when to trigger these alarms and when to clear them.

Related parameters are `rquality`, `rburst`, `minburst`, `maxdelay`, `galertclear`, `balertclear` and `dalertclear`.

Alarms are reported in the system logging as INFORM messages. For system logging information, see Chapter 14, “Monitoring”.

Voice Quality Monitoring reports statistics for VoIP media streams coming from the WAN only. For VoIP media streams coming from LAN their quality is not measured because it is assumed LANs to not suffer from network impairments as the WANs do.

Voice quality Monitoring reports statistics for the following CODECs:

- G.711 u-law
- G.711 A-law
- G.726-32k
- G.728-class
- G.729-class (but not G.729D and G.729E)
- GSM Full-Rate (6.10)

This example configures the Voice Quality monitoring as follows:

```
Jitter Buffer: static
Alarm for low quality R-factor: yes
Alarm for excessive bursting R-factor: yes
Alarm for excessive delay: yes
```

Low R-Factor: 50
 Excessive bursting R-factor: 50
 Excessive bursting R-factor duration: 1000ms
 Excessive delay: 100ms

- 1 Enter the following command:

```
NPE> config call analyzer jb static quality yes burst yes delay yes
rquality 50 rburst 50 minburst 1000 maxdelay 100
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the results of the configuration, enter the following command:

```
NPE> show call analyser
```

- The display will be similar to the following:

Call Analyser:

JB Type	static
JB Minimum	10
JB Maximum	60
JB Nominal	30
Roundtrip Delay	60 ms

Alarms:

Quality	yes
Burst	yes
Delay	yes
R-Quality	50
R-Burst	50
Min Burst	1000 ms
Max Delay	100 ms
Min Quality Alert Clear	3 sec
Min Burst Alert Clear	3 sec
Min Delay Alert Clear	3 sec

Show Statistics

The following command displays a summary of the quality of voice calls.

- To show a summary view of the quality of voice calls, enter the following command:

```
NPE> show call quality
```

- The display will be similar to the following:

Monitored Calls:

EP-ID	EP-Name	MOS-LQ	MOS-CQ	R Factor	RTP Rx	Loss	Codec
call.two	4982	4.20	4.18	92	515	0.00	PCMU

Following are descriptions of the information fields:

- IP-ID, EP-Name

Report the source of the VoIP media stream monitored.

- MOS-LQ, MOS-CQ, R Factor

Report the scores respectively for Mean Opinion Score - Listening Quality, Mean Opinion Score - Conversation Quality and R-Factor. These values depend on the CODEC used and on how much the traffic is disrupted through the network: packet loss, delay, jitter, etc.

- RTP Rx

Reports the number of RTP packets received from the source. The field Loss reports how many packets have been lost.

- Codec

Reports the CODEC used by the source.

NOTE: This command does not report information if the CODEC is not a CODEC supported by Voice Quality Monitor. See "Introduction" on page 205.

The following command displays a full view of the quality of voice calls. It displays the values of the different parameters used to estimate the quality of calls (MOS and R-Factor scores).

- To show a full view of the quality of voice calls, enter the following command:

NPE> **stats call quality**

- The display will be similar to the following:

Monitored Calls:

EP-ID	MOS-LQ	RTP Rx	JB Admit	JB Early	JB OOO	JB URun
EP-Name	MOS-CQ	Lost	JB Disc	JB Late	JB Dup	JB ORun

call.tw*4.20		884	884	1	0	0
4982	4.18	0	0	0	0	0

Following are descriptions of the information fields:

- IP-ID, EP-Name

Report the source of the VoIP media stream monitored.

- MOS-LQ, MOS-CQ

Report the scores respectively for Mean Opinion Score - Listening Quality, Mean Opinion Score - Conversation Quality. These values depend on the CODEC used and on how much the VoIP traffic is disrupted through the network: packet loss, delay, jitter.

- RTP Rx

Reports the number of RTP packets received from the source.

- Loss

Reports how many packets have been lost.

- JB

Reports the statistics of the Jitter Buffer simulated to deduce how much the VoIP traffic is disrupted.

NOTE: This command does not report information if the CODEC is not a CODEC supported by Voice Quality Monitor. See "Introduction" on page 205.

The following command displays alarms. Alarms are sent to the system logging. For more information about system logging, see Chapter 14, "Monitoring".

- To show the statistics about the alarms, enter the following command:

NPE> **show logging internal**

- The display will be similar to the following:

Message

```
-----
09:33:19: (:100001) Excessive Bursting alert on call detected
09:33:19: (:100001) Excessive Bursting alert on call cleared
```

Following are descriptions of the information fields:

- The first column shows time.
- The second column shows the source of the VoIP stream for which the alarm is triggered.
- The third column reports which alarm is detected or cleared:
 - **Low Quality:** low R-Factor
 - **Excessive Bursting:** excessive bursting R-factor
 - **Excessive Delay:** excessive delay

The following command displays statistics about the alarms. This command reports the number of alarms triggered.

- To show the statistics about the alarms, enter the following command:

```
NPE> show call alarms
```

- The display will be similar to the following:

Alarm Stats:

```
Low Quality          6
Excessive Burst      15
Excessive Delay      0
```

Following are descriptions of the information fields:

- Low Quality

Reports the number of alarms reported because of a low R-Factor.
- Excessive Burst

Reports the number of alarms reported because of an excessive bursting R-factor.
- Excessive Delay

Reports the number of alarms reported because of an excessive delay.

Configuring MGCP User Agent

This section provides guidelines to configure the MGCP User Agent (MGCP UA).

The MGCP UA must be considered as a VoIP MGCP phone located on the LAN. It is binded to the FXS (phone) port of the ICAD80. The identifier of this port is 1. MGCP identification (domain name) is supported by MAC address only.

The MGCP UA currently supports the following features:

- CODECs G.711 u-law, G.711 a-law and G.729
- RFC 2833
- Modem pass through
- Fax pass through

To configure the MGCP UA, the following steps are recommended:

- MGCP protocol
- FXS port
- MGCP UA

MGCP Protocol

The configuration of the MGCP protocol applies to the MGCP UA only. It does not apply to the MGCP SC. The MGCP protocol can be modified for interoperability purposes within the MGCP environment.

The following changes can be applied to the MGCP protocol:

- Domain format (currently, the only one supported is by MAC address)
- The maximum number of re-transmission when a request does not get an answer
- Timer before restarting the MGCP UA in the case the MGCP server does not answer anymore

NOTE: The MGCP protocol is configured so the MGCP UA tries to get registered to the MGCP server as soon as it is started using RSIP. MGCP UA is not functional until it is registered.

Configuration Requirements

There are no requirements to configure the MGCP protocol.

Configuration Commands

```
NPE> config mgcp ua settings
```

Table 91 describes the parameters for `config mgcp ua settings`.

Table 91 MGCP Protocol Configuration Parameters

Parameter	Description
domainformat	Format of MGCP Endpoint Domain Names (MACAddr)
maxretxcount	Max Number of Successive Re-transmission for User Agent

Configure MGCP protocol

This example configures the MGCP protocol as follows:

Domain format: MAC address

Maximum number of re-transmission: 5

- 1 Enter the following command:

```
NPE> config mgcp ua settings domainformat MACAddr maxretxcount 5
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the configuration of the MGCP protocol, enter the following command:

```
NPE> show mgcp ua settings
```

- The display will be similar to the following:

MGCP Protocol Settings:

DomainFormat	MACAddr
MUAMaxReTxNum	10
MUARestartDelay	50000

Configure FXS Port

The considerations for configuring the FXS port are as follows:

- A country code to adjust the settings of the port to specific parameters required by the selected country. Refer to "Country Codes" on page 439.
- The type of the jitter buffer to interface the DSP: adaptive or fixed
- A DSP gain

Configuration Requirements

There are no requirements to configure the FXS port.

Configuration Commands

NPE> config system info

Table 92 describes the parameters for config system info.

Table 92 System Parameters Configuration Parameters

Parameter	Description
unit	Unit name of this box
country	ISO-3166 two letter country code

NPE> config voice jitterbuffer

Table 93 describes the parameters for config voice jitterbuffer.

