

X6004

IP PBX

User's Guide

Default Login Details

LAN IP	https://192.168.1.12
WAN IP	https://172.16.1.1
User Name	admin
Password	1234

Firmware Version 1.20
Edition 1, 06/2010

www.zyxel.com

The logo for ZyXEL, featuring the brand name in a bold, blue, sans-serif font. The 'Z' and 'y' are lowercase, while 'XEL' are uppercase.

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the X6004 using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your hardware connections.

- Web Configurator Online Help

Embedded web help for descriptions of individual screens and supplementary information.

- Command Reference Guide

The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the X6004.

- Support Disc

Refer to the included CD for support documents.

- ZyXEL Web Site

Please refer to www.zyxel.com for additional support documentation and product certifications.

Documentation Feedback

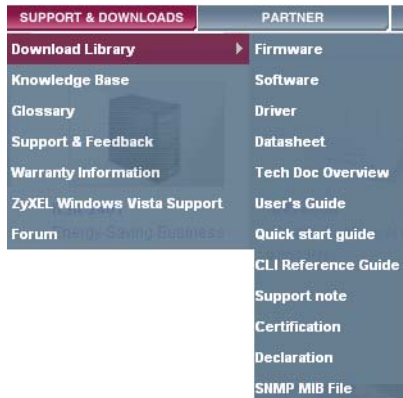
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- **Download Library**

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the documentation in order to better understand how to use your product.

- **Knowledge Base**

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- **Forum**

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.











Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The X6004 may be referred to as the "X6004", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The X6004 icon is not an exact representation of your device.

<p>The X6004</p> 	<p>Computer</p> 	<p>Notebook computer</p> 
<p>Server</p> 	<p>DSLAM</p> 	<p>Firewall</p> 
<p>Telephone</p> 	<p>Switch</p> 	<p>Router</p> 
<p>Internet</p> 		

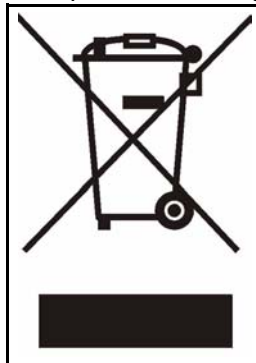
Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Caution: Risk of explosion if battery (on the motherboard) is replaced by an incorrect type. Dispose of used batteries according to the instructions. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.

- Warning! To avoid risk of electric shock, remove only one card at a time and do not place fingers or objects inside the chassis. Cover empty slots with slot covers.

This product is recyclable. Dispose of it properly.



Contents Overview

User's Guide	25
Introduction	27
How It Works	35
Tutorials	41
Technical Reference	99
The Web Configurator	101
Network Deployment	111
Server	125
Auto Provision	153
QoS	169
Voice Mail	173
Phonebook	179
DSP Management	187
Office Hours	193
Authority Group	197
Ring Group	229
Pickup Group	239
Click-To-Talk Group	243
Group Access Code	253
Outbound Line Group	257
Auto-Attendant	291
LCR	309
Group Management	317
Call Services	327
ZyStack	355
ACD	365
Monitor	379
Status Observation	385
System Log	401
Call Detail Record (CDR)	413
ACD Logs	423
Administrator Accounts	431
Diagnostics	437
Inactivity Timer	445
.....	446
Remote Management	447
TFTP Management	467

System File Maintenance	469
License Control	477
Web Portal	483
IVR System	503
Troubleshooting	509
Product Specifications	521

Table of Contents

About This User's Guide	3
Document Conventions.....	5
Safety Warnings.....	7
Contents Overview	9
Table of Contents.....	11
Part I: User's Guide.....	25
Chapter 1	
Introduction.....	27
1.1 Overview	27
1.1.1 Voice over Internet Protocol (VoIP) Implementation	28
1.1.2 PBX Telephony Features	29
1.1.3 Scalable Design	30
1.1.4 Automatic Call Distribution	30
1.1.5 Click-To-Talk	30
1.1.6 Mobile Phone Extensions	31
1.2 Ways to Manage the X6004	31
1.3 Good Habits for Managing the X6004	31
1.4 LEDs	32
Chapter 2	
How It Works	35
2.1 Call Routing	35
2.1.1 Call Routing Terms	35
2.2 Internal Call Routing	37
2.3 Outbound Call Routing	38
Chapter 3	
Tutorials.....	41
3.1 Making Internal Calls	43
3.1.1 Configure SIP Extensions	43
3.1.2 Connect IP Phones	46
3.1.3 Register IP Phones	47

3.1.4 Auto Provisioning	48
3.2 Making PSTN Calls	50
3.2.1 The PSTN Connection	50
3.2.2 Creating a Dialing Rule for PSTN	53
3.2.3 Assigning an LCR to an Authority Group	55
3.3 Making ITSP Calls	56
3.3.1 The ITSP Connection	57
3.3.2 Creating a Dialing Rule for ITSP	61
3.3.3 Assigning an LCR to an Authority Group	64
3.4 Making ISDN Calls	65
3.4.1 The ISDN Connection	66
3.4.2 Creating a Dialing Rule for ISDN	69
3.4.3 Assigning an LCR to an Authority Group	71
3.5 ISDN Network Configuration Examples	73
3.5.1 Example 1: Small/Medium Business	74
3.5.2 Example 2: Company with Existing PBX	75
3.5.3 Example 3: Company with Existing PBX and Expanding Employees	76
3.6 Using Call Features	76
3.6.1 Customizing Feature Codes	77
3.6.2 Using the Voicemail Feature	77
3.7 Using Your Web Portal	78
3.7.1 Your Information	78
3.7.2 Accessing the Web Portal	79
3.7.3 Changing Your Security Information	80
3.7.4 Personalizing Your Settings	81
3.7.5 Setting Up Voicemail	84
3.7.6 Using the Web Phone (IP Phone Users Only)	85
3.8 Capturing Packets Using the Web Configurator	86
3.9 Creating an Automated Menu System	89
3.9.1 Menu Design and Call Routing	89
3.9.2 Create an Agent Identity	91
3.9.3 Create a Skill	92
3.9.4 Create an Auto-Attendant	95

Part II: Technical Reference 99

**Chapter 4
The Web Configurator 101**

4.1 Introduction	101
4.2 System Login	101
4.3 The System Screen	103

4.3.1 The Navigation Panel	104
4.4 Dashboard - System Information	107
4.5 Saving Your Configuration	108
4.6 Icons in the Web Configurator	108
4.7 Resetting the X6004	109
4.8 Rebooting the X6004	109
4.9 Logging Out of the Web Configurator	110
4.10 Help	110
Chapter 5	
Network Deployment	111
5.1 Overview	111
5.1.1 What You Can Do in this Chapter	111
5.1.2 What You Need to Know	112
5.1.3 Before You Begin	113
5.2 The LAN Screen	114
5.2.1 The Static LAN IP Address Screen	115
5.3 The WAN Screen	116
5.4 The DDNS (Dynamic DNS) Screen	117
5.4.1 DYNDNS Wildcard	117
5.4.2 Configuring the DDNS Screen	118
5.5 The NTP (Network Time Protocol) Screen	119
5.6 The Static Route Screen	120
5.6.1 Configuring the Static Route Screen	121
5.6.2 Adding a Static Route	121
5.7 The VLAN Screen	122
5.8 Network Technical Reference	123
Chapter 6	
Server	125
6.1 Overview	125
6.1.1 What You Can Do in this Chapter	126
6.1.2 What You Need to Know	126
6.1.3 Before You Begin	129
6.2 The IP-PBX Server Global Screen	130
6.3 The FXO Screen	132
6.4 The FXS Screen	133
6.5 The BRI Screen	134
6.6 The PRI Screen	136
6.7 The Call Block Screen	139
6.7.1 The Call Blacklist Screen	140
6.8 The Feature Code Screen	141
6.9 The E-Mail Screen	144

6.10 The Fake IP Screen	145
6.11 The Peer to Peer Screen	146
6.11.1 How the Peer-to-Peer SIP Connection Works	147
6.11.2 Add Peer-to-Peer Local Net	148
6.11.3 How Local Net and Peer-to-Peer Work Together	148
6.12 Network Technical Reference	150
Chapter 7	
Auto Provision	153
7.1 Overview	153
7.1.1 What You Can Do in this Chapter	153
7.1.2 What You Need to Know	154
7.1.3 Before You Begin	155
7.2 Auto Provision Screen	155
7.2.1 Batch File Format	156
7.2.2 Auto Provision Edit Settings	157
7.2.3 Auto Provision View SPTGEN	158
7.3 snom Profile Setup	159
7.3.1 What is snom?	160
7.3.2 snom Batch Configuration XML File	161
7.3.3 snom Profile Setup: Edit	161
7.3.4 snom Profile Setup: View SPTGEN	162
7.3.5 snom Feature Key Setting	163
7.3.6 snom Firmware Upgrade	164
7.4 Auto Firmware Upgrade Screen	165
7.5 EZ Provision	167
Chapter 8	
QoS.....	169
8.1 Overview	169
8.1.1 What You Can Do in this Chapter	169
8.1.2 What You Need to Know	169
8.1.3 Before You Begin	171
8.2 The QoS Screen	171
Chapter 9	
Voice Mail.....	173
9.1 Overview	173
9.1.1 What You Can Do in this Chapter	173
9.1.2 What You Need to Know	173
9.2 The Voice Mail Screen	174
9.3 Accessing Voice Mail	175

Chapter 10	
Phonebook	179
10.1 Overview	179
10.1.1 What You Can Do in this Chapter	179
10.1.2 What You Need to Know	179
10.1.3 Before You Begin	180
10.2 The Phonebook Configuration Screen	181
10.2.1 The Import Phonebook Screen	182
10.3 The LDAP Phonebook Screen	183
10.4 The Local Phonebook Screen	184
10.4.1 Local Phonebook Add/Edit Screen	185
Chapter 11	
DSP Management.....	187
11.1 Overview	187
11.1.1 What You Can Do in this Chapter	187
11.1.2 What You Need To Know	187
11.1.3 Before You Begin	188
11.2 Installing and Removing DSP Modules	188
11.2.1 How to Install a DSP Module	188
11.2.2 How to Remove a DSP Module	189
11.3 The DSP Management Screen	190
Chapter 12	
Office Hours	193
12.1 Overview	193
12.1.1 What You Can Do in this Chapter	193
12.1.2 What You Need To Know	193
12.1.3 Before You Begin	193
12.2 Office Hour Screen	194
Chapter 13	
Authority Group	197
13.1 Overview	197
13.1.1 What You Can Do in this Chapter	198
13.1.2 What You Need to Know	199
13.2 The Authority Group Screen	200
13.2.1 The Extension Query Result Screen	201
13.2.2 The Add/Edit Authority Group Screen	202
13.2.3 The Authority Group Configuration Screen	203
13.3 Extension Features	204
13.3.1 The Batch Add Screen	205
13.3.2 Add a SIP Extension: The Basic Screen	207

13.3.3 Configure SIP Extensions: The Basic Screen	208
13.3.4 The SIP Extension Call Forward Screen	209
13.3.5 The DND White List Screen	213
13.3.6 The Find Me List Screen	214
13.3.7 The Blacklist Screen	215
13.3.8 The SIP Extension Voice Mail Settings Screen	216
13.3.9 The SIP Extension Advanced Screen	217
13.3.10 The Auto Provision Screen	219
13.3.11 The Add an FXS Extension Screen	220
13.3.12 Configure FXS Extensions: the Basic Screen	221
13.3.13 The FXS Extension Call Forward Screen	222
13.3.14 The FXS Extension Voice Mail Screen	222
13.3.15 The FXS Extension Advanced Screen	223
13.3.16 The Add a BRI Extension Screen	223
13.3.17 Configure BRI Extensions: the Basic Screen	225
13.3.18 The BRI Extension Call Forward Screen	226
13.3.19 The BRI Extension Voice Mail Screen	226
13.3.20 The BRI Extension Advanced Screen	226
13.4 Authority Group Technical Reference	227
Chapter 14	
Ring Group	229
14.1 Overview	229
14.1.1 What You Can Do in this Chapter	229
14.1.2 What You Need to Know	229
14.1.3 Before You Begin	230
14.2 The Ring Group Screen	233
14.2.1 The New Ring Group Screen	233
14.2.2 The Edit Ring Group Screen	234
14.2.3 The Configure Ring Group Screen	235
14.2.4 The Add/Edit Page Group Screen	236
14.2.5 The Add/Edit Hunt Group Screen	237
Chapter 15	
Pickup Group	239
15.1 Overview	239
15.1.1 What You Can Do in this Chapter	239
15.1.2 Before You Begin	240
15.1.3 Pickup Group Example	240
15.2 The Pickup Group Screen	241
15.2.1 Add/Edit Pickup Groups	242
Chapter 16	
Click-To-Talk Group	243

16.1 Overview	243
16.1.1 What You Can Do in this Chapter	244
16.1.2 Before You Begin	244
16.2 The Click-To-Talk Group Screen	246
16.2.1 Add a Click-To-Talk Group	247
16.2.2 Edit a Click-To-Talk Group	248
16.2.3 Manage Click-To-Talk Group Extensions	249
16.2.4 Click-To-Talk Extension Settings	251
Chapter 17	
Group Access Code.....	253
17.1 Overview	253
17.1.1 What You Can Do in this Chapter	254
17.1.2 What You Need to Know	254
17.2 The Group Access Code Screen	254
17.2.1 The Group Access Code Screen	255
Chapter 18	
Outbound Line Group.....	257
18.1 Overview	257
18.1.1 What You Can Do in this Chapter	258
18.1.2 What You Need to Know	258
18.1.3 Before You Begin	261
18.2 Outbound Line Group Screen	262
18.2.1 Add/Edit FXO Trunk	263
18.2.2 Configure an FXO Trunk	264
18.2.3 Auto-Attendant for Incoming Analog Calls	265
18.3 Add/Edit PRI Trunk	266
18.3.1 Configure a PRI Trunk	267
18.3.2 Auto-Attendant for Incoming PRI Calls	270
18.4 Add/Edit BRI Trunk	271
18.4.1 Configure a BRI Trunk	272
18.4.2 Auto-Attendant for Incoming BRI Calls	276
18.5 Add/Edit SIP Trunk	276
18.5.1 Configure a SIP Trunk	277
18.5.2 Auto-Attendant for SIP Trunks	282
18.6 Add/Edit Trusted Peer	284
18.6.1 Configure a Trusted Peer	285
18.6.2 Auto-Attendant for Trusted Peer	289
Chapter 19	
Auto-Attendant.....	291
19.1 Overview	291

19.1.1 What You Can Do in this Chapter	291
19.1.2 What You Need to Know	292
19.2 The Default Screen	294
19.3 The Customized Screen	295
19.3.1 The Add/Edit Auto-Attendant Screen	296
19.3.2 Advanced Settings: Office Hours	297
19.3.3 The Add/Edit Office Hours Auto-Attendant Screen	299
19.3.4 The Auto-Attendant Sub Menu Screen	300
19.3.5 Advanced Settings: Night Service	301
19.3.6 Advanced Settings: Greetings	303
19.4 Technical Reference	305
Chapter 20	
LCR.....	309
20.1 Overview	309
20.1.1 What You Can Do in this Chapter	310
20.1.2 What You Need to Know	310
20.1.3 Before You Begin	311
20.2 LCR List	311
20.2.1 LCR Configuration	312
20.2.2 Add/Edit LCR Dial Condition	314
Chapter 21	
Group Management	317
21.1 Overview	317
21.1.1 What You Can Do in this Chapter	318
21.1.2 What You Need to Know	318
21.1.3 Before You Begin	322
21.2 Group Management Screen	322
21.2.1 The Overview Screen	324
21.2.2 Edit Group Management Associations	326
Chapter 22	
Call Services.....	327
22.1 Overview	327
22.1.1 What You Can Do in this Chapter	327
22.1.2 What You Need to Know	328
22.1.3 Before You Begin	328
22.2 The Emergency Call Screen	329
22.2.1 Configuring the Emergency Call Screen	329
22.3 The Conference Calling Screen	331
22.3.1 Configuring the Conference Calling Screen	331
22.3.2 The Conference Calling Edit and Add Screen	332

22.4 The Music on Hold Screen	333
22.4.1 Global Setting Screen	334
22.4.2 Custom Music On Hold	334
22.4.3 Add or Edit a Music On Hold Profile	335
22.4.4 Upload a Music On Hold Profile	336
22.5 The Distinctive Ring Screen	337
22.6 The Auto Callback Screen	338
22.7 The Call Park Screen	339
22.7.1 Configuring the Call Parking Screen	340
22.8 The Call Waiting Screen	341
22.8.1 Configuring the Call Waiting Screen	343
22.8.2 Call Waiting Example - 1	344
22.8.3 Call Waiting Example - 2	344
22.9 The Call Transfer Screen	345
22.9.1 Configuring the Call Transfer Screen	345
22.10 Call Recording	345
22.10.1 Configuring the Call Recording Screen	347
22.10.2 Querying Call Recordings	348
22.10.3 Call Recordings File List	349
22.11 TAPI	349
22.11.1 Setting Up the TAPI Server Driver	350
22.11.2 Sending Call Invites from Microsoft Outlook	352
Chapter 23	
ZyStack	355
23.1 Overview	355
23.1.1 What You Can Do in this Chapter	355
23.1.2 What You Need to Know	355
23.1.3 Before You Begin	357
23.2 ZyStack Configuration	357
23.2.1 ZyStack Add Screen	358
23.2.2 ZyStack Edit Screen	359
23.3 ZyStack Intranet Setup	360
23.3.1 ZyStack Add Intranet	361
23.4 ZyStack Status	362
Chapter 24	
ACD	365
24.1 Overview	365
24.1.1 What You Can Do in this Chapter	366
24.1.2 What You Need to Know	366
24.2 The ACD Global Screen	368
24.3 The Agent Screen	369

24.3.1 The Agent Settings Screen	370
24.4 The Skill Screen	371
24.4.1 The Skill Settings Screen	372
24.5 The Skill Menu Screen	377
24.5.1 The Skill Menu Settings Screen	378
Chapter 25	
Monitor.....	379
25.1 Overview	379
25.2 The System Information Screen	379
25.3 SNMP	382
25.3.1 Supported MIBs	383
25.3.2 SNMP Traps	383
25.3.3 Configuring SNMP	384
Chapter 26	
Status Observation.....	385
26.1 Overview	385
26.2 What You Can Do in this Chapter	385
26.2.1 What You Need to Know	385
26.3 The SIP Peer Screen	386
26.4 The FXS Peer Status Screen	388
26.5 The BRI Peer Status Screen	389
26.6 The CTI Peer Status Screen	390
26.7 The FXO Trunk Status Screen	391
26.8 The SIP Trunk Status Screen	392
26.9 The BRI Trunk Status Screen	393
26.10 The PRI Trunk Status Screen	394
26.11 The ACD Queue Screen	396
Chapter 27	
System Log.....	401
27.1 Overview	401
27.1.1 What You Can Do in this Chapter	401
27.1.2 What You Need to Know	401
27.2 The View Log Screen	402
27.2.1 Filter Log Results Screen	404
27.3 The Log Setting Screen	405
27.3.1 Active Log Summary Screen	406
27.3.2 System Log Configuration Screen	408
27.3.3 Edit Syslog Server Settings Screen	411
Chapter 28	
Call Detail Record (CDR).....	413

28.1 Overview	413
28.1.1 What You Can Do in this Chapter	413
28.1.2 What You Need to Know	413
28.2 The Configuration Screen	414
28.2.1 Configure your remote server	416
28.3 The Backup Screen	417
28.4 The Query Screen	418
28.4.1 The Report Screen.....	420
28.5 CDR Technical Reference	421
Chapter 29	
ACD Logs.....	423
29.1 Overview	423
29.1.1 What You Can Do in this Chapter	423
29.1.2 Before You Begin	423
29.2 The Configuration Screen	423
29.2.1 Configure your remote server	425
29.3 The Backup Screen	426
29.4 The Query Screen	427
29.4.1 ACD Report Screen	428
Chapter 30	
Administrator Accounts	431
30.1 Overview	431
30.1.1 What You Can Do in this Chapter	431
30.1.2 What You Need to Know	431
30.2 The Logged-In Administrator Screen	432
30.3 The Administrator List Screen	433
30.3.1 Add an Administrator	434
30.3.2 Edit an Administrator Account	435
Chapter 31	
Diagnostics.....	437
31.1 Overview	437
31.1.1 What You Can Do in this Chapter	437
31.1.2 What You Need to Know	437
31.2 The Information Collect Screen	438
31.3 The Packet Capture Screen	440
31.4 The Voice Sniffer Screen	442
Chapter 32	
Inactivity Timer.....	445
32.1 Overview	445

32.2 The Inactivity Timer Screen	445
.....	446
Chapter 33	
Remote Management.....	447
33.1 Overview	447
33.1.1 What You Can Do in this Chapter	447
33.1.2 What You Need to Know	448
33.2 The WWW Screen	449
33.3 The WWW > Add/Edit Screen	450
33.4 The SSH Screen	451
33.5 The SSH > Add/Edit Screen	452
33.6 The FTP Screen	453
33.7 The FTP > Add/Edit Screen	454
33.8 The ICMP Screen	455
33.9 The ICMP > Add/Edit Screen	456
33.10 The CTI Screen	457
33.10.1 The CTI Add/Edit Screen	458
33.11 Remote Management Technical Reference	459
Chapter 34	
TFTP Management.....	467
34.1 TFTP Management	467
Chapter 35	
System File Maintenance.....	469
35.1 Overview	469
35.1.1 What You Can Do in this Chapter	469
35.1.2 What You Need to Know	469
35.2 The Backup & Restore Screen	471
35.2.1 Batch Add SIP Extensions Template File	473
35.3 The Firmware Upgrade Screen	473
35.4 Technical Reference	474
Chapter 36	
License Control.....	477
36.1 Overview	477
36.1.1 What You Can Do in this Chapter	477
36.1.2 What You Need to Know	477
36.1.3 Before You Begin	478
36.2 The Registration Screen	479
36.3 The Service Screen	480
36.4 The License Status Screen	481

Chapter 37	
Web Portal	483
37.1 Overview	483
37.1.1 What You Can Do in this Chapter	484
37.1.2 What You Need to Know	484
37.2 Account Settings	485
37.3 Call Forwarding and Blocking	487
37.3.1 Office Hours	489
37.3.2 DND White List	491
37.3.3 Find Me List	491
37.3.4 Blacklist	492
37.4 Voice Mail Settings	493
37.5 Web Phone	494
37.6 Utility Download	495
37.6.1 The Outlook Plugin	496
37.6.2 TAPI Client Driver	498
37.6.3 Sending Call Invites from Microsoft Outlook	501
Chapter 38	
IVR System	503
38.1 Overview	503
38.1.1 What You Need to Know About IVR	503
Chapter 39	
Troubleshooting	509
39.1 Power, Hardware Connections, and LEDs	509
39.2 X6004 Access and Login	510
39.3 Internet Access	513
39.4 Advanced Features	514
39.5 Reset the X6004 to Its Factory Defaults	515
39.6 The Console Port	516
39.6.1 Use the Console Port to Access the CLI	516
39.6.2 The Login Screen	516
39.6.3 The Initrd Screens	517
Chapter 40	
Product Specifications	521
Appendix A IP Addresses and Subnetting	529
Appendix B Open Software Announcements	541
Appendix C Legal Information	565
Index	569

PART I

User's Guide

Introduction

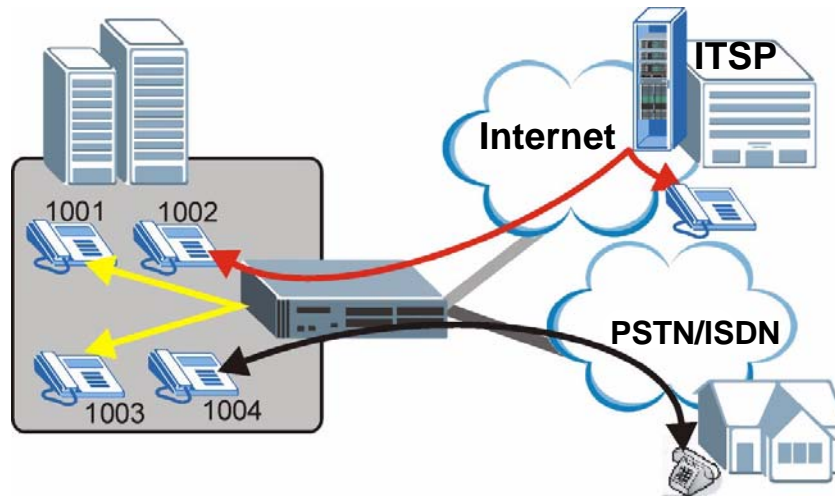
This chapter introduces the main features and applications of the X6004.

1.1 Overview

An IP PBX is a telephone exchange device located at a company site which allows an organization to set up and control calls. IP stands for Internet Protocol, and PBX stands for Private Branch Exchange. A regular company telephone switchboard is an example of a PBX. The company's telephones are connected to the IP PBX. The IP PBX is then connected to the outside world via connections to any combination of the following networks:

- A traditional Public Switched Telephone Network (PSTN)
- A broadband Internet connection to an Internet Telephony Service Provider (ITSP)
- An Integrated Services Digital Network/Basic Rate Interface Network (ISDN BRI)
- An Integrated Services Digital Network/Primary Rate Interface Network (ISDN PRI T1/E1)

Each telephone connected to an IP PBX has an extension assigned to it. An extension is a unique telephone number within an organization typically consisting of only a few digits. People inside the company can call each other by dialing extensions. Calls to the outside world go through the IP PBX to the PSTN, ITSP or ISDN.

Figure 1 IP PBX Example

The X6004 can function as a stand alone telephone switchboard for a small organization. It can also supplement a legacy PBX within an organization by providing VoIP telephony features.

1.1.1 Voice over Internet Protocol (VoIP) Implementation

The X6004 uses SIP (Session Initiation Protocol) to communicate with other SIP devices. SIP is an internationally-recognized standard for implementing Voice over Internet Protocol (VoIP).

The following figure shows SIP devices communicating with the X6004.

A: IP Phones - Telephones that convert voice into IP packets and vice versa (for example ZyXEL's V-500).

B: Softphones - Software-based phones installed on PCs.

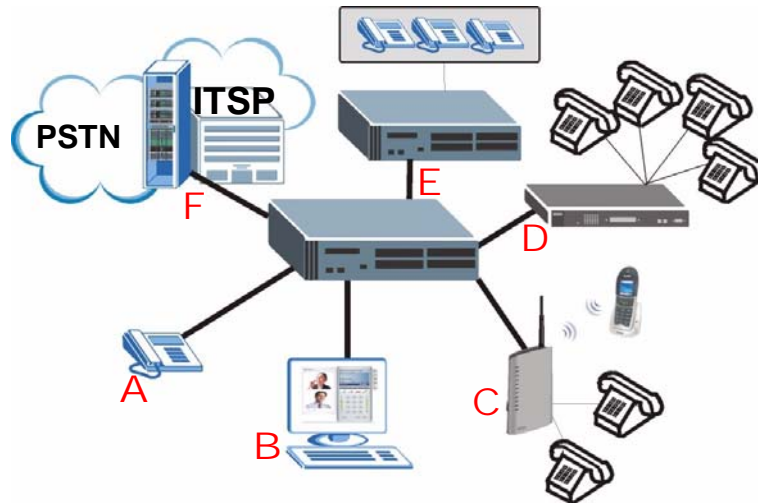
C: VoIP Gateways - Devices (for example ZyXEL's P-2302HWUDL) with built in SIP processing which allow traditional analog phones or cordless phones to use them as a link to the IP PBX.

D: ATAs - Analog Telephone Adapters (for example ZyXEL's P-2024) aggregate a large number of analog phones and convert their signal into IP packets.

E: Peer IP PBXs - Other SIP based IP PBXs with which you communicate over an IP network. This allows you to call the telephones connected to the peer IP PBX without going through a telephone service provider.

F: SIP Servers - Servers (D) located at your Internet Telephony Service Provider (ITSP) which process outgoing calls from the X6004 and direct them to IP phones on the Internet or traditional phones on the PSTN.

Figure 2 SIP Devices and the X6004



1.1.2 PBX Telephony Features

The X6004 allows you to set up and manage features on an internal telephone network without relying on your telephone service provider. The following are just a few examples:

- Conference calls
- Voicemail
- Call Forwarding

The X6004 integrates with your IP network. For example you can:

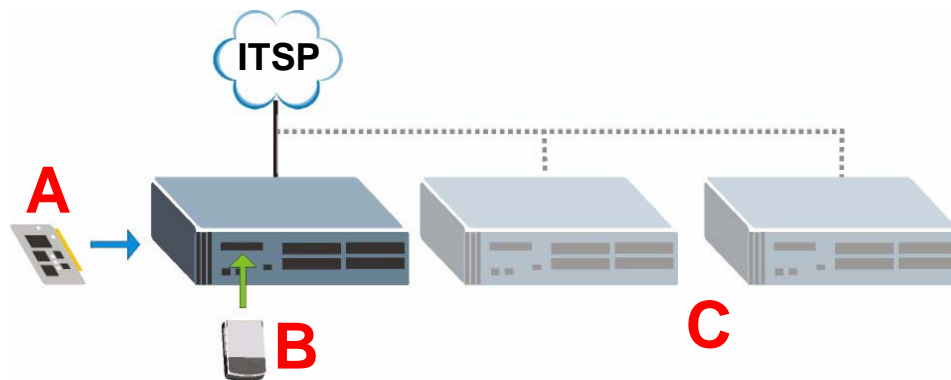
- Import an LDAP-based (Lightweight Directory Access Protocol) contact list to serve as the phonebook for the IP phones on your network.
- Set up the X6004 to send users email notifications or complete voice messages as attachments when they receive voicemail.

1.1.3 Scalable Design

The X6004 can be used stand alone to provide intercom (calling by extension) and VoIP features in a small business environment. The X6004's capability can be expanded by:

- **A** - Adding DSP (Digital Signal Processing) modules in the device's bottom to handle more concurrent telephone connections. DSP modules are chips which convert analog information into digital data and vice versa.
- **B** - Adding a hard disk to store a greater volume of voice messages and call records.
- **C** - Connecting several X6004s together to manage a larger telephone network.

Figure 3 Scalable Design



1.1.4 Automatic Call Distribution

Automatic Call Distribution (ACD) allows you to distribute incoming calls to specific groups of phones connected to your telephone network. Distributed calls can then be sent to individual people based on assigned skill sets. This is known as Skill-Based Routing (SBR). When the X6004 receives an incoming call, it categorizes the call by "skill". Next, it assigns the call to the one of the agents associated with that skill. Skills are defined by the X6004 administrator and constitute a set of rules that work in tandem with the auto-attendant to assign incoming calls to groups of agents.

1.1.5 Click-To-Talk

The Click-To-Talk (CTT) feature allows you to create an HTML link that you can embed on a Web page; a person visiting that web page can click it to connect directly to a phone on the other end. This Web-based communication uses the SIP voice protocol, with an Adobe Flash-based client on one side, an IP phone on the other, and the managing X6004 in the middle.

1.1.6 Mobile Phone Extensions

This feature gives users the freedom to access their telephone extensions anywhere in the world, regardless of the type of telecommunications device they are using: cell phone, VoIP, or landline. The “mobile” aspect that the end user can always be on the move and still receive calls sent to their telephone extension.

1.2 Ways to Manage the X6004

Use any of the following methods to manage the X6004.

- Web Configurator. This is recommended for everyday management of the X6004 using a (supported) web browser. You can also use the web configurator for firmware upgrades and configuration backup/restore.
- Command Line Interface. Line commands offer an alternative to the web configurator and in some cases are necessary to configure advanced features.
- FTP. Use FTP for firmware upgrades.

1.3 Good Habits for Managing the X6004

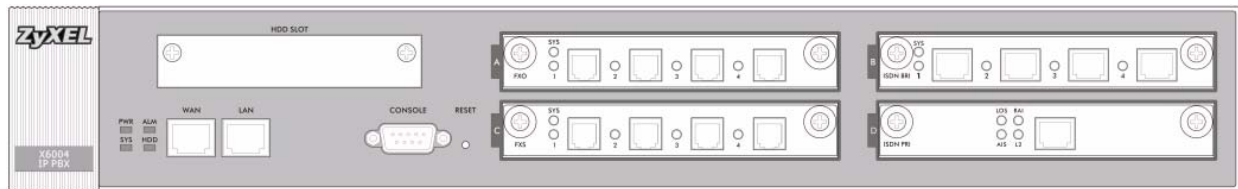
Do the following things regularly to make the X6004 more secure and to manage the X6004 more effectively.

- Change the administrator password. Use a password that’s not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the administrator password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the X6004 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the X6004. You could simply restore your last configuration.

1.4 LEDs

The figure below shows the LEDs on the X6004.

Figure 4 LEDs



The following table describes the LEDs.

Table 1 LEDs

LED	COLO R	STATUS	DESCRIPTION
PWR	Green	On	The X6004 is turned on.
		Off	The X6004 is off.
SYS	Green	Blinking	The X6004 is rebooting and performing self-diagnostic tests.
		On	The X6004 is on and functioning properly.
		Off	The power is off or the X6004 is not ready/malfunctioning.
ALM	Red	On	There is a hardware failure.
		Off	The X6004 is functioning normally.
HDD	Orange	Blinking	The X6004 is writing to the hard disk.
		Off	The X6004 is not writing to the hard disk or does not have a hard disk installed.
FXS, FXO, FXS/FXO, ISDN BRI Interface Card LEDs			
SYS	Green	On	The interface card is functioning properly.
		Off	The interface card is off or is not recognized by the X6004.
FXS 1~4, FXS S1~S2	Green	On	The line is in use.
		Off	The line is not in use.
FXO 1~4, FXO O1~O2	Green	On	The line is connected and receiving a signal.
		Off	The line is not connected.
ISDN BRI 1~4	Green	On	The line is connected and receiving a signal.
		Off	The line is not connected.
		Blinking	At least one ISDN connection is active.
ISDN PRI Interface Card LEDs			
LOS (Loss of Signal)	Red	On	The line is down or not connected.
		Off	The line is operating properly.

Table 1 LEDs (continued)

LED	COLO R	STATUS	DESCRIPTION
RAI (Remote Alarm Indication)	Yellow	On	The remote device receives the ISDN physical layer alarm from the X6004 and responds with this alarm.
		Off	The ISDN physical layer is operating properly without any remote alarms.
AIS (Alarm Indication Signal)	Yellow	On	The X6004 detects an ISDN physical layer issue and sends this local alarm.
		Off	The ISDN physical layer is operating properly without any local alarms.
L2 (Layer 2)	Green	On	The link is connected and able to receive signals.
		Off	The link is down.
		Blinking	The system is booting up or at least one voice connection is active.
All 4 LED		Blinking	System fails.
		Off	There is a system configuration error.

How It Works

This chapter is an overview of different logical components and how they work together to route calls on the X6004.

2.1 Call Routing

The two main functions of any IP-PBX are routing internal calls and handling calls to and from the outside world.

The following sections explain how these functions are performed on the X6004.