Table 93 Voice Jitterbuffer Configuration Parameters

Parameter	Description
mode	Jitter Buffer Type (fixed adaptive)
maximum	Maximum delay introduced by the jitter buffer (ms), for Adaptive Mode only
nominal	Nominal delay introduced by the jitter buffer (ms), for both modes
minimum	Minimum delay introduced by the jitter buffer (ms), for Adaptive Mode only

Configure FXS Port

This example configures the FXS port as follows:

Country: US

Jitter buffer: Fixed, 60ms

- 1 Enter the following commands:

NPE> config system info country US

NPE> config voice jitterbuffer mode fixed nominal 60

- 2 Save the configuration. Enter:

NPE> save

Show Configuration

- To show the configuration of the FXS port (country), enter the following command:

NPE> show system info

- The display will be similar to the following:

System Info:

```
Unit Name      MyUnit
Bootcode Ver   1.10.0007
App. Ver       ICAD T2 2.02.0135
System Type    NP40
Memory         79/128 MB
Country        United States of America (US)
Up time        0 days, 4 hours, 33 mins & 20 secs
```

- To show the configuration of the FXS port (jitter buffer and gain), enter the following command:

```
NPE> show voice jitterbuffer
```

- The display will be similar to the following:

```
Voice Jitter Buffer Settings:
```

```
Mode          fixed
Maximum       120 ms
Nominal       60 ms
Minimum       20 ms
```

Show Status

The following command shows the status of the tone of the FXS port.

- To show the status of the tone of the FXS port, enter the following command:

```
NPE> show media tone
```

- The display will be similar to the following:

```
Media Tones
```

```
Index TDM Port VPM Chan1 VPM Chan2 DTMF Detection Tone Send DTMF Send
-----
0      0      0      1      on      off      off
```

Following are descriptions of the information fields:

- port/channel 0/0
Represent the FXS port.
- DTMF detection
Reports if DTMF detection is enabled.
- Tone Send
Reports if the tone is sent out on the FXS port.
- DTMF Send
Reports if DTMF is sent out on the FXS port.

Show Statistics

The following command displays the statistics of the Jitter Buffer.

- To show the statistics of the Jitter Buffer, enter the following command:

```
NPE> stats voice jitterbuffer
```

- The display will be similar to the following:

```
Jitter Buffer Stats:
```

	Port	Frames Duplicated	OverFlow	OutSeq	NullPkts
		CurrElem	UnderRun	Dropped	LatePkts

1	0		0	0	0
	0		0	0	0
2	0		0	0	0
	0		0	0	0
3	0		0	0	0
	0		0	0	0
4	0		0	0	0
	0		0	0	0

Following are descriptions of the information fields:

- **frames**
Number of frames played out
- **currelem**
Number of elements in the jitter buffer.
- **overflow**
Number of times jitter buffer overflowed.
- **underrun**
Number of times jitter buffer under-runs.
- **outseq**
Number of out of sequence packets.
- **dropped**
Number of dropped packets.
- **nullpkts**
Number of null packets.
- **latepkts**
Number of late dropped packets.
- **duplicated**
Number of duplicate packets dropped.

Configure MGCP UA

Configuring MGCP UA is to define the following:

- How to be authenticated to the MGCP server
- Which CODEC(s) are supported for negotiation purposes
Up to 4 CODECs can be configured: codec1, codec2, codec3 and codec4. Codec1 is the first preferred choice while codec4 is the last preferred one.
CODEC can be set to either G.711 u-law, G.711 a-law or G.729 with 10ms or 20ms RTP packet interval.
- To activate specific features (RFC 2833 for DTMF, modem pass-through or fax pass-through) depending on the analog device (telephone, modem or fax) connected to the phone port.
In the case of a modem, the port can be configured:
 - To not support such device type (MPT OFF)
 - To support such device and force media to G.711 Echo Cancellation (MPT ON)
 - To support such device type and enable re-negotiation of the CODEC with the remote party when modem tone is detected (MPT AUTO).
 In the case of a fax, the port can be configured as follows:
 - To not support such device type (FAX OFF)

- To support such device and force media to G.711 Echo Cancellation (FAX CC_ON)

Currently, the following feature is not supported:

- Fax T.38

Configuration Requirements

The MGCP Session Controller must be configured. See "Configuring MGCP Session Controller" on page 209.

The MGCP protocol and the FXS port should be configured before setting up the MGCP UA. See "MGCP Protocol" on page 226 and "Configure FXS Port" on page 226.

Configuration Restraints

A codec that configured as NOTUSED will act as a terminator in the preferred codec list; subsequent codecs will be ignored.

For example, if the codec parameters are set as below, codec3 and codec4 will be ignored by ICAD80; they will not be implemented.

```
codec1 PCMU_10
codec2 NOTUSED
codec3 PCMU_20
codec4 PCMA_20
```

Configuration Commands

```
NPE> config mgcp ua port
```

Table 94 describes the parameters for `config mgcp ua port`.

Table 94 MGCP User Agent Configuration Parameters

Parameter	Description
[Port]	A valid FXS interface port number
name	The friendly display name
userID	User ID to form the MGCP Endpoint ID
codec1	The first codec and packet time selection (PCMU_10 PCMU_20 PCMA_10 PCMA_20 G729A_10 G729A_20 NOTUSED)
codec2	The second codec and packet time selection (PCMU_10 PCMU_20 PCMA_10 PCMA_20 G729A_10 G729A_20 NOTUSED)
codec3	The third codec and packet time selection (PCMU_10 PCMU_20 PCMA_10 PCMA_20 G729A_10 G729A_20 NOTUSED)
codec4	The fourth codec and packet time selection (PCMU_10 PCMU_20 PCMA_10 PCMA_20 G729A_10 G729A_20 NOTUSED)
rfc2833	Whether to use RFC2833 for DTMF
payload	RFC2833 payload type (PT)
mpt	Modem pass-through (MPT) (Off On)
fax	Fax Relay mode (Off CC_ON)
up	Whether the MGCP UA port is enabled

Configure MGCP UA

This example configures the MGCP User Agent for an analog telephone as follows:

Name: uap1
User ID: uap1
RFC2833 DTMF: yes
RFC2833 payload type: 96
Enabled: yes

- 1 Enter the following command:

```
NPE> config mgcp ua port 1 name uap1 userid uap1 rfc2833 yes payload 96
running
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Show Configuration

- To show the configuration of the MGCP UA, enter the following command:

```
NPE> show mgcp ua port 1
```

- The display will be similar to the following:

MGCP User Agent:

Port	Name UserID	Codec1 Codec2	Codec3 Codec4	RFC2833 Payload	MPT Fax	VAD Running
0-1	7001	pcmu_20	G729A_20	yes	Off	no
	4083747001	pcma_20	NOTUSED	96	Off	no

Show Status

The following command shows the status of the MGCP UA.

- To show the status of the MGCP UA, enter the following command:

```
NPE> show mgcp ua status
```

- The display will be similar to the following:

MGCP UA Ports:

Port	LineStatus
0-1	Inactive

Following are descriptions of the information fields

- LineStatus reports the status of the analog device:
 - Idle: the analog device is on-hooked
 - OB (OutBound) Calling: the analog device is off-hooked or a phone number is being dialed
 - OB (OutBound) Proceeding: the remote party rings
 - IB (InBound) Proceeding: the analog device rings
 - Disconnecting: the remote party is disconnected
 - Connected: the analog device is in communication

The following command shows the status of the VoIP communication terminating the MGCP UA.

- To show the status of the VoIP communication terminating the MGCP UA, enter the following command:

```
NPE> show media stream
```

- The display will be similar to the following:

```
Media Stream
```

```

Index Channel Codec Allocated Codec Used Codec State Connection Packet
-----
0      0      G711u, G711a, * G711u      STARTED      RTP(rx/tx)*

```

Following are descriptions of the information fields:

- index/channel 0/0
Represents the FXS port.
- Codec Allocated
Reports the CODEC(s) offered during the MGCP/SDP negotiation.
- Codec Used, Codec State Connection
Report the status of the communication. In this example the connection is started and uses CODEC G.711 u-law.

Show Call Statistics

This section provides references to commands to visualize call statistics. These commands are independent from the Signaling protocol used to establish calls, MGCP or SIP.

Show Commands

```
NPE> show calls current
```

Table 95 describes the information displayed by `show calls current`.

Table 95 Current Calls

Parameter	Description
aname	A Party name identifier
anumber	A Party number (if known)
bname	B Party name identifier
bnumber	B Party number (if known)
type	Where the call is originating from
state	Current state of the call
protocol	What protocol the calling party is using
quality	RTCP-XR derived MOS quality scores (MOS-LQ/MOS-CQ)
starttime	Start time of the call
duration	Time elapsed since start of the call

```
NPE> show calls history
```

Table 96 describes the information displayed by `show calls history`.

Table 96 Call History

Parameter	Description
<code>aname</code>	A Party name identifier
<code>anumber</code>	A Party number (if known)
<code>bname</code>	B Party name identifier
<code>bnumber</code>	B Party number (if known)
<code>type</code>	Where the call is originating from
<code>state</code>	Current state of the call
<code>protocol</code>	What protocol the calling party is using
<code>quality</code>	RTCP-XR derived MOS quality scores (MOS-LQ/MOS-CQ)
<code>starttime</code>	Start time of the call
<code>duration</code>	Time elapsed since start of the call

Show Current calls

- To show the current calls, enter the following command:

```
NPE> show calls current
```

- The display will be similar to the following:

Call List:

A Party A Number	B Party B Number	Type State	Protocol Quality	Start Time Duration
Sophia 6017 6017	6016,Sophia 6016	Outbound Connected	MGCP 4.20/4.18	FEB 24 03:24:24 2006 13 seconds

Following are descriptions of the information fields:

- Type
Reports if the call is originated from LAN (OutBound) or from WAN (InBound).
- State
Reports the state of the call:
 - Proceeding: the call is in progress
 - Connected: the call is established
 - Failed: the call terminated abnormally
 - Succeed: the call terminated normally

The field `Quality` reports the quality of the stream coming from WAN. It reports a MOS. In the case the CODEC used is not supported by Voice Quality Monitoring (see "Voice Quality Monitoring (VQM)" on page 221) or no RTP traffic is received, this field reports "Not measured".

Show Call History

- To show the call history, enter the following command:

```
NPE> show calls history
```

- The display will be similar to the following:

Call History:

A Party	B Party	Type	Protocol	Start Time
A Number	B Number	State	Quality	Duration

Sophia 6017	6016,Sophia	Outbound	MGCP	FEB 24 03:24:24 2006
6017	6016	Succeed	4.20/4.18	13 seconds

Following are descriptions of the information fields

- History can be filled with up to 250 entries. It is filled in a FIFO mode; the last call is inserted at the end.
- The fields are the same as described in "Show Current calls" on page 233.

Configuring MGCP Endpoints

This section provides guidelines to configure MGCP endpoints located in LAN.

For a MGCP endpoint to place and receive calls, the following are required:

- The MGCP endpoint must be allowed by Access Control List (ACL).
- The MGCP endpoint must be registered to the MGCP server through the MGCP SC.
- The MGCP UA must be considered as a normal MGCP endpoint located in LAN.

Access Control List (ACL)

To configure Access Control List, refer to "Access Control List (ACL)" on page 215.

For the MGCP UA Access Control List does not need to be configured. The MGCP UA is automatically allowed to place and receive calls. It cannot be disallowed.

Registration

The MGCP endpoints need to be registered to the MGCP server through the MGCP SC using the MGCP method RSIP.

To make this happen, the MGCP endpoints must be configured as following:

- MGCP endpoint identification must be per MAC address.
- MGCP Call Agent must be the LAN IP address of the ICAD80.
- MGCP Call Agent port must be the one configured to the one configured in the MGCP SC (LAN Rx port).

For information for a Cisco MGCP phone 7960, firmware POM3-07-5-00, the following configuration would be required (interactive menu or text configuration file):

- **use_mac_name:** 1 (enabled)
- **mgcp_gw_controller:** LAN IP address of the IACAD40
- **mgcp_output_port:** LAN RX port of the MGCP SC

When the phone is correctly registered, it is reported by the command `show mgcp sc endpoints`. An example follows.

MGCP Session Controller endpoints:			
Endpoint ID	EP Addr	EP Port	Act Calls
Endpoint Name	TelNo	CA Port	Timeout

4083746017@00152b177677	10.0.1.57	2427	0
Sophia 6017	6017	2432	3436

To configure the registration of the MGCP UA refer to "Configuring MGCP User Agent" on page 225. The command `show mgcp sc endpoints` would report the following when it gets successfully registered to the MGCP server.

MGCP Session Controller endpoints:

Endpoint ID	EP Addr	EP Port	Act Calls
Endpoint Name	TelNo	Lan Domain	Timeout

4083747001@001111111111	127.0.0.1	2429	0
		2429	3434

The information that identifies the MGCP UA is `AP Addr`, which is set to the loopback IP address 127.0.0.1.

12

VoIP SURVIVABILITY

This chapter provides information about VoIP survivability: LCR configuration for SIP and MGCP signaling protocols; lifeline failover for power outage.

Introduction

This section provides guidelines for configuring the ICAD80 for local call routing (LCR), also known as VoIP Survivability, which supports the following features:

- Ensures emergency calls are routed to the external voice network
- Ensures local calls

Local Call Routing

When the VoIP service is unreachable, LAN endpoints normally cannot make calls; they cannot reach destinations on either the LAN or the WAN. This may occur in the following scenarios:

- The VoIP server is unreachable from the ICAD80
Signaling packets cannot be sent to the VoIP server.
- The VoIP service goes down
Calls are sent out, but calls/replies cannot be received. If one server is available, failover can be used to continue operation. See page 172 for SIP failover mode, and page 208 for MGCP failover mode. However if all servers are down, VoIP service will be unavailable.

When VoIP service is unreachable, the ICAD80 switches to LCR mode. Calls originated from LAN VoIP phones or from the Integrated User Agent can still be routed to another VoIP phone, an Integrated User Agent, or the PSTN through the FXO port or the SIP gateway. When LCR takes place, only basic telephone services are supported.

- Local calls (between LAN endpoints) are established through the ICAD80, acting as a VoIP server (SIP server or MGCP Call Agent).
- Calls identified as external calls are routed to PSTN through the FXO interface of the ICAD80, or through a SIP/PSTN gateway located in the LAN.

When a VoIP server is again reachable and available, the ICAD80 returns to the normal (VoIP) mode for calls.

Lifeline Failover

Should the ICAD80 lose power, all FXS ports are physically switched to one FX0 port; this allows receiving and sending external calls.

When power is down, the ICAD80 is non-operational; functions such as VoIP and QoS configurations are not supported.

Local Call Routing

This section provides guidelines for configuring Local Call Routing.

Configuration Requirements

SIP or MGCP Session Controllers must be configured. For SIP, see Chapter 10, “SIP Configuration”. For MGCP, see Chapter 11, “MGCP Configuration”.

Configuration Main Menu

```
NPE> config lcr accounts
```

Table 97 describes the parameters of `config lcr accounts`.

Table 97 LCR Configuration Main Menu

Parameter	Description
[dn]	Dial Number of the account
type	Type of the account (SIP MGCP)
id	ID of the account

The CLI command `lcr accounts` informs ICAD80 the location of a local endpoint, when the user ID /endpoint ID does not contain information about the telephone number. For example, when a SIP account is defined by a name string, this command tells the ICAD80 the telephone number of that account.