2.1.1 Call Routing Terms

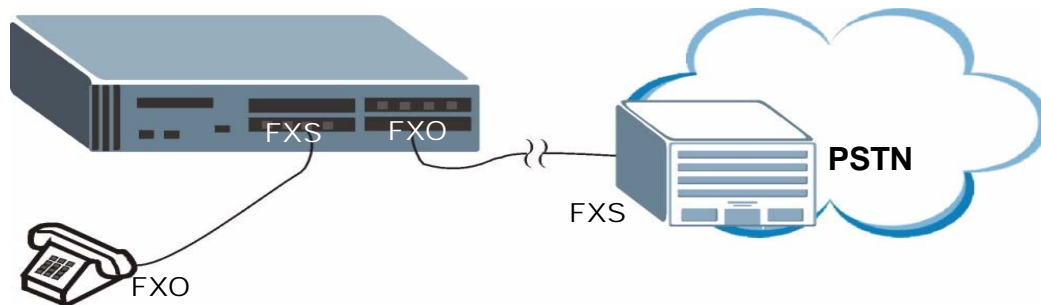
The following are some terms related to ZyXEL's IP-PBX implementation.

- **Extension** - This is a unique number assigned to each telephone connected to the X6004. Extensions are used to make calls between phones connected to the X6004 and to route calls from the outside world to their correct target. Extensions fall into the following two groups:
 - **SIP Extension** - This is an extension assigned to a SIP (Session Initiation Protocol) based IP phone connected to the X6004. Alternatively this could be an extension assigned to an analog phone which connects to the X6004 via a VoIP gateway device.
 - **FXS (Foreign Exchange Subscriber) Extension** - This is an extension assigned to an analog phone directly connected to a port on an FXS interface card installed on the X6004 (See [Figure 5 on page 36.](#)) The FXS ports on the X6004 work the same way as the phone sockets in your home. In your home you are a subscriber to the telephone services of your local telephone company and when you connect an analog phone to the X6004 you subscribe to the telephone services of the X6004.
 - **ISDN BRI (Basic Rate Interface) Extension** - This is an extension assigned to an ISDN phone directly connected to the X6004.
- **Authority Group** - This is a set of extensions. Each extension can only belong to one authority group. Authority groups manage extensions by allowing them to make only certain types of calls. For example, if you create two authority groups, you can allow one group to make local calls and long distance calls and the second authority group to make local calls only.

- **Outbound Line Group** - This is a set of connections or lines going to the outside world.
- **SIP Trunk** - This is a connection to your ITSP (Internet Telephony Service Provider).
- **ISDN BRI/PRI Trunk** - This is a connection to your ISDN Service Provider.
- **Trusted Peer** - This is a connection to another IP PBX or SIP server. The trusted peer device must also specify your X6004 as a trusted peer.
- **FXO (Foreign Exchange Office) Trunk** - This type of outbound line group consists of telephone cables connected to ports on an FXO interface card on the X6004. The telephone cables lead to the PSTN (Public Switched Telephone Network), or in other words your traditional (non-VoIP) telephone company. FXO ports always point in the direction of the telephone services.

The figure below shows the relationship between FXS and FXO ports.

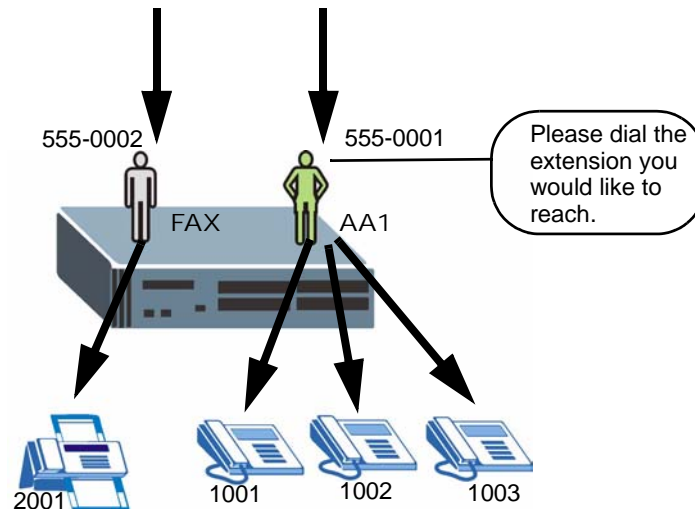
Figure 5 FXS and FXO Ports



- **LCR (Least Cost Routing)** - This is a rule which specifies which outbound line group is used when making an outbound call. It consists of a dialing condition, for example dial **0** to make a call via a specific FXO trunk or dial **1** for calls via a SIP trunk. LCRs also set priority to which outbound line group should be tried first, second, third and so on when making outbound calls with the same dialing condition.
- **Auto-Attendant** - This is a feature which routes incoming calls to their proper extension. An auto-attendant is assigned to each outbound line group and it services incoming calls on those lines. If your organization has two outbound line groups, each with a specific telephone number for incoming calls, then you

can assign a different auto-attendant for each incoming line. Assign one auto-attendant for general calls to the extensions in your organization (for example **AA1**) and one auto-attendant for direct routing to a FAX machine (for example **FAX**).

Figure 6 Auto-Attendant



2.2 Internal Call Routing

Internal call routing refers to calls between extensions on the X6004. People simply dial the extension they want to call. The X6004 checks to see if the number dialed is an existing extension and forwards the call to that extension. The X6004 by default allows people with extensions from one authority group to call extensions in another authority group. You can, however, block calls between authority groups if your organization requires such a setting.

The configuration requirement for setting up internal call routing are:

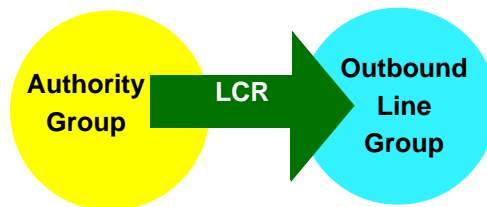
- 1 Create an authority group.
- 2 Create extensions in the authority group.

2.3 Outbound Call Routing

Outbound call routing refers to calls originating from an extension on the X6004, going via an outbound line group to a telephone outside your organization. Outbound call routing requires that an authority group is linked to an outbound line group. The link between the two is an LCR (Least Cost Routing). LCRs contain the dialing rules for outbound line groups. Authority groups need to be associated to LCRs to gain access to the outbound line groups.

In the most basic setup example an organization has one authority group (with all of the company's extensions), one outbound line group and an LCR which grants the authority group access to outbound lines. Everyone in the organization has the same rights to use outbound lines.

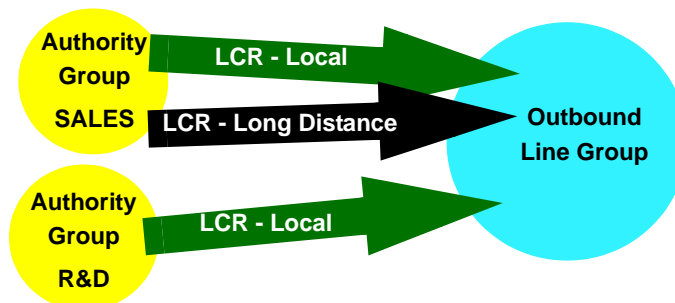
Figure 7 Outbound Call Routing - Basic



In a more advanced example, you can create two authority groups, still have one outbound line group and two different LCRs. You can now control the types of outbound calls that can be made by each authority group.

In the figure below, the **SALES** authority group has a local call LCR and a long distance LCR associated to it. This allows its group members to make both local and long distance calls via the outbound line group. R&D authority group only has the local LCR associated to it so its group members can only make local calls via the outbound line group.

Figure 8 Outbound Call Routing - Advanced



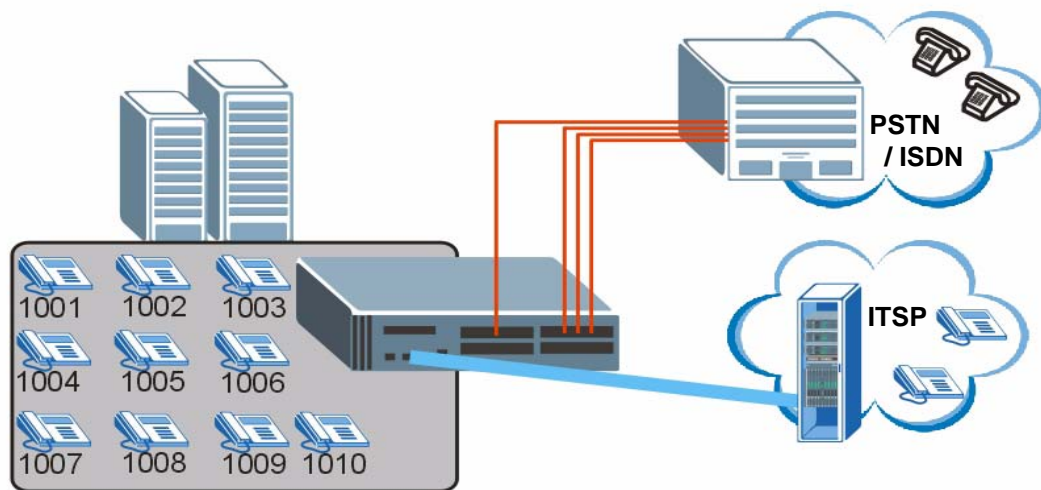
The configuration requirement for setting up outbound call routing are:

- 1 Create an authority group.
- 2 Create extensions in the authority group.
- 3 Create an outbound line group.
- 4 Create LCRs and add outbound line groups to them.
- 5 Associate LCRs to authority groups.

Tutorials

This chapter provides some examples of using the web configurator to set up and use the X6004. Specifically, the tutorials will show you how to set up the X6004 for a telephone network as shown in the following figure.

Figure 9 Tutorial Overview



The tutorials include:

Table 2 Tutorials Overview

TUTORIAL GOAL	STEPS
Making Internal Calls	<ul style="list-style-type: none"> • Configure SIP Extensions • Connect IP Phones • Register IP Phones • Auto Provisioning
Making PSTN Calls	<ul style="list-style-type: none"> • The PSTN Connection • Creating a Dialing Rule for PSTN • Assigning an LCR to an Authority Group
Making ITSP Calls	<ul style="list-style-type: none"> • The ITSP Connection • Creating a Dialing Rule for ITSP • Assigning an LCR to an Authority Group

Table 2 Tutorials Overview

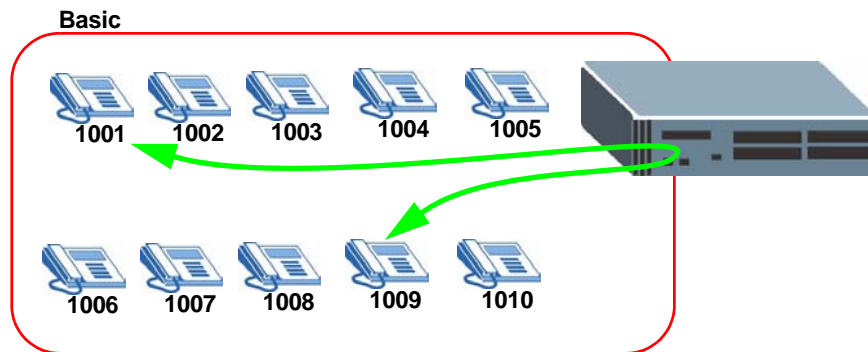
TUTORIAL GOAL	STEPS
Making ISDN Calls	<ul style="list-style-type: none"> • The ISDN Connection • Creating a Dialing Rule for ISDN • Assigning an LCR to an Authority Group
ISDN Network Configuration Examples	<ul style="list-style-type: none"> • Example 1: Small/Medium Business • Example 2: Company with Existing PBX • Example 3: Company with Existing PBX and Expanding Employees
Using Call Features	<ul style="list-style-type: none"> • Customizing Feature Codes • Using the Voicemail Feature
Using Your Web Portal	<ul style="list-style-type: none"> • Your Information • Accessing the Web Portal • Changing Your Security Information • Personalizing Your Settings • Setting Up Voicemail • Using the Web Phone (IP Phone Users Only)
Capturing Packets Using the Web Configurator	
Creating an Automated Menu System	<ul style="list-style-type: none"> • Create an Agent Identity • Create a Skill • Create an Auto-Attendant

Note: This chapter assumes that you have already configured your network settings. See the Network Wizard section in the QSG or [Chapter 5 on page 111](#) for more information.

3.1 Making Internal Calls

This tutorial sets up the internal telephone extensions on your network. At the end of this tutorial you should be able to call between extensions. The next figure shows the telephone extensions (**1001 - 1010**) configured in this tutorial. All of the extensions are members of an authority group called **Basic** (you need to create an authority group before configuring extensions, see [Chapter 2 on page 35](#) for more information). The figure also shows an internal call between extensions **1001** and **1009**.

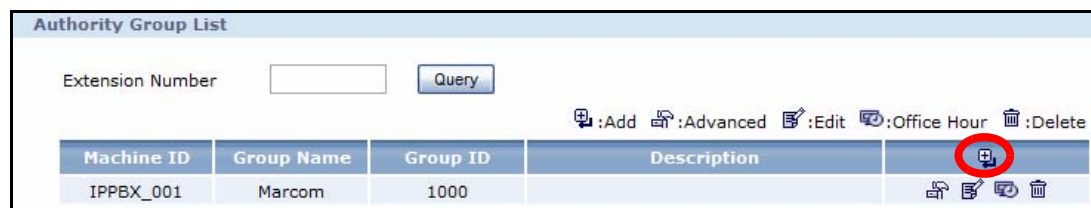
Figure 10 Internal Calls



3.1.1 Configure SIP Extensions

The following section introduces how to create the authority group called **Basic** and ten SIP extensions **1001** to **1010** on the X6004. The number of extensions you can create is limited by your service subscription (see [Section 36.1.2 on page 477](#) for more information).

- 1 In the web configurator, click **Configuration > PBX > Extension Management > Authority Group** to open the following screen.



- Click the **Add** icon to open the following screen. Enter the name of the group (**Basic** in this example) and click **Add**. The **Machine ID** field is a name automatically assigned to the X6004.

Authority Group Setting

Machine ID: IPPBX_001

Group Name:

Group ID:

Description:

- The new authority group displays in the following screen. Now you will add SIP extensions to the authority group. Click the new authority group's **Advanced** icon.

Authority Group List

Extension Number:

:Add :Advanced :Edit :Office Hour :Delete


Machine ID	Group Name	Group ID	Description	
IPPBX_001	Marcom	1000		

- The following screen displays. Click **Batch Add** to configure multiple SIP accounts at the same time.

Peer List

SIP Peer

:Add :Edit :Delete

<input type="checkbox"/>	User Name	Type	Extension Number	Description	
<input type="checkbox"/>					

- Configure the screen as shown next. The SIP extension number and any configured **SIP Auth. Password** prefix and/or postfix make up the SIP password. The SIP password must be at least four digits. This example uses ten four-digit SIP extensions **1001 - 1010** that are also used as the SIP usernames. The SIP passwords are comprised of the combination of **Prefix + Extension + Postfix**. In this example, the **SIP Auth. Password Prefix** value is **11** and the **Postfix** value

is **99**. The SIP username for extension **1001** is **1001** and the SIP password for this extension is **11100199**. You do not need to configure the **Prefix** and **Postfix** values as long as the SIP password length is at least four digits long. Click **Apply** and wait for the X6004 to create the ten extensions.

Batch Add SIP Peers

Group: Marcom ▼

Start Number:

Step/Interval:

Amount:

SIP Auth. Password: Prefix: Postfix:

DTMF Mode: info ▼

CODEC Setting

CODEC Pool

- G.726
- H.263
- H.261
- G.722 (pass-through)
- G.722 AMR-WB (pass-through)

CODEC List

- G.729
- G.711 u-law
- G.711 a-law

6 The SIP extensions display as shown here.

Peer List

SIP Peer

➕: Add ➔: Edit 🗑: Delete

<input type="checkbox"/>	User Name	Type	Extension Number	Description	⊕
<input type="checkbox"/>	5000	SIP	5000		📄 🗑
<input type="checkbox"/>	5002	SIP	5002		📄 🗑
<input type="checkbox"/>	5004	SIP	5004		📄 🗑
<input type="checkbox"/>	5006	SIP	5006		📄 🗑
<input type="checkbox"/>	5008	SIP	5008		📄 🗑
<input type="checkbox"/>	5010	SIP	5010		📄 🗑
<input type="checkbox"/>	5012	SIP	5012		📄 🗑
<input type="checkbox"/>	5014	SIP	5014		📄 🗑
<input type="checkbox"/>	5016	SIP	5016		📄 🗑
<input type="checkbox"/>	5018	SIP	5018		📄 🗑

- 7 Keep a list of the SIP passwords (the **Prefix + Extension Number + Postfix** combinations in this example). When you deploy the network's IP phones, you will need this information for SIP registration. See [Section 3.1.2 on page 46](#) for information on configuring your IP phones.

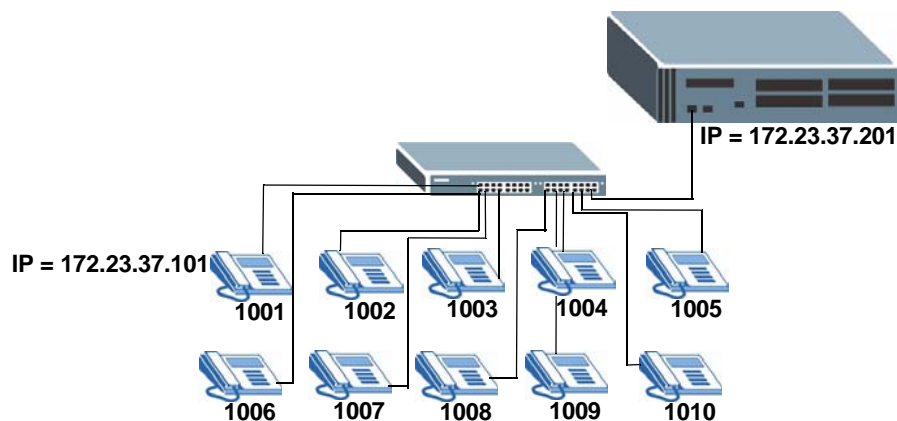
The extension number serves as the password the user uses to log into the X6004 to configure his extension's call forwarding, call blocking, phonebook, voice mail, and other settings. See [Chapter 37 on page 483](#) for more information.

- 8 If the IP phone is from ZyXEL and supports auto provisioning, use section [Section 3.1.4 on page 48](#) to map the SIP extensions to your network's SIP devices.

3.1.2 Connect IP Phones

You can now set up your IP phones. The next figure shows the network connections of the IP phones and the X6004. In this example, all of the IP phones and the X6004 are connected to an Ethernet switch and are all assigned IP addresses in the same subnet.

Figure 11 Connect IP Phones



3.1.3 Register IP Phones

After your network connections have been made, you can proceed with the SIP registration of the IP phones on your network. The next figure shows a typical SIP registration screen of a ZyXEL IP phone. This is a sample screen only, but it includes all the key fields necessary to complete a SIP registration. It shows the SIP registration of an IP phone with the extension **1001**.

Figure 12 Example IP Phone SIP Registration Screen

SIP Settings

SIP Account: SIP 1

Active

Number: 1001

SIP Local Port: 5060 (1024-65535)

SIP Server Address: 172.23.37.201

SIP Server Port: 5060 (1024-65535)

REGISTER Server Address: 172.23.37.201

REGISTER Server Port: 5060 (1024-65535)

SIP Service Domains: 172.23.37.201

Send Caller ID

Voice Mail Number: **1001

DNS SRV

Authentication

User Name: 1001

Password: *****

Apply Advance Setup

EXAMPLE

Extension Number of IP Phone

IP Address of the X6004

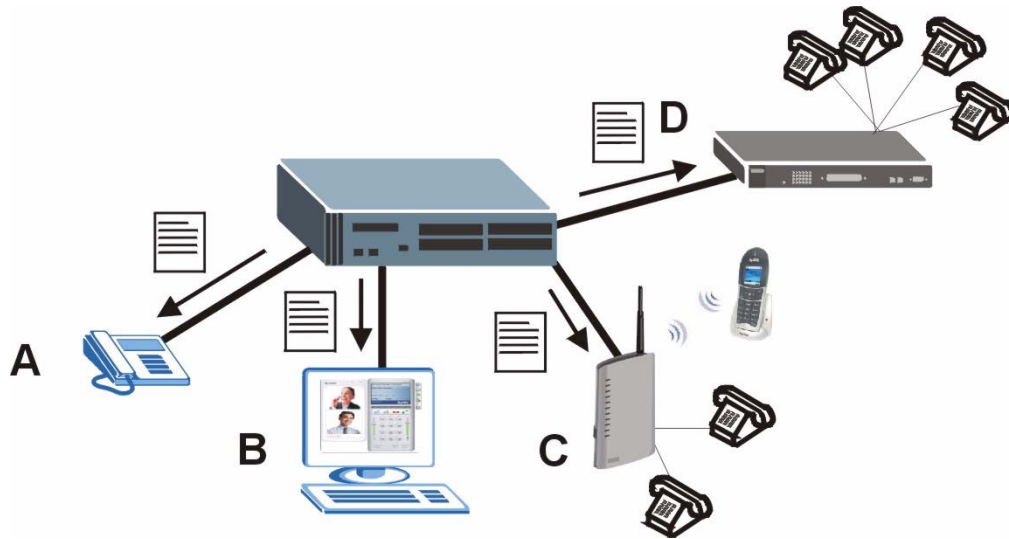
SIP Password (Prefix + Extension + Postfix)

Complete the SIP registration for all the IP phones on your network. When all the phones are registered, you can make internal calls by dialing the extension number assigned to each phone.

3.1.4 Auto Provisioning







A ZyXEL IP phone that supports auto provisioning can get a configuration text file from the X6004 (see [Appendix on page 521](#) for supported IP phones). The configuration file contains the SIP settings that the SIP device uses to register with the X6004. The following graphic shows an IP phone (A), softphone (B), VoIP gateway (C), and ATA (D) downloading configuration text files from the X6004.

Figure 13 Auto Provisioning



After you configure the SIP extensions (see [Section 3.1.1 on page 43](#)) and make your network connections (see [Figure 11 on page 46](#)), use the following directions to map each SIP extension to the appropriate SIP device. You need the MAC address of each SIP device (or the serial number if it is a softphone).

- 1 Click **Configuration > PBX > Server Configuration > Auto Provision**. Then click a SIP extension's **Edit** icon.

Auto Provision					
Configuration					
Phone Numbers	MAC Address	Serial No.	SPTGEN File Exist	Edit	View SPTGEN
1001			No		
1002			No		
1003			No		

- Enter the SIP device's MAC address (or serial number if it is a ZyXEL softphone). This example is for a softphone with a serial number of 1234567890. Click **Set Profile**.

Auto Provision Setting

Provisioning Setting

MAC Address:

Serial No.:

Auto Provision Active: On

Auto Provision Interval Time: (seconds) <1~26000000>

Auto Provision Delay Time: (seconds)

ATA device:

Port No.:

- The serial number of the softphone that is to use the SIP extension displays in the summary screen.

Auto Provision

Configuration

:Edit

Phone Numbers	MAC Address	Serial No.	SPTGEN File Exist	Edit	View SPTGEN
1001		1234567890	No	<input type="button" value="Edit"/>	<input type="button" value="View SPTGEN"/>
1002			No	<input type="button" value="Edit"/>	<input type="button" value="View SPTGEN"/>
1003			No	<input type="button" value="Edit"/>	<input type="button" value="View SPTGEN"/>

- Repeat these steps to map each SIP extension to a SIP device's MAC address or serial number.

3.1.4.1 Configuring the IP Phones for Auto Provisioning

Configure the ZyXEL IP phones to receive configuration information from the X6004. This typically involves enabling auto provisioning and specifying the protocol to use (HTTP at the time of writing). See the documentation that came with your ZyXEL IP phone for information on how to do this.

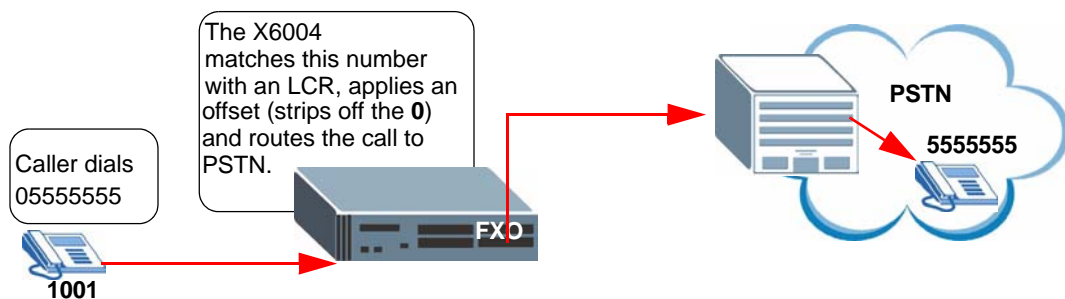
Once the IP phones receive their configuration information via auto provisioning, they will automatically register with the X6004. You can make internal calls by dialing the extension number assigned to each phone.

3.2 Making PSTN Calls

The following section shows you how to make and receive calls via a connection to the PSTN. This example covers:

- **The PSTN Connection** - configuring the outbound line group (connection settings) from the FXO interface card to the PSTN.
- **Creating a Dialing Rule for PSTN** - creating a rule which tells the X6004 when to use the PSTN connection when completing outbound calls.
- **Assigning an LCR to an Authority Group** - giving extensions the right to make outbound calls via the PSTN connection.

Figure 14 Making a PSTN Call

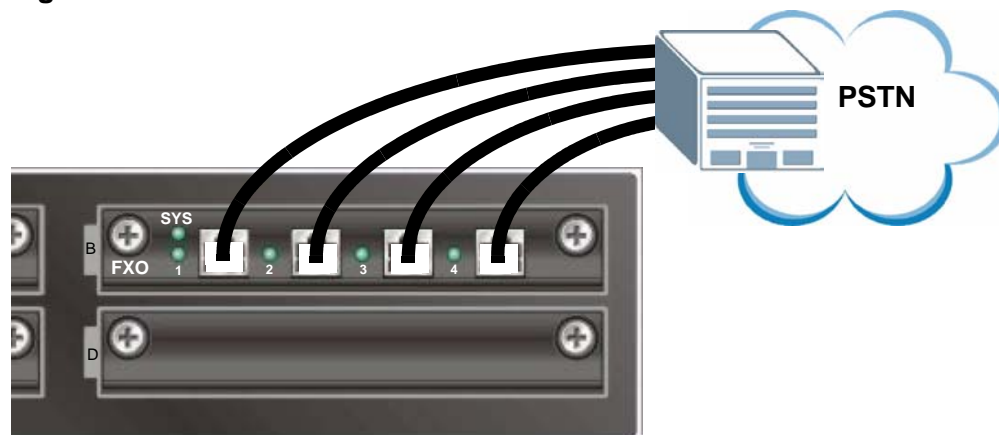


3.2.1 The PSTN Connection

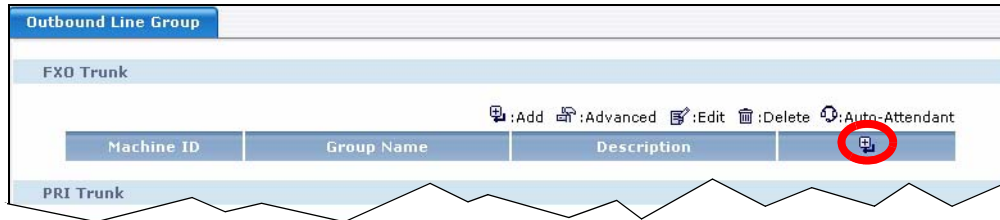
This example assumes that the X6004 has an FXO interface card already installed (refer to the Quick Start Guide) and that you have connected your telephone cables to the outlets that connect to your local telephone company. The front of your X6004 should look as shown in the following figure.

In this example, the FXO interface card is installed in slot **B** and ports **1-4** are used for the connections. You will use this information in a web configurator screen later.

Figure 15 FXO Interface Card Connection



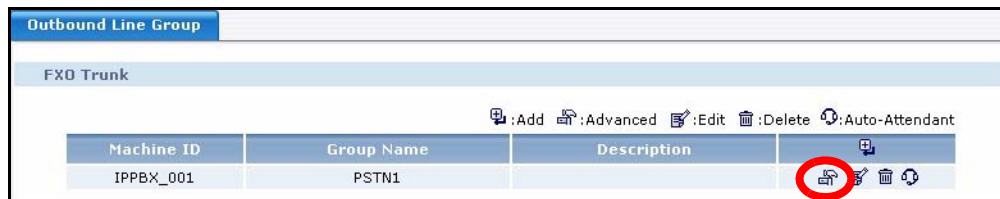
- 1 In the web configurator, click **Configuration > PBX > Outbound Line Management > Outbound Line Group** to open the following screen.



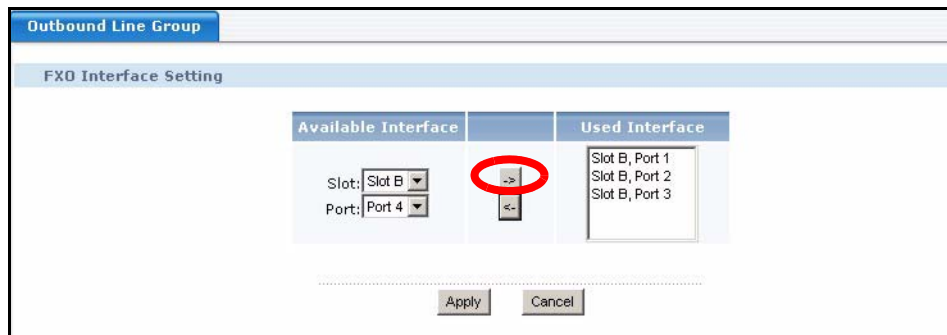
- 2 Click the **Add** icon in the **FXO Trunk** section to open the following screen. Enter the name of the group (**PSTN1** in this example) and click **Apply**. Note the **Machine ID** field (this is a name automatically assigned to the X6004). In some web configurator screens, the outbound line group is identified in the following format **Machine ID:Group Name**, so in our example it is **IPPBX_001:PSTN1**.

The screenshot shows the 'Outbound Line Group' configuration page, specifically the 'FXO Interface' section. It features three input fields: 'Machine ID' with a dropdown menu showing 'IPPBX_001', 'Group Name' with a text box containing 'PSTN1', and 'Description' with an empty text box. Below the fields are two buttons: 'Apply' and 'Back to Outbound Group'.

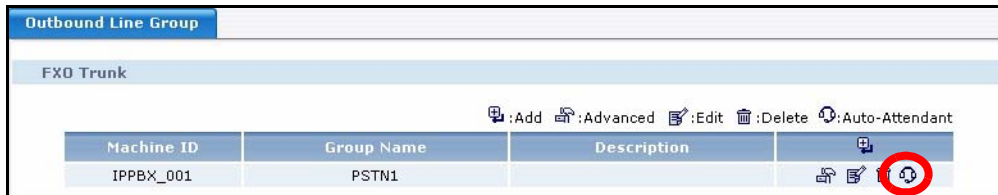
- 3 The new outbound line group displays in the following screen. Now you will add the FXO connections to the outbound line group. Click the outbound line group's **Advanced** icon.



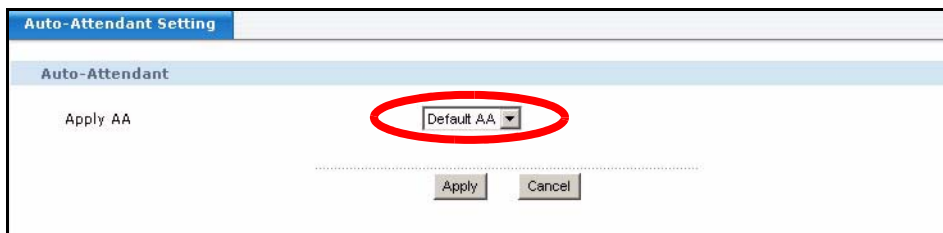
- 4 The following screen displays. Select the FXO interfaces that you want to add to this outbound line group and click the **Right** icon to move them to the **Used Interface** column. Click **Apply** when you are done.



- 5 The **Outbound Line Group** screen displays again. Click the **Auto-Attendant** icon. **Auto-Attendant** routes incoming calls (see [Chapter 19 on page 291](#) for details).



- 6 Make sure the **Default AA** option is selected (**FAX** is used to forward calls to a single extension, such as your FAX machine's extension) and click **Apply**.



- 7 People from the outside world can now call the X6004 using the PSTN numbers provided by your local telephone company. The **Default AA** prompts the callers to dial the extension they would like to reach. See [Section 3.2.2 on page 53](#) for information on how to set up a dialing rule so that the extensions on your network can connect to the PSTN.

3.2.2 Creating a Dialing Rule for PSTN





The following sections show you how to create outbound dialing rules (also referred to as Least Cost Routing or LCR).

The LCRs determine which outside line the X6004 should use to complete outbound calls. In our example we want to use the **PSTN1** outbound line group to complete local calls.

Figure 16 Outbound Calls via PSTN



- 1 In the web configurator, click **Configuration > PBX > Outbound Line Management > LCR** to open the following screen.

LCR List				
Delete				
Apply LCR Sequence Add Edit Delete				
<input type="checkbox"/>	LCR Name	Description		
<input type="checkbox"/>	ezout	easy to call out	↕	
<input type="checkbox"/>	local_call	local call LCR	↕	
<input type="checkbox"/>	long_distance_call	long distance call LCR	↕	
<input type="checkbox"/>	international_call	international call LCR	↕	
Delete				

- 2 Click the **Edit** icon in the **local_call** section to open the following screen. Select the outbound line group from the pool column that you want to add to this LCR (in our example this is **IPPBX_001:PSTN1** as configured in [Section 3.2.1 on page 50](#)), then click the **Right** icon to move them to the **Selected** column. Click **Apply** to save the outbound line group in the LCR and then click the **Add** icon to configure a dial condition. |

The screenshot displays the 'LCR List / LCR Item' configuration interface. Under the 'LCR Data' section, the 'LCR Name' is 'local_call' and the 'Description' is 'local call LCR'. The 'Max Call Time' is set to 'sec.'. The 'Outbound line group' section features two columns: 'Pool' and 'Selected'. The 'Pool' column contains 'IPPBX_001:ITSP1', and the 'Selected' column contains 'IPPBX_001:PSTN1'. The 'Apply' button is circled in red. Below this, the 'Dial Condition List' section shows a table with one row labeled 'Dial Condition' and an 'Add' icon circled in red.

- 3 The **Dial Condition** screen appears as shown.
- Type **0** followed by a period (.) in the **Dial Condition** field. This means that this LCR will be used when callers dial any number that begins with a **0**. The period (.) is a wildcard character, meaning anything can follow the zero.
 - Test the dial condition. In our example, we tested the number **05555555** to see if it matches our dial condition. You can test any number by typing it in the **Number Pattern Test** field and clicking the **Right** icon; an **O** appears, if the number typed in matches the dial condition and an **X** appears if it does not match the dial condition.
 - Specify an offset value. In our example, we configure an offset value of **1**. The offset value tells the X6004 how many initial digits (if any) it should strip off of the dialed number before routing the call to the external line. See [Figure 3 on page 56](#) for an example.