```
NPE> config lcr settings
```

Table 98 describes the parameters of `config lcr settings`.

Table 98 LCR Configuration Main Menu

Parameter	Description
lcbmode	Local Call Backup Mode (INT LGW)
ecnumber	Emergency Call Number
obaccess	Outbound access digit
areacode	Area code of this installation
coprefix	Central Office Prefix of this installation
enlength	Extension Number Length

Following are details of the parameter:

- `lcbmode`
How to route an external call: specifies if external calls are established through the FX0 port of the ICAD80 (INT) or through a VoIP/PSTN gateway (LGW) co-located on the LAN.

MCGCP gateways are not supported.

- `ecnumber`

Emergency number, at the installation location, used by session controller. `ecnumber` is used to route the emergency call externally. This parameter can also be used to assure bandwidth during normal operations (non-LCR).

- `obaccess`, `areacode`, `coprefix`, `enlength`

Number information about the location; identifies if a dialed number is destined for a local endpoint. These parameters should be set to accurately reflect the number plan; when VoIP is available, using an outbound number makes an outside call (`obaccess`), and/or automatically checking the first digits for an internal call (`enlength`) when an outbound number is not entered by the caller.

- `obaccess` only applies for hosted PBS service. In this situation, outbound calls are provided by dialing an outbound prefix, such as 9 555 1212. Otherwise, leave this value blank.

- `areacode`, `coprefix`, and `enlength` define a complete telephone number plan, specified for local accounts. For example: 408 374 1001.

408 indicates `areacode`

374 indicates `prefix`

1001 indicates external subscriber

All these parameters should be used; they help LCR identify if a telephone number is a local endpoint. A configuration example is provided in "Example 2" on page 240.

Configure LCR Accounts

Configuring LCR accounts is not always required.

LCR accounts are not required if the IDs of the LAN endpoints are numbers.

LCR accounts are needed if the IDs of the LAN endpoints are alphanumeric. In this case, to contact the LAN endpoints, the ICAD80 (acting as a VoIP server) needs to know the telephone numbers of the endpoints.

If not configured, only VoIP phones that allow entering alphanumeric IDs can place calls, not other entities, such as the User Agent.

This example creates an entry as follows:

Phone number: 5555 (dial four digits to connect to an office telephone: local endpoint)

SIP ID: `call.five`

- 1 Enter the following command:

```
NPE> config lcr accounts 5555 type SIP id call.five
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Configure LCR Settings

Configuring the LCR settings is only required to make calls through the FXO port of the ICAD80 or through a SIP VoIP/LAN gateway located in LAN.

The advantage of the latter solution (via gateway in LAN) is multiple calls can be active, whereas in the first case (via FXO port), only one call can be active.

Example 1

The following example configures the FXO port to handle emergency calls.

- 1 Enter the following command:

```
NPE> config lcr settings lcbmode INT
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

Example 2

The following example uses the prefix “9” for outbound calls. The setup is as follows:

```
prefix for outbound calls: 9
area code: 408
company office prefix: 374
length of extension number: 4
```

- 1 Enter the following command:

```
NPE> config clr settings obaccess 9 areacode 408 coprefix 374
enlength 4
```

- 2 To save the configuration, enter:

```
*NPE*> save
```

This configuration will support calls as follows:

Number dialed Action

```
2210 4-digit call, check local accounts only
9411 outbound call for 411
93742210 check local accounts only for 2210
96872210 route 6872210 to PSTN
914083472210 check local accounts only for 2210
914086872210 route 14086872210 to PSTN
```

Show Configuration

- To show the results of the LCR account configuration, enter the following command:

```
NPE> show lcr accounts
```

- The display will be similar to the following:

LCR Accounts:

DN	Type	ID
2222	SIP	call.two
4444	SIP	call.four
5555	SIP	call.five

- To show the results of the LCR settings, enter the following command:

```
NPE> show lcr settings
```

- The display will be similar to the following:

LCR Settings:

LCBMode	ECNumber	OBAccess	AreaCode	COPrefix	ENLength
INT	911	9			4

Show Status

The Session Controller either runs in normal mode (all calls are established through a VoIP server) or in LCR mode (local calls and emergency calls are handled by the ICAD80, acting as a VoIP server; other calls are rejected).

- To show the status of the LCR mode, enter the following command (example for SIP):

```
NPE> show sip sc status
```

- The display will be similar to the following:

```
SIP Session Controller status:

      SSC Started           Yes
      SSC Server Ready     No
      My Wan IpAddr        0.0.0.0
      Wan Rx Port          5060
      Lan Rx Port          5060
      CAC Max Calls        500
```

Following are descriptions of the information fields

- **SSC Server Ready**

Yes: Session Controller runs in normal mode.

No: Session Controller runs in LCR mode.

Show Connections

- To show the connections established in LCR mode, enter the following command:

```
NPE> show lcr connection
```

- The display will be similar to the following:

```
Connection List:
```

Caller	Called	To	Type
call.two	call.five	5555	Internal

Following are descriptions of the information fields:

- **Caller, Called**

The Identifiers of the source and destination of the call, respectively.

- **To**

The phone number that was called.

- **Type**

Reports if the call is established between two LAN endpoints or between a LAN endpoint and the PSTN. Note that a LAN endpoint can also be the Integrated User Agent.

Lifeline Failover

If the ICAD80 loses power, all FXS ports are physically switched to one FXO port; this allows receiving and sending external calls, including emergency calls.

When power is down, all 16 FXS ports are connected to one FXO port; on the breakout box, ports 1–16 (FXS) will be physically connected to port 17 (FXO). This connectivity creates a *party line*.

- Only one FXS port can dial out or receive a direct call
- When one FXS port is connected to an outside call, all other FXS ports can access that connection

Figure 6 illustrates lifeline failover connectivity.

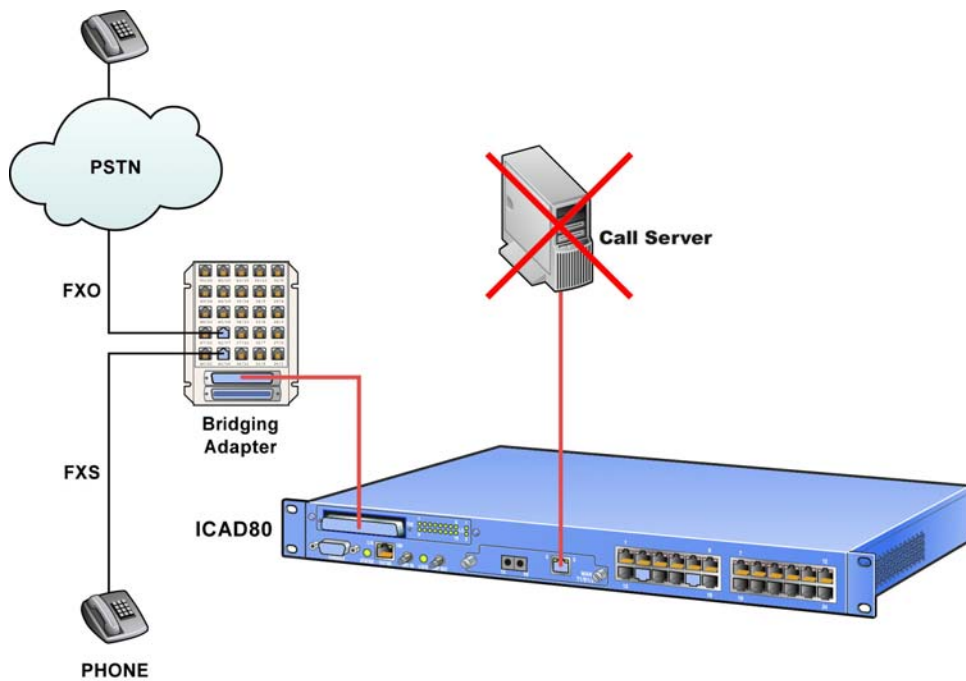


Figure 6 Power Failure

If power failure occurs, the ICAD80 will automatically use the FXO lifeline to route calls from the FXS ports directly to PSTN.

A

UPGRADE SOFTWARE

This appendix provides information for upgrading ICAD80 software.

Introduction

The software that can be upgraded or re-installed in a ICAD80 are the application (image) and the bootloader code. This process is supported by Web UI, a feature of ICAD80.

For more information about Web UI, see Appendix B, "Web UI".

Check Boot Code

It is recommended to check the current version of bootloader code in the ICAD80. At the release of this document, version 9 (X.XX.0009) or greater should be used when upgrading software. For instructions to check the version of bootloader code, see "View Bootloader Code" on page 306.

If the bootloader code must be upgraded, see "Upgrading Software Via Web UI" on page 303.

Table 144 *File Names*

File Type	File Name
Image	app.bin
Bootloader	boot.bin

Images

Two images can be stored in ICAD80 in locations slot 1 and slot 2 on the compact flash. This feature allows you to save an image when upgrading the application software.

Only one image can be primary (default): the image that is used to run ICAD80. The other image is secondary: an alternate image that you can select to run, should it be necessary. For instructions to select which image is default, see "Change Default Application Image" on page 306.

Upgrading Software Via Web UI

This section provides instructions to upgrade the application or bootloader software of the ICAD80. Your workstation can access the ICAD80 through the Internet or a LAN connection.

This procedure assumes the ICAD80 has been physically installed in the network and is operational.

Requirements

- The Internet browser on your workstation must be either Microsoft Internet Explorer or Mozilla FireFox.
- The IP address of the ICAD80 must be known.
- The name of the upgrade software file must be known.

-
- The location of the file must be known. e.g., it must be available at a known location on your workstation.
To acquire the upgrade software, contact your IT manager or Customer Support.
- The instructions follow.

Upgrade Software via Web UI

Login

- 1 Enter the IP address of the ICAD80 on the web browser, which can be done via HTTP or HTTPS:
 - HTTP
Enter the IP address using http:
<http://xxx.xxx.xxx.xxx>
 - HTTPS
Enter the IP address using https:
<https://xxx.xxx.xxx.xxx>The login window opens, requesting your user name and password. See Figure 7.

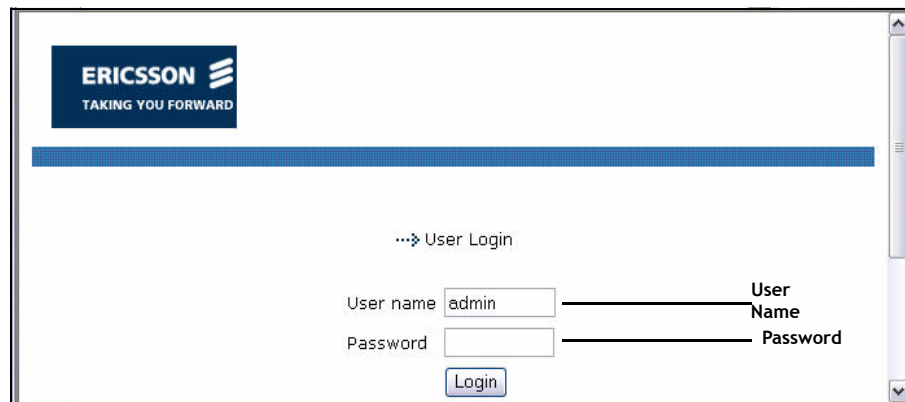


Figure 7 Web UI Login Window

- 2 Enter your user name and password in the appropriate text boxes: Name, Password.
The default name is [admin](#).
The default password is [admin](#).
NOTE: The password is case sensitive.
- 3 Press the Login button.
WEB UI opens with the System Screen, which shows current system statistics.

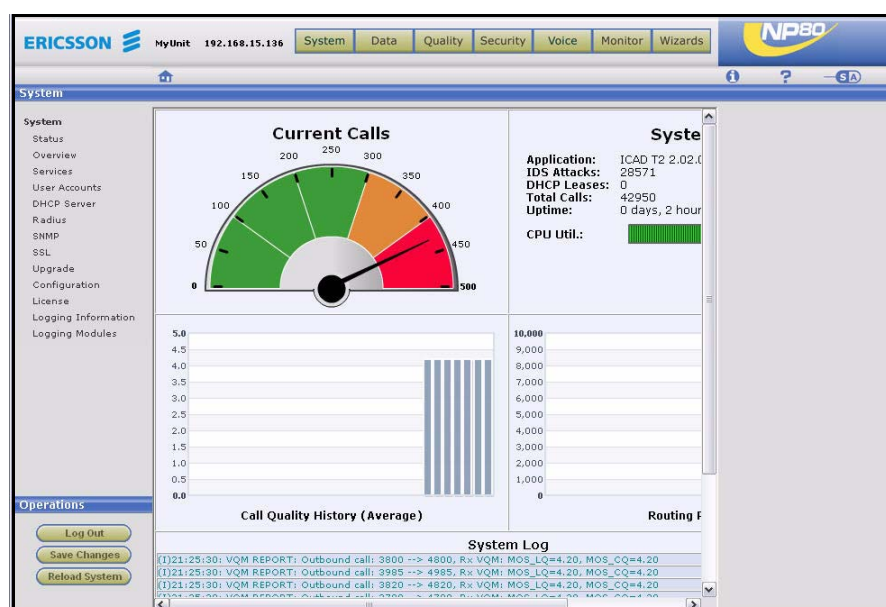


Figure 8 Default Window after Login

4 Logging in is complete.

Upgrade Software

5 Under the configuration menu, select upgrade. See Figure 9.