- Click **Apply** to save your settings.

LCR List / LCR Item / Dial Condition

Dial Condition

LCR Name: local_call

Dial Condition: 0.

Number Pattern Test: 05555555

Dial Number Viewer

Channel	Offset	Length	Prefix	Postfix
IPPBX_001:PSTN1	1			

Apply Cancel

- 4 You are done configuring the LCR. However, before it can be used by any of the phones connected to the X6004, the LCR needs to be assigned to an appropriate authority group.

3.2.3 Assigning an LCR to an Authority Group

The **Group Management** screen allows you to give an authority group (and the extensions in that group) the right to use an LCR (outbound dial condition). In our example, we give the authority group **Basic** the right to call out using the LCR **local_call**.

Procedure:

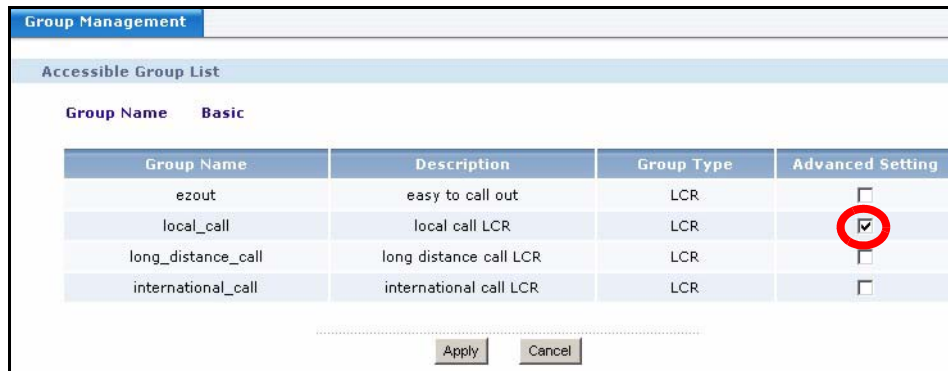
- 1 Click **Configuration > PBX > Group Management** to view the following screen.

Group Management

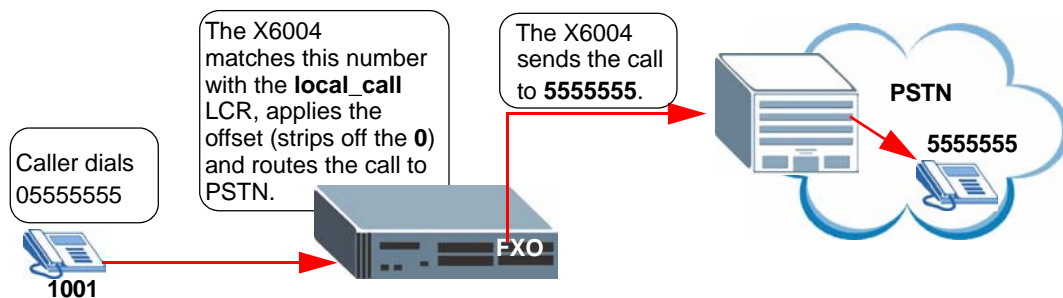
Authority Group

Machine ID	Group Name	Description	Advanced Setting
IPPBX_001	Basic		LCR

- Click the **Advanced** icon in the **Authority Group** section (in this example there is only one authority group - **Basic**) of the screen to view the screen as shown. Select the checkbox in the **Advanced** column of the **local_call** LCR as shown below. Click **Apply**.



- You can now use the telephones that are part of the **Basic** authority group to make outbound calls using the PSTN connection. The following figure summarizes the outbound call process for this example.

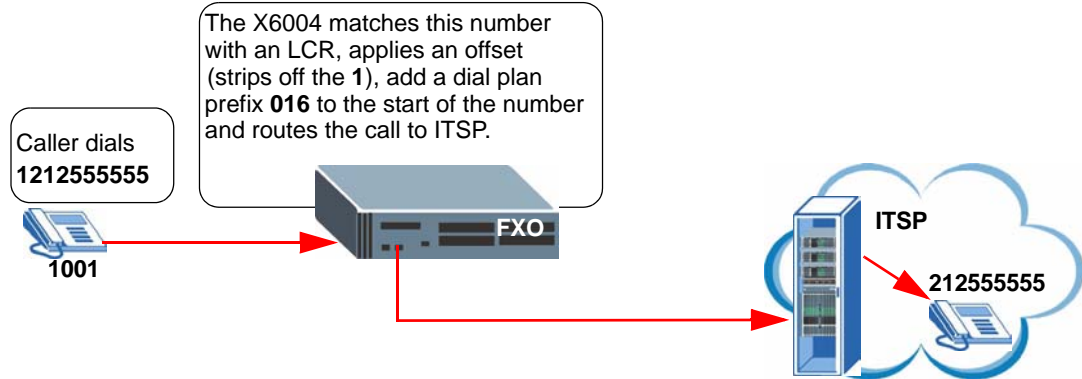


3.3 Making ITSP Calls

The following section shows you how to make and receive calls via a connection to the PSTN. This example covers:

- The ITSP Connection** - configuring the outbound line group (connection settings) from the X6004 to the ITSP.
- Creating a Dialing Rule for ITSP** - creating a rule which tells the X6004 when to use the ITSP connection when completing outbound calls.

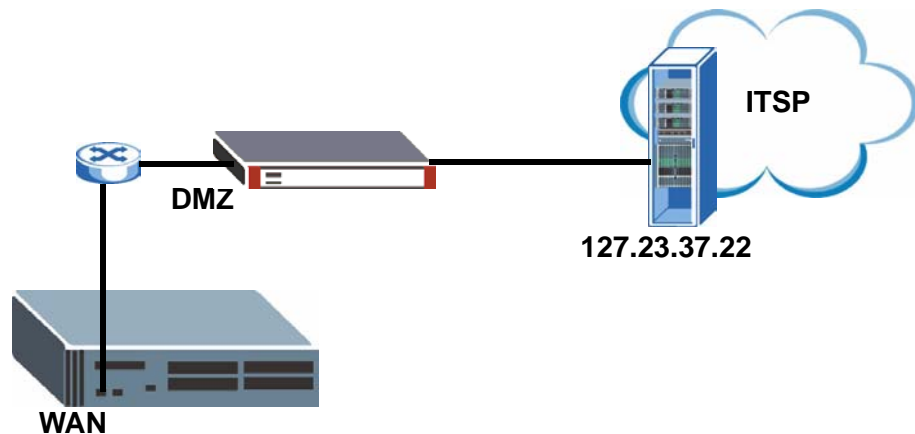
- **Assigning an LCR to an Authority Group** - giving extensions the right to make outbound calls via the ITSP connection.



3.3.1 The ITSP Connection

The following section introduces how to configure a connection to the ITSP. This example assumes that the X6004 has a network connection to the SIP server at your ITSP. The following figure shows the network configuration used in this example.

Figure 17 Network Connection to ITSP

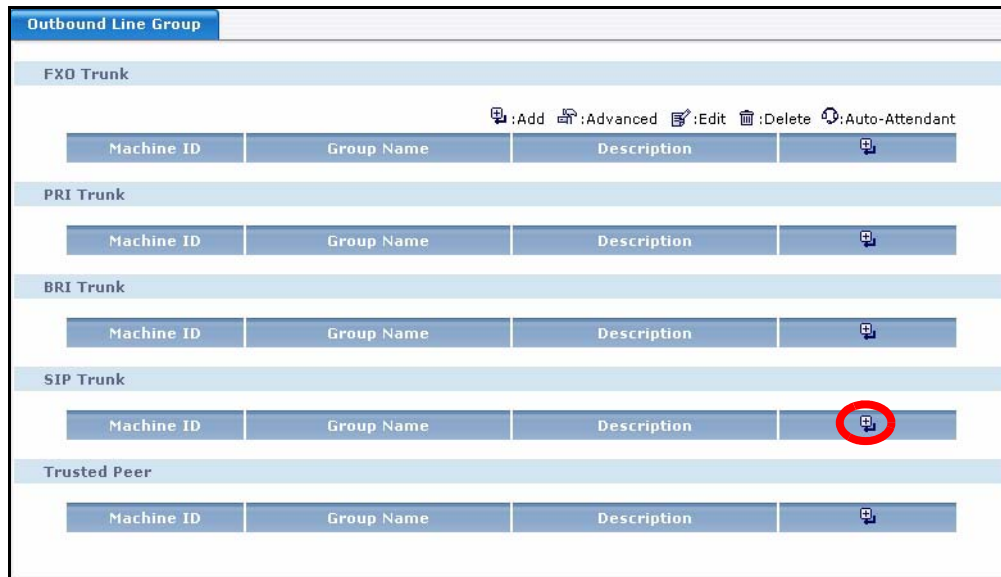


The following table describes sample account information as provided by the ITSP:

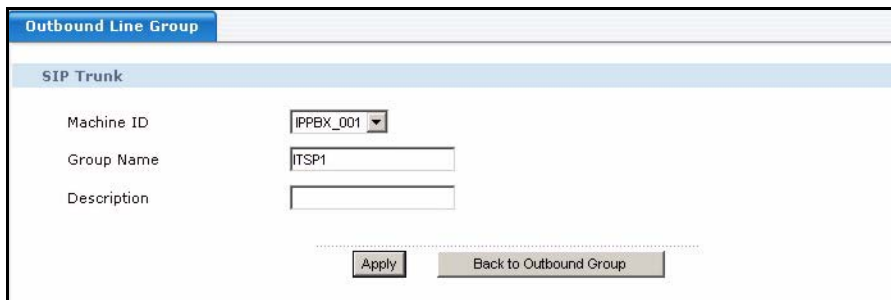
Table 3 Sample VoIP Account Information

INFO	VALUES	INFO	VALUES
SIP Number	5551122	SIP Service Domain	127.23.37.22
SIP Server Address	127.23.37.22	DTMF Mode	SIP-INFO
SIP Server Port	5060	SIP Username	5551122
Register Server Address	127.23.37.22	SIP Password	1234
Register Server Port	5060	Codecs supported	G.726, G.729A

- 1 In the web configurator, click **Configuration > PBX > Outbound Line Management > Outbound Line Group** to open the following screen.



- 2 Click the **Add** icon in the **SIP Trunk** section to open the following screen. Enter the name of the group ("ITSP1" in this example) and click **Apply**. Note the **Machine ID** field (this is a name automatically assigned to the X6004), in some management screens the outbound line group is identified in the following format **Machine ID:Group Name**, so in our example it is **IPPBX_001:ITSP1**.



- The new outbound line group displays in the following screen. Now you will configure the connection to your ITSP. Click the outbound line group's **Advanced** icon.

The screenshot displays the 'Outbound Line Group' configuration page. At the top, there is a blue header with the text 'Outbound Line Group'. Below this, the page is organized into sections for different trunk types: FXO Trunk, PRI Trunk, BRI Trunk, SIP Trunk, and Trusted Peer. Each section contains a table with columns for 'Machine ID', 'Group Name', and 'Description'. In the FXO Trunk section, there are additional icons for 'Add', 'Advanced', 'Edit', 'Delete', and 'Auto-Attendant'. In the SIP Trunk section, there is one entry with 'Machine ID' 'IPPBX_001' and 'Group Name' 'ITSP1'. The 'Advanced' icon (a gear) for this entry is circled in red. The 'Trusted Peer' section also contains a table with the same columns.

- The following screen displays. Fill in the fields with the information provided by your ITSP (in our example we use the sample information as shown in [Table 3 on page 58](#)). Click **Apply** when you are done.

SIP Trunk Setting

Representative Num:

Proxy Server Address:

SIP Server Port:

REGISTER Server Address:

REGISTER Server Port:

Service Domain: Disable Define service domain:

Outbound Proxy: Disable Define outbound proxy:

Outbound Proxy Port:

DTMF Mode:

Privacy: Disable Enable

Specific Support: None Nortel (MCS 5100/5200) Huawei

Proxy Require:

Channel-limit: Range (1~128)

Session Timer

enable Session Timer

Minimum SE: sec. (90 ~ 1800)

Session Expires: sec. (90 ~ 86400, must > Minimum SE)

CallerID Setting

CallerID Viewer: From: "Extension" <Extension@server IP>

CallerID Name & Number:

- Extension + Extension
- Extension + Representative Num
- Representative Num + Representative Num
- Extension + Representative Num (DDI/DID mapped)
- Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped)

The Extension Prefix:

Authentication

User Name:

Password:

CODEC Setting

CODEC Pool: G.729, H.263, H.261, H.264, MP4

CODEC List: G.729, G.711 u-law, G.711 a-law

- The **Outbound Line Group** screen displays again. Click the **Auto-Attendant** icon in the **SIP Trunk** section of the screen.

Outbound Line Group

FXD Trunk

:Add :Advanced :Edit :Delete :Auto-Attendant

Machine ID	Group Name	Description	

PRI Trunk

Machine ID	Group Name	Description	

BRI Trunk

Machine ID	Group Name	Description	

SIP Trunk

Machine ID	Group Name	Description	
IPPBX_001	ITSP1		

Trusted Peer

Machine ID	Group Name	Description	

- 6 Make sure the **Default AA** option is selected (**FAX** is used to forward calls to a single extension, such as your FAX machine's extension) and click **Apply**.

Auto-Attendant Setting

Apply AA: **Default AA**

DDI/DID Mapping Setting

Representative Number

DDI/DID Mask: 0 (0 means unlimited)

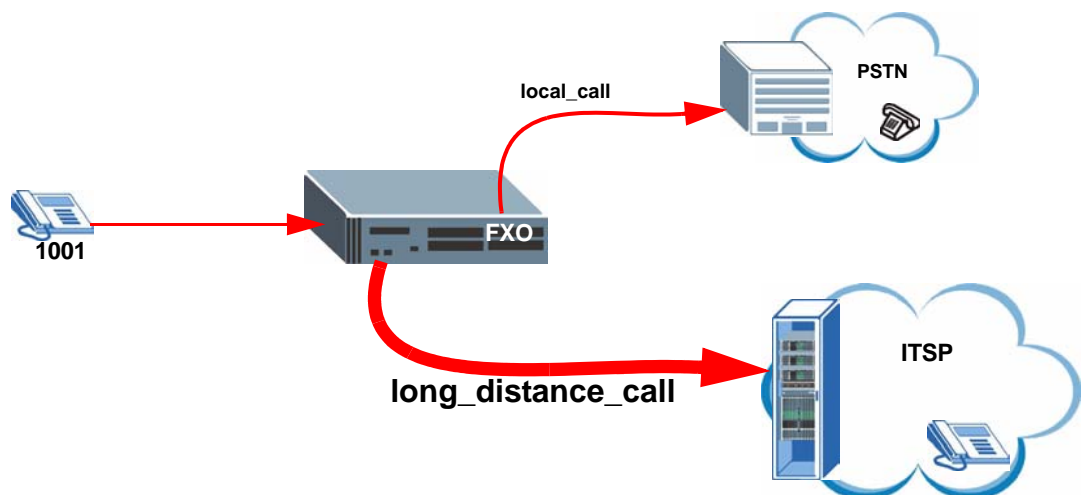
DDI/DID Number	Extension Number	
		<input checked="" type="radio"/> <input type="radio"/> Auto-Attendant

- 7 People from the outside world can now call the X6004 using the numbers provided by your ITSP. The **Default AA** prompts the callers to dial the extension they would like to reach. See [Section 3.3.2 on page 61](#) for information on how to set up a dialing rule so that the extensions on your network can make calls via your ITSP.

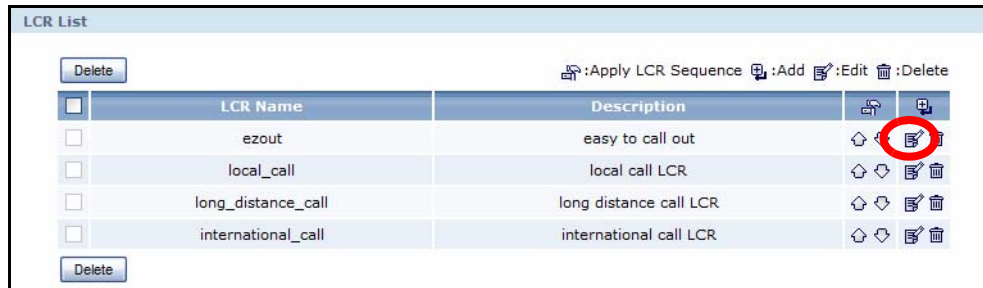
3.3.2 Creating a Dialing Rule for ITSP

In our example we want to use the **ITSP1** outbound line group to complete long distance calls. This is done by configuring the **long_distance_call** LCR. This figure also shows the **local_call** LCR we created in [Section 3.2.2 on page 53](#).

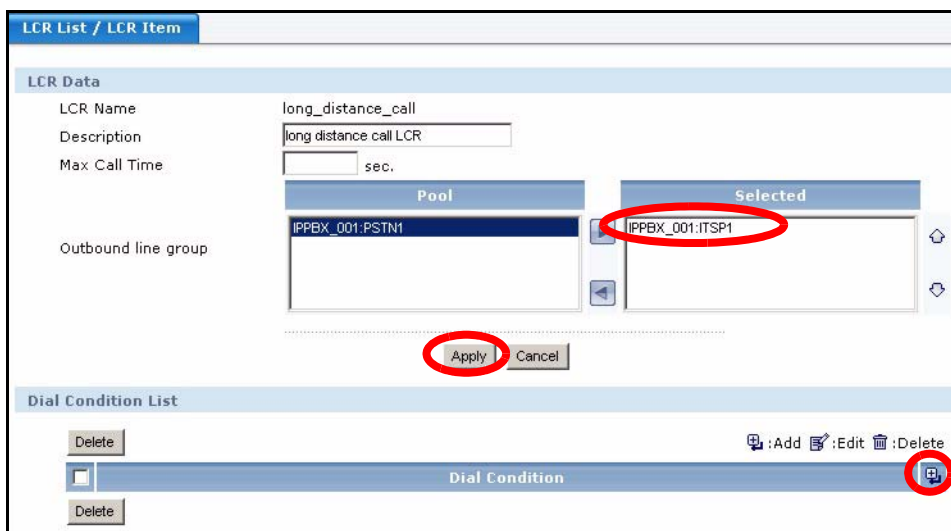
Figure 18 Outbound Calls via ITSP



- 1 In the web configurator, click **Configuration > PBX > Outbound Line Management > LCR** to open the following screen.



- 2 Click the **Edit** icon in the **long_distance_call** section to open the following screen. Select the outbound line group from the pool column that you want to add to this LCR (in our example this is **IPPBX_001:ITSP1** as configured in [Section 3.3.1 on page 57](#)), then click the **Right** icon to move it to the **Selected** column. Click **Apply** to save the outbound line group in the LCR and then click the **Add** icon to configure a dial condition.



- 3 The **Dial Condition** screen appears as shown.
 - Type **1XXXXX** followed by a period (.) in the **Dial Condition** field. This means that this LCR will be used when callers dial any 7 or greater digit number that begins with a **1**. The **X** stands for any digit 0 to 9 and is used to create a minimum length condition. The period (.) is a wildcard indicating that any number can follow the **1XXXXX** condition.
 - Test the dial condition. In our example, we tested the number **1212555555** to see if it matches our dial condition. You can test any number by typing it in the **Number Pattern Test** field and clicking the **Right** icon; an **O** appears if the number typed in matches the dial condition and an **X** appears if it does not match the dial condition.

- Specify an offset value. In our example, we configure an offset value of **1**. The offset value tells the X6004 how many initial digits (if any) it should strip off of the dialed number before routing the call to the external line.
- Specify a prefix number. In this example, our ITSP has a special dial plan for long distance calls. A caller must dial **016** in order to take advantage of the dial plan. By adding **016** in the **Prefix** field, the X6004 automatically adds **016** to calls that match this dial condition. See [Figure 3 on page 65](#) for an example.
- Click **Apply** to save your settings.

LCR List / LCR Item / Dial Condition

Dial Condition

LCR Name: long_distance_call

Dial Condition: 1XXXXX:

Number Pattern Test: 1212555555

Dial Number Viewer

Channel	Offset	Length	Prefix	Postfix
IPPBX_001:ITSP1	1		016	

- 4 You are done configuring the LCR. However, before it can be used by any of the phones connected to the X6004, the LCR needs to be assigned to an appropriate authority group.

3.3.3 Assigning an LCR to an Authority Group

The **Group Management** screen allows you to give an authority group (and the extensions in that group) the right to use an LCR (outbound dial condition). In our example, we give the authority group **Basic** the right to call out using the LCR **long_distance_call**.

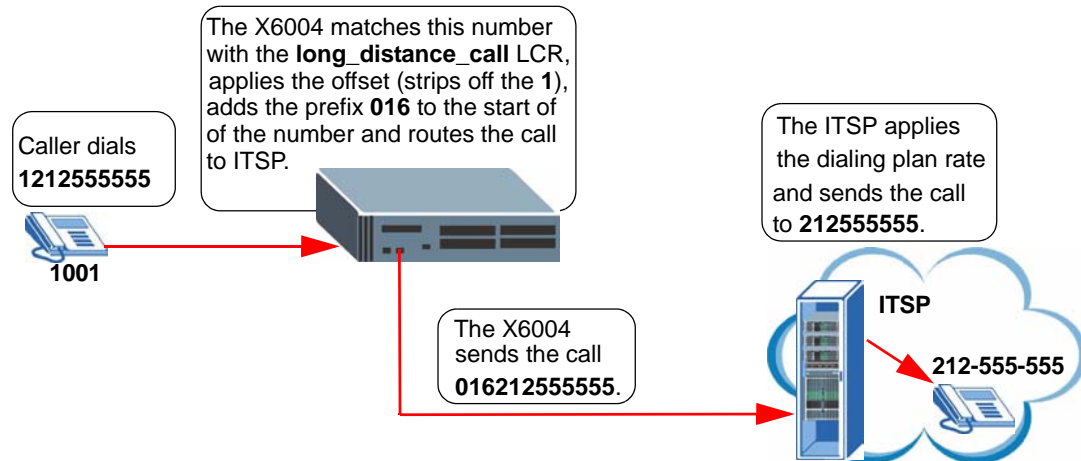
- 1 Click **Configuration > PBX > Group Management** to view the following screen.

Group Management			
Authority Group			
Machine ID	Group Name	Description	Advanced Setting
IPPBX_001	Basic		
FXO Trunk			
Machine ID	Group Name	Description	Advanced Setting
IPPBX_001	PSTN1		
SIP Trunk			
Machine ID	Group Name	Description	Advanced Setting

- 2 Click the **Advanced** icon in the **Authority Group** section (in this example there is only one authority group - **Basic**) of the screen to view the screen as shown. Select the checkbox in the **Advanced** column of the **long_distance_call** LCR as shown below. Click **Apply**.

Group Management			
Accessible Group List			
Group Name		Basic	
Group Name	Description	Group Type	Advanced Setting
ezout	easy to call out	LCR	<input type="checkbox"/>
local_call	local call LCR	LCR	<input checked="" type="checkbox"/>
long_distance_call	long distance call LCR	LCR	<input checked="" type="checkbox"/>
international_call	international call LCR	LCR	<input type="checkbox"/>

- 3 You can now use the telephones that are part of the **Basic** authority group to make long distance calls using the ITSP connection. The following figure summarizes the outbound call process for this example.

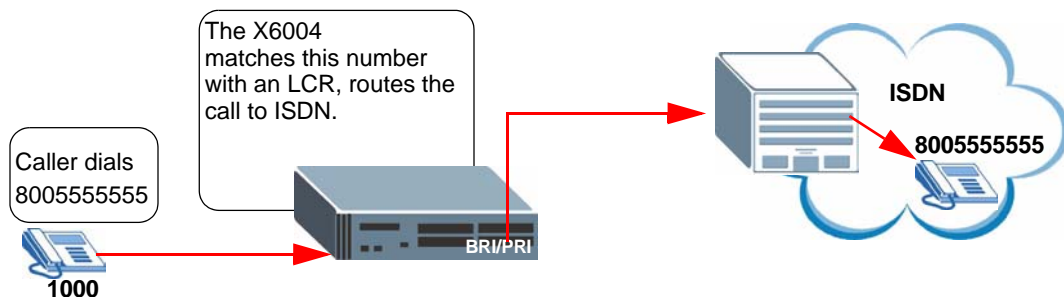


3.4 Making ISDN Calls

The following section shows you how to make and receive calls via a connection to the ISDN. This example covers:

- **The ISDN Connection** - configuring the outbound line group's connection settings from the BRI/PRI interface card to the ISDN.
- **Creating a Dialing Rule for ISDN** - creating a rule which tells the X6004 when to use the ISDN connection when completing outbound calls.
- **Assigning an LCR to an Authority Group** - giving extensions the right to make outbound calls via the ISDN connection.

Figure 19 Making an ISDN Call

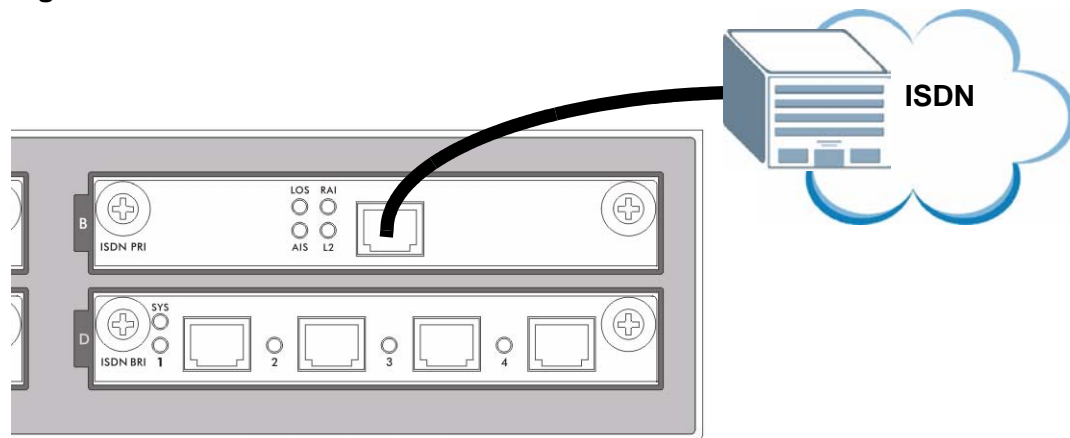


3.4.1 The ISDN Connection

/This example assumes that the X6004 has an ISDN PRI interface card already installed (refer to the Quick Start Guide) and that you have connected your telephone cables to the outlets that connect to your local telephone company. The front of your X6004 should look as shown in the following figure.

Note: In this example, a PRI interface card is installed in slot **B** and port **1** is used for the connection. You will use this information in a web configurator screen later.

Figure 20 PRI Interface Card Connection



The following table describes our sample PRI information as provided by the telephone service provider:

Table 4 Sample PRI Information

SWITCH TYPE	NT/TE MODE	LINEBUILDOUT	FRAMING	CODING
NET5	NT	120	CRC4	HDB3

- 1 In the web configurator, click **Configuration > PBX > Server Configuration > Server > PRI** to open the following screen.

Specify which PRI interface card you want to configure in the **Slot** and **Port** fields.

Then configure the **Switch Type**, **NT/TE Mode**, **LineBuildOut**, **Framing** and **Coding** fields according to the settings on the peer end of PRI device or on the set up information provided by your telephone service provider. See [Section 6.6 on page 136](#) for more information.

Click **Apply** to save your changes.

PRI Setting

PRI Configuration Machine ID: Slot: Port:

Switch Type

NT/TE Mode

LineBuildOut

Framing

Coding

Digit Handling

Speaking Volume Level:

Listening Volume Level:

- 2 Click **Configuration > PBX > Outbound Line Management > Outbound Line Group** to open the following screen.

Outbound Line Group

FXO Trunk

Machine ID	Group Name	Description	
			<input type="button" value="Add"/>

PRI Trunk

Machine ID	Group Name	Description	
			<input type="button" value="Add"/>

BRI Trunk

Machine ID	Group Name	Description	
			<input type="button" value="Add"/>

SIP Trunk

Machine ID	Group Name	Description	
			<input type="button" value="Add"/>

Trusted Peer

Machine ID	Group Name	Description	
			<input type="button" value="Add"/>

- Click the **Add** icon in the **PRI Trunk** section to open the following screen. Enter the name of the group (**OG_PRI1** in this example) and click **Apply**. Note the **Machine ID** field (this is a name automatically assigned to the X6004). In some web configurator screens, the outbound line group is identified in the following format **Machine ID:Group Name**, so in our example it is **IPPBX_001:OG_PRI1**.

PRI Trunk Setting

Machine ID: IPPBX_001

Group Name:

Description:

- The new outbound line group displays in the following screen. Now you will add the FXO connections to the outbound line group. Click the outbound line group's **Advanced** icon.

Outbound Line Group

FXO Trunk

Machine ID | Group Name | Description | [Add] [Advanced] [Edit] [Delete] [Auto-Attendant]

PRI Trunk

Machine ID	Group Name	Description	[Add] [Advanced] [Edit] [Delete] [Auto-Attendant]
IPPBX_001	OG_PRI1		[Add] [Advanced] [Edit] [Delete] [Auto-Attendant]

- The following screen displays. Assume that you want calls on Slot **B** and Port **1** to be answered by the Auto-Attendant, so select **AA** and the correct slot and port. Click the **Right** icon to move the slot and port to the **Used Interface** column. Click **Apply** when you are done.

PRI Trunk Setting

Option: DDI/DID AA Direct

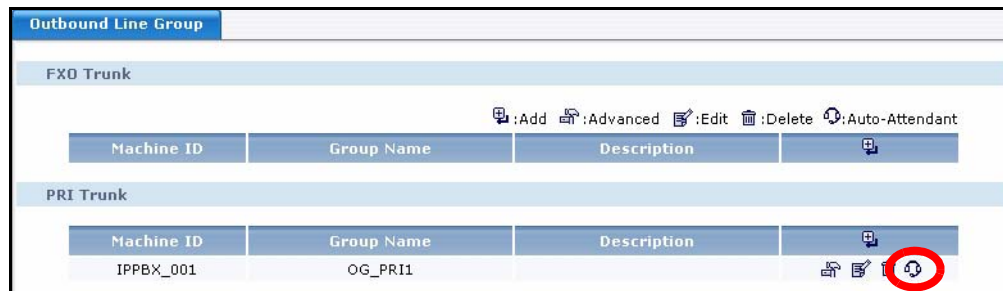
Available Interface	Used Interface
Slot: Slot C Port: Port 1	

Incoming Calling Party Number

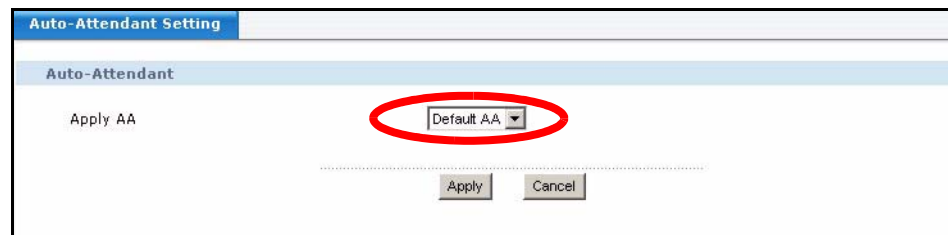
Type of Number	Prefix
Unknown	<input type="text"/>
National	<input type="text"/>
International	<input type="text"/>
Network Specific	<input type="text"/>
Subscriber	<input type="text"/>
Abbreviated	<input type="text"/>

[Apply] [Cancel]

- 6 The **Outbound Line Group** screen displays again. Click the **Auto-Attendant** icon. **Auto-Attendant** routes incoming calls (see [Chapter 19 on page 291](#) for details).



- 7 Select the **Default AA** option and click **Apply**.



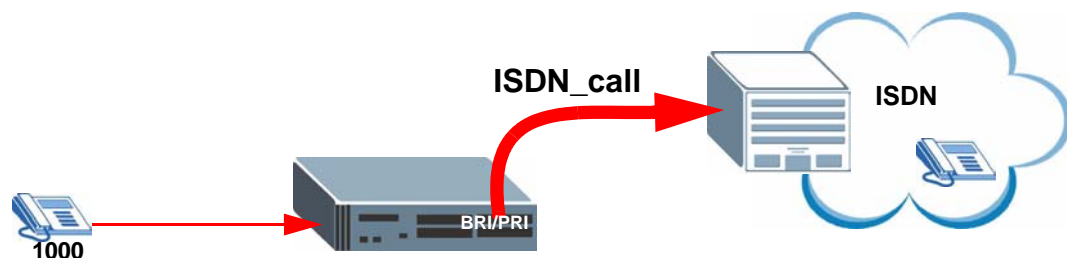
- 8 People from the outside world can now call the X6004 using the ISDN numbers provided by your local telephone company. The **Default AA** prompts the callers to dial the extension they would like to reach. See [Section 3.4.2 on page 69](#) for information on how to set up a dialing rule so that the extensions on your network can connect to the ISDN.

3.4.2 Creating a Dialing Rule for ISDN

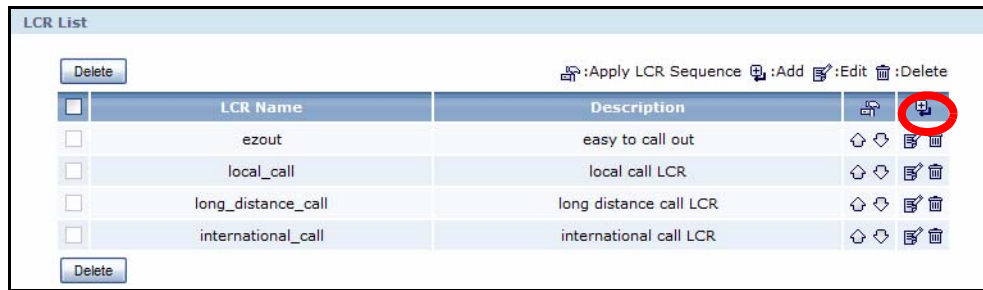
The following sections show you how to create outbound dialing rules (also referred to as Least Cost Routing or LCR).

The LCRs determine which outside line the X6004 should use to complete outbound calls. In our example we want to use the **OG_PRI 1** outbound line group to complete local calls.

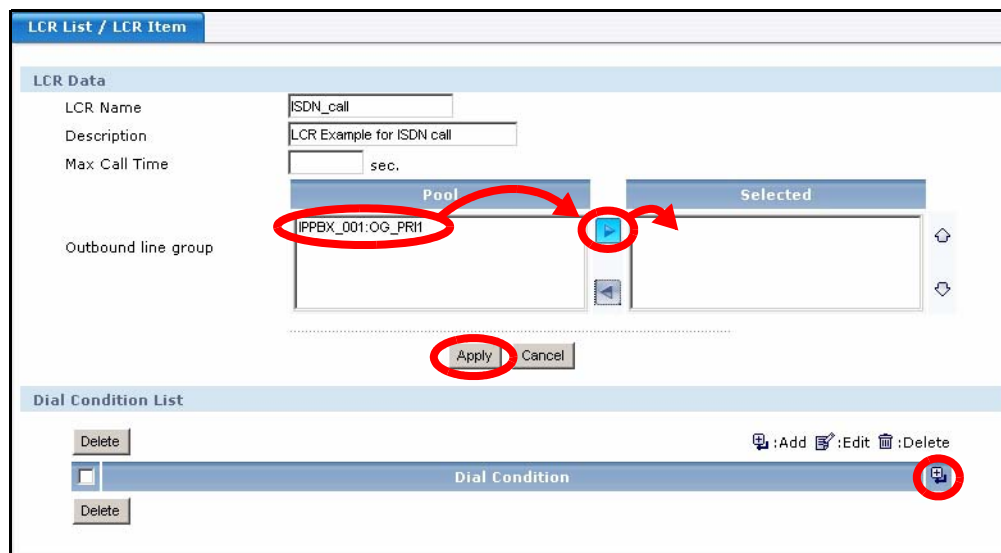
Figure 21 Outbound Calls via ISDN



- 1 In the web configurator, click **Configuration > PBX > Outbound Line Management > LCR** to open the following screen.



- 2 Click the **Add** icon to open the following screen. Select the outbound line group from the pool column that you want to add to this LCR (in our example this is **IPPBX_001:OG_PRI1** as configured in [Section 3.4.1 on page 66](#)), then click the **Right** icon to move them to the **Selected** column. Click **Apply** to save the outbound line group in the LCR and then click the **Add** icon to configure a dial condition.



- 3 The **Dial Condition** screen appears as shown.
 - Type **800** followed by a period (.) in the **Dial Condition** field. This means that this LCR will be used when callers dial any number that begins with **800**. The period (.) is a wildcard character, meaning anything can follow the 800.
 - Test the dial condition. In our example, we test the number **8005555555** to see if it matches our dial condition. You can test any number by typing it in the **Number Pattern Test** field and clicking the **Right** icon; an **O** appears, if the number typed in matches the dial condition and an **X** appears if it does not match the dial condition.
 - Leave the offset value empty. In our example, we do not need to configure the offset value. See [Figure 21 on page 69](#) for an example.

- Click **Apply** to save your settings.

LCR List / LCR Item / Dial Condition

Dial Condition

LCR Name: ISDN_call

Dial Condition: 800.

Number Pattern Test: 8005555555

Dial Number Viewer

Channel	Offset	Length	Prefix	Postfix
IPPBX_001:OG_PRI1				

Apply Cancel

- 4 You are done configuring the LCR. However, before it can be used by any of the phones connected to the X6004, the LCR needs to be assigned to an appropriate authority group.

3.4.3 Assigning an LCR to an Authority Group

The **Group Management** screen allows you to give an authority group (and the extensions in that group) the right to use an LCR (outbound dial condition). In our example, we give the authority group **Basic** the right to call out using the LCR **ISDN_call**.

- 1 Click **Configuration > PBX > Group Management** to view the following screen.

Group Management

Authority Group

Machine ID	Group Name	Description	Advanced Setting
IPPBX_001	Basic		ISDN

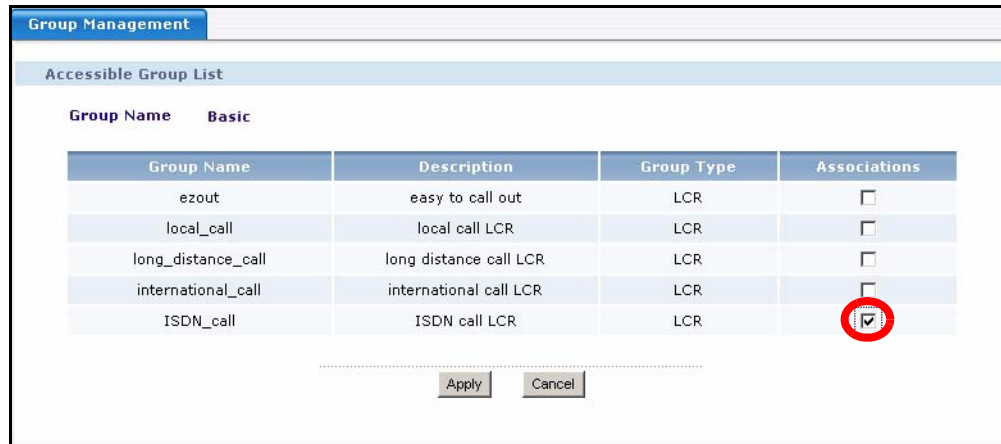
FXO Trunk

Machine ID	Group Name	Description	Advanced Setting
IPPBX_001	PSTN1		

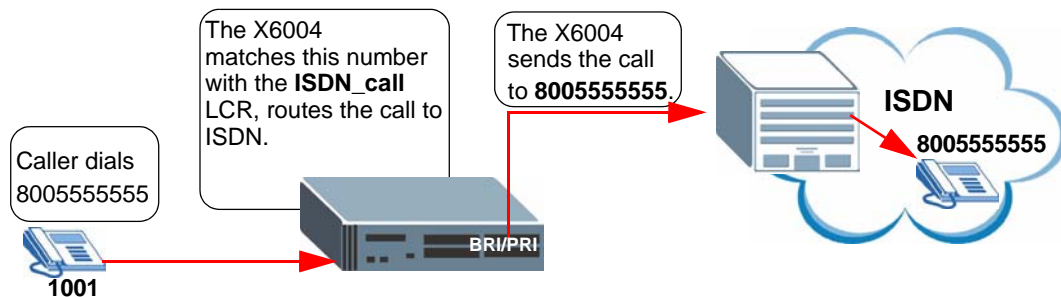
SIP Trunk

Machine ID	Group Name	Description	Advanced Setting

- Click the **Advanced** icon in the **Authority Group** section (in this example there is only one authority group - **Basic**) of the screen to view the screen as shown. Select the checkbox in the **Advanced** column of the **ISDN_call** LCR as shown below. Click **Apply**.



- You can now use the telephones that are part of the **Basic** authority group to make outbound calls using the ISDN connection. The following figure summarizes the outbound call process for this example.

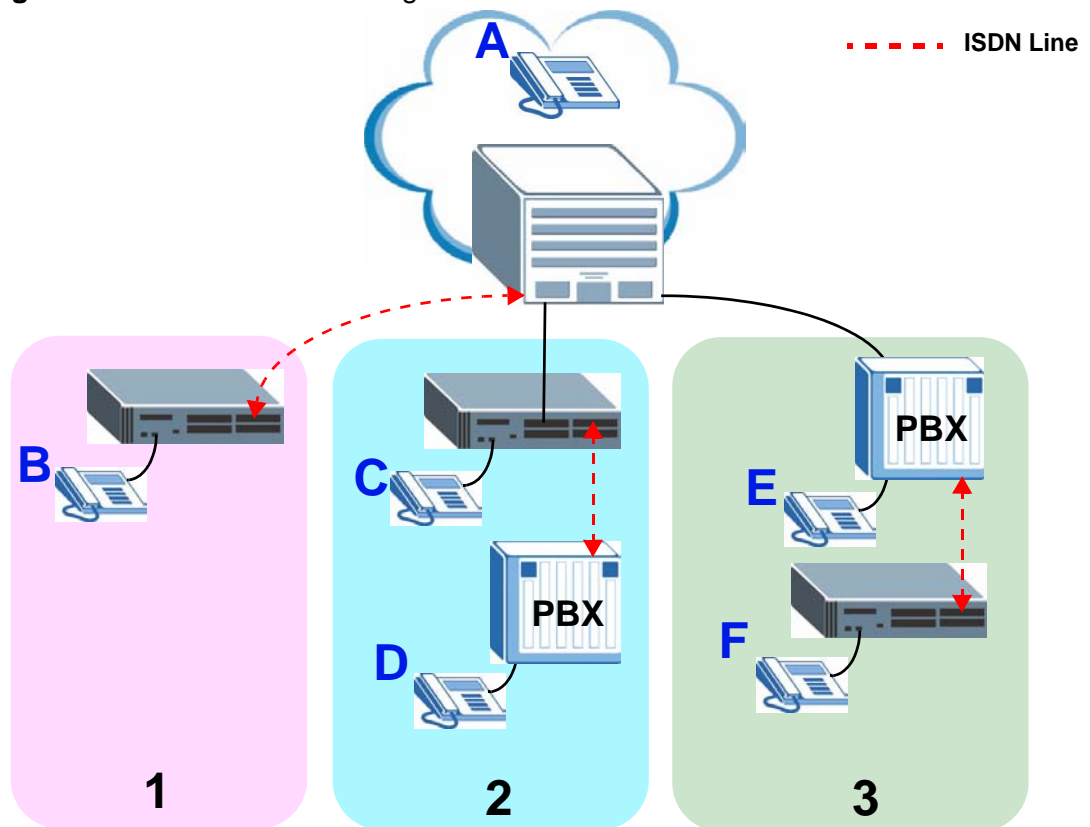


3.5 ISDN Network Configuration Examples

The following section shows you some examples of deploying the X6004 using ISDN in organizations of various sizes.

The following figure shows the three examples (1 ~ 3).

Figure 22 ISDN Network Configuration



3.5.1 Example 1: Small/Medium Business

For a small/medium company, the X6004 is the only device that forwards ISDN calls between the company and the telephone service provider.

- For an example of configuring ISDN settings, see [Section 3.4 on page 65](#).
- If you want outsiders to dialing in directly to extensions without going through the Auto-Attendant, follow the instruction until step 5, select **DDI/DID** and configure the settings as following.

Figure 23 ISDN Network Configuration

PRI Trunk Setting

Option **DDI/DID** AA Direct

Directory Number

Available Interface		Used Interface
Slot: <input type="text" value="Slot C"/> <input type="button" value="v"/> Port: <input type="text" value="Port 1"/> <input type="button" value="v"/>	<input type="button" value="▶"/> <input type="button" value="◀"/>	<input type="button" value="▲"/> <input type="button" value="▼"/>

DDI/DID Mapping

DDI/DID Mask

DDI/DID Number	Extension Number	
<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

Outgoing Calling Party Number

Type of Number

Calling Party Number Prefix

Incoming Calling Party Number

Type of Number	Prefix
Unknown	<input type="text"/>
National	<input type="text"/>
International	<input type="text"/>
Network Specific	<input type="text"/>
Subscriber	<input type="text"/>
Abbreviated	<input type="text"/>

In the DDI/DID Mapping, define **DDI/DID Mask** (the digits of the **Directory Number** on the right) for extension mappings. For example, you define **4** for the DDI/DID Mask and add **1001** to **1001** for the mapping rule. So an incoming call 8005551001 will be forwarded to the extension.

3.5.2 Example 2: Company with Existing PBX

For a company which already has a PBX. The X6004 is deployed between the PBX and the telephone service provider. You can connect the X6004 to the telephone service provider using PSTN connection (see [Section 3.2 on page 50](#)). Comparing to use the FXO interface cards, the number of simultaneous calls supported is greater and the cost is lower. In this example, we use one PRI line between the X6004 and the PBX to support up to 23 (using T1) or up to 30 (using E1) voice channels. The capacity and cost for call number support is greater than using FXO interface cards. (Using 4 FXO interface cards supports only 16 simultaneous calls.)

- See an example of configuring ISDN settings in [Section 3.4 on page 65](#).
- If you want the callers from the PBX's extensions not to go through the Auto-Attendant, follow the instruction until step 5, select one of the following settings and continue the other settings according the instruction.
 - If you don't want incoming calls to go through the Auto-Attendant, select **Direct** and configure settings as following (leave the **Calling Party Number** section empty except you want to define the trusted callers). Then click **Apply**.

Figure 24 Example: Direct

PRI Trunk Setting

Option DDI/DID AA Direct

Available Interface		Used Interface
Slot: <input type="text" value="Slot C"/> Port: <input type="text" value="Port 1"/>	<input type="button" value="▶"/> <input type="button" value="◀"/>	<input type="button" value="▲"/> <input type="button" value="▼"/>

Calling Party Number

Length

Trusted Peer	
<input style="width: 90%;" type="text"/>	<input type="button" value="⊕"/>

Incoming Calling Party Number

Type of Number	Prefix
Unknown	<input style="width: 80%;" type="text"/>
National	<input style="width: 80%;" type="text"/>
International	<input style="width: 80%;" type="text"/>
Network Specific	<input style="width: 80%;" type="text"/>
Subscriber	<input style="width: 80%;" type="text"/>
Abbreviated	<input style="width: 80%;" type="text"/>

- If you are using BRI line(s) and you want to have multiple subscriber numbers on one port, select **MSN** and configure the settings as following. Then click **Apply**.

Figure 25 Example: MSN

The screenshot shows a configuration window titled "Outbound Line Group" with a sub-section "BRI Trunk Setting". Under "Option", there are four radio buttons: "DDI/DID", "AA", "Direct", and "MSN", with "MSN" selected. The "Number" field contains "1001". Under "Used Interface", there are three dropdown menus: "Slot:" set to "Slot D", "Port:" set to "Port 1", and "MSN:" set to "MSN 1". At the bottom are "Apply" and "Cancel" buttons.

Note: We don't use DDI/DID in this type of example because DDI/DID is mainly used for outsiders to call extensions.

3.5.3 Example 3: Company with Existing PBX and Expanding Employees

For a company which has a PBX, and is expanding to include more employees, or a new branch office (for example). The X6004 is behind the PBX system connected using a PRI line.

- See an example of configuring ISDN settings in [Section 3.4 on page 65](#).
- Like Example 2, you can also select **Direct** (if you want the callers from the PBX's extensions to the X6004's not to go through the Auto-Attendant) or **MSN** (if you are using BRI line(s) and you want to have multiple subscriber numbers on one port).

Note: Like **Example 2**, we don't use DDI/DID in this type of example because DDI/DID is mainly used for outsiders to call extensions.

3.6 Using Call Features

The X6004 has built-in call features for functions such as call forwarding, call blocking, voicemail and so on. These features can be activated or accessed by dialing specific numbers from the phones connected to the X6004. The numbers used to access call features are called call feature codes. This section shows you how to customize call features. It also describes how to configure a ZyXEL IP phone (V300 is used in our example) to access voicemail by using the voicemail feature code. See [Section 6.8 on page 141](#) for more information on all call features.

3.6.1 Customizing Feature Codes

Click **Configuration > PBX > Server Configuration > Server > Feature Code** to display the codes used for the X6004's call features. You can change the codes in this screen. Provide the users with a list of the features and corresponding codes. Users on your network can then dial a code from their telephone to activate a specific feature. For example, dialing ***96** transfers a call.

Figure 26 Server > Feature Code

Feature Code Setting			
Black List On	<input type="text" value="*67"/>	Black List Off	<input type="text" value="*85"/>
Block no ID On	<input type="text" value="*77"/>	Block no ID Off	<input type="text" value="*87"/>
Call Forward On	<input type="text" value="*72"/>	Call Forward Off	<input type="text" value="*73"/>
Call Forward VM	<input type="text" value="*74"/>	Call Forward Busy On	<input type="text" value="*90"/>
Call Forward Busy Off	<input type="text" value="*91"/>	Call Forward Busy VM	<input type="text" value="*92"/>
Call Forward No Answer On	<input type="text" value="*82"/>	Call Forward No Answer Off	<input type="text" value="*83"/>
Call Forward No Answer VM	<input type="text" value="*84"/>	Call Transfer	<input type="text" value="*96"/>
Direct Pickup	<input type="text" value="*95"/>	DND On	<input type="text" value="*78"/>
DND Off	<input type="text" value="*79"/>	DND VM	<input type="text" value="*80"/>
Follow Me On	<input type="text" value="*22"/>	Follow Me Off	<input type="text" value="*23"/>
Group Pickup	<input type="text" value="*94"/>	Personal IVR	<input type="text" value="*"/>
Voice Mail	<input type="text" value="**"/>	Second Dial	<input type="text"/>
Mobile Extension On	<input type="text" value="*97"/>	Mobile Extension Off	<input type="text" value="*98"/>
Mobile Extension Auto On/Off	<input type="text" value="*99"/>		

3.6.2 Using the Voicemail Feature

The voicemail feature code as assigned in [Section 3.6.1 on page 77](#) is ******. Users can dial ****** followed by their extension number to access their voicemail. For example, a caller from extension **1001** can dial ****1001** to access voicemail messages.

Some IP phones allow you to configure automatic dialing of feature codes to perform common tasks. The following figure shows the web configurator screen of ZyXEL's V300 IP phone. ZyXEL's V300 IP phone can be configured to automatically

access voicemail by pressing the **VOICE MAIL** button located on its keypad. This is done by typing the call feature number into the **Voice Mail Number:** field.

Figure 27 ZyXEL V300 Voicemail Configuration

The screenshot shows the 'SIP Settings' configuration page for 'SIP 1'. The 'Voice Mail Number' field is set to '**1001'. A red circle highlights the word 'EXAMPLE' in the top right corner of the configuration area, and another red circle highlights the 'Voice Mail Number' field.

3.7 Using Your Web Portal

Every phone user has a personal web portal on the X6004. You can log in and make changes to your account setup, and IP phone users also use the web phone. The web phone is just like the telephone you usually use to make calls from this extension; you can call all the same numbers in the same way.

The following sections show examples of how to access the X6004's web portal, configure your own personal settings, and use the web phone.

3.7.1 Your Information

In this example, your network administrator has given you some information, as shown in the following table. You can also use this table to note down your own personal information, if you like.

Table 5 Your Information

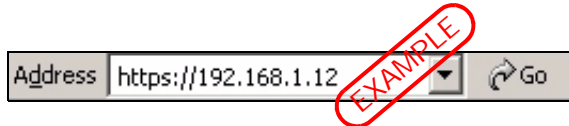
	EXAMPLE INFORMATION	YOUR INFORMATION
Extension Number	1001	
PIN Code	5678	
Web Portal IP Address	https://192.168.1.12	

3.7.2 Accessing the Web Portal

Take the following steps to access your phone account's web portal.

Open a web browser (like Internet Explorer) and enter the IP address you were given.

Figure 28 Tutorial: Web Portal IP Address



Note: Don't forget the "s" in "https://" - this "s" indicates a secure IP address, which means that communication between your computer and the X6004 (including your phone calls) cannot be intercepted by anyone else.

The following screen displays.

Figure 29 Tutorial: Log In

 A screenshot of the ZyXEL IPPBX X6004 login page. The page has a blue header with the ZyXEL logo. Below the header, it says "IPPBX X6004". There is a language dropdown set to "English". The first section is for extension and PIN code login, with fields for "Extension" and "PIN Code" circled in red. The second section is for administrator login, with fields for "Username" and "Password". A note at the bottom says "Please turn on the Javascript and ActiveX control setting on Internet Explorer and trun off the block popup window application." and there are "Login" and "Reset" buttons, with the "Login" button circled in red.

Enter your extension number ("1001") in the **Extension** field, and enter your PIN code ("5678") in the **PIN Code** field. Click **Login**.

3.7.3 Changing Your Security Information

It is very important that you change your security information as soon as possible, since it could be guessed by others if it was generated automatically.

The **Peer Info** screen displays when you log in. It allows you to change the password for your VoIP account (displayed as **SIP Auth Password**) and the PIN code you use to access the web portal, voicemail and the IVR (Interactive Voice Response) system (displayed as **Web/IVR/VM PIN Code**).

Note: The **SIP Auth Password** field does not display if you connect to the X6004 using a regular analog telephone system.

Figure 30 Tutorial: Changing Security Information



SIP Peer 1001 configuration and information	
Group	Sales
SIP Auth. User Name	1001
SIP Auth. Password	**** (Confirm ****)
Web/IVR/VM PIN Code	**** (Confirm ****)
.....	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

- Enter the new **SIP Auth Password** in the field on the left, and enter it again in the field on the right. Click **Apply**.
- Enter the new **Web/IVR/VM PIN Code** in the field on the left, and enter it again in the field on the right. Click **Apply**.

3.7.4 Personalizing Your Settings

Next, configure your extension's call settings. Click the **Forward/Block** tab at the top of the screen.

The following screen displays.

Figure 31 Tutorial: Configuring Call Settings

The screenshot shows the 'Call Forward Setting' configuration page. It includes the following sections and options:

- Call Forward Setting**
 - Office Hours: Office Hours
 - DND(Do Not Disturb): Disable Enable (White List) Voice Mail
 - Blind Forward: Disable Enable (Extension Number:) Voice Mail
 - Busy Forward: Disable Enable (Extension Number:) Voice Mail
 - No Answer Forward: Disable Enable (Find Me List) Voice Mail
 - After Office Hours: Disable Enable (Extension Number:) Voice Mail
- Call Blocking Setting**
 - Black list: Disable Enable (Black List)
 - Block the calls without Caller ID: Disable Enable
- Mobile Extension Setting**
 - Mobile Extension Status: No Specified

Buttons for 'Apply' and 'Reset' are located at the bottom of the form.

The following table shows the example call setting information. You can also use this table to make a note of the call settings you want to configure, if you like.

Table 6 Tutorial: Call Settings

	EXAMPLE INFORMATION	YOUR INFORMATION
Office Hours	Monday ~ Friday, 09:00 ~ 17:30	
Do Not Disturb (no-one can call you, except for people on the White List)	Disable	
White List (people who can still call you when Do Not Disturb is on)	555 123456 555 234567 555 345678 555 456789	

Table 6 Tutorial: Call Settings

	EXAMPLE INFORMATION	YOUR INFORMATION
Call Forwarding (whether or not incoming calls are redirected, and where they are sent)	Blind Forward: Disable Busy Forward: Voicemail No Answer Forward: Find Me List After Office Hours: Voicemail	
Find Me List (other extensions where you might be found)	987 654 321	
Black List (people you don't want to call you at all)	555 999888 555 888777	
Block Calls Without Caller ID	Disable	

Take the following steps to configure this screen.

- 1 **Office Hours:** Ensure that the **Mon** through **Fri** boxes are checked in the office hours sub-screen. Clear the **Sat** and **Sun** boxes. (You can access the office hours sub-screen by clicking the **Office Hours** button.)

In the **Time** field, use the drop-down lists to enter **09 : 00 ~ 17 : 30**.

- 2 **Do Not Disturb:** Ensure that **Disable** is selected. You can turn this on later if you want.
- 3 **White List:** Click the **White List** button. In the screen that displays, enter each phone number in the **Number** field and click **Add** after each one. Click **Apply** when you are finished.

- 4 **Call Forwarding:** Ensure that **Blind Forward** is set to **Disable**. In the **Busy Forward** row, select **Voice Mail**. In the **No Answer Forward** row, select **Enable** and click **Find Me List**.

In the screen that displays, enter each phone number in the **Number** field and click **Add** after each one. Click **Apply** when you are finished.

In the **After Office Hours** row, select **Voice Mail**.

- 5 **Black List:** Select **Enable** and click the **Black List** button. In the screen that displays, enter each phone number in the **Number** field and click **Add** after each one. Click **Apply** when you are finished.

- 6 **Block Calls Without Caller ID:** Ensure that **Disable** is selected.
- 7 Click **Apply**. Your call settings are successfully configured!

3.7.5 Setting Up Voicemail

Next, you can set up your voicemail inbox to automatically send your received messages as audio files to your email inbox. It is recommended that you do this so that your voicemail inbox does not fill up (if it fills up, no new messages can be recorded).

Click the **Voice Mail** tab at the top of the screen.

The following screen displays.

Figure 32 Tutorial: Setting Up Voicemail

The following table shows the example voicemail settings. You can also use this table to make a note of the voicemail settings you want to configure, if you like.

Table 7 Tutorial: Voicemail Settings

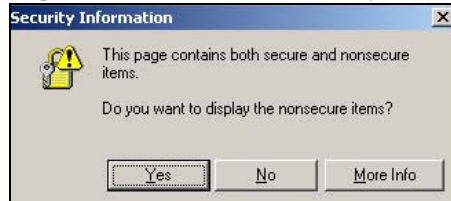
	EXAMPLE INFORMATION	YOUR INFORMATION
Received E-mail Address (the address to which you want the voicemail sent)	user_abcd@examplecorp.com	
Attached Voice File (send the audio file to your email account)	Yes	
Delete Voice Message After Mailed	Yes	

To configure this screen, enter your email address in the **Received E-mail Address** field, select **Attached Voice File** and select **Delete Voice Message After Mailed**. Click **Apply**.

3.7.6 Using the Web Phone (IP Phone Users Only)

Click the **Web Phone** tab at the top of the screen. If a screen similar to the following displays, click **Yes**.

Figure 33 Tutorial: Security Pop-Up



The following screen displays.

Figure 34 Tutorial: The Web Phone





Note: Make sure you have a headset (or speakers and a microphone) connected to your computer, and that your sound card is working correctly (try listening to an audio file or recording a voice note to check, if there is a problem).

The following table describes how to use the web phone to perform some basic phone functions.

Table 8 Tutorial: Basic Web Phone Call Features

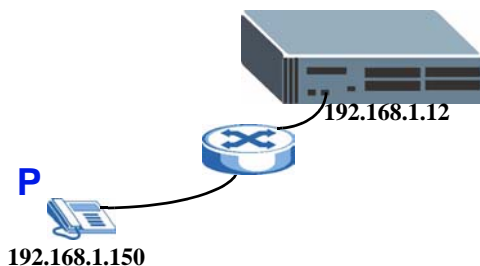
FEATURE	PROCEDURE
Dial a number	Click each numeral using the mouse pointer. The number displays on the screen. Use the "Clear" (C) button to delete a numeral.
Make a call	Dial the number, then press the "Dial/Pick up" () button.
Receive a call	When a call is incoming, press the "Dial/Pick up" () button.
End a call	Press the "Hang up" () button.
Adjust the speaker volume	Use the slider on the left of the keypad.

Table 8 Tutorial: Basic Web Phone Call Features

FEATURE	PROCEDURE
Adjust the microphone volume	Use the  slider on the right of the keypad.
Mute the speakers and the microphone	Click the Mute button below the keypad.
Use the phone book	Click the Phone Book tab to the right of the web phone. The phone book appears, displaying your contact list. Select what you want to search for (a name or extension number, for instance) from the drop-down list, enter the search term in the box and click on the magnifying glass () to search. You can also arrange the contact list entries by clicking on one of the headings.

3.8 Capturing Packets Using the Web Configurator

The following section shows you how to capture packets using the X6004 web configurator. You may need to do this if there are problems. In this example, a SIP phone (**P**) fails to register to the X6004.

Figure 35 Tutorial: Basic Troubleshooting Using Packet Capture

Do the following to capture packets between **P** and the X6004:

- 1 First create a **Debug admin** administrator account. Go to **Maintenance > Administration > Administrator List**, click **Add** and the following screen appears. In this example, we use the settings as follows
 - Username: **debug**
 - Password: **1234**

- Rank Level: Select **Debug admin**

Then click **Apply**.

The screenshot shows a web form titled "Add admin" with a sub-header "Create a new administrator". The form includes the following fields and values:

- Username: debug
- Password: ****
- Confirm Password: ****
- Description: For diagnostic
- Rank: Level : Debug admin

At the bottom of the form, there are two buttons: "Apply" and "Cancel".

- 2 Open another browser and log into the X6004 using the newly created debug admin account.
- 3 Go to **Maintenance > Administration > Diagnostics > Packet Capture** and fill in the following information.
 - Interface: LAN
 - Host: 192.168.1.150
 - Protocol: All
 - Stop capture after: 3000 packets
 - Stop capture after: 600 seconds

Then click **Capture Now**.

The screenshot shows a web form titled "Packet Capture" under the "Information Collect" section. The form includes the following fields and values:

- Machine ID: IPPBX_001
- Interface: LAN
- Host: 192.168.1.150
- Protocol: All
- Stop capture after: 3000 Packets(1~3000)
- Stop capture after: 600 Sec.(1~600)

At the bottom of the form, there are two buttons: "Capture Now" and "Download".

- 4 Re-initialize the SIP phone. This helps to get a complete packet capturing.

- 5 Wait several seconds, click **Stop Capture**, **Download** and then **Save** to save the capturing file on your computer.
- 6 Use a packet capturing tool (such as Ethereal) to open the file and analyze the possible root cause.

In this example, registration fails because the SIP username must be a number and not letters (**bob** in this example) for the X6004.

The screenshot shows the Ethereal interface with a filter set to 'sip'. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
9	12.916968	192.168.1.150	192.168.1.12	SIP	Request: REGISTER sip:bob@192.168.1.12:5060
10	12.923515	192.168.1.12	192.168.1.150	SIP	Status: 404 Not found
36	15.353043	192.168.1.150	192.168.1.12	SIP	Request: REGISTER sip:bob@192.168.1.12:5060
37	15.359059	192.168.1.12	192.168.1.150	SIP	Status: 404 Not found

The packet details for the selected packet (No. 36) are:

```

Identification: 0x0505 (1285)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (0x11)
  Header checksum: 0xb0a3 (correct)
  Source: 192.168.1.150 (192.168.1.150)
  Destination: 192.168.1.12 (192.168.1.12)

```

If you cannot solve the problem, you should contact customer support and send this file.

You may be asked to provide another file containing more real-time system information. Select **Maintenance > Administration > Diagnostics > Information Collect** and click **Collect Now**. Wait several seconds, then click **Download** and **Save** to save the file on your computer.

3.9 Creating an Automated Menu System

The Automatic Call Distribution (ACD) system allows you to set up automated audio menus and the connections between them which will allow incoming phone calls to be routed to the best available people to receive them. For example, if the Acme Widget company sells its products in two different countries (the United States and Mexico), then it would probably want to set up a customer service line that can direct callers based on their language preference.

Before getting started, there are a few ACD-specific terms with which you should familiarize yourself first:

- **Agent** - An agent is a callee, or the person who ultimately receives an incoming call. Agents are grouped according to skills.
- **Skill** - A skill is a specific function that an agent performs. For example, in the Acme Widget company's customer support department, some of the agents are fluent in English while others are fluent in Spanish. Both English and Spanish are labeled as skills for the purpose of routing calls through the ACD system.
- **Auto-Attendant (AA)** - The auto attendant is the crux of the automated menu system. It functions as a kind of automated switch board operator. When properly configured, the X6004 auto-attendant can be the foundation of any automatic menu system, replete with custom audio recordings which the caller hears when first dialing in and keypad-responsive menus which guide them to their intended recipients.

For a full description of all available ACD and Auto-Attendant features on the X6004, see [Chapter 24 on page 365](#) and [Chapter 19 on page 291](#), respectively.

3.9.1 Menu Design and Call Routing

First, you want to design your call center's automated audio menu "map". Start by asking yourself a few key questions, such as: How are calls going to be routed once a person dials the phone number assigned to the system? What is the first level of menus the caller encounters? After the call makes his selection, then what is the second level of menus? After the second level of menus, are calls then sent to an agent?

For the Acme Widget company, the company manager decides he wants to divide the menus up by languages first (English and Spanish), and then skills (Order Status, Technical Support, and Operator) for each language, each of which contains its own set of agents.

In order to do this, he must map his connections:

Table 9 Tutorial: Example Automated Menu Design

1ST MENU	SUBMENUS	SKILLS	AGENTS
Language Selection	English	Order Status	Tom Pam Steven
		Technical Support	Steven George
		Accounts and Billing	George
	Spanish	Estado del Pedido	Eddie Susan Maria
		Apoyo Técnico	Maria Alejandro
		Cuentas y Facturación	Alejandro

- The first menu and the submenus both utilize an auto-attendant. Auto-attendants are set up in the **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized** screen. This portion of the tutorial is described in [Section 3.9.4 on page 95](#).
- The skills are the intermediaries between the AA submenu and the agents. Skills are set up in the **Configuration > ACD > Skill** screen. This portion of the tutorial is in [Section 3.9.3 on page 92](#).
- The agents associated are the ultimate destination for incoming calls to the system. Agents are set up in the **Configuration > ACD > Agent** screen. This portion of the tutorial can be found in [Section 3.9.2 on page 91](#).

Although the usage order is 1st Menu - Submenus - Skills - Agents, we have to build our system in reverse order by starting with the ACD-based agents and skills and then work our backwards toward the auto-attendant-based menus. This is because the auto-attendant menus require the skills to already be defined when setting them up as part of an automated menu system, while skills require agents to be pre-defined as they are set up.

3.9.2 Create an Agent Identity

Now that you have more or less mapped out your automated menus and call routes, it's time to actually start building them on the X6004. The first thing we're going to do is create our agent identities. This allows us to assign the agents immediately to skills as we create them in the next section.

To create an agent identity:

- 1 Log into the X6004, then go to the **Configuration > ACD > Agent** screen.



- 2 For each of your agents, click the **Add** button to open the **Agent Settings** screen, and configure the following items:

Agent ID: Enter between 3 and 20 digits to serve as the agent's identification number. This number has no relation to any other number or account ID in other features on the X6004, but it is required for the agent to log into the ACD system from his telephone.

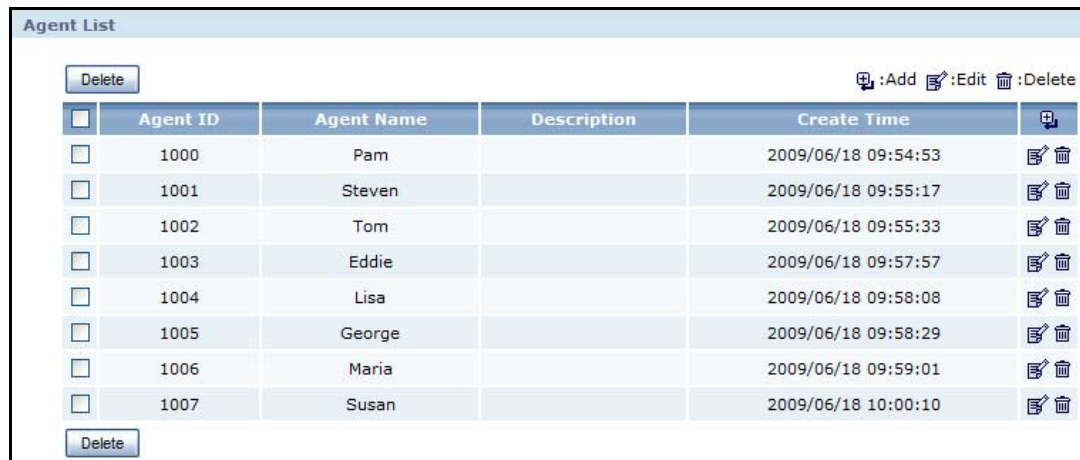
Password: Enter between 1 and 32 digits for the agent's password. As with the Agent ID, this is required to log into the ACD system from an agent's telephone.

Agent Name: Enter between 1 and 32 alphanumeric characters here that will be associated with the skills and skill menus in subsequent sections. While you can use an agent's real name, it is certainly not necessary. In fact, if multiple people log in on the same agent ID, it is recommended you use a more neutral name to identify them (such as 'Accounting' for a team as opposed to 'Julia', who happens to be one accountant on the team).