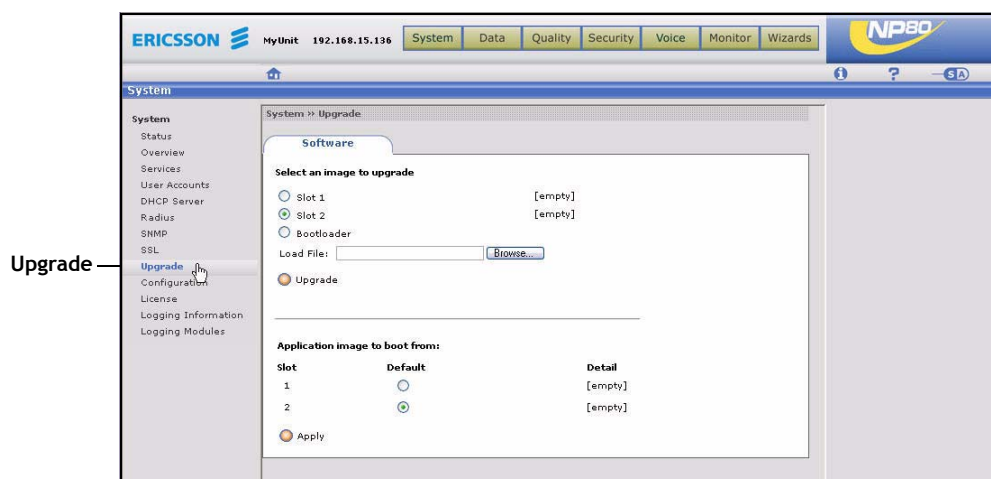


Figure 9 Upgrade Image

6 In the Upgrade tab, select which image (slot) to upgrade:

- » Slot 1 and Slot 2 represent the application software (images) that are present on ICAD80.
- » The image (slot) that is upgraded is automatically set as the (default) image the ICAD80 runs on. After installation, the default image can be changed. (Refer to "Change Default Application Image" on page 306.)
- » Bootloader represents the application that loads in the new image.

7 In the Load File text box, select the file to upload.

If necessary, use Browse to locate the file.

- 8 Click the **Upgrade** button.
Several messages will display.
When the upgrade is complete the message **Updated** will appear.
- 9 To complete the upgrade, reboot the ICAD80. To do so, select the **Reset System** button under Operations. See Figure 10.

IMPORTANT: Do not reboot the ICAD80 until after the **Updated** message is displayed.

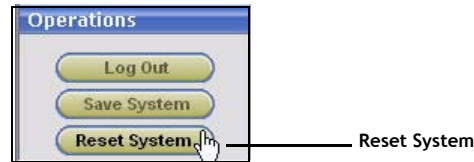


Figure 10 Reset System

- 10 Upgrading the software is complete.
NOTE: When the ICAD80 reboots, the Internet connection will be lost.
To re-connect to the unit, you will have to login. See "Login" on page 304.
- 11 It is recommended to verify the software was successfully installed. See "Verify Software Installation" on page 306.

Verify Software Installation

- 1 If you are already logged in, proceed to the next step. Otherwise, login to the ICAD80 through the Web UI. See "Login" on page 304.
- 2 On the menu bar, select **System**. See Figure 11.

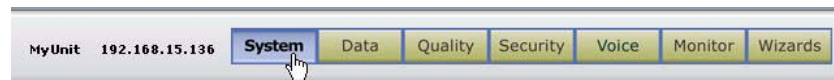


Figure 11 Menu Bar

- 3 Under the configuration menu, select **Upgrade**. See Figure 9 on page 305.
- 4 Under the section **Application image to boot from:**, the current image files will be listed under **Detail**.
Under **Default**, the highlighted button indicates which image is set for default.
- 5 This procedure is complete.

Change Default Application Image

- 1 If you are already logged in, proceed to the next step. Otherwise, login to the ICAD80 through the Web UI. See "Login" on page 304.
- 2 On the menu bar, select **System**. See Figure 11 on page 306.
- 3 Under the configuration menu, select **Upgrade**. See Figure 9 on page 305.
- 4 Under the section **Application image to boot from:**, select the desired image for default. To do so, select the appropriate button under default. See Figure 9 on page 305.
- 5 Select the button **Apply**.
- 6 This procedure is complete.

View Bootloader Code

- 1 If you are already logged in, proceed to the next step. Otherwise, login to the ICAD80 through the Web UI. See "Login" on page 304.

- 2 On the menu bar, select **System**. See Figure 11 on page 306.
- 3 Under the configuration menu, select **Overview**. See Figure 9 on page 305.
 - The System Information section will show the version of the bootloader software.
 - The version of the default application will also be displayed.

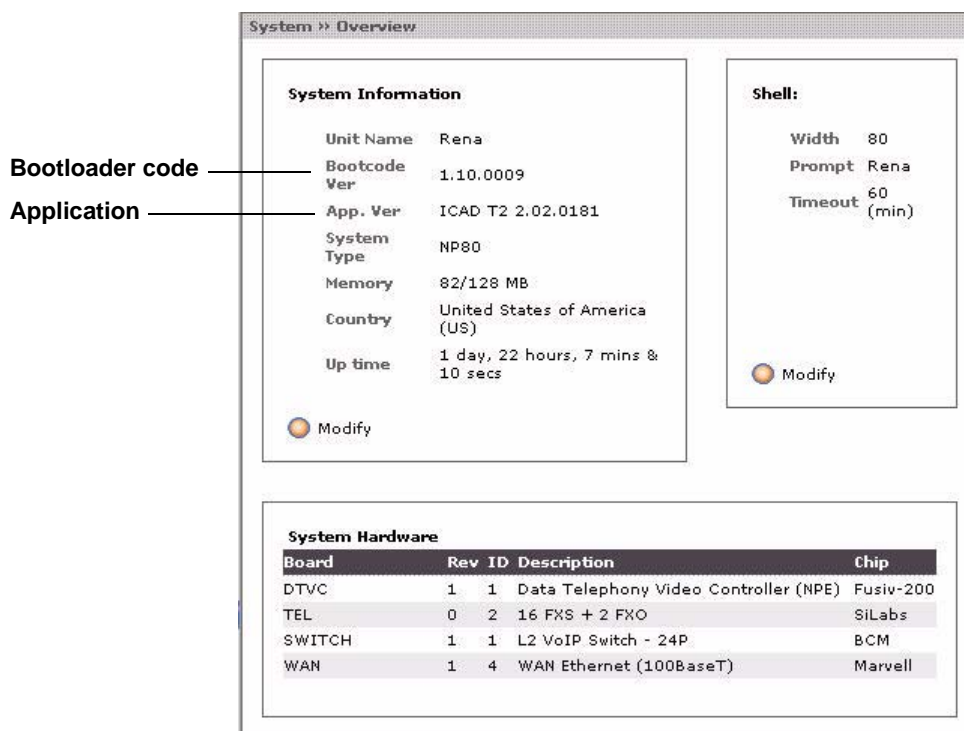


Figure 12 Software System Overview

- 4 This procedure is complete.

Find IP Address via CLI

This procedure assumes the following:

- Your PC is connected to the CONSOLE port of the ICAD80 through a serial port cable
- Tera Term Pro, or a similar terminal emulator, is running on your PC.

NOTE: This procedure uses Tera Term Pro.

For information about third-party software, see Appendix C, “Third Party Software”.

- 1 On the PC, connect to the ICAD80 through the terminal simulator. See Figure 13.
 - a Select **File**, and then, **New Connection** from the menu bar.
 - b In the window that opens, *Tera Term: New Connection*, select the **Serial** button.
 - c Select the appropriate **COM Port**.
 - d Click **OK**.



Figure 13 Connect to ICAD80

- 2 The monitor will display the following:

User:

- 3 Enter the default user name: **admin**.

The response will be as follows:

Password:

- 4 Enter the default password: **admin**.

The prompt will appear: NPE>

NOTE: The prompt may after system information has been displayed.

- 5 Enter the following command:

NPE> **show interface IP**

- 6 The display will be similar to the following:

"eth0" info: [WAN Port]