Description: This field is optional, allowing you to add supplementary information to the agent. This only appears on the **Configuration > ACD > Agent** screen. Enter up to 64 alphanumeric characters.

- 3 Click **Apply** when you are done.

After you have created all your agents, your agent list should look similar to this:



<input type="checkbox"/>	Agent ID	Agent Name	Description	Create Time		
<input type="checkbox"/>	1000	Pam		2009/06/18 09:54:53		
<input type="checkbox"/>	1001	Steven		2009/06/18 09:55:17		
<input type="checkbox"/>	1002	Tom		2009/06/18 09:55:33		
<input type="checkbox"/>	1003	Eddie		2009/06/18 09:57:57		
<input type="checkbox"/>	1004	Lisa		2009/06/18 09:58:08		
<input type="checkbox"/>	1005	George		2009/06/18 09:58:29		
<input type="checkbox"/>	1006	Maria		2009/06/18 09:59:01		
<input type="checkbox"/>	1007	Susan		2009/06/18 10:00:10		

3.9.3 Create a Skill

The next step is to define our skills. Doing this second allows us to link the agents we created in the previous section to the skills we're going to create in this section. It also allows us to later assign these very same skills to the auto attendant menus when they are, in turn, created.

In the context of the X6004, a skill is a set of rules that define how incoming calls are sent to the agents who are associated with that skill. For example, if the Acme Widget company defines "Technical Support" as a skill, then any caller who presses the key for that skill is immediately forwarded to the first available person whose agent identity appears on that skill's rule list.

To create a new skill:

- 1 Go to the **Configuration > ACD > Skill** screen.



<input type="checkbox"/>	Number	Skill Name	Description	Create Time	
--------------------------	--------	------------	-------------	-------------	--

- 2 For each of skill, click the **Add** button to open the **Skill Settings** screen, and assign configure the following items:

Skill Setting

Number	<input type="text" value="766"/>
Skill Name	<input type="text" value="Order Status"/>
Description	<input type="text"/>
Skill Menu	<input type="text" value="-----"/> ▾
Ring Strategy	<input type="text" value="Fewest Calls"/> ▾
No Login Action	<input type="text" value="Voice Mail"/> ▾ <input type="text" value="2001"/>
No Available Action	<input type="text" value="Backup Skill"/> ▾ <input type="text"/>
Timeout Action	<input type="text" value="Backup Skill"/> ▾ <input type="text"/>
Waiting Music	<input type="text" value="default"/> ▾
Max. Waiting Calls	<input type="text" value="64"/>
Waiting Timeout	<input type="text" value="180"/> sec.
Ring Agent Timeout	<input type="text" value="15"/> sec.
Service Level	<input type="text" value="30"/> sec.
Position Report Frequency	<input type="text" value="60"/> sec. (0:disable)
Periodic Announce Frequency	<input type="text" value="60"/> sec. (0:disable)
Announce	<input type="text" value="x"/> <input type="text" value="Playback"/> <input type="text" value=""/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Periodic Announce	<input type="text" value="x"/> <input type="text" value="Playback"/> <input type="text" value=""/> <input type="button" value="Browse..."/>
Create Time	

Skill Member

Priority : ▾

Available Exten.		Member
1003/Eddie	▶	1002/Tom:1
1004/Lisa	▶	1000/Pam:1
1005/George	▶	1001/Steven:2
1006/Maria	▶	
1007/Susan	▶	

Number: Enter an identification number of this skill. This is required to link the skill to a skill menu in the next section. You can use between 3 and 20 digits.

Skill Name: Enter a descriptive name for this skill. For example, "Order Status" since this will be the skill that forwards all calls requesting order status information to the appropriate people.

Ring Strategy: This option allows you to choose how a call is forwarded to the agents associated with this skill. When a call comes in, it is not logistically possible for the X6004 to forward the call to every associated agent. Therefore, a ring strategy must be employed. For example, let's say we're configuring the "Order Status" skill. We know from part I that the company manager intends on having two agents linked to this skill (Pam and Steven). He decides that the person who

has received the fewest number of incoming calls since logging in should always be the first to answer the next incoming call. He therefore sets the **Ring Strategy** option to **Fewest Calls**. For more information about this option, see [Section 24.4.1 on page 372](#).

No Login Action: This option determines how the X6004 handles incoming calls to the agents associated with this skill when none of them have logged on yet. The company manager decides to let voice mail pick up missed calls when neither of the agents logs in, and enters the actual telephone extension for Pam.

No Available Action: This is similar to the previous option, but tells the X6004 how to handle incoming calls to the agents associated with this skill when they are all already engaged in conversation. The company manager knows that not every agent in every skill will be occupied all of the time, and so he chooses **Backup Skill** as the setting for this field. However, until he creates additional skills he will not be able to choose which backup skill takes over in the event all agents associated with this one are busy.

Timeout Action: This is similar to the preceding two options, determining how the X6004 handles incoming calls when an agent does not answer or pick up after a certain amount of time.

Max Waiting Calls: Enter the maximum number of calls that will be allowed to queue up if the agents are already engaged in conversation. The company manager chooses to let the default of 64 calls remain as it is. In a small office environment, it seems unlikely that they will have an issue with a call backlog.

Priority/Member: This is where you select the agents whom you want to link to this skill. The **Priority** determines which people receive calls first (followed by **Ring Strategy**); if two people are set for priority 1 and the third set for priority 2, then the calls are first directed to the priority 1 agents. Only when both of those agents are unavailable do calls get directed to priority 2 agents. In this example, the company manager assigns priority 1 to Tom and Pam and priority 2 to Steven, because Steven also fields call for Technical Support. This way, he won't receive as many calls for Order Status as the other two, giving him more time to field calls for his primary skill.

- 3 Click **Apply** when you are done.

Note: After you create a number of skills, you may want to edit them again to update the **No Logon Action**, **No Available Action** and **Timeout Action** fields if they use the **Backup Skill** setting.

After you have created all your skills, your skill list should look similar to this:

Skill List					
<input type="button" value="Delete"/>		<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			
<input type="checkbox"/>	Number	Skill Name	Description	Create Time	<input type="button" value="Edit"/>
<input type="checkbox"/>	766	Order Status		2009/06/18 14:45:49	<input type="button" value="Edit"/>
<input type="checkbox"/>	785	Technical Support		2009/06/18 14:47:01	<input type="button" value="Edit"/>
<input type="checkbox"/>	797	Accounts and Billing		2009/06/18 15:15:12	<input type="button" value="Edit"/>
<input type="checkbox"/>	866	Estado del Pedido		2009/06/18 15:16:42	<input type="button" value="Edit"/>
<input type="checkbox"/>	885	Apoyo Técnico		2009/06/18 15:18:11	<input type="button" value="Edit"/>
<input type="checkbox"/>	897	Cuentas y Facturació		2009/06/18 15:19:24	<input type="button" value="Edit"/>
<input type="button" value="Delete"/>					

3.9.4 Create an Auto-Attendant

The final step in building our automated menu system is to configure our auto-attendant. For the Acme Widget company, we require two auto-attendants: one to handle the first menu tier (English / Spanish) and another to handle the submenu tier (Skills). Once a caller gets to the submenu, his call can then be forwarded to a live person, or in otherwords, an agent.

- 1 Go to the **Configuration > PBX > Outbound Line Management > Auto-Attendant** screen then select the **Customized** tab.
- 2 Click the **Add** button.

Auto-Attendant List			
			<input type="button" value="Add"/> <input type="button" value="Advanced"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
ID	Name	Description	<input type="button" value="Add"/>
			<input type="button" value="Add"/>

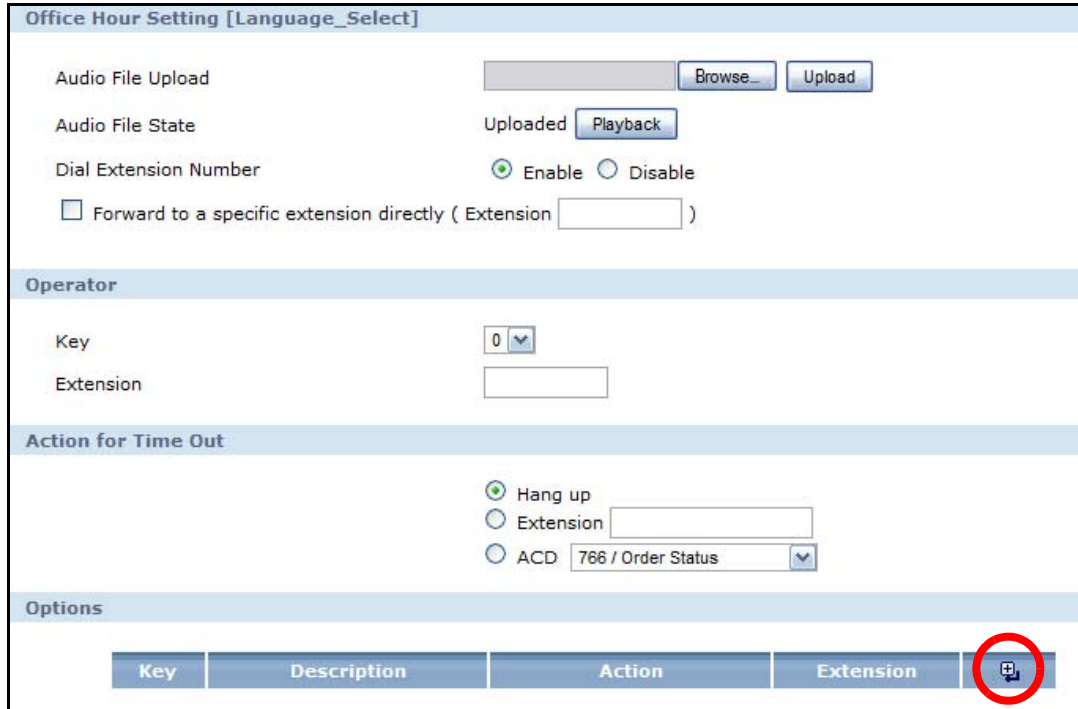
- 3 On the **Auto Attendant Setting** screen, enter a Name and a Description (optional) for your first auto-attendant. The company manager of the Acme Widget company enters Language_Select, since this will be the first automated menu where callers choose either English or Spanish.

Auto-Attendant Setting	
Name	<input type="text" value="Language_Select"/>
Description	<input type="text"/>

- 4 After the creating your first auto-attendant, click the **Advanced** button.



- 5 On the **Office Hour Settings** screen, we're going to first configure our menu **Options**; click the **Add** button.



- 6 On the **Option Settings** screen, enter a keypad number and action for your auto-attendant. Because this is the language selection auto-attendant for the Acme Widget company, the company manager enters "1" for **Key**, "English" for **Description**, and selects "Forward to next menu" for **Action**. The action selected here is quite important because it allows us to open up the second tier submenu.



- 7 Click **Apply** to save these settings, then repeat this process for any other menu options (such as “Spanish” for the Acme Widget company). The final screen may look something like this:

Office Hour Setting [Language_Select]

Audio File Upload

Audio File State Uploaded

Dial Extension Number Enable Disable

Forward to a specific extension directly (Extension)

Operator

Key

Extension

Action for Time Out

Hang up

Extension

ACD

Options

Key	Description	Action	Extension	
1	English	Forward to next menu	<input type="button" value="Next Menu"/>	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
2	Spanish	Forward to next menu	<input type="button" value="Next Menu"/>	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Note: Don't forget to upload the actual audio file that you want to play when a caller accesses this menu. For example, “Press 1 for English or 2 for Spanish”. You can do that using the **Audio Upload** option on this screen. See [Section 19.3.2 on page 297](#) for details on this.

- 8 Click the **Next Menu** button for the first menu choice. In this case, it would be for English under the **Options** category. This is where you will configure the option's submenu, which will connect to all of our skills.

Then click the **Add** button to add the first submenu item, such as “Order Status”.

Sub Menu of AA [Key Sequence : 1]

Audio File Upload

Audio File State No audio file!

Dial Extension Number Enable Disable

Options

Key	Description	Action	Extension	
				<input type="button" value="Add"/>

- 9 On the **Option Settings** screen, enter the keypad number and action for the submenu item. The company manager for the Acme Widget company enters “1” for **Key**, “Order Status” for **Description**, selects “Forward to a skill” for **Action**, and finally selects “766/Order Status” for the **Extension**. The extensions available on this list correspond directly to the ACD skills created earlier.

Option Setting

Key: 1

Description: Order Status

Action: Forward to a skill

Extension: 766/Order Status

- 10 Click **Apply** to save these settings, then repeat this process for any other menu options (such as “Technical Support” and “Accounts and Billing” for the Acme Widget company). The final screen may look something like this:

Sub Menu of AA [Key Sequence : 1]

Audio File Upload: [Browse...] [Upload]

Audio File State: No audio file! [Playback]

Dial Extension Number: Enable Disable

Options

Key	Description	Action	Extension	
1	Order Status	Forward to skill	766/Order Status	[Edit] [Delete]
2	Technical Support	Forward to skill	785/Technical Support	[Edit] [Delete]
3	Accounts and Billing	Forward to skill	797/Accounts and Billing	[Edit] [Delete]

Note: Don't forget to upload the actual audio file that you want to play when a caller accesses this menu. For example, “Press 1 for English or 2 for Spanish”. You can do that using the **Audio Upload** option on this screen. See [Section 19.3.2 on page 297](#) for details on this.

- 11 Repeats steps 5 through 10 to create a second submenu, such as the Spanish submenu for the Acme Widget company.

Congratulations! If you followed each of the steps described in this tutorial, then you should have the barebones structure of an automated menu system for your telephone network.

PART II

Technical Reference

The Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy X6004 setup and management via an Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels. You must have Flash installed.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

- 1 Start your web browser.
- 2 Type "https://" and the IP address of the X6004 (for example, the default LAN IP address is **192.168.1.12** and the default WAN IP address is **172.16.1.1**) in the Location or Address field. Press [ENTER].
- 3 The login screen appears. The default username is **admin** and associated default password is **1234**. Enter your login credentials and click **Login**.

Note: The upper part of the login screen is for logins into the web phone feature. See [Chapter 37 on page 483](#).

Figure 36 Web Configurator: Login

ZyXEL

IPPBX X6004

Language : English

Enter Extension number and PIN Code then click Login.

☺ Extension :

🔒 PIN Code :

Enter Administrator Username and Password then click Login.

☺ Username :

🔒 Password :

(max. 32 alphanumeric, printable characters and no spaces)

Note :
Please turn on the Javascript and ActiveX control setting on Internet Explorer and trun off the block popup window application.

Login Reset

- 4 A screen opens up prompting you to change the default user name and password. Change the default password, note it down and put it in a safe place. Click **Apply** to go to the status screen of the web configurator.

ZyXEL

Username/Password Setup

As a security precaution, it is highly recommended that you change the admin username & password.

Old Password

Username

Password

Confirm Password

(max. 32 alphanumeric, printable characters and no spaces)

Apply Ignore

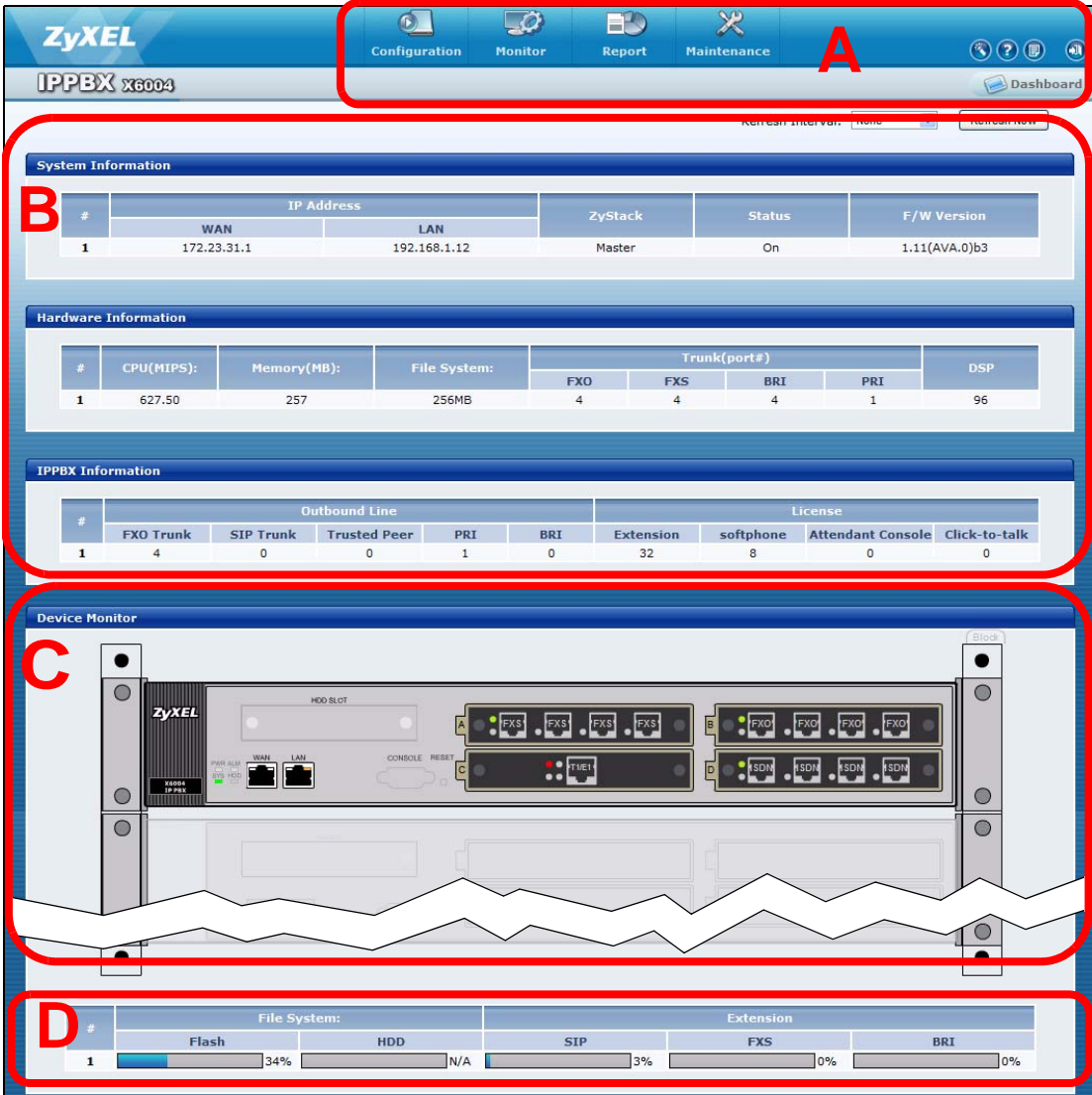
Note: The first time you log in to the X6004 a wizard guides you through initial network configuration. See the Quick Start Guide for an initial setup example.

4.3 The System Screen

The **System** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of the web configurator screen.

Figure 37 Web Configurator System Screen



A - The navigation buttons link you to configuration menus of the X6004, the quick keys allow you to view built-in help files, access the wizard, view the about screen and logout. Use the **Dashboard** button to go to the main status page from any web configurator screen.

B - The main part of the screen displays general information about the X6004 you are logged in to and any X6004 that are part of a ZyStack (see [Chapter 23 on page 355](#)).

C - The device monitor is a graphical representation of the X6004 status and other X6004 in a ZyStack. You can quickly view LED status, voice interface card status and peer X6004 status. Alternatively, mouse over the ZyXEL logo or the individual ports to view more detailed status information. Click on the ZyXEL logo to go to the status screen of the X6004 or click on the individual ports to go to their configuration screens.

D - The bottom part of the screen shows you the amount of flash memory and hard disk storage used as well as the extension capacity for the SIP accounts, FXS and BRI ports.

4.3.1 The Navigation Panel

Go to individual feature configuration screens via the navigation buttons. The following table shows you the submenus (navigation panels) associated with each navigation button. The following table describes the links in the navigation panels.

Table 10 Navigation Panel Links

LINK	DESCRIPTION
Network	Use these screens to configure network settings on the X6004.
LAN	Use this screen to configure the LAN IP address of the X6004.
WAN	Use this screen to configure the WAN IP address of the X6004.
DDNS	Use this screen to specify DNS servers that the X6004 uses for domain name to IP address mappings.
NTP	Use this screen to configure the time settings on the X6004.
Static Route	Use this screen to specify any static routes for the X6004.
VLAN	Use this screen to configure the WAN and LAN VLAN settings of the X6004.
PBX	Use these screens to configure settings related to the telephony functions of the X6004.
Server Configuration	Use these screens to configure the X6004 global settings, auto provisioning, quality of service, voice mail, phonebook, DSP (Digital Signal Processor) and office hour settings.
Extension Management	Use these screens to create and manage extension numbers for the IP, FXS (analog) and ISDN phones connected to the X6004, ring and pickup groups and access codes for each authority group (a set of extension numbers).

Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
Outbound Line Management	Use these screens to configure outbound line configurations to FXO, ITSP, trusted peer, ISDN BRI/PRI connections, auto-attendant global settings and create and manage outbound dialing rules.
Group Management	Use this screen to associate groups with dialing rules. This specifies which outbound lines members of a department can use.
Call Services	Use these screens to configure emergency call settings, conference calling, music on hold settings, distinctive ring settings, auto callback, call parking, call waiting and call transfer.
ZyStack	Use these screens to configure a group of X6004's to work together.
Configuration	Use this screen to add peer X6004s.
Intranet	Use this screen to specify IP subnets for which the X6004 routes IP phones to a ZyStack member.
Status	Use this screen to check the status of peer X6004s.
ACD	Use these screens to configure the X6004's Automatic Call Distribution (ACD) features
ACD Global	Use this screen to set up the global 'wrap up' time for each call.
Agent	Use these screens to set up agent accounts.
Skill	Use these screens to configure skill sets and the call parameters associated with them.
Skill Menu	Use this screen to configure skill menus.
Monitor	These screens allow you to view the status of your X6004 or if you set up a ZyStack you can view the status of all the participating X6004s.
System Information	Use this screen to view network configuration, hardware information, line and license settings on the X6004.
SNMP	Use this screen to configure SNMP settings.
Status Observation	Use these screens to view status details about extensions and outbound line groups configured on the X6004.
SIP Peer	Use this screen to view status information about SIP extensions configured on the X6004.
FXS Peer	Use this screen to view status information about FXS extensions configured on the X6004.
BRI Peer	Use this screen to view status information about ISDN BRI extensions configured on the X6004.
CTI Peer	Use this screen to view status information about the X6004's Computer Telephony Integration (CTI) connections.
FXO Trunk	Use this screen to view status information about FXO outbound line groups configured on the X6004.
SIP Trunk	Use this screen to view status information about SIP outbound line groups configured on the X6004.
BRI Trunk	Use this screen to view status information about ISDN BRI outbound line groups configured on the X6004.
PRI Trunk	Use this screen to view status information about ISDN PRI outbound line groups configured on the X6004.

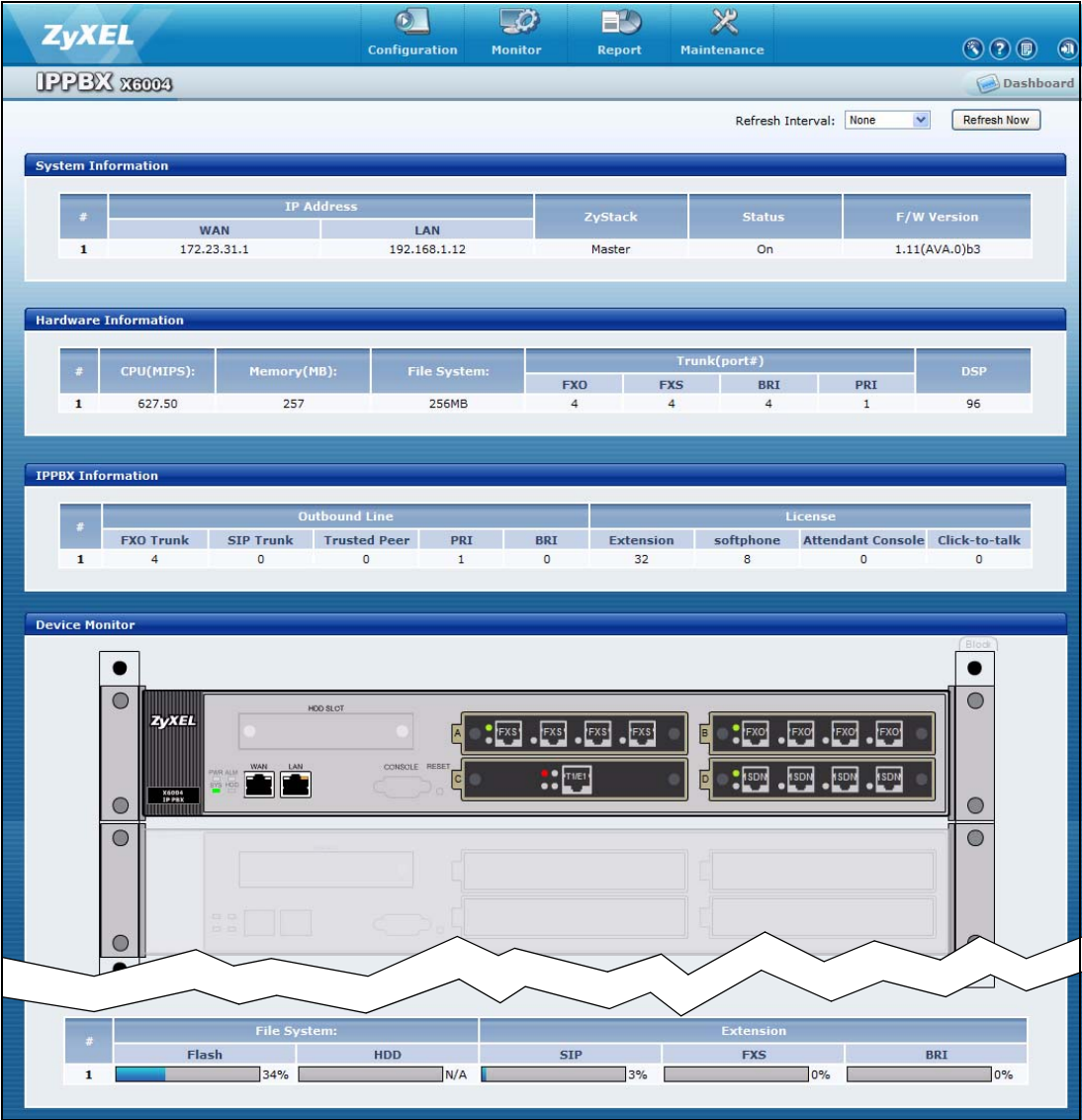
Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
ACD Queue	Use this screen to view the status of calls coming into the ACD queue as well as information about the agents for particular skills.
Logs	Use these screens to view system logs, configure log settings and search the CDR (Call Detail Record) database.
System Logs	Use these screens to view and configure system logs on the X6004.
CDR	Use these screens to manage CDR collection and to query the CDR database.
ACD	Use these screens to manage ACD data collection and to query the ACD database.
Administration	Use these screens to manage administrator accounts and use diagnostic features on the X6004.
Logged-In Administrator	Use this screen to change the password of the currently logged in administrator account.
Administrator List	Use this screen to manage administrator accounts on the X6004.
Diagnostics	Use this screen to configure data capture of VoIP packets for analysis.
Inactivity Timer	Use this screen to configure administrator inactivity timeout value on the X6004's web configurator.
Remote Management	Use this screen to configure remote management settings (for example, FTP and HTTPS access) on the X6004.
TFTP Management	Use this screen to load files such as phone firmware to the X6004 so TFTP client devices can check the X6004 for the latest file and download it.
Backup & Restore	Use this screen to backup and restore the configuration or reset the X6004 to its factory defaults.
Firmware Upgrade	Use this screen to perform firmware upgrades on the X6004.
License Control	Use this section to make sure that your X6004 is registered with myZyXEL.com.
Registration	Use this screen to register your X6004 with myZyXEL.com. If you don't have an account with myZyXEL.com, follow the directions in this screen to set one up.
Reboot	Use this screen to reboot the X6004.

4.4 Dashboard - System Information

The **Dashboard** screen contains system information about the X6004. It is also a graphical representation of the X6004 and any ZyStack members (if configured). Click the **Dashboard** button in any of the web configurator screens to view the screen as shown.

Figure 38 Dashboard



Select how often you want to update the information in the **Dashboard** screen and click **Refresh Now** to apply your setting. You can also click **Refresh Now** to update the screen immediately. See the similar field descriptions in [Table 146 on page 380](#).











4.5 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes.

4.6 Icons in the Web Configurator

The following table describes the icons used in the configuration screens of the X6004.

Table 11 Icon Explanation Table

ICON	NAME	DESCRIPTION
	Add	This icon is used to create new components, such as extensions or groups.
	Edit	This icon takes you to a screen where you can perform basic configuration changes.
	Advanced	This icon takes you to the main configuration screen of most features.
	Delete	Use this icon to remove components, such as extensions or groups.
	Auto Attendant	This screen takes you to a screen where you can select an auto attendant.
	Reboot	This icon reboots the X6004 or another member of a ZyStack (if configured).
	Up	This icon is used to move items higher in priority.
	Down	This icon is used to move items lower in priority.
	Left	Use this icon to move selected items from right to left in a screen.
	Right	Use this icon to move selected items from left to right in a screen.

4.7 Resetting the X6004

If you forget the administrator password, you will need to reset the X6004 back to the factory defaults.

Use the **RESET** button on the front panel of the X6004 to reset the X6004 back to factory defaults. Press and hold the **RESET** button for 10 seconds. The X6004 will reload its factory defaults.

The X6004 is reinitialized with a default configuration file including the default administrator username (admin) and password (1234). The LAN IP address of the X6004 also reverts to the default 192.168.1.12 and the WAN IP address reverts to 172.16.1.1.

4.8 Rebooting the X6004

If the X6004 is not performing as expected, you can reboot the system as a basic troubleshooting step. Rebooting the X6004 does not change any of the configuration settings. Rebooting simply restarts all of the subsystems (voice processing, network interfaces and so on) and reloads the latest saved configuration on the X6004.

Click **Maintenance > Reboot** to open the **Reboot** screen. Click the **Reboot** button to restart the X6004.

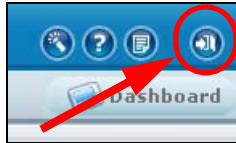
Figure 39 Maintenance > Reboot



4.9 Logging Out of the Web Configurator

Click the **Logout button** (👤) in the navigation panel to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

Figure 40 Web Configurator: Logout Link



4.10 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** (?) link from a web configurator screen to view an online help description of that screen.

Network Deployment

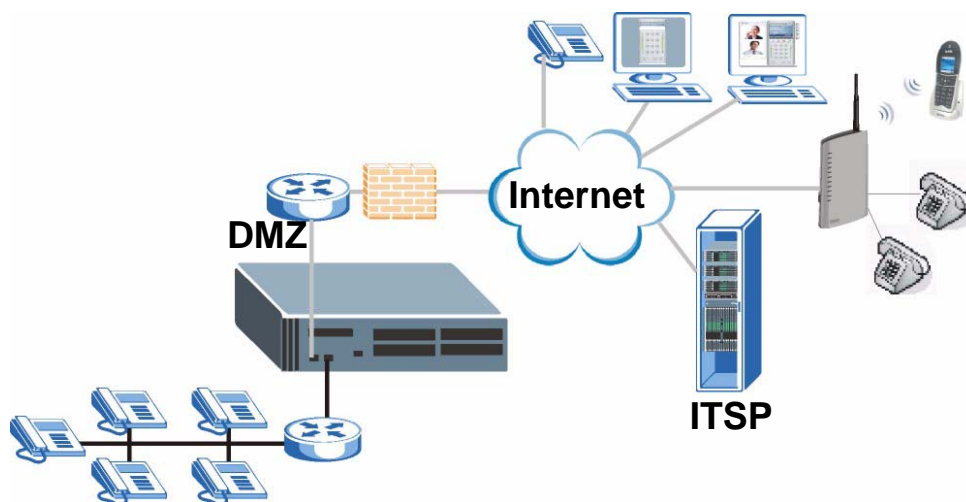
5.1 Overview

This chapter shows you how to deploy the X6004 on your network, using the **Configuration > Network** screens.

The following diagram shows a sample network deployment of the X6004. The WAN port is connected to a DMZ interface on the default gateway router. The X6004 uses the WAN interface to connect to a SIP server at the ITSP. SIP IP devices use the WAN IP address of the X6004 to connect to it.

On the LAN, SIP IP phones use the LAN IP address of the X6004 to connect to it.

Figure 41 Network Deployment Overview



5.1.1 What You Can Do in this Chapter

- Use the **LAN** screen to set up the LAN IP address of the X6004. See [Section 5.2 on page 114](#).
- Use the **WAN** screen to set up a connection with the ISP or the default gateway router. See [Section 5.3 on page 116](#).
- Use the **DDNS** screen to configure your Dynamic DNS settings. See [Section 5.4 on page 117](#).

- Use the **NTP** screen to configure time settings on the X6004. See [Section 5.5 on page 119](#).
- Use the **Static Route** screen to look at static routes in the X6004. See [Section 5.6 on page 120](#).
- Use the **VLAN** screen to configure VLAN settings in the X6004. See [Section 5.7 on page 122](#).

5.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

LAN

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area.

WAN

WANs link geographically dispersed locations in other cities or around the globe including switched and permanent telephone circuits, terrestrial radio systems and satellite systems.

DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. For instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of any network device before you can access it. The ISP (or network administrator) should tell you the DNS server addresses, usually in the form of an information sheet, when you sign up.

DDNS

Dynamic DNS maps your dynamic IP address to a static domain name. You can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider to use this service.

NTP

Network Time Protocol allows devices to synchronize their time setting with an external time server.

Static Routes

When you configure static routes on the X6004, you are informing the X6004 about how to reach networks and devices that are not reachable via the default gateway.

VLANs

Virtual Local Area Networks, standardized as IEEE 802.1Q, allow a physical network to be partitioned into various logical networks. Only stations on the same logical network can intercommunicate.

5.1.3 Before You Begin

Before you deploy the X6004, you should consider the following:

- If the X6004 has dynamically assigned IP address from your ISP, then you should configure DDNS (Dynamic DNS). This allows the IP devices on the WAN to establish connections with the X6004.
- If the X6004 is behind a firewall, then you must make sure that you create firewall rules to let VoIP traffic pass through to the X6004.
- If the X6004 is behind a NAT router, then you must make sure that you configure forwarding rules for VoIP communication to get to the X6004.
- If the IP phones on your LAN are located in different subnets, then you have to configure static routes to ensure that the IP phones can connect to the X6004 and vice versa.

5.2 The LAN Screen

Use this screen to set up the LAN IP address of the X6004. To access this screen, click **Configuration > Network > LAN**.

Figure 42 Network > LAN

The screenshot shows two configuration screens. The top screen, titled "LAN Ethernet TCP/IP Setting", contains the following fields: IP Address (192.168.1.12), Subnet Mask (255.255.255.0), a checked checkbox for "DHCP Server on LAN Service", Default Gateway, DNS, IP Pool Start Address, and Pool Size. There are "Apply" and "Reset" buttons at the bottom. The bottom screen, titled "Static LAN DHCP List", shows a table with columns for selection, ID, IP Address, and MAC Address. There are "Delete" buttons and "Add", "Edit", and "Delete" icons at the top right.

Each field is described in the following table.

Table 12 Network > LAN

LABEL	DESCRIPTION
LAN Ethernet TCP/IP Settings	The IP address you configured here is the SIP server IP address that the IP phones on your LAN connect to.
IP Address	Enter the IP address of the X6004 on the LAN.
IP Subnet Mask	Enter the subnet mask of the LAN.
DHCP Server on LAN Service	Select this to allow the X6004 to assign IP addresses to IP phones on the network to which it is connected. It cannot function as a router in this capacity.
Default Gateway	Enter the DHCP server's default gateway IP address.
DNS	Enter the DNS server IP addresses
IP Pool Start Address	Enter the first IP address in the IP pool.
Pool Size	Enter the maximum number of IP addresses to be issued by the DHCP server.
Static LAN DHCP List	This section allows you to configure a list of static IP addresses. These IPs will not be used by the DHCP server.
Delete	Select an item from list, then click this button to remove it. Once removed, it becomes eligible for issuance by the DHCP server.
Select	Check a box to select an item from the list.
IP Address	This displays a DHCP-issued IP address on your network and its associated MAC Address.
MAC Address	This displays the MAC address associated with the IP address.

Table 12 Network > LAN (continued)

LABEL	DESCRIPTION
Add	Click this button to add a new static IP address to the list.
Edit	Click this edit an item in the list.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to set every field in this screen to its last-saved value.

5.2.1 The Static LAN IP Address Screen

This screen allows you to configure a static IP address for use in conjunction with a DHCP server run on the X6004. Click the **Add** button in the **Network > LAN** screen to display this screen. You can also click the **Edit** button to display this screen to edit an already existing item in the list.

Figure 43 Static LAN IP Address

Each field is described in the following table.

Table 13 Network > LAN

LABEL	DESCRIPTION
IP Address	Enter an IP address to be used as a static IP.
MAC Address	Enter the MAC address of the device to receive this IP address.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to return to the previous screen.

5.3 The WAN Screen

You can configure your connection to the ISP or the default gateway router as well as DNS server information. This allows the X6004 to communicate with IP devices on the WAN.

Use this screen to set up a connection with the ISP or the default gateway router. To access this screen, click **Configuration > Network > WAN**.

Figure 44 Network > WAN

WAN Ethernet TCP/IP Settings

Get automatically from ISP

Static IP (Default)

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS:

Each field is described in the following table.

Table 14 Network > WAN

LABEL	DESCRIPTION
WAN Ethernet TCP/IP Settings	
Get automatically from ISP	Select this if your ISP did not assign you a static IP address. Click Renew to send a request to the DHCP server for a new IP address.
Static IP (Default)	Select this if your ISP or network administrator assigned you a static IP address.
IP Address	Enter the IP address provided by your ISP or network administrator.
Subnet Mask	Enter the subnet mask your ISP or network administrator provided for the remote node.
Default Gateway	Enter the IP address your ISP or network administrator provided for the default gateway to the Internet.
Primary DNS	Enter the IP address of the DNS server your ISP or network administrator provided to you.
Secondary DNS	Enter the IP address of the second DNS server your ISP or network administrator provided to you. If you were not provided one, leave this field blank.

Table 14 Network > WAN (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to set every field in this screen to its last-saved value.

5.4 The DDNS (Dynamic DNS) Screen

Dynamic DNS allows you to map your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you. SIP IP phones can access the SIP server on the X6004 using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

5.4.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

5.4.2 Configuring the DDNS Screen

Use this screen to configure your Dynamic DNS settings. To access this screen, click **Configuration > Network > DDNS**.

Figure 45 Network > DDNS

Each field is described in the following table.

Table 15 Network > DDNS

LABEL	DESCRIPTION
Enable DDNS	Select this to enable the DDNS feature on your X6004.
DDNS Type	Select the type of service that you are registered for with your Dynamic DNS service provider.
Username	Type your user name.
Password	Type the password assigned to you.
Domain name	Type the domain name assigned to your X6004 by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Wildcard	Select the check box to enable DynDNS Wildcard.
Interface	This field displays the interface registered to use DDNS services. On the X6004 it always displays "WAN".
Mail Exchanger	Use this field if the mail exchange server in your organization has a dynamically assigned IP address and you have not already registered it with a Dynamic DNS provider. Enter the domain name of your mail exchange server.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

5.5 The NTP (Network Time Protocol) Screen

Use this screen to configure time settings on the X6004. To access this screen, click **Configuration > Network > NTP**.

Figure 46 Network > NTP

Each field is described in the following table.

Table 16 Network > NTP

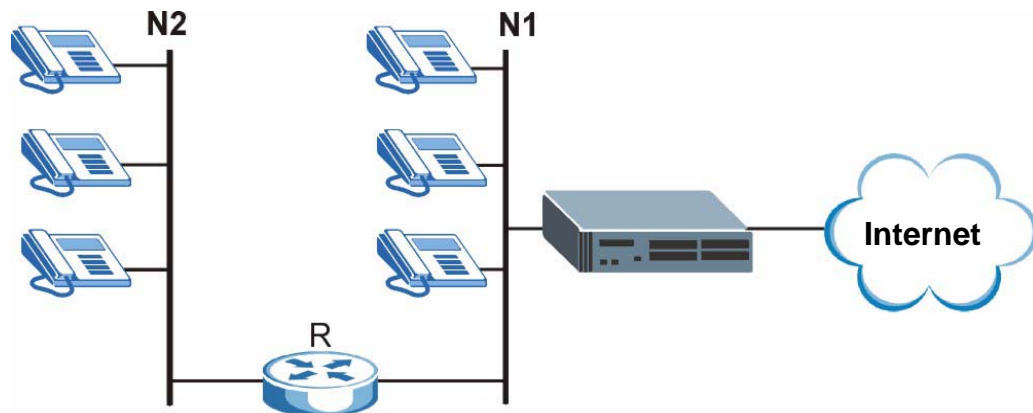
LABEL	DESCRIPTION
Current Time and Date	This section displays the current date and time.
Time and Date Setup	
Manual	Select this if you want to specify the current date and time in the fields below.
New Time	Enter the new time in this field, and click Apply .
New Date	Enter the new date in this field, and click Apply .
Get from Time Server	Select this if you want to use a time server to update the current date and time in the X6004.
Time Server Address 1/2	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.

Table 16 Network > NTP (continued)

LABEL	DESCRIPTION
Time Zone Setup	
Time Zone	Select the time zone at your location.
Enable Daylight saving	Select this if your location uses daylight savings time. Daylight savings is a period from late spring to fall when many places set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter which hour on which day of which week of which month daylight-savings time starts.
End Date	Enter which hour on which day of which week of which month daylight-savings time ends.
Offset	Enter the amount of time (1, 1.5, 2, 2.5, ... or 5.5 in hours) by which to adjust the time during daylight saving period.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

5.6 The Static Route Screen

In a subnetted LAN environment the X6004 is typically connected to a router. The router specifies the subnet to which the X6004 is directly connected and the X6004 has no knowledge of the subnets beyond. For instance, the X6004 knows about the IP phones in subnet N1 in the following figure. However, the X6004 is unable to route a packet to phones in subnet N2 because it doesn't know that there is a route through Router 1 (R). Static routes tell the X6004 about the subnets beyond the router to which it is directly connected.

Figure 47 Example of Static Routing Topology

5.6.1 Configuring the Static Route Screen

Use this screen to look at static routes in the X6004. Click **Configuration > Network > Static Route** to open the **Static Route** screen.

Figure 48 Network > Static Route



The following table describes the labels in this screen.

Table 17 Network > Static Route

LABEL	DESCRIPTION
Delete	Select this checkbox and click Delete to remove this static route from the X6004.
Destination Network	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This is the subnet mask of the static route.
Gateway IP	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN port. The gateway helps forward packets to their destinations.
Network Interface	This field specifies the interface of the static route.
Add/Delete	Use the Add and Delete icons to create or remove static routes respectively.

5.6.2 Adding a Static Route

Click the **Add** icon in the **Configuration > Network > Static Route** screen. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 49 Static Route > Add

The following table describes the labels in this screen.

Table 18 Static Route > Add

LABEL	DESCRIPTION
Add a New Static Route	
Destination Network	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	Select the IP subnet mask.
Gateway IP	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN port. The gateway helps forward packets to their destinations.
Network Interface	This is a read-only field indicating that this static route is configured for the LAN.
Apply	Click Apply to save your changes back to the X6004.
Cancel	Click Cancel to begin configuring this screen afresh.

5.7 The VLAN Screen

Use this screen to configure VLAN settings in the X6004. Click **Configuration > Network > VLAN** to open the **VLAN** screen.

Figure 50 Network > VLAN

Device	Priority / VLAN ID	Enable
WAN VLAN Tag	0 / 4000 (1 ~ 4094)	<input type="checkbox"/>
LAN VLAN Tag	0 / 4001 (1 ~ 4094)	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 19 Network > VLAN

LABEL	DESCRIPTION
Device	This displays a network interface.
Priority / VLAN ID	Select a priority level (0~7) and enter a VLAN ID (1~4094) you want the traffic is tagged with when it flows through the network interface.
Enable	Select this to insert the specified VLAN tag to the outgoing packets flowing through the network interface.
Apply	Click Apply to save your changes back to the X6004.

5.8 Network Technical Reference

This section contains background material relevant to the **Network** screens.

IEEE 802.1Q Tagged VLANs

An IEEE 802.1Q tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the device on which they were created. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for the device. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

IEEE 802.1p Priority Level

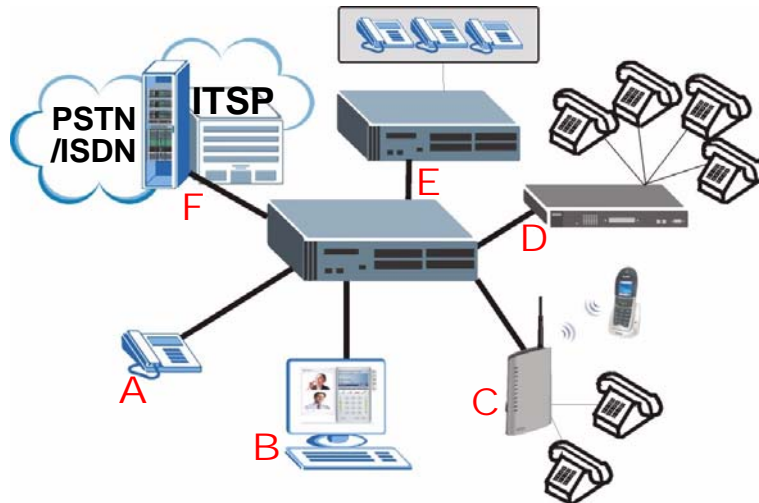
IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the incoming port.

6.1 Overview

This chapter shows you how to set up your X6004 SIP server settings on the X6004. It also covers parameters for FXO/FXS, ISDN BRI/PRI channels, call blocking settings, feature codes and email settings.

The following diagram shows SIP devices communicating with the X6004. In SIP some devices act as clients and others as servers. For example, in the figure below, devices **A-D** act as clients and must register with the X6004 before they are able to make calls via the X6004. The X6004 also is a client in relation to the SIP server located at the ITSP (**F**). The X6004 must register with the ITSP SIP server before calls can be routed to telephones outside its network. Finally, two SIP servers can act as peers, as shown with another X6004 (**E**) in the figure below. In this case, both X6004s must register with each other before they can forward each other's calls.

Figure 51 SIP Devices and the X6004



6.1.1 What You Can Do in this Chapter

- Use the **Global** screen to configure X6004's global VoIP settings. See [Section 6.2 on page 130](#).
- Use the **FXO** screen to configure FXO ports if you want to connect your X6004 to a traditional PBX's FXS ports. See [Section 6.3 on page 132](#).
- Use the **FXS** screen to configure FXS ports if you want to connect analog phones to your X6004. See [Section 6.4 on page 133](#).
- Use the **BRI** screen to configure the BRI line settings to the peer device your X6004 connects to. See [Section 6.5 on page 134](#).
- Use the **PRI** screen to configure the PRI line settings to the peer device your X6004 connects to. See [Section 6.6 on page 136](#).
- Use the **Call Block** screen to configure the black list settings which is not allowed to call into your X6004. See [Section 6.7 on page 139](#).
- Use the **Feature Code** screen to configure feature code settings. It allows users to dial a code on their phone's keypad to enable or disable a feature your X6004 supports. See [Section 6.8 on page 141](#).
- Use the **E-Mail** screen to configure email settings. It allows users to send voice mails or cdr backup data through the email server. See [Section 6.9 on page 144](#).
- Use the **Fake IP** screen to configure settings that may help you to avoid any potential VoIP problems that result from having the X6004 behind a NAT router. See [Section 6.10 on page 145](#).
- Use the **Peer-to-Peer** screen to set up a direct connection between two IP phones on the same subnet. See [Section 6.11 on page 146](#).

6.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

FXO Channel

An FXO channel is a connection from the X6004 to a traditional PBX (for example a PSTN connection) via one of the FXO ports installed on the X6004. After you install the FXO interface card on the X6004 (see the Quick Start Guide), you must configure how the X6004 adjusts the signal volume sent to and received from a traditional PBX.

FXS Channel

An FXS channel is a connection from the X6004 to an analog phone via one of the FXS ports installed on the X6004. After you install the FXS interface card on the X6004 (see the Quick Start Guide), you can configure how the X6004 adjusts the signal volume sent to and received from a connected device such as an analog phone or a PBX.

BRI/PRI

BRI (Basic Rate Interface) and PRI (Primary Rate Interface) are Integrated Services Digital Network (ISDN) physical layer standard and used to transmit voice and user data. BRI is used in homes or small companies providing data rates up to 128 kbps. PRI is used in larger enterprises providing data rates more than 1.5 Mbps.

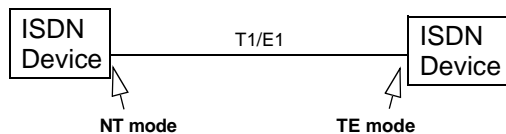
T1/E1

T1 and E1 are ISDN PRI line types. Both are telecommunication standards widely used in North America and Japan (T1) or outside of them (E1) to transmit voice and data between devices. T1 provides up to 1.544 Mbps and E1 provides up to 2.048 Mbps of connectivity.

NT/TE

TE (Terminal Equipment) refers to an ISDN user device such as an ISDN telephone, video telephone, digital fax machine (also known as G4 fax machine). The NT (Network Terminal) is the termination device between TEs and ISDN central office (CO). The NT is responsible for performance, monitoring, power transfer, and multiplexing of the channels. You must connect a TE device (configured as TE mode) to a NT device (configured as NT mode) to access an ISDN network.

Table 20 ISDN NT/TE Configuration Example



Types of ISDN Switches

There are many different ISDN switch types from different vendors in the world. The PRI interface card enables the X6004 to communicate with the following PRI switches.

- 4ESS - AT&T 4ESS switch type for the U.S. (ISDN PRI only)
- 5ESS - AT&T 5ESS switch type for the U.S. (ISDN PRI only)
- DMS - NT DMS-100 switch type for the U.S. (ISDN PRI only)
- NI2 - ISDN US NI2 PRI (TR 1268)
- NET5 - NET5 ISDN PRI switches (Europe)
- AUS - Australian TS014 switches (ISDN PRI only)
- Q.SIG

The BRI interface card enables the X6004 to communicate with the following BRI switches.

- 5ESS - AT&T basic rate switches
- MDS100
- NI1 - National ISDN-1 switches
- ENT3 - Euro-ISDN switches (UK and others)
- AUS - Australian TS013 switches

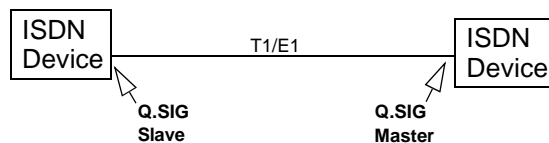
Q.SIG

Q.SIG is a protocol used for ISDN PRI voice signaling. Q.SIG enables the X6004 to connect PBXs and central office switches (COs) using the Q.SIG protocol. The X6004 can be a Q.SIG master or Q.SIG slave.

- Master - is responsible for layer 2 signaling and initiates the negotiation.
- Slave - responds master's signaling.

You must connect a Q.SIG master device to a Q.SIG slave device. An example of a Q.SIG configuration is shown next.

Figure 52 Q.SIG Configuration Example

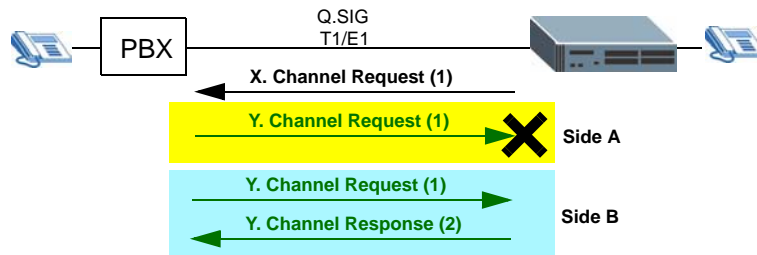


Side A/B Settings in Q.SIG

When using Q.SIG, the side A and B settings are used to avoid voice channel collision. See an example in the following figure. In E1, there are 30 voice channels. X6004 (**X**) requests to use channel 1 for an outgoing call and waits for **Y**'s response. Almost at the same time, **X** receives **Y**'s request to also use channel 1 for an outgoing call. If you configure **X** to use the side A, **X** will ignore **Y**'s

channel request. But if you use the side B setting, **X** will response the **Y** with the recommendation for another channel like channel 2.

Figure 53 Avoid Voice Channel Collision in Q.SIG



RTP

When you make a VoIP call using SIP, the RTP (Real Time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

NAT

Network Address Translation (NAT) replaces an IP address used inside one network with a different IP address that is used within another network.

Peer-to-Peer

Peer-to-peer networking has a number of participants whose devices assume the roles of both client and server. Although they are interconnected across existing network lines and hardware, they do not require a central server to manage their data nor do they behave strictly as clients. All participants in a peer-to-peer network can provide data to the others (like a server) while simultaneously receiving data from them (like a client). This type of distributed networking relies on the computing resources of each participant to create and maintain the data swarm. As such, a participant with limited resources can dramatically impact the efficiency of a small peer-to-peer network for the worse; fortunately, as the network grows in size the weakest links are rapidly overshadowed by the bigger, faster participants.

6.1.3 Before You Begin

Before you start configuring FXO/FXS/BRI/PRI on your X6004, you should install corresponding interface cards on your X6004.

6.2 The IP-PBX Server Global Screen

Use this screen to set up the SIP server settings on the X6004. SIP clients, such as the IP phones on your network, must enter this information when registering with the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Server**.

Figure 54 Server > IP-PBX Global Setting

IPPBX Global Setting

SIP Server Realm Name:

Port: Default: Alternative 1: 2:

Default SIP Client Registration Expiration: NAT: (60~86400)Sec. Non-NAT: (60~86400)Sec

RTP Port Range: ~

Default Ring Time: (1~300)Sec.

Codec G723.1: Disable Enable

Enable Personal AA: From external call From internal call

DNS SRV: Disable Enable

Enable Session Timer :

Minimum SE : Sec. (90 ~ 1800)

Session Expires : Sec. (90 ~ 86400, must ≥ Minimum SE)

Each field is described in the following table.

Table 21 Server > IP-PBX Global Setting

LABEL	DESCRIPTION
SIP Server Realm Name	A realm is a set of usernames and passwords used by SIP client devices to authenticate with a SIP server. The X6004 supports a single realm. When SIP clients register with the X6004, they must provide the name of the realm they belong to as well as the username and password. Type the realm name which the extensions that register with the X6004 must provide for authentication.
Port	Enter the X6004's listening port number or keep the default value. This is the port number your SIP clients need to use to register with the X6004. You can also enter up to two different alternate ports.

Table 21 Server > IP-PBX Global Setting (continued)

LABEL	DESCRIPTION
Default SIP Client Registration Expiration	<p>The X6004 is a SIP registrar server. A SIP registrar server maintains a database of SIP identity-to-IP address (or domain name) mapping. The X6004 checks your username, password and realm when you register.</p> <p>Enter the number of seconds SIP clients are registered with the X6004 before their registration record is deleted.</p> <p>Make sure that the client SIP devices are configured to re-register at an interval smaller than the time set in this field.</p> <p>You can enter expiration times for SIP clients that use NAT as well as those that do not.</p>
RTP Port Range	<p>When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer.</p> <p>Enter the listening port number(s) for RTP traffic or keep the default values. Enter the port number at the beginning of the range in the first field and enter the port number at the end of the range in the second field.</p>
Default Ring Time	Specify for how many seconds the X6004 sends a ringing tone to client devices for incoming calls.
Codec G723.1	<p>Select Enable to turn on support for G723.1 voice codec or select Disable to turn off support for the G723.1 voice codec.</p> <p>Note: This setting only takes effect after a system restart.</p>
Disable Personal AA	<p>Select From external call to disable the X6004's Auto-Attendant feature for calls received from outside the PBX-managed telephone system.</p> <p>Select From internal call to disable the X6004's Auto-Attendant feature for calls received from within the PBX-managed telephone system.</p>
DNS SRV	<p>Select Enable to have the X6004 query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls. Doing this, however, could impact the X6004's performance.</p> <p>Select Disable to turn off the DNS SRV query. This is the X6004's default setting for this feature.</p>
Enable Session Timer	Select this to enable the session timer.
Minimum SE	Enter the minimum time in seconds before an idle SIP connection expires. You can enter a value between 90 and 1800.
Session Expires	<p>Enter the duration in seconds before an idle SIP connection expires. You can enter a value between 90 and 86400.</p> <p>The value entered in this field must be greater than or equal to the value entered in the Minimum SE field.</p>
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

6.3 The FXO Screen

Use this screen to configure settings related to the FXO lines configured on the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Server > FXO**.

Figure 55 Server > FXO

The screenshot shows the 'FXO Setting' configuration window. It contains the following fields and values:

- FXO Configuration:** Machine ID: IPPBX_001, Slot: Slot_A, Port: Port_3
- Tx Volume:** Level: 0
- Rx Volume:** Level: 0
- Busy Detect:** Count: 2
- Country Code:** Code: Default

At the bottom of the window are two buttons: 'Apply' and 'Reset'.

Each field is described in the following table.

Table 22 Server > FXO

LABEL	DESCRIPTION
FXO Configuration	Use these fields to specify the FXO interface which you want to configure.
Machine ID	Specify the X6004 for which you want to configure FXO settings. This field is only configurable if you have more than one X6004 working in a ZyStack.
Slot	Specify which FXO interface card you want to configure. The cards are identified by the extension card slot they are installed in. Select one of the slots or select All to make the settings the same for all FXO interface cards.
Port	Specify the FXO port on the FXO interface card you want to configure.
TX Volume	Select the volume level transmitted from the X6004. -6 is the quietest, and 6 is the loudest.
RX Volume	Select the volume level transmitted to the X6004. -6 is the quietest, and 6 is the loudest.
Busy Detect	<p>The X6004 listens for a tone to detect if an FXO line has been hung up. This tone differs by region and it may also differ slightly between carriers. In some cases the X6004 may mistake background noise for a busy line signal.</p> <p>This setting defines the number of busy tones the X6004 needs to recognize before actually considering the line to be busy.</p> <p>You should select a low value, if you have a good connection. Select a higher value, if your FXO connection is of lower quality to avoid false hang-ups.</p>

Table 22 Server > FXO (continued)

LABEL	DESCRIPTION
Country Code	The signals used to indicate a busy line or an available line differ by country. You must select the country code for the location of the X6004. The X6004 can then recognize whether the FXO line is in use or available. Select default to reset the country code value to the factory defaults.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

6.4 The FXS Screen

Use this screen to configure settings for the analog phones connected to the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Server > FXS**.

Figure 56 Server > FXS

The screenshot shows the 'FXS Setting' configuration window. It includes the following fields and values:

- FXS Configuration:** Machine ID: IPPBX_001, Slot: Slot_A, Port: Port_1
- Tx Volume:** Level: -2
- Rx Volume:** Level: -2
- Dial Interval:** Sec.: 3
- Country Code:** Code: Default

At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

Each field is described in the following table.

Table 23 Server > FXS

LABEL	DESCRIPTION
FXS Configuration	Use these fields to specify the FXS interface which you want to configure.
Machine ID	Specify the X6004 for which you want to configure FXS settings. This field is only configurable if you have more than one X6004 working in a ZyStack.
Slot	Specify which FXS interface card you want to configure. The cards are identified by the extension card slot they are installed in. Select one of the slots or select All to make the settings the same for all FXS interface cards.
Port	Specify the FXS port on the FXS interface card you want to configure.
Tx Volume	Select the volume level transmitted from the X6004. -6 is the quietest, and 6 is the loudest.

Table 23 Server > FXS (continued)

LABEL	DESCRIPTION
Rx Volume	Select the volume level transmitted to the X6004. -6 is the quietest, and 6 is the loudest.
Dial Interval	Enter the number of seconds the X6004 should wait after you stop dialing numbers (from FXS extensions) before it makes the phone call.
Country Code	The signals used by telephone companies to indicate a busy line or an available line differ by country. You must select the country code for the location of the X6004. The X6004 can then detect whether the FXS line is in use or available.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

6.5 The BRI Screen

Use this screen to configure ISDN BRI interface settings on the X6004. Click **Configuration > PBX > Server Configuration > Server > BRI Configuration** to view the screen as shown next.

Note: You have to reboot the X6004 manually to apply changes in the **Switch Type**, **NT/TE mode**, or **TEI** fields.

Figure 57 Server > BRI Configuration

The screenshot shows the 'BRI Setting' configuration window. It includes the following fields and controls:

- BRI Configuration:** Machine ID: IPPBX_001, Slot: Slot_D, Port: Port_1
- Switch Type:** NET3
- NT/TE Mode:** TE
- TEI:** Dynamic (selected), Fixed
- Digit Handling:** En-bloc
- Tx Volume:** Level: -2
- Rx Volume:** Level: -2
- Buttons:** Apply, Reset

Each field is described in the following table.

Table 24 Server > BRI Configuration

LABEL	DESCRIPTION
BRI Configuration	Use these fields to specify the ISDN BRI interface which you want to configure.
Machine ID	Specify the X6004 for which you want to configure ISDN BRI settings. This field is only configurable if you have more than one X6004 working in a ZyStack.

Table 24 Server > BRI Configuration (continued)

LABEL	DESCRIPTION
Slot	Specify which ISDN BRI interface card you want to configure. The cards are identified by the extension card slot they are installed in. Select one of the slots or select All to make the settings the same for all ISDN BRI interface cards.
Port	Specify the BRI port on the ISDN BRI interface card you want to configure.
Switch Type	Select a switch type according to your area and the technology your telephone company uses. Generally, U.S. telephone exchanges use 5ESS switches while Europe uses NET3 and Australia uses AUS switches. As of this writing, the X6004 only supports NET3.
NT/TE Mode	Select NT (Network Terminal) or TE (Terminal Equipment) to decide the X6004's role when connecting to an ISDN device. See NT/TE on page 127 for more information.
TEI	This Terminal Endpoint Identifier is used to uniquely identify each TE device. Select Dynamic to automatically request an ID when the X6004 is connected to the network. Or select Fixed and enter a number (0-63) provided from your telephone company. Note: You must configure the same TEI on the X6004 and its connected BRI device.
Digit Handling	Specify the signalling method the X6004 accepts to receive a callee's number through a specified BRI port. En-bloc: The X6004 expects to receive a complete callee's number at one time. Overlap: The X6004 expects to receive digits of a callee's number one-by-one. Note: If the switch type is "NT", then Digital Handling can select "Overlap" or "En-bloc". Note: If the switch type is "TE", then Digital Handling can select "En-bloc" only.
Tx Volume	Select the volume level transmitted from the X6004. -6 is the lowest, and 6 is the loudest.
Rx Volume	Select the volume level transmitted to the X6004. -6 is the lowest, and 6 is the loudest.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

6.6 The PRI Screen

Use this screen to configure ISDN PRI interface settings on the X6004. Click **Configuration > PBX > Server Configuration > Server > PRI Configuration** to view the screen as shown next.

Note: You have to reboot the X6004 manually to apply changes in the **Switch Type** or **NT/TE mode** fields.

Figure 58 Server > PRI Configuration

The screenshot displays the 'PRI Setting' configuration page. It features a list of settings on the left and their corresponding values in dropdown menus on the right. At the bottom, there are 'Apply' and 'Reset' buttons.

Setting	Value
PRI Configuration	Machine ID: IPPBX_001, Slot: Slot_C, Port: Port_1
Switch Type	NET5
NT/TE Mode	TE
LineBuildOut	120
Framing	CRC4
Coding	HDB3
Digit Handling	Overlap
Tx Volume	Level: -2
Rx Volume	Level: -2

Buttons: Apply, Reset

Figure 59 Settings for PRI Switch Types

4ESS	5ESS	DMS
Switch Type: 4ESS	Switch Type: 5ESS	Switch Type: DMS
NT/TE Mode: NT	NT/TE Mode: NT	NT/TE Mode: NT
LineBuildOut: CSU 0	LineBuildOut: CSU 0	LineBuildOut: CSU 0
Framing: ESF	Framing: ESF	Framing: ESF
Coding: B8ZS	Coding: B8ZS	Coding: B8ZS

NI2	NET5	AUS
Switch Type: NI2	Switch Type: NET5	Switch Type: AUS
NT/TE Mode: NT	NT/TE Mode: NT	NT/TE Mode: NT
LineBuildOut: CSU 0	LineBuildOut: 120	LineBuildOut: 120
Framing: ESF	Framing: CRC4	Framing: CRC4
Coding: B8ZS	Coding: HDB3	Coding: HDB3

Q.SIG
Switch Type: Q.SIG
Q.SIG Type: Master SIDE: A
LineBuildOut: 120
Framing: CRC4
Coding: HDB3

Each field is described in the following table.

Table 25 Server > PRI Configuration

LABEL	DESCRIPTION
PRI Configuration	Use these fields to specify the ISDN PRI interface which you want to configure.
Machine ID	Specify the X6004 for which you want to configure ISDN PRI settings. This field is only configurable if you have more than one X6004 working in a ZyStack.
Slot	Specify which ISDN PRI interface card you want to configure. The cards are identified by the extension card slot they are installed in. Select one of the slots or select All to make the settings the same for all ISDN PRI interface cards.
Port	Specify the PRI port on the ISDN PRI interface card you want to configure.
Switch Type	Select a switch type depending on T1 or E1 mode and the technology your telephone company uses. You can select 4ESS , 5ESS , DMS , NI2 or CAS_T1_EM_IS switch type if you connect the port to a T1 line while you can select NET5 , AUS or Q.SIG switch type if you connect the port to a E1 line.

Table 25 Server > PRI Configuration (continued)

LABEL	DESCRIPTION
NT/TE Mode	Select NT (Network Terminal) if a TE device (for example, an ISDN phone) connects to the specified port. Select TE (Terminal Equipment) if this port connects to a NT device (for example, a PBX). See NT/TE on page 127 for more information.
Q.SIG Type	Select the role of a PRI interface in an ISDN Q.SIG network (Master or Slave) and the method to avoid channel collision (SIDE A or SIDE B). The setting is only available for the switch type Q.SIG .
LineBuildOut	This specifies the transmission and receiving levels to cable length. Depending on a T1 or E1 line the port is connected to, you have the following options. T1: You can select one of the following options based on the necessary transmission/receiving level (using CSU) or possible cable distance your estimated between two PRI peers (using DSX). CSU 0 = 0 dB CSU 75 = 7.5 dB CSU 15 = 15 dB CSU 225 = 22.5 dB DSX 110 = 0~110 ft. DSX 220 = 110~220 ft. DSX 330 = 220~330 ft. DSX 440 = 330~440 ft. DSX 550 = 440~550 ft. DSX 660 = 550~660 ft. E1: Select one of the following options based on the possible cable distance your estimated between two PRI peers. 120 = 120 ft.
Framing	This is a type of framing which decides the way to align framing channels. You have to configure same framing type in both connected PRI devices. Depending on a T1 or E1 line the port is connected to, you have the following options. T1: SF (Super Frame), ESF (Extended Super Frame). E1: CRC4 (Cyclic Redundancy Check 4), NonCRC4 (None Cyclic Redundancy Check 4).

Table 25 Server > PRI Configuration (continued)

LABEL	DESCRIPTION
Coding	<p>This is a type of line code which helps to against signal loss during transmission. You have to configure same coding type in both connected PRI devices.</p> <p>Depending on a T1 or E1 line the port is connected to, you have the following options.</p> <p>T1: AMI (Alternate Mark Inversion), B8ZS (Binary Eight Zero Substitution).</p> <p>E1: AMI (Alternate Mark Inversion), HDB3 (High Density Bipolar of order 3 code).</p>
Digit Handling	<p>Specify the signalling method the X6004 accepts to receive a callee's number through a specified PRI port.</p> <p>En-bloc: The X6004 expects to receive a complete callee's number at one time.</p> <p>Overlap: The X6004 expects to receive digits of a callee's number one-by-one.</p>
Tx Volume	Select the volume level transmitted from the X6004. -6 is the lowest, and 6 is the loudest.
Rx Volume	Select the volume level transmitted to the X6004. -6 is the lowest, and 6 is the loudest.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

6.7 The Call Block Screen

Use this screen to have the X6004 not accept incoming calls from specific phone numbers or calls without caller ID. Click **Configuration > PBX > Server Configuration > Server > Call Block** to view the screen as shown next.

Figure 60 Server > Call Block

System-wide Call Block	
Black list	<input checked="" type="radio"/> Disable <input type="radio"/> Enable (<input type="text" value="Black list"/>)
Anonymous block:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Each field is described in the following table.

Table 26 Server > Call Block

LABEL	DESCRIPTION
Black list	Select Disable to turn call blocking off on the X6004. Select Enable to turn on call blocking on the X6004. Click Black list to configure the phone numbers you want to block from calling into the X6004. See Section 6.7.1 on page 140 .
Anonymous block:	Select Disable to allow any incoming calls routed by the X6004. Select Enable to block calls without caller ID from being routed by the X6004.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

6.7.1 The Call Blacklist Screen

Use this screen to set up a list of phone numbers that are not allowed to call into the X6004.

You can also use the letters **X**, **Z** and **N** to represent numbers you want to block. The letter “**X**” represents any digit from 0-9, **Z** any digit from 1-9 and **N** any digit from 2-9. For example, enter **023XXXXXX** to block any 9 digit number that starts with **023** from calling the extensions configured on the X6004.

Furthermore, you can use the period (.) as a wildcard, to block any numbers that begin with a pattern of digits you specify. For example, enter **555.** to block any numbers starting with the string **555** from calling the extensions configured on the X6004.

To access this screen, click **Configuration > PBX > Server Configuration > Server > Call Block(AA) > Black List**.

Figure 61 Call Block > Black List

Each field is described in the following table.