```

Interface          eth0
Flags              (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP
MULTICAST >
IP Address/Mask    172.16.1.217/255.255.255.0
MTU                1500
DHCP               off
Lease obtained     N/A
Lease expires      N/A
MAC Address        00:15:93:FF:00:F8
Speed              AUTONEG

```

"eth1" info: [LAN PORT]

```

Interface          eth1
Flags              (A843) < UP BROADCAST RUNNING SIMPLEX LINKUP
MULTICAST >
IP Address/Mask    192.168.1.1/255.255.255.0
MTU                1500
DHCP               off
Lease obtained     N/A
Lease expires      N/A
MAC Address        00:15:93:FF:00:F9
Speed              N/

```

"fr0" info: [T1 WAN PORT]

```

Interface          fr0

```

Flags	(20C1) < UP RUNNING NOARP LINKUP >
IP Address/Mask	10.12.0.1/255.255.255.0
MTU	4096
DHCP	off
MAC Address	00:00:00:00:00:00
Speed	N/A

7 This procedure is complete.

- If connecting to the ICAD80 through the WAN port, use the eth0 or the T1 address.
- If connecting to the ICAD80 through a LAN port, use the eth1 address.

A

- access control 61
 - Access Control List. See ACL
 - account
 - add user 62
 - remove group 66
 - remove user 65
 - ACL 163, 195
 - authentication 164, 196
 - configure 195
 - SIP UA 183
 - Acrobat Reader 311
 - add
 - ARL 105
 - group 64
 - static route 95
 - address forwarding
 - NAT 128
 - address learning process 105
 - Address Resolution Logic. See ARL
 - Address Resolution Protocol. See ARP
 - admin
 - default password 62
 - admin accounts
 - default setting 41
 - admin groups
 - default setting 41
 - admin rights
 - default setting 42
 - aging time 105
 - alarm
-

- frame relay 74
 - LEDs 73
- ALG
 - configure 132
- ALL 54
- Application Layer Gateway. See ALG
- ARL
 - add 105
 - add entry 105
 - aging time 105
 - configure 105
 - entries 105
 - flush 107
 - remove 107
 - remove entry 107
- ARP
 - configure 93
 - delete 94
 - flush table 95
 - subnetwork 93
 - table 93
- audit logging
 - configure 257
- authentication 241
 - ACL 164, 196
 - RADIUS client 241
 - user management 61
- authenticationfail 276
- auto
 - download files 251
- automatic mode
 - SIP server 152
- B**
- back pressure 100
- bandwidth
 - control, GoS 438
- BE 439
- Best Effort. See BE
- C**
- CAC
 - configure 199
 - maximum calls 201
 - QoS 199
- cache
 - delete TFTP 252
 - file 250
 - TFTP 251
- Call Admission Control. See CAC
- call history 182
- call server
 - keep-alive 186
- CAR 145
- CDP
 - configure 284
- CDP packets
 - monitor 284
- change password 67
- check DNS client 88
- Cisco Discovery Protocol. See CDP
- classification 438
- CLI
 - auto run command 59
 - command groups 49
 - command keyword
 - all 54
 - custom help 50
 - debug
 - help 51
 - debug commands 48, 49
 - help
 - <tab> 50
 - ? 50
 - specific 50
 - interactive mode 53
 - keyword
 - no 53
 - maintenance commands 47, 49
 - help 51
 - on-line help 47
 - prefixes 49
 - save configuration 59
 - syntax 52
 - valid prefixes 50
 - variables 50
- client
 - DNS 87
- CODEC
 - MGCP VQM 202
 - VQM 169
- coldstart 276
- configuration
 - dump 54
 - save 59
- configure
 - ACL 195
 - ALG 132
 - ARP 93
 - ARP flush table 95
 - audit logging 257
 - CAC 199
 - CDP 284
 - DHCP relay 246
 - DHCP server 243

- DNS client 87
- DNS relay 246
- dynamic routing 96
- file system 225
- firewall 118
- firewall (security policies) 118
- FxS port 206
- host keys, regenerate 229
- IDS 121
- IDS anomaly 122
- IDS flood 123
- IDS scan 124
- IDS spoof 125
- interface
 - eth0 71
 - eth1 70
 - NAT 129
 - vlan 81
- LCR accounts 219
- LCR settings 219
- LMI 77
- logging destination 261
- logging level 259
- MBR 193
- MCGP MSP 190
- MGCP ACL 214
- MGCP endpoints 214
- MGCP fail-over 188
- MGCP server 187
- MGCP session controller 189
- MGCP UA 209
- MGCP user agent 205
- MGCP VQM 201
- NAT 128
 - address forwarding 130
 - port forwarding 130
 - static 131
- NAT interface 129
- NAT policy 129
- NAT port forwarding 133
- NAT public 131
- netflow 273
- permanent virtual circuit 74
- port mirroring 107
- QoS 138
 - DiffServ/ToS 111
 - IEEE 802.1p 111
 - port 111
 - priority 112
 - traffic classification 143
- QoS layer 2 109
- QoS quality group 141
- QoS traffic classification 142
- QoS type 112
- quality groups 139
- RADIUS client 241
- routing table 95
- security
 - NAT 133
- SIP
 - additional servers 153
- SIP ACL 163
- SIP CAC 166
- SIP endpoints 183
- SIP fail-over 152
- SIP load balance 153
- SIP Media BRidge (MBR) 161
- SIP server 151
- SIP session controller 156
- SIP SSP 157
- SIP VQM 168
- SNMP 276
- SNMP trap 279
- SNTP relay 248
- SNTP time 87
- SSH host keys 232
- SSH server 231
- SSL certificate 235
- SSL CSR 235
- SSL key 235
- static route delete 96
- static routing 95
- telnet server 224, 230, 231, 238, 240, 246, 247, 248
- TFTP cache 250, 251
- TFTP relay 249
- time 85
- VLAN 112
 - LAN 114
 - WAN 114
- VLAN interface 80
- WAN port 102
- watchdog 89
- web server 233, 237
- Configuring 71
- Connection Protocol 313
- connection timeout 120
- console
 - logging destination 261
- CSR 234
- customer support
 - hardware system 90
- D**
- debug
 - system exceptions 89

- debug commands
 - syntax 52
- default password
 - admin 62
 - user 62
- default setting
 - admin accounts 41
 - admin rights 42
 - admins group 41
 - disabled 45
 - enabled 44
 - eth0 41
 - eth1 41
 - IP interface 41
 - LAN port 100
 - media 43
 - QoS layer 2 44
 - security policies 42
 - security policy
 - LAN to ICAD40 42
 - LAN to WAN 42
 - telnet WAN to ICAD40 43
 - Web UI LAN to WAN 43
 - Web UI WAN to ICAD40 43
 - ssh/sftp 44
 - telnet 44
 - user accounts 41, 42
 - user group 41
 - userbasic rights 42
 - voice ACL 43
 - voice parameters 42
 - WAN port 103
 - web server management 44
- delete
 - ARP entry 94
 - TFTP cache 252
- DHCP
 - eth0 interface 71
 - option 42 248
 - option 6 247
 - option 66 249
- DNS
 - primary server 88
- DNS client
 - check 88
 - configure 87
- documentation feedback 2
- DSA host keys 228, 232
 - regenerate 232
- dump
 - show configuration 54
- dynamic routing
 - configure 96

E

- Endpoint Status Handling. See ESH
- ESH 165
 - SIP 165
- eth0
 - default setting 41
 - DHCP 71
- eth1
 - default setting 41
- exception
 - system 256
 - system error 90
- exceptions
 - system 89

F

- fail-over
 - MGCP server 188
 - SIP server 152
- failover
 - lifeline 221
- feedback, documentation 2
- file
 - cache 250
 - logging destination 262
- file system
 - management 225
- firewall
 - connection timeout 120
 - remove 120
 - rules 119
 - security policies 118
- flow control
 - back pressure 100
 - LAN 100
 - pause frames 100
 - QoS 100
 - QoS constraints 110
 - WAN 103
- flush
 - ARL 107
 - ARP table 95
- forwarding database
 - remove ARL 107
- frame relay
 - LMI 77
- front port 99
- FTP
 - download files 251
- FxS
 - port 206

G

- GoS 435
 - classification 438
 - multiplexing 439
 - policing 438
 - processes 437
- GoS classes 138
- group
 - add 64
 - remove 66
- Guarantee of Service. *See* GoS

H

- hardware
 - monitor 255
- history
 - call 182
- http
 - connection timeout 121

I

- ICAD40
 - connectivity 41
 - description 40
- ICMP
 - statistics 266
- IDS
 - anomaly 121, 122
 - clear statistics 127
 - configure 121
 - flood 121, 123
 - log 128
 - scan 121, 124
 - spoof 121, 125
 - statistics 125
- IEEE 802.1p
 - QoS
 - priority queue 109
- Interface
 - eth1 70
 - WAN 71
- interface
 - eth0 71
 - LAN 70
 - lan 70
 - NAT 129
 - VLAN 80
 - WAN 71
- internal
 - logging destination 262
- intrusion detection service. *See* IDS
- IP
 - connectivity services 239

- default settings 41
- routing stack 264
- stack statistics 264

- IP address
 - VLAN 80

- IP host
 - uplink 99

K

- keep-alive
 - MGCP 186
- keepalive 190
- key
 - CSR 234
 - DSA 228
 - DSA host 232
 - upload public 229, 233

L

- LAN
 - ARL 105
 - port mirroring 108
 - VLAN 114
- LAN port
 - default settings 100
 - statistics 102
- LCR 217
 - accounts 219
 - settings 219
- LED
 - loss of carrier 73
 - loss of synchronization 73
 - master mode 73
 - slave mode 73
- lifeline failover 221
- link
 - QoS 138
- linkdown 276
- linkup 276
- LMI 77
- Load Balance
 - SIP 153
- Local Call Routing. *See* LCR
- Local management interface. *See* LMI
- log
 - IDS 128
- logging
 - map 260
 - system security 257
- logging destination
 - configure 261
- logical links
 - MGCP 185

- login
 - default password
 - admin 62
 - user 62
- M**
- MAC address
 - ACL 164
 - ARL 105
 - learning process 105
- maintenance commands
 - syntax 52
- management
 - GoS 436
- manual mode
 - SIP server 152
- map
 - ARL 105
- MBR
 - configure 193
 - status 194
- Media 185
- media
 - default setting 43
- Media BRidge (MBR) 161
- Media Gateway Control Protocol. See MGCP
- messages
 - syslog server 262
- MGCP
 - keep-alive 186, 190
 - relay headers 190
 - server
 - priorities 187
 - services 186
 - session controller 186, 189
 - signalling messages 190
 - signalling proxy 190
 - statistics 201
 - user agent 186
 - VQM 201
- MGCP Signaling Proxy. See MSP
- MGPC protocol 206
- mii
 - port 99
- mii0
 - WAN port 102
- monitor
 - CDP packets 284
 - customer support 255
 - logging level 259
 - MGCP voice quality 202
 - netflow 273
 - operation details 258
 - operation errors 258
 - operation information 258
 - PMON 270
 - SNMP 276
 - system exception 256
 - system hardware 255
 - system information 256
 - system module 258
 - system operations 257
 - voice quality 284
- MSP 190
- multiplexing
 - GoS 439
- N**
- NAT
 - address forwarding 128
 - configure 128
 - configure address forwarding 134
 - configure security 133
 - policy 129
 - port forwarding 128
 - reverse 128
 - standard 128
 - static 128
 - WAN interface 129
- netflow
 - configure 273
 - monitor 273
 - reported information 273
- network
 - discovery 284
 - vlan 69
- Network Address Translation. See NAT
- NO 53
- P**
- password
 - change 67
- pause frames 100
- permanent virtual circuit
 - configure 74
- ping 239
 - DNS client 88
- PMON
 - monitor 270
 - statistics 272
- policy
 - NAT 129
- port
 - 0 - 4 99

- front 99
- FxS 206
- LAN
 - clear statistics 102
 - flow control 100
 - mode 99
 - speed 99
 - statistics 102
- mii 99
- mirror 107
- VLAN 112
- WAN
 - configure 102
 - flow control 103
 - mii0 102
 - mode 103
 - speed 103
 - statistics 104
- port forwarding
 - NAT 128
- port mirroring
 - configure 107
 - LAN 108
 - remove 109
- port number
 - QoS
 - priority queue 109
- priority
 - queues
 - IEEE 802.1p 109
 - port 109
 - routing 109
- priority queues 109
- protocol
 - connection 313
- protocol
 - MGCP 206
 - Transport Layer 313
 - user authentication 313
- Protocol Monitoring. *See* PMON
- PVC
 - see permanent virtual circuit 74
- Q**
- QoS
 - BE (best effort) 139
 - best effort
 - link capacity 139
 - CAC 199
 - CAR 145
 - class values 140
 - configure 138
 - configure link 138
 - cumulative statistics 144
 - DiffServ/ToS 111
 - flow control 100, 110
 - GoS classes 138
 - IEEE 802.1p 109
 - instantaneous statistics 146
 - layer 2 109
 - links 138
 - model matrix, GoS 439
 - policing 138
 - port number 109
 - priority queues 109
 - quality groups 138, 139
 - quality guaranteed class 140
 - remove group 142
 - remove link 139
 - remove traffic classification 144
 - security policies 138
 - statistics 144
 - ToS/DiffServ 110
 - traffic classification 138, 143
 - traffic flow 142
 - type 112
 - IEEE 111
 - port 111
 - setting 110
 - voice traffic 137
- QoS layer 2
 - default setting 44
- quality groups
 - QoS 139
- quality guaranteed class
 - QoS 140
- R**
- RADIUS client 241
- registration
 - SIP 183
- relay
 - DHCP 246
 - DNS 246
 - SNTP 248
 - TFTP 249
 - TFTP cache 250
- remove
 - ARL 107
 - mirroring 109
 - QoS group 142
 - QoS link 139
 - QoS traffic classification 144
 - VLAN 115
- reverse
 - NAT 128

- rights
 - user 64
- RIP
 - ICAD40 support 96
- routing
 - dynamic 96
 - priority 109
 - static 95
 - traffic
 - interfaces 69
- rules
 - firewall 119
- S**
- security policies
 - default setting 42
- Security Policies. See firewall
- server
 - DHCP 243
 - primary, DNS 88
 - SFTP 227
 - SSH 231
 - telnet 230
 - web 233
- servers
 - SIP additional servers 153
- service
 - authentication 241
 - VoIP phone 243
 - web UI 224, 230, 231, 238, 240, 246, 247, 248
- session controller
 - keep-alive 186
 - MGCP 186, 189
 - SIP 150
- Session Initiation Protocol. See SIP
- SFTP
 - SSH 227
- SHA 62
- SIP
 - ACL 163
 - CAC 166
 - concurrent calls 150
 - configure server 151
 - endpoints 183
 - ESH 165
 - load balance 153
 - Media BRidge 161
 - media connection 163
 - overwrite media 150
 - registration 183
 - relay messages 150
 - server
 - automatic mode 152
 - manual mode 152
 - session controller 150, 156
 - SSP 157
 - terminal accounts 150
 - user agent 150
 - VQM 168
- SIP Signalling Proxy. See SSP
- SNMP
 - traps 276, 279
- SNMP agent 276
- SNTP
 - relay 248
 - time 85
- sntp
 - time
 - modify 87
- SSH
 - internet access 313
- SSH-AUTH] 313
- SSH-CONNECT 313
- SSH-TRANS 313
- SSL
 - certificate 235
 - certificate signing request 234
 - web server 233
- SSL certificate
 - configure 235
- SSL connection
 - SSL CSR 234
 - SSL key 234
- SSL CSR
 - configure 235
 - upload 237
- SSL key
 - configure 235
- standard
 - NAT 128
- static
 - NAT 128
- static route
 - add 95
 - delete 96
- static routing
 - configure 95
- statistic
 - QoS instantaneous 146
- statistics
 - call 181
 - clear
 - WAN port 105

- clear IDS 127
- ICMP 266
- IDS 125
- IP stack 264
- LAN
 - clear 102
- LAN port 102
- MGCP 201
- MGCP call quality 204
- MGCP logging internal 204
- MGCP packets 191
- MGCP SC calls 192
- MGCP voice quality 203
- netflow 275
- PMON 272
- QoS 144
- QoS cumulative 144
- SIP packets 159
- SIP SC calls 162
- SIP voice quality 170
- TCP 268
- UDP 267
- WAN port 104
- status
 - FxS port 208
 - MBR 194
 - SIP MBR 162
- summary
 - system operations 263
- syslog
 - emergency message 261
 - logging destination 262
 - server
 - messages 262
- system
 - exceptions 89
 - hardware 90
 - operations
 - summary 263
- system crash 256
- system error
 - show exceptions 90
- system exception
 - monitor 256
- system hardware
 - monitor 255
- system information
 - monitor 256
- system module
 - log 258
- system operations
 - monitor 257
- system security
 - logging 257
- T**
- table
 - ARP 93
- TCP
 - statistics 268
- tcp
 - connection timeout 121
- telnet
 - client 230
 - open session 231
 - server 230
- Tera Term Pro 311
- TFTP
 - cache 250
 - configure cache 251
 - download files 251
 - server 248, 249
- TFTP relay 249
- time
 - modify 87
 - SNTP client 85
- timeout connection 120
- ToS/DiffServ
 - QoS
 - priority queue 110
- traceroute 240
- traffic
 - best effort (QoS) 139
 - classification (QoS) 143
 - contention 137
 - filter
 - netflow 273
 - ICMP 266
 - IP stack 264
 - TCP 268
 - trace 270
 - voice 137
- traffic classification 118, 142
- traffic flow
 - quality groups 142
- Transport Layer Protocol 313
- trapmib 280
- U**
- UDP
 - logging destination 262
 - statistics 267
- uplink
 - IP host LAN 99
 - IP host WAN 102

- mirror traffic constraint 108
- port features 99
- user
 - active 67
 - default password 62
 - remove account 65
 - remove rights 66
 - rights 64
- user accounts
 - default setting 42
 - default settings 41
- user agent
 - MGCP 186, 205
 - SIP 150
- User Authentication Protocol 313
- user groups
 - default setting 41
- userbasic rights
 - default setting 42
- V**
- vid
 - VLAN 113
- VLAN
 - configure 112
 - ID 113
 - LAN 114
 - name 113
 - port 112
 - remove 115
 - route traffic 80
 - trunking 113
 - vid 113
 - WAN 114
- voice ACL
 - default setting 43
- voice parameters
 - default setting 42
- voice quality
 - monitor 284
- Voice Quality Monitoring. See VQM
- VQM 168
 - CODECs 169
 - MGCP 201
 - MGCP CODEC 202
- W**
- WAN
 - clear statistics 105
 - default setting 103
 - VLAN 114
- WAN port
 - statistics 104
 - warmstart 276
 - watchdog
 - configure 89
 - web server
 - configure 237
- X**
- X509 CSR 234