Table 27 Call Block > Black List

LABEL	DESCRIPTION
Number	Type the telephone number you want the X6004 to block from calling extensions in your telephone network. Click Add to place this number in the blacklist. You can also use the letters N, X and Z to represent numbers and the period "." to include any number that starts with the digits you specify.
Delete	Highlight an existing telephone number in the blacklist and click the Delete icon to remove this telephone number from the blacklist.
Apply	Click this to save your changes.
Cancel	Click this to go back to the Call Block screen.

6.8 The Feature Code Screen

Use this screen to set values for the feature codes the X6004 supports from an IP phone's extension. Users can dial these codes to enable or disable the features listed below for their extension settings by entering these codes on their phone's keypad. Click **Configuration > PBX > Server Configuration > Server > Feature Code** to open the screen as shown.

Figure 62 Server > Feature Code

Feature Code Setting

Black List On	<input type="text" value="*67"/>	Black List Off	<input type="text" value="*85"/>
Block no ID On	<input type="text" value="*77"/>	Block no ID Off	<input type="text" value="*87"/>
Call Forward On	<input type="text" value="*72"/>	Call Forward Off	<input type="text" value="*73"/>
Call Forward VM	<input type="text" value="*74"/>	Call Forward Busy On	<input type="text" value="*90"/>
Call Forward Busy Off	<input type="text" value="*91"/>	Call Forward Busy VM	<input type="text" value="*92"/>
Call Forward No Answer On	<input type="text" value="*82"/>	Call Forward No Answer Off	<input type="text" value="*83"/>
Call Forward No Answer VM	<input type="text" value="*84"/>	Call Transfer	<input type="text" value="*96"/>
Direct Pickup	<input type="text" value="*95"/>	DND On	<input type="text" value="*78"/>
DND Off	<input type="text" value="*79"/>	DND VM	<input type="text" value="*80"/>
Follow Me On	<input type="text" value="*22"/>	Follow Me Off	<input type="text" value="*23"/>
Group Pickup	<input type="text" value="*94"/>	Personal IVR	<input type="text" value="*"/>
Voice Mail	<input type="text" value="**"/>	Second Dial	<input type="text"/>
Mobile Extension On	<input type="text" value="*97"/>	Mobile Extension Off	<input type="text" value="*98"/>
Mobile Extension Auto On/Off	<input type="text" value="*99"/>	Internal Operator(0 or 9)	<input type="text"/> Ext. <input type="text"/>

The following table describes the labels in this screen.

Table 28 Server > Feature Code

LABEL	DESCRIPTION
Feature code setting	The codes you enter are dialed by individuals to manage the features listed below for their extension.
Black List On	This code is used to enable call blocking for numbers on the personal blacklist of an extension.
Black List Off	This code is used to disable call blocking for numbers on the personal blacklist of an extension.
Block no ID On	This code is used to enable call blocking for calls without a caller ID.
Block no ID Off	This code is used to disable call blocking for calls without a caller ID.
Call Forward On	This code is used to enable call forwarding.
Call Forward Off	This code is used to disable call forwarding.
Call Forward VM	This code is to forward an incoming call to voice mail system when the call was forwarded to this extension.
Call Forward Busy On	This code is used to enable call forwarding when an extension is busy.
Call Forward Busy Off	This code is used to disable call forwarding when an extension is busy.
Call Forward Busy VM	This code is to forward an incoming call to voice mail system when the call was forwarded to this extension and this extension is busy.
Call Forward No Answer On	This code is used to enable call forwarding when there is no answer at an extension.
Call Forward No Answer Off	This code is used to disable call forwarding when there is no answer at an extension.
Call Forward No Answer VM	This code is to forward an incoming call to voice mail system when the call was forwarded to this extension and no one answers the call.
Call Transfer	This code is used to transfer calls.
Direct Pickup	This code is used to pick up calls for your extension from a different extension.
DND On	This code is used to turn the Do Not Disturb feature on for this extension.
DND Off	This code is used to turn the Do Not Disturb feature off for this extension.
DND VM	This code is to forward an incoming call to voice mail system when the call was forwarded to this extension and this extension is set Do Not Disturb.
Follow Me On	This code is used to turn the Follow Me feature on for this extension.
Follow Me Off	This code is used to turn the Follow Me feature off for this extension.
Group Pickup	This code is used for pickup calls for your extension from a different extension in the same pickup group.
Personal IVR	This code is used to edit personal configuration for an extension via the handset.
Voice Mail	This code is used to access voice mail on the X6004.

Table 28 Server > Feature Code (continued)

LABEL	DESCRIPTION
Second Dial	<p>This code is used to get a second dialtone. When you enter the Second Dial code from your phone, the X6004 opens a connection to the outside telephone network.</p> <p>For example, in many office environments you cannot access an outside dialtone unless you press “9” or “0” first. A number dialed without such a prefix is considered internal and thus routed to the appropriate extension. If that extension does not exist, an error is returned.</p> <p>Leave this field blank if you do not require people using your telephone network to dial a specific number to access an outside line.</p> <p>Note: You only need to enable this function if your phone network is analog-based (such as one that uses FXS). Digital phone systems such as SIP and BRI do not require it.</p> <p>Note: If you enable this function on a digital network, a person does not need to use the Second Dial number in conjunction with any phone numbers dialed.</p>
Mobile Extension On	<p>This code is used to activate a mobile extension.</p> <p>For example, if your IP PBX extension has been configured to use your cell phone as a mobile extension, you can dial into the X6004 with your cell phone and then enter this code. That tells the X6004 to send all calls to your extension to your cell phone.</p>
Mobile Extension Off	<p>This code is used to turn off the mobile extension feature.</p> <p>For example, if all calls currently incoming to your extension are sent to your cell phone, you can dial into the X6004 and then enter this code. That tells the X6004 to stop sending calls intended for your extension to your cell phone.</p>
Mobile Extension Auto On/Off	<p>This code is used to activate the mobile extension feature from your regular telephone extension.</p> <p>Once activated, calls are sent both to your extension and to the phone designated as the mobile extension.</p> <p>When you turn off this feature from your regular telephone extension, then calls are no longer sent simultaneously to both your extension and the mobile extension; they are sent strictly to your regular extension.</p>
Internal Operator (0 or 9)	<p>Use the first field of this code to set which number (0 or 9) internal users dial to reach the internal operator. Use the second field to specify the operator’s extension number. The extension must already exist in the X6004.</p>
Apply	<p>Click this to save your changes.</p>
Reset	<p>Click this to set every field in this screen to its last-saved value.</p>

6.9 The E-Mail Screen

Use this screen to configure the mail server information through which the X6004 sends voice mails and CDR (Call Detail Record) files to the email addresses which you configured in extension voice mail (see [Section 13.3.8 on page 216](#)) and CDR (see [Section 28.2 on page 414](#)) screens. Click **Configuration > PBX > Server Configuration > Server > E-Mail** to view the screen as shown next.

Figure 63 Server > E-Mail

Each field is described in the following table.

Table 29 Server > E-Mail

LABEL	DESCRIPTION
E-Mail Server	Specify a mail server's IP address.
Sender	Specify the sender's email address.
SMTP Authentication	Select this and enter your username and password if user authentication is required in the mail server.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

6.10 The Fake IP Screen

Use this screen to configure settings that may help you to avoid any potential VoIP problems that result from having your X6004 behind a NAT router.

When enabled, the X6004 replaces the IP address inside all outgoing SIP packets with the IP address of the upstream NAT router on your network. When the packets get to their destination, the destination device can send its response to the embedded address of the NAT router. The NAT router then forwards the packets downstream to the X6004, which in turn sends them to the device on the local end of the telephone conversation.

Note: This feature should be used if the NAT router does not utilize SIP ALG.

Click **Configuration > PBX > Server Configuration > Server > Fake IP** to view the screen as shown next.

Figure 64 Server > Fake IP

Each field is described in the following table.

Table 30 Server > Fake IP

LABEL	DESCRIPTION
Fake IP	Select Disable to turn this feature off or Enable to turn it on. By default, the Fake IP feature is disabled. If you enable it, you must assign a value to the Fake IP Setting field.
Fake IP Setting	Enter the public IP address that the upstream NAT router uses to send out the X6004's SIP traffic. This is the IP address that will be inserted into all outgoing SIP traffic.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

6.11 The Peer to Peer Screen

Use this screen to allow the X6004 to set up a direct connection between two IP phones on the same subnet. This allows the X6004 to remain free of the loading burden and free up IP PBX resources (such as DSP channels). When a special feature request is made by either end of the connection, such as call parking or music on hold, then the X6004 re-establishes control of the connection to implement the feature.

Click **Configuration > PBX > Server Configuration > Server > Peer to Peer** to view the screen as shown next.

Figure 65 Server > Peer-to-Peer

Each field is described in the following table.

Table 31 Server > Peer-to-Peer

LABEL	DESCRIPTION
Peer to Peer	
Peer to Peer	Select Disable to turn this feature off or Enable to turn it on. By default, the Peer-to-Peer feature is disabled. If you enable it, you should set up the Local Net for Peer to Peer .
Local Net for Peer to Peer	
Delete	Click this to delete the selected item(s) in this list.
Select	Check this box to mark an item in this list for deletion.
Local Net for Peer to Peer	This displays the network on which Peer to Peer connections may be made. For example, if the Local Net IP address is 192.168.1.0/24, then any device with an IP from 192.168.1.1 to 192.168.1.254 can make a peer connection to any other device in the same host range.
Add	Click this to add a new entry to the local net list.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

6.11.1 How the Peer-to-Peer SIP Connection Works

The following is a basic explanation of how the X6004 creates a peer-to-peer SIP connection between two IP phones within the same host range.

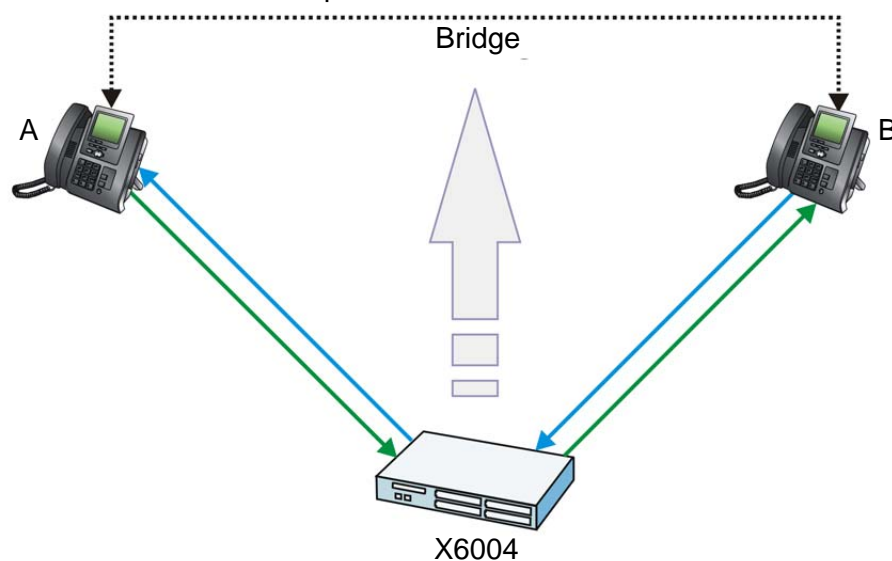
- 1 The first phone (**A**) sends an invite for the other phone to the X6004. This invite includes its IP address and which codecs it can use.
- 2 Next, the X6004 accepts the invite on behalf of the second phone (**B**) and sends an acknowledgement back to **A**.
- 3 The X6004 sends an new invite to **B**. This invite includes the X6004's IP address and the codecs it has in common in with **A**.

For example, if **A** says it can use the G.723, Speex, and GSM codecs but the X6004 is set to G.723, then the X6004 lets **B** know that only the G.723 codec is available for the telephone call.

- 4 When **B** accepts the invite from the X6004, it sends back an acknowledgement. The X6004 has now received confirmation from both phones of their IP addresses and an mutually agreed upon codec.
- 5 The X6004 sends out a re-invite to both **A** and **B** that includes both IP addresses and the codec to be used. This allows the two phones to create a bridge directly with one another. The X6004 then removes itself from the communication chain.

Note: If either phone A or B requests to use a feature specific to the X6004, such as call parking or music on hold, the X6004 interrupts the direct communication bridge and re-establishes control of the two SIP connections.

Figure 66 A Peer-to-Peer Example



6.11.2 Add Peer-to-Peer Local Net

Use this screen to add a subnet IP address to the localnet table for making peer-to-peer connections. To access this screen, click **Configuration > PBX > Server Configuration > Server > Peer to Peer** and click the **Add** icon in the **Local Net for Peer to Peer** table.

Figure 67 Peer-to-Peer > Local Net

Each field is described in the following table.

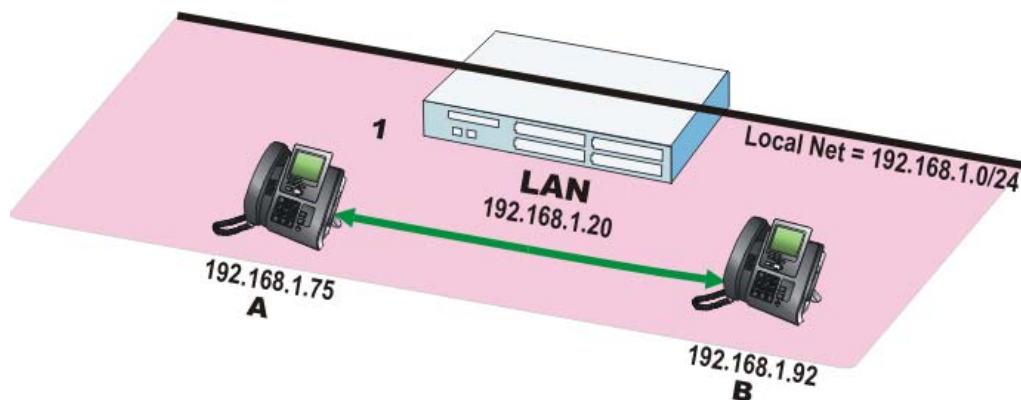
Table 32 Peer to Peer > Local Net

LABEL	DESCRIPTION
IPv4 subnet in CIDR format	Enter an IPv4-compatible IP address in this field then select the length of the subnet mask from the list. This option defines a subnet for which the X6004 can set up peer-to-peer networking. For more information on subnetting, see Appendix A on page 529 .
Apply	Click this to save your changes.
Cancel	Click this to go back to the Fake IP screen.

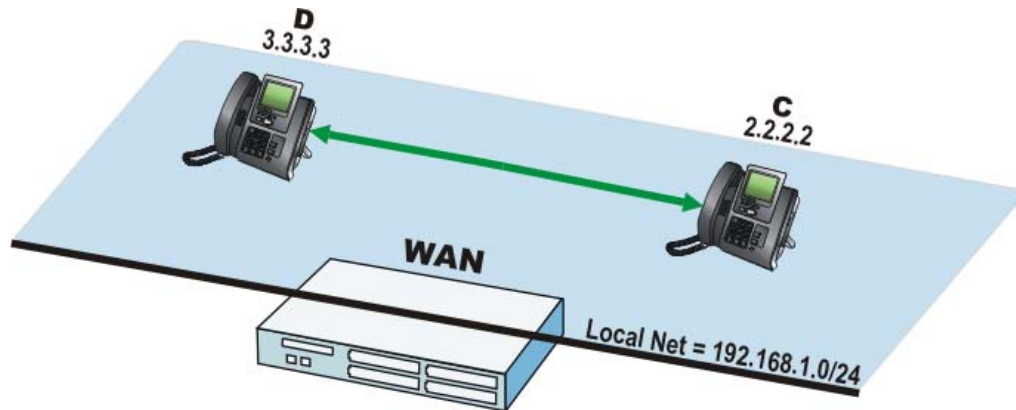
6.11.3 How Local Net and Peer-to-Peer Work Together

Peer-to-peer calls can be made through the X6004, but with certain limitations:

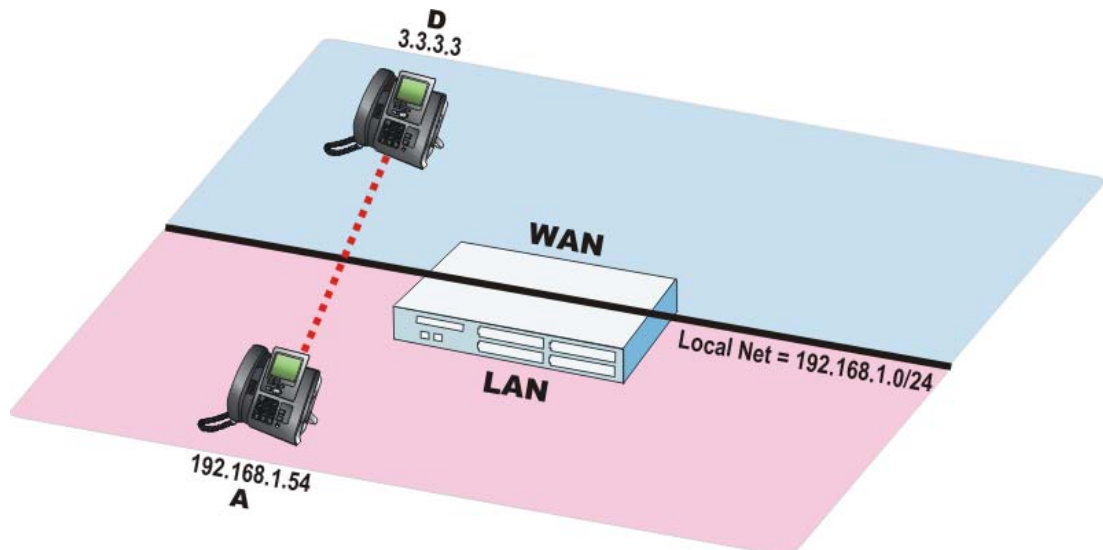
- 1 Peer-to-peer calls can be made between any devices on the LAN if they belong to a subnet listed in the same localnet table.



- 2 Peer-to-peer calls can be made between devices on the WAN if neither device belongs to a subnet listed in the localnet table.



- 3 However, peer-to-peer calls cannot be made between devices if one of them belongs to a subnet listed in the localnet table and the other does not.



Furthermore, the devices making a peer-to-peer connection:

- Must have a common codec they can use between them.
- Must use SIPInfo for DTMF.
- Must not be using NAT.

If they cannot meet these conditions, the peer-to-peer connection will fail and the call will be routed through the X6004 instead.

For more information on adding different subnets to the localnet table, see [Section 6.11 on page 146](#).

6.12 Network Technical Reference

This section contains background material relevant to the **Server** screens.

ISDN Overview

ISDN (Integrated Service Digital Network) is a circuit-switched telephone network system. In ISDN, there are two types of channels: B-channels and D-channels. ISDN allows digital transmission of voice, video and data over ordinary telephone copper wires using B-channels with 64 kbps bandwidth. D-channels are mainly used for signaling and control with 16 kbps or 64 kbps bandwidth depending on service levels.

There are two service levels in ISDN as follows.

- BRI (Basic Rate Interface): BRI contains two 64 kbps B channel and one 16 kbps D channel (2B+1D). A BRI user can have up to 128 kbps service.
- PRI (Primary Rate Interface):
 - North America and Japan use 23B+1D, with a total bandwidth of 1.544 Mbps (T1).
 - Europe, Australia and most of the rest of the world use the slightly higher capacity E1 which is 30B+1D with a total bandwidth of 2.048 Mbps.

Auto Provision

7.1 Overview

This chapter shows you how to set up auto provisioning for the SIP clients of the X6004.

Auto provisioning allows administrators to configure VoIP related settings on ZyXEL's SIP clients from a central location. You can set up and maintain a configuration file associated with a SIP extension on the X6004. Auto provisioning has the VoIP devices periodically download the configuration file from the X6004.

Note: Check the documentation that came with your ZyXEL softphone, IP phone, ATA or other device to see if it supports auto provisioning.

The configuration file contains the settings you configure for a specific telephone extension in your organization. It also contains SIP settings necessary for the device to register with the X6004. The configuration file is encrypted using 3DES (Triple Data Encryption Standard). See [Chapter 13 on page 197](#) for more information on extensions and [Chapter 6 on page 125](#) for more information on SIP settings.

7.1.1 What You Can Do in this Chapter

- Use the **Auto Provision** screen to configure auto provisioning files for your ZyXEL VoIP devices connected to this Device. See [Section 7.2 on page 155](#).
- Use the **snom Profile Setup** screen to configure auto provisioning for the snom VoIP devices connected to this Device. See [Section 7.3 on page 159](#).
- Use the **Auto Firmware Upgrade** screen to configure the information that IP phones connected to the X6004 will use to upgrade their own firmware from an FTP server. See [Section 7.4 on page 165](#).
- Use the **EZ Provision** screen to set the administrator PIN code required for initiating EZ provisioning between the X6004 and an unconfigured IP phone. See [Section 7.5 on page 167](#).

7.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

SPTGEN file

This is a configuration file that can be downloaded by ZyXEL devices that support SPTGEN.

How to Configure Auto Provisioning

Take the following steps to configure auto provisioning for the VoIP devices on your network. See also [Chapter 3 on page 41](#) for an auto provisioning tutorial.

- 1 Configure extensions that you want to assign to VoIP devices on your network. See [Chapter 13 on page 197](#).
- 2 Create an SPTGEN file. Use the **Auto Provision** screen, described in [Section 7.2 on page 155](#), to create this file. You will need one of the following: the MAC address of the IP phone or ATA or the serial number associated with a ZyXEL softphone. This information is used to uniquely identify the device that you want to assign an extension to.
- 3 Configure the auto provisioning compliant ZyXEL device (or softphone) to receive configuration information from the X6004. This typically involves specifying the protocol used for auto provisioning. At the time of writing, you can use HTTP protocol for auto provisioning with the X6004. See the documentation that came with your ZyXEL device for information on how to do this.

How Auto Provisioning Works

When a ZyXEL device is configured for auto provisioning, it attempts to find an auto provisioning server on its network. ZyXEL devices use Simple Service Discovery Protocol (SSDP) to find the IP address of an auto provisioning server (for example the X6004). This process is referred to as auto discovery. Some ZyXEL devices allow you to enter the IP address of the auto provisioning server.

Note: The auto discovery process is limited to your LAN.

Once a ZyXEL VoIP devices finds the X6004, it sends an HTTP request for a configuration file. The X6004 checks to see if it has a configuration file associated with the serial number or MAC address of the ZyXEL device requesting the configuration file. If the X6004 has the configuration file, then it sends the configuration file to the ZyXEL VoIP device.

You can also upload csv format files to the X6004 for batch configuring ZyXEL's IP phones.

7.1.3 Before You Begin

Before you start configuring Auto Provisioning on your X6004, you should prepare the following:

- Create SIP extension(s) that you want to assign to your VoIP devices in the **PBX > Extension Management > Authority Group > Advanced > SIP Peer**.
- Find your ZyXEL VoIP devices' MAC addresses and serial numbers on the devices' back panel or package boxes. Use those to associate SIP numbers to your VoIP devices.

7.2 Auto Provision Screen

If an auto provisioning file has been configured for a SIP extension, this screen displays the mapping between SIP extensions and ZyXEL VoIP device's MAC addresses or serial numbers. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision**.

Figure 68 Server Configuration > Auto Provision

Each field is described in the following table.

Table 33 Server Configuration > Auto Provision

LABEL	DESCRIPTION
Service Configuration	
Machine ID	This indicates the X6004's identification number.

Table 33 Server Configuration > Auto Provision (continued)

LABEL	DESCRIPTION
Auto Provision	Select Enable to turn on auto provisioning for this device, or Disable to turn it off.
Batch Configuration	
Batch File Upload	Click Browse to locate a csv format file for batch configuring ZyXEL's IP phones, and Upload to copy it to the X6004. Each entry in the batch file consists of the extension number followed by a comma "," and a SIP device's MAC address or serial number.
Current SIP Peer List	
Phone Numbers	This field displays the extension number configured on the X6004.
MAC Address	This field displays the MAC address of the ZyXEL device specified to receive configuration settings from the X6004. This field is blank for extensions assigned to software based IP phones.
Serial No.	This field displays the serial number of the software based IP phone specified to receive configuration settings from the X6004. This field is blank for extensions assigned to hardware based IP phones.
SPTGEN File Exist	This field displays Yes , if a configuration file (SPTGEN file) has been created. It displays No , if an SPTGEN file has not been created.
Phone Type	This field displays the type of phone connected to the X6004 using SIP.
Edit	Click the Edit icon to create a configuration file and associate it with a ZyXEL device on your network. The Auto Provision Settings screen opens.
View SPTGEN	Click the Advanced icon to view the settings in the configuration file.

7.2.1 Batch File Format

Each entry in the batch file consists of the extension number followed by a comma "," and either a SIP device's MAC address or a serial number.

The extension number must be 3~10 numbers (0~9).

A MAC address must be 12 hexadecimal digits.

A serial number can be up to 10 numbers (0~9) and letters (A~Z).

For example, if extension 2222 goes to a SIP device with MAC address 12:34:56:78:90:AB, specify "2222,1234567890AB" as the entry. If an extension goes to a softphone, specify a serial number, such as "123456ABCD" for example, instead of a MAC address. So if extension 3333 goes to a softphone, specify an entry like "3333, 123456ABCD".

7.2.2 Auto Provision Edit Settings

Use this screen to set up the auto provisioning settings for an extension on the X6004 and associate it with a ZyXEL device on your network. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision > Edit**.

Figure 69 Auto Provision > Edit

Auto Provision Profile Setting	
MAC Address	<input type="text" value="000111111111"/>
Serial No.	<input type="text"/>
Auto Provision Active	<input checked="" type="checkbox"/> On <input type="button" value="v"/>
Auto Provision Interval Time	<input type="text" value="43200"/> (seconds) <21600~604800>
Auto Provision Delay Time	<input type="text" value="Random"/> (seconds) <input type="button" value="v"/>
ATA device	<input type="checkbox"/>
Port No.	<input type="text" value="1"/> <input type="button" value="v"/>

Each field is described in the following table.

Table 34 Auto Provision > Edit

LABEL	DESCRIPTION
Auto Provision Profile Setting	These settings apply to the phone number (extension) you specified in the Auto Provision screen.
MAC Address	Specify the MAC address of the ZyXEL device that receives configuration settings from the X6004 for this extension. This field is left blank for extensions assigned to software based IP phones.
Serial No.	Specify the serial number of the software based IP phone that receives configuration settings from the X6004 for this extension. This field is left blank for extensions assigned to hardware based IP phones.
Auto Provision Active	Choose On , if you want to activate auto provisioning for this extension or choose Off if you want to deactivate auto provisioning for this extension.
Auto Provision Interval Time	Specify the amount of time in seconds to have SIP clients wait before the next time of provision file downloading from the X6004. Enter the time range between 21600 to 604800 seconds (between 6 to 168 hours). The default value is 43200 seconds (12 hours).
Auto Provision Delay Time	If many SIP clients download auto-provisioning files from the X6004 at the same time, the X6004 may be overloaded. The total interval between auto provisioning file downloads is the interval time plus the delay time. For example of SIP phone A has the interval time of 10 hours and delay time of 10 seconds, the next auto provisioning download will be 10 hours and 10 seconds later. Select 1~30 seconds or leave it as default, Random , which is to have a random delay time of between 1 to 30 seconds for each SIP client.

Table 34 Auto Provision > Edit (continued)

LABEL	DESCRIPTION
ATA device	Select this if the ZyXEL device to which you are sending this configuration file is an ATA device. An ATA (Analog Telephone Adapter) device typically has multiple analog telephones connected to it and can have unique configuration files for each port that it supports.
Port No.	Specify the ATA phone port number that you want to create this configuration file for.
Set Profile	Click Set Profile to create the configuration file and return to the Auto Provision screen.
Cancel	Click Cancel to go back to the Auto Provision screen without saving any changes.

7.2.3 Auto Provision View SPTGEN

Use this screen to view the configuration file (SPTGEN) file for a specific extension. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision** and click the **Advanced** icon next to the extension for which you want to view the SPTGEN file.

The SPTGEN file displays the configuration settings sent from the X6004 to a ZyXEL device configured for auto provisioning. Click **Cancel** to go back to the **Auto Provision** screen.

7.3 snom Profile Setup

If an auto provisioning file has been configured for a SIP extension, this screen displays the mapping between SIP extensions and snom VoIP device's MAC addresses or serial numbers. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision > snom Profile Setup**.

Figure 70 Auto Provision > snom Profile Setup

The screenshot shows the 'snom Profile Setup' configuration page. It is divided into three main sections:

- Service Configuration:** Contains a table with two columns: 'Machine ID' and 'Auto Provision'. The 'Machine ID' column has the value 'IPPBX_001'. The 'Auto Provision' column has two radio buttons: 'Disable' (selected) and 'Enable'. Below the table is an 'Apply' button.
- Batch Configuration:** Contains two rows. The first row is 'XML download' with a 'Download' button. The second row is 'Batch XML upload' with a 'File path' input field, a 'Browse...' button, and an 'Upload' button.
- Current SIP Peer List:** Contains a table with the following columns: 'Phone Number', 'MAC Address', 'Serial No.', 'SPTGEN File Exist', 'Phone type', 'Edit', and 'View SPTGEN'. Above the table are icons for ':Edit' and ':Advanced'. Below the table are two buttons: 'snom Feature Key Setting' and 'snom Firmware Upgrade'.

Each field is described in the following table.

Table 35 Auto Provision > snom Profile Setup

LABEL	DESCRIPTION
Service Configuration	
Machine ID	This indicates the X6004's identification number.
Auto Provision	Select Enable to turn on auto provisioning for this device, or Disable to turn it off.
Batch Configuration	
XML download	With the snom auto provision service enabled and at least one peer with the phone type set to snom auto provision, you can click Download to download a single XML file containing the configuration of all the SIP peers with the phone type set as snom.
Batch XML upload	After you've downloaded the XML batch configuration file, you can edit it and use Browse and Upload to copy it to the X6004.

Table 35 Auto Provision > snom Profile Setup (continued)

LABEL	DESCRIPTION
Current SIP Peer List	
Phone Numbers	This field displays the extension number configured on the X6004.
MAC Address	This field displays the MAC address of the ZyXEL device specified to receive configuration settings from the X6004. This field is blank for extensions assigned to software based IP phones.
Serial No.	This field displays the serial number of the software based IP phone specified to receive configuration settings from the X6004. This field is blank for extensions assigned to hardware based IP phones.
SPTGEN File Exist	This field displays Yes , if a configuration file (SPTGEN file) has been created. It displays No , if an SPTGEN file has not been created.
Phone Type	This field displays the type of phone connected to the X6004 using SIP.
Edit	Click the Edit icon to create a configuration file and associate it with a ZyXEL device on your network. The Auto Provision Settings screen opens.
View SPTGEN	Click the Advanced icon to view the settings in the configuration file.

7.3.1 What is snom?

A pioneer in the VoIP field, **snom technology AG** develops IP phones for use in corporate environments with an emphasis on quality, security and interoperability. As such, the ZyXEL X6004 is designed to work as seamlessly as possible with a variety of snom products.

For more information, visit <http://www.snom.com>. If you have a snom product and are unsure how it works with autoprovisioning, feature key settings, or firmware upgrades, consult the documentation that came with it.

7.3.2 snom Batch Configuration XML File

Here is an example of the snom batch configuration XML file.

```
<?xml version="1.0" encoding="utf-8"?>
<settings>
  <phone-settings e="2">
    <setting_server perm="RW">http://192.168.1.12:8080/provision/snom-lan-
{mac}.htm</setting_server>
    <update_policy perm="">auto_update</update_policy>
    <pnp_config perm="">on</pnp_config>
    <firmware_status perm="">http://192.168.1.12:8080/provision/
snom_300.xml</firmware_status>
    <user_active idx="1" perm="">on</user_active>
    <user_name idx="1" perm="">2222</user_name>
    <user_pname idx="1" perm="">2222</user_pname>
    <user_host idx="1" perm="">192.168.1.12</user_host>
    <user_hash idx="1" perm="">e5dd5800c7323de00c2f8f06173588c9</user_hash>
    <user_expiry idx="1" perm="">3600</user_expiry>
    <codec1_name idx="1" perm="">18</codec1_name>
    <codec2_name idx="1" perm="">0</codec2_name>
    <codec3_name idx="1" perm="">8</codec3_name>
    <codec4_name idx="1" perm="">2</codec4_name>
    <codec5_name idx="1" perm="">3</codec5_name>
    <codec6_name idx="1" perm="">18</codec6_name>
    <codec7_name idx="1" perm="">4</codec7_name>
    <user_dtmf_info idx="1" perm="">sip_info_only</user_dtmf_info>
    <user_dynamic_payload idx="1" perm="">off</user_dynamic_payload>
  </phone-settings>
</settings>
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

7.3.3 snom Profile Setup: Edit

Use this screen to set up the auto provisioning settings for a snom extension on the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision > snom Profile Setup** and then click the **Edit** button for a specific extension.

Figure 71 snom Profile Setup > Edit

Auto Provision Profile Setting	
MAC Address	<input type="text"/>
Auto Provision Active	Update automatically <input type="button" value="v"/>
Product	snom_300 <input type="button" value="v"/>

Each field is described in the following table.

Table 36 snom Profile Setup > Edit

LABEL	DESCRIPTION
Auto Provision Profile Setting	
MAC Address	Specify the MAC address of the ZyXEL device that receives configuration settings from the X6004 for this extension. This field is left blank for extensions assigned to software based IP phones.
Auto Provision Active	Choose On , if you want to activate auto provisioning for this extension or choose Off if you want to deactivate auto provisioning for this extension.
Product	Select the snom VOIP product to be targeted by this auto provision profile. This ensures greater compatibility between it and the X6004.
Set Profile	Click Set Profile to create the configuration file and return to the snom Profile Setup screen.
Cancel	Click Cancel to go back to the snom Profile Setup screen without saving any changes.

7.3.4 snom Profile Setup: View SPTGEN

Use this screen to view the configuration file (SPTGEN) file for a specific extension. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision > snom Profile Setup** and click the **Advanced** icon next to the extension for which you want to view the SPTGEN file.

The SPTGEN file displays the configuration settings sent from the X6004 to a snom device configured for auto provisioning. Click **Cancel** to go back to the **snom Profile Setup** screen.

7.3.5 snom Feature Key Setting

Use this screen to configure the feature key settings for the snom VoIP devices connected to the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision > snom Profile Setup** then click the **snom Feature Key Setting** button.

Figure 72 snom Profile Setting > snom Feature Key Setting

Key List	Active	Type
P1	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P2	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P3	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P4	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P5	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P6	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P7	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P8	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P9	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P10	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P11	On <input type="radio"/> Off <input checked="" type="radio"/>	None
P12	On <input type="radio"/> Off <input checked="" type="radio"/>	None

Each field is described in the following table.

Table 37 snom Feature Key Setting

LABEL	DESCRIPTION
snom Feature Key Setting	
Key List	This list corresponds to the special feature keys on snom VoIP phone.
Active	Select either On or Off to enable or disable a key code for the feature key in question.
Type	Select a feature key action from this list. This only applies to the feature key if you made it active. For more information on feature key codes and their associated actions, see Section 6.8 on page 141 .
Set Feature Key	Click Set Feature Key to create the configuration file and return to the snom Profile Setup screen.
Cancel	Click Cancel to go back to the snom Profile Setup screen without saving any changes.

7.3.6 snom Firmware Upgrade

Use this screen to configure the firmware upgrade URLs for the snom VoIP devices connected to the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision > snom Profile Setup** then click the **snom Firmware Upgrade** button.

Figure 73 snom Profile Setting > snom Firmware Upgrade

Product List	URL
Snom 300	<input type="text"/>
Snom 320	<input type="text"/>
Snom 360	<input type="text"/>
Snom 370	<input type="text"/>
Snom 820	<input type="text"/>
Snom 870	<input type="text"/>
Snom m3	<input type="text"/>

Each field is described in the following table.

Table 38 snom Firmware Upgrade

LABEL	DESCRIPTION
snom Firmware Upgrade	
Product List	This list corresponds to the snom products supported by the X6004.
URL	Enter the upgrade URL for the device in question. You can find this URL and any other upgrade information at the product page on the official snom website.
Set Firmware Url	Click Set Firmware URL to save the URL(s) entered on this page.
Cancel	Click Cancel to go back to the snom Profile Setup screen without saving any changes.

7.4 Auto Firmware Upgrade Screen

Use this screen to configure the information that IP phones connected to the X6004 will use to upgrade their own firmware from an FTP server. To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision > Auto Firmware Upgrade**.

Figure 74 Auto Provision > Auto Firmware Upgrade

Auto Firmware Upgrade Setting	
Firmware Version	<input type="text"/>
FTP Server Address	<input type="text"/>
FTP Server Username	<input type="text"/>
FTP Server Password	<input type="text"/>
Firmware Upgrade Confirm	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Firmware Upgrade Start Time	<input type="text"/>
Firmware Upgrade End Time	<input type="text"/>

Each field is described in the following table.

Table 39 Auto Provision > Auto Firmware Upgrade

LABEL	DESCRIPTION
Firmware Version	Enter the filename of the firmware to be uploaded to the connected IP phones.
FTP Server Address	Enter the FTP address that hosts the firmware. Note: You must enter the full FTP path here or the upgrade will fail.
FTP Server Username	Enter the login username for the FTP server. Note: This will be used by every phone connected to the X6004 so be sure it does not have any restrictions or security issues, such as one used by an administrator.
FTP Server Password	Enter the login password for the FTP server. Note: This will be used by every phone connected to the X6004 so be sure it does not have any restrictions or security issues, such as one used by an administrator.

Table 39 Auto Provision > Auto Firmware Upgrade (continued)

LABEL	DESCRIPTION
Firmware Upgrade Confirm	<p>Select Enable to prompt IP phone users in their IP phone LCDs to confirm a firmware upgrade or not. IP phone users are prompted as soon as their phones log into the network when a firmware upgrade is available.</p> <p>Select Disable to turn this function off, allowing all IP phones connected to the X6004 to upgrade themselves without user intervention.</p> <p>Note: This feature is disabled by default.</p>
Firmware Upgrade Start Time	<p>Enter the hour and minutes that the firmware upgrade is to begin. If you use this option, you must also set a corresponding Firmware Upgrade End Time to complete the time range.</p> <p>During this time range, each phone on the network randomly sets a time between the start time and the end time in which to connect to the FTP server and upgrade itself.</p> <p>Note: This option only works when the Firmware Upgrade Confirm setting has been disabled.</p>
Firmware Upgrade End Time	<p>Enter the hour and minutes that the firmware upgrade is to end. If you use this option, you must also set a corresponding Firmware Upgrade Start Time to complete the time range.</p> <p>During this time range, each phone on the network randomly sets a time between the start time and the end time in which to connect to the FTP server and upgrade itself.</p> <p>Note: This option only works when the Firmware Upgrade Confirm setting has been disabled.</p>
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

7.5 EZ Provision

EZ provisioning is an Interactive Voice Response (IVR) system which allows the administrator to deploy new phones without accessing the Web Configurator.

To access this screen, click **Configuration > PBX > Server Configuration > Auto Provision > EZ Provision**.

Figure 75 Auto Provision > EZ Provision

Each field is described in the following table.

Table 40 Auto Provision > EZ Provision

LABEL	DESCRIPTION
New PIN Code	Enter up to 8 digits to be used as your administrator IVR PIN code.
Confirm PIN Code	Re-enter the PIN code from the previous field to confirm it.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

8.1 Overview

This chapter shows you how to configure the X6004's Quality of Service (QoS) settings in the **Configuration > PBX > Server Configuration > QoS** screen.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as VoIP.

The following problems can occur on a congested network with poor QoS settings:

- **Latency** - delay of packet delivery. This can cause echoes during a conversation.
- **Jitter** - variations in delay of packet delivery. This could cause strange sound effects. The X6004 utilizes a jitter buffer to minimize the effects of jitter.
- **Packet Loss** - packets are dropped due to an overwhelming amount of traffic on the network. Some degree of packet loss will not be noticeable to the end user, but as packet loss increases the quality of sound degrades.

The X6004 can be configured to change the priority field of IP packets for all outgoing RTP (Real Time Protocol) packets. The X6004 supports Type of Service (ToS) and Differentiated Services (Diffserv) for implementing QoS. Configure the X6004 with the QoS settings that your network uses for VoIP.

8.1.1 What You Can Do in this Chapter

Use the **QoS** screen to configure the type of QoS you want to use, and to specify the level of service you want to use for the X6004's traffic on your network. See [Section 8.2 on page 171](#).

8.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

ToS

The X6004 supports the following classes of service for outgoing VoIP packets.

- **Minimize Delay** - Use this when the time it takes for a packet to travel from the source host to destination host (latency) is most important.
- **Maximize Throughput** - Use this when the volume of data transmitted in any period of time is important.
- **Maximize Reliability** - Use this when it is important that you have some certainty that the data will arrive at the destination without retransmission being required.
- **Minimize Cost** - Use this when it is important to minimize the cost of data transmission. Network providers may offer two types of service (for example fiber and copper) and charge differently depending on which you use. In this case, choosing "minimize cost" may inform the network provider to use the lower-cost route to send your VoIP traffic.

Note: It is recommended to use the **Minimize Delay** class for VoIP traffic.

DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets (based on the application types and traffic flow) so that they receive specific per-hop treatment at DiffServ-compliant network devices along their route. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different forwarding treatment. Resources can then be allocated according to the DSCP values and the configured policies.

The X6004 allows you to mark outgoing frames with following PHB classifications:

Assured Forwarding (AF) - This is a PHB group allowing you to choose from one of four classes of forwarding assurance. Each class has three choices of drop precedence to choose from. When congestion occurs, the DS nodes on your network treat all IP packets marked with the same class and drop precedence identically. DS nodes can be configured to protect packets with lower drop precedence value by discarding packets with a higher drop precedence value.

Expedited Forwarding (EF) - The EF PHB defines a single DSCP designed for simulating a private end-to-end pipeline across a DiffServ network. IP packets are marked for high priority low-loss, low-latency, low-jitter, assured-bandwidth end to end service through DS domains. This is recommended for use with VoIP traffic as it addresses the factors that cause degradation in sound quality.

Class Selector (CS) - IP packets are marked with values partially backwards-compatible with known current uses of IP precedence field. The packets marked with higher values are given higher priority than those with lower values.


8.1.3 Before You Begin

Before you start configuring QoS on your X6004, you should know the type of QoS your network uses, and the relevant setting that you want to assign to the X6004's traffic.

8.2 The QoS Screen

Use this screen to set up the QoS settings on the X6004. To access this screen, click **Configuration > PBX > Server Configuration > QoS**.

Figure 76 Server Configuration > QoS



The screenshot shows a configuration screen for QoS. On the left, the label 'QoS' is displayed. To its right, there are two dropdown menus. The first dropdown menu is set to 'TOS'. The second dropdown menu is set to 'minimize delay'.

Each field is described in the following table.

Table 41 Server Configuration > QoS

LABEL	DESCRIPTION
QoS	<p>Select the QoS method you want to use to mark outgoing frames on the X6004.</p> <p>You can choose:</p> <ul style="list-style-type: none"> • TOS and then select one of the four classes of service supported on the X6004: minimize delay, maximize throughput, maximize reliability or minimize cost. • DS (DiffServ) and then select the DSCP value to mark the outgoing packets. You can choose: one of the AF (Assured Forwarding), EF (Expedited Forwarding) or one of the CS (Class Selector) values. • User Define and then enter a value to assign to the ToS field in decimal notation. You can set the value to a value from 0 to 255. The X6004 displays the value you enter in hexadecimal notation. • None, if you do not want to mark the ToS field of the outgoing VoIP packets.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

Voice Mail

9.1 Overview

This chapter shows you how to set up voice mail for the X6004's calls, using the **Configuration > PBX > Server Configuration > Voice Mail** screen.

Voice mail messages on the X6004 are stored on the built-in flash memory of the X6004. To ensure that one user does not utilize a disproportionate amount of voice mail capacity, you can limit the voice mail resources on a per user basis.

9.1.1 What You Can Do in this Chapter

Use the **Voice Mail** screen to set maximum call lengths for one or all calls. See [Section 9.2 on page 174](#).

9.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Voicemail Forwarding Method

You can manage your voice mail messages by forwarding them to email accounts associated with each telephone extension on the X6004. See [Chapter 13 on page 197](#) for information on how to configure email forwarding of voice mail messages.

Access Personal Voice Mail

Users can access their personal voice mail system by dialing the feature code for voice mail (by default, **) followed by their extension number. In the voice mail system, users can manage their personal voice messages, record their temporary greeting or messages which are played when they are unavailable or busy. See [Section 9.3 on page 175](#).

9.2 The Voice Mail Screen

Use this screen to set up the voice mail settings on the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Voice Mail**.

Figure 77 Server Configuration > Voice Mail

Voice Mail Setting	
Max Length per Call:	<input type="text" value="90"/> seconds
Max Usage per User:	<input type="text" value="300"/> seconds
E-mail Content	
E-mail Subject:	(Enter up to 150 characters including spaces) <input type="text" value="[PBX]: New message MSGNUM in mailbox MAILBOX"/>
E-mail Body:	(Enter up to 350 characters including spaces) <div style="border: 1px solid black; padding: 5px;"> <p>Dear Sir/Madam:</p> <p>just wanted to let you know you were just left a DUR long message (number MSGNUM) in mailbox MAILBOX from CALLERID, on DATE, so you might want to check it when you get a chance. Thanks!</p> <p>--PBX</p> </div>
Remaining characters: <input type="text" value="139"/>	
Allowed variables:	
DUR : The duration of the voice mail	
MSGNUM : The queue number of the new received voice mail in the mailbox	
MAILBOX : The extension number of the mailbox owner	
CALLERID : The extension number of the caller	

Each field is described in the following table.

Table 42 Server Configuration > Voice Mail

LABEL	DESCRIPTION
Voice Mail Management	
Max Length per Call	Specify the maximum number of seconds for each voice mail message. This value can be from 1 to 90 seconds.
Max Usage per User	Specify the maximum number of seconds for all voice mail messages for each extension. When a user hits this limit then the X6004 will no longer save voice mail messages. This value can be from 1 to 300 seconds. A hard disk installed can increase this value to up to 5000 seconds.
E-mail Content	
E-mail Subject	Enter up to 150 alphanumeric characters (a-z, A-Z, 1-0, all punctuation included) as the subject line for e-mails sent out by the X6004 to notify users of pending voice mails.

Table 42 Server Configuration > Voice Mail (continued)

LABEL	DESCRIPTION
E-mail Body	<p>Enter up to 350 alphanumeric characters (a-z, A-Z, 1-0, all punctuation included) as the body text for e-mails sent out by the X6004 to notify users of pending voice mails.</p> <p>You can also use the following X6004-specific variables to include custom information about the voice mail:</p> <ul style="list-style-type: none"> • DUR: This is the duration of the voice mail in hh:mm:ss format (hours, minutes, and seconds). • MSGNUM: This is the queue number of the voice mail in the mailbox. The more voice mails you have received, the higher this number. • MAILBOX: This is the telephone extension number of the mailbox owner. • CALLERID: This is the telephone extension of the person who left the voice mail. • DATE: This is the timestamp of when the voice mail was received.
Permissible Input	This field indicates the remaining number of characters available to you as you type your e-mail body text.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to set every field in this screen to its last-saved value.

9.3 Accessing Voice Mail

Users can access their personal voice mail system by dialing the feature code for voice mail followed by their extension number. The feature code for voice mail is configured in the **Configuration > PBX > Server Configuration > Server > Feature Code** screen (see [Section 6.8 on page 141](#)). For example, if the feature code for voice mail is a double asterisks (**), then a caller (with extension **1001**) must dial ****1001** to access his personal voice mail system from any extension of the X6004.

Personal voice mail can be accessed as an internal call or users can call from an outside line and dial the feature code for voice mail followed by their extension when an auto-attendant prompts them to dial the extension they wish to reach.

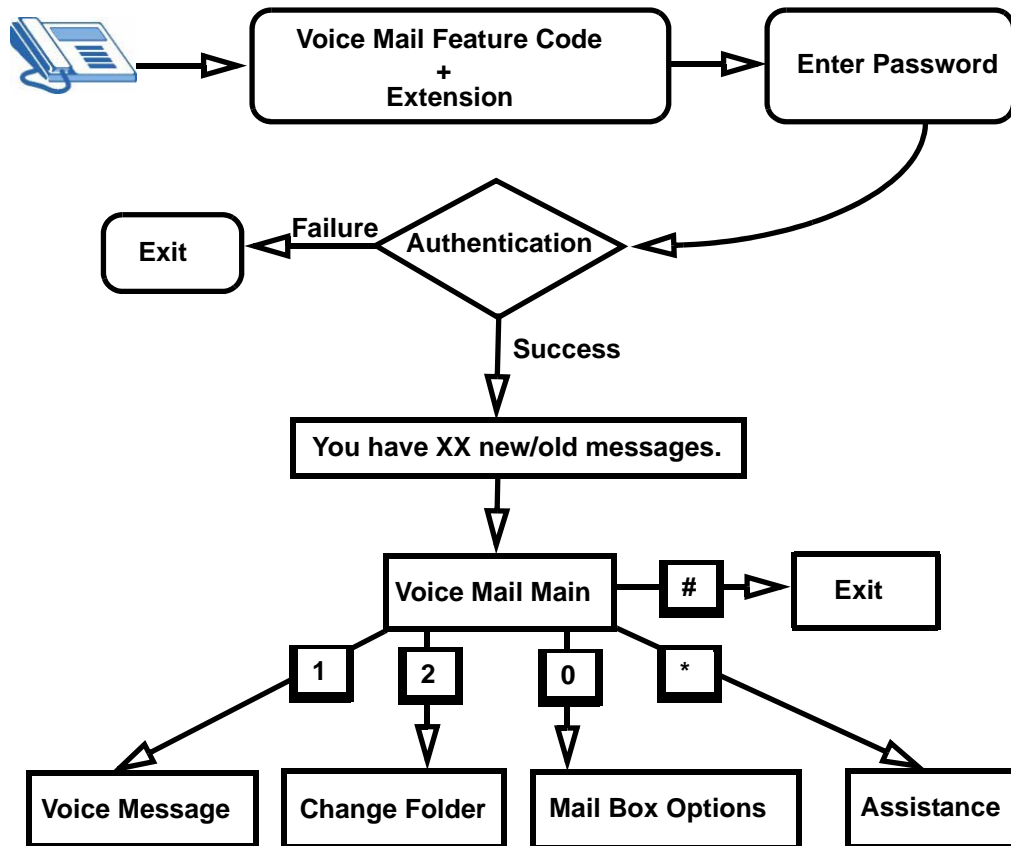
Users must authenticate before entering their voice mail system. When users dial into their personal voice mail they are prompted to enter their PIN. The voice mail PIN is assigned to each extension when the extension is created. See [Section 13.3.3 on page 208](#) for information on how to configure the voice mail PIN for SIP extensions, [Section 13.3.12 on page 221](#) for analog phone extensions and [Section 13.3.17 on page 225](#) for ISDN extensions. If a user authenticates successfully, the system prompts the number of new or old voice messages available for him or her in the system. Then he or she is guided through the personal voice mail menus via pre-recorded audio prompts. If a user fails to authenticate, the X6004 plays a

message indicating that an incorrect password was entered and the call is dropped after three trials.

Personal Voice Mail Main Flow

The following figure describes the main flow in the personal voice mail system.

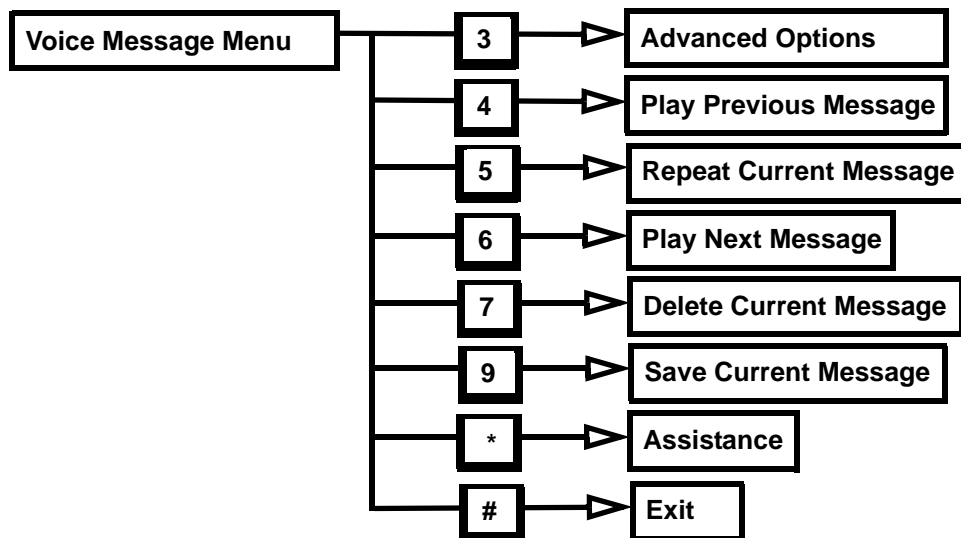
Figure 78 Personal Voice Mail Flow



Voice Message Menu

The following figure describes the **Voice Message Menu**. From **Voice Mail Main**, press number **1** on your phone keypad to enter this menu. The X6004 will play you a new message. Then you can choose either one of the following options for the next action.

Figure 79 Personal Voice Mail: Voice Message Menu

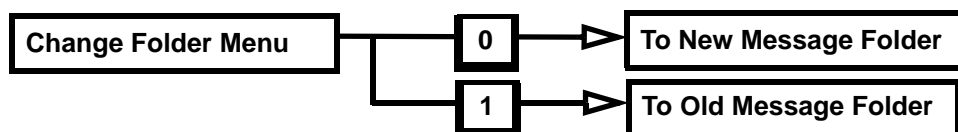


If you press number **9** to save the current message, you can choose which folder to save it. The options are the same as the options in the **Change Folder Menu**. See [Figure 80](#).

Change Folder Menu

The following figure describes the **Change Folder Menu**. From **Voice Mail Main**, press number **2** on your phone keypad to enter this menu. This menu allows you to switch the current folder to another folder in the voice mail system. Then system will play you the number of old messages stored in the folder to which you have switched. In this way, you can find an old message easily and replay it.

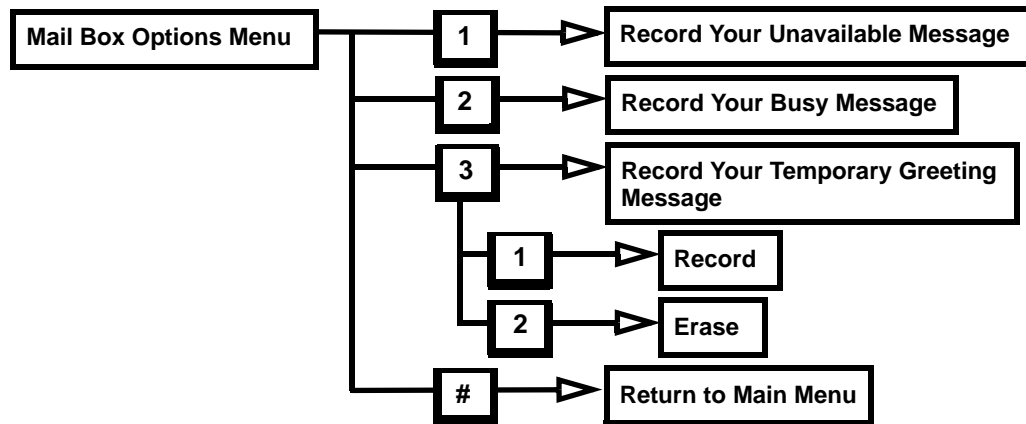
Figure 80 Personal Voice Mail: Change Folder Menu



Mail Box Options Menu

The following figure describes the **Mail Box Options Menu**. From **Voice Mail Main**, press number **0** on your phone keypad to enter this menu. This menu allows you to record your messages which are played for the initial greeting or when you (your extension) is unavailable, busy.

Figure 81 Personal Voice Mail: Mail Box Options Menu



After recording a message for unavailable, busy and/or temporary greeting, press the following number on your phone keypad to:

- 1 - accept what you recorded and save
- 2 - play what you recorded
- 3 - re-record the message

Voice Messages Storage

A voice message is stored as a .wav file and the size is about 8 KB per second. A storage of 64 MB can store messages recorded for about two hours in total. When you enable ZyStack, voice messages are stored on each X6004, not on the master X6004 centrally.

Phonebook

10.1 Overview

This chapter shows you how to set up a phonebook for the X6004.

There are two ways to set up a phone book on the X6004.

- You can create an LDAP (Lightweight Directory Access Protocol) phonebook, which imports entries from an LDAP directory on your network.
- You can also create local phonebook entries via the web configurator of the X6004. The entries in the phonebook are available to users on your network via the personal web portal of the X6004 (see [Chapter 37 on page 483](#) for more information on the web portal).

You can configure either type of phonebook, or both. If you configure both phonebooks, then the entries from both phonebooks (duplicate entries included) are displayed to the end users.

10.1.1 What You Can Do in this Chapter

- Use the **Phonebook Configuration** screen to set up a connection to an LDAP server on the X6004 and to either import or export your local phonebook.
- Use the **LDAP Phonebook** screen to map the values associated with the account entries on the LDAP server to the phonebook values stored on the X6004.
- Use the **Local Phonebook** screen to set up the X6004's local phonebook settings.

10.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

LDAP Directories

LDAP directories are commonly used to store user based information within an organization. For example, email clients such as Outlook use LDAP to query address book entries from an LDAP directory. The X6004 is capable of sending

LDAP queries to an LDAP server to create and keep up-to-date the phone book entries on the X6004.

The Local Phonebook

The local phonebook on the X6004 can be created by adding phonebook entries via the web configurator. You can also export the local phonebook into a text file. The text file can be edited and imported back to the X6004 via the web configurator.

10.1.3 Before You Begin

If you intend to configure the X6004 to use an LDAP phonebook, you need the following information about the LDAP server on your network to issue an LDAP query from the X6004:

- LDAP Server IP address - this is the IP address of the LDAP server you want to query.
- Port number - this is the port number that the LDAP user to receive LDAP queries.
- RootDN - this is the username used to authenticate with the LDAP server. This information is configured on the LDAP server. Refer to your LDAP server documentation.
- Password - this is the password used to authenticate with the LDAP server.
- BaseDN - this string identifies the location on the LDAP server where the phone book information is stored. LDAP directories are divided into subdirectories and you need to enter the right subdirectory in order to search for the information for your phonebook.
- LDAP database field - these are names of the fields on the LDAP database that you want to obtain information from. Each record on the LDAP database contains many fields and you need to provide the correct field names in order to obtain the data.

10.2 The Phonebook Configuration Screen

Use this screen to set up a connection to an LDAP server on the X6004, select which phonebooks are transferred to the ZyXEL or snom VoIP phones, and to either import or export your local phonebook.

To access this screen, click **Configuration > PBX > Server Configuration > Phonebook > Configuration**.

Figure 82 Phonebook > Configuration

The screenshot shows the 'Phonebook > Configuration' screen. It is divided into three main sections:

- LDAP Phonebook Setting:** Contains fields for 'LDAP Enable' (checkbox), 'LDAP Server', 'LDAP Port', 'RootDN', 'Password', and 'BaseDN'.
- Phonebooks selection for phone:** Contains 'Phonebooks selection:' with three checked checkboxes: 'LDAP', 'Local', and 'Extensions in system'. Below this is an 'Apply' button.
- Local Phonebook Export/Import:** Contains 'Export phonebook file:' with an 'Export' button, and 'Import phonebook file:' with a text input field, a 'Browse...' button, and an 'Import' button.

Each field is described in the following table.

Table 43 Phonebook > Configuration

LABEL	DESCRIPTION
LDAP Phonebook Setting	Use this section to configure your connection settings to the LDAP database containing the phonebook entries you want to import to the X6004.
LDAP Enable	Check this box to enable LDAP based phonebook on the X6004.
LDAP Server	Specify the IP address of the server containing the LDAP database.
LDAP Port	Specify the port the LDAP server uses for sending the phonebook to the X6004.
RootDN	Specify the login name of the LDAP server.
Password	Specify the password for the LDAP server.
BaseDN	Enter the string identifying the location on the LDAP server where the information you need for your phonebook is stored.

Table 43 Phonebook > Configuration (continued)

LABEL	DESCRIPTION
Apply	Click this to import the phonebook information from the LDAP server.
Phonebooks selection for phone	Use this section to select which phonebooks to transfer to the ZyXEL or snom VoIP phones.
Phonebooks selection	Select LDAP to transfer the LDAP server's account entries to the ZyXEL or snom VoIP phones. Select Local to transfer the X6004's phonebook to the ZyXEL or snom VoIP phones. Select Extensions in system to transfer the X6004's extensions to the ZyXEL or snom VoIP phones.
Local Phonebook Export/Import	Use this section to download the local phonebook from the X6004 to your local computer or another location on your network or to upload a text file containing your phonebook entries to the X6004.
Export phonebook file	Click Export to save your local phonebook to your local computer or another location on your network. A screen appears prompting you for a location to download your phonebook file.
Import phonebook file	Type the path to or click Browse and locate the text file containing a local phonebook. Then click Import to upload the phonebook file to the X6004. The X6004 displays the Import Phonebook screen, which allows you to review the local phonebook entries before saving them to the X6004.

10.2.1 The Import Phonebook Screen

The following screen appears after you click **Import** in the **Phonebook Config** screen.

Figure 83 Phonebook > Import Phonebook

Import Phonebook							
Name	Ext.	Home	Mobile	E-Mail	Logon Name	Country	Department
Test	4444	5555555	0955555555	test@test.com	test	USA	sales
Tomasz H	5000	12-2233344	098887878787	thasinski@yahoo.com	Tomasz H	United	R

.....

Review the phonebook entries and click **Apply** to save this phonebook to the X6004. This overrides any previously stored local phonebook entries. Click **Cancel** if you don't want to save this phonebook to the X6004. See [Section 10.4 on page 184](#) for information on the individual fields in the local phonebook entries.

10.3 The LDAP Phonebook Screen

Use this screen to map the values associated with the account entries on the LDAP server to the phonebook values stored on the X6004. You can also view the LDAP phonebook entries and configure how often the X6004 updates the LDAP phonebook from the LDAP server. To access this screen, click **Configuration > PBX > Server Configuration > Phonebook > LDAP Phonebook**.

Figure 84 Phonebook > LDAP Phonebook

The screenshot shows the 'LDAP Phonebook' configuration interface. It features two main sections:

- LDAP Search Filter:** A grid of input fields for mapping LDAP fields to phonebook fields.

Name	<input type="text" value="displayName"/>	Ext.	<input type="text" value="telephoneNumber"/>
E-Mail	<input type="text" value="mail"/>	Country	<input type="text" value="c"/>
Logon Name	<input type="text" value="userPrincipalName"/>	Home	<input type="text" value="homePhone"/>
Mobile	<input type="text" value="mobile"/>	Department	<input type="text" value="department"/>

 There are 'Modify' and 'Default' buttons to the right of the Home and Department fields.
- LDAP Phonebook:**
 - Latest Update: 2006/09/29 13:25:53
 - A table with columns: Name, Ext., Home, Mobile, E-Mail, Logon Name, Country, Department.
 - Regular update at : everyday

Each field is described in the following table.

Table 44 Phonebook > LDAP Phonebook

LABEL	DESCRIPTION
Name	Specify the field name in the LDAP database that you want to map the Name field of the LDAP phonebook to.
E-mail	Specify the field name in the LDAP database that you want to map the E-mail field of the LDAP phonebook to.
Logon Name	Specify the field name in the LDAP database that you want to map the Logon Name field of the LDAP phonebook to.
Mobile	Specify the field name in the LDAP database that you want to map the Mobile field of the LDAP phonebook to.
Ext.	Specify the field name in the LDAP database that you want to map the Ext. field of the LDAP phonebook to.
Country	Specify the field name in the LDAP database that you want to map the Country field of the LDAP phonebook to.
Home	Specify the field name in the LDAP database that you want to map the Home field of the LDAP phonebook to.
Department	Specify the field name in the LDAP database that you want to map the Department field of the LDAP phonebook to.
Modify	Click Modify to save any changes you made to the mappings of the fields on the LDAP phonebook to the LDAP database.

Table 44 Phonebook > LDAP Phonebook (continued)

LABEL	DESCRIPTION
Default	Click Default to set every field in this screen to the factory defaults configured on the X6004. Note: This not only sets the fields to default values but also automatically saves the default mappings to the X6004.
Name.. Department	This table displays the phonebook entries retrieved from the LDAP database.
Regular update at	Select this and specify the time in hour and minute format at which the X6004 should update the LDAP phonebook with the LDAP database. Click Set to save this setting.
Refresh	Click Refresh to immediately update the LDAP phonebook with the LDAP database.

10.4 The Local Phonebook Screen

Use this screen to set up the local phonebook settings on the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Phonebook**.

Figure 85 Phonebook > Local Phonebook

Local Phonebook								
<input type="checkbox"/>	Name	Ext.	Home	Mobile	E-Mail	Logon Name	Country	Department
<input type="checkbox"/>	LocalUser1	9999				Peter		

Each field is described in the following table.

Table 45 Phonebook > Local Phonebook

LABEL	DESCRIPTION
Local Phonebook	This screen allows you to view, edit and remove local phonebook entries on the X6004.
Delete	Select the Delete checkbox and click Delete to remove a local phonebook entry from the X6004.
Name	This field displays the Name field value of the local phonebook entry.
Ext.	This field displays the Ext. field value of the local phonebook entry.
Home	This field displays the Home field value of the local phonebook entry.
Mobile	This field displays the Mobile field value of the local phonebook entry.
E-mail	This field displays the E-mail field value of the local phonebook entry.
Logon Name	This field displays the Logon Name field value of the local phonebook entry.

Table 45 Phonebook > Local Phonebook (continued)

LABEL	DESCRIPTION
Country	This field displays the Country field value of the local phonebook entry.
Department	This field displays the Department field value of the local phonebook entry.
Add / Edit / Delete	<p>Click the Add icon to configure a new entry in the local phonebook.</p> <p>Click the Edit icon to change the values of an existing local phonebook entry.</p> <p>Click the Delete icon to remove an entry from the local phonebook.</p>

10.4.1 Local Phonebook Add/Edit Screen

The screens for editing or adding entries to the local phonebook contain the same fields. Only the screen used to add local phonebook entries is shown below. Use this screen to configure phonebook entries on the X6004. Click the **Add** (or **Edit**) icon in the **Local Phonebook** screen to view the screen as shown.

Note: Only the **Add Local Phonebook** screen is shown. In the **Edit Local Phonebook** screen, some of the fields are read-only.

Figure 86 Local Phonebook Add/Edit Screen

The screenshot shows a web-based form titled "New PBX Phonebook". The form contains the following fields, each with a corresponding text input box:

- Name
- Ext.
- Home
- Mobile
- E-Mail
- Logon Name
- Country
- Department

At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Each field is described in the following table.

Table 46 Local Phonebook Add/Edit Screen

LABEL	DESCRIPTION
New/Edit PBX Phonebook	Use these fields to add (or edit) local phonebook entries. Note: You must fill in the name field in order to save this local phonebook entry. All the other fields can be left blank.
Name	Type a Name value for this local phonebook entry. This field is limited to 20 alphanumeric (a-z, A-Z, 0-9) characters. Spaces and dashes are also allowed. You cannot change this value if you are editing an existing local phonebook entry.
Ext.	Type an Ext. value for this local phonebook entry. This field is limited to 20 numeric characters (0-9).
Home	Type a Home value for this local phonebook entry. This field is limited to 20 numeric characters (0-9).
Mobile	Type a Mobile value for this local phonebook entry. This field is limited to 20 numeric characters (0-9).
E-mail	Type a E-mail value for this local phonebook entry. This field is limited to 127 printable ASCII characters, spaces, "=" and "+" are not allowed.
Logon Name	Type a Logon Name value for this local phonebook entry. This field is limited to 127 printable ASCII characters, spaces are allowed but "=" is not.
Country	Type a country value for this local phonebook entry. This field is limited to 127 printable ASCII characters, spaces are allowed but "=" is not.
Department	Type a Department value for this local phonebook entry. This field is limited to 127 printable ASCII characters, spaces are allowed but "=" is not.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to return to the Local Phonebook screen without saving your changes.

DSP Management

11.1 Overview

This chapter shows you how to install additional Digital Signal Processing (DSP) modules in the X6004 and how to manage the X6004's DSP resources.

The X6004 uses DSP modules to convert analog audio to digital signals, and vice versa.

The X6004 is equipped with an onboard DSP module and two extensible DSP slots by default. You can upgrade the existing DSP module with one or two that can process more channels. You can also install a second module to increase the number of calls the X6004 can handle simultaneously. See the product specification in [Chapter 40 on page 521](#) for details about the X6004's DSP modules.

This chapter shows you how to install and uninstall additional DSP modules in the X6004. It also discusses how to manage the DSP resources on the X6004.

11.1.1 What You Can Do in this Chapter

Use the **DSP Management** screen to manage the DSP channels available on the X6004. See [Section 11.3 on page 190](#).

11.1.2 What You Need To Know

The following terms and concepts may help you as you read through the chapter.

DSP Channels

DSP modules are classified by the number of channels they are capable of processing. A normal phone conversation takes up to two channels, since the X6004 must encode the outgoing analog audio while simultaneously decoding the incoming digital audio.

DSP Management

The X6004 automatically detects the number of DSP channels available for processing telephone conversations. The number of available DSP channels is based on the DSP modules installed on the X6004.

The X6004 automatically assigns DSP channels to service the analog phone connections (FXS ports) available on the X6004. It also automatically assigns DSP channels to the analog connections to the PSTN (FXO ports).

The remaining DSP channels are shared among all services which require DSP resources on the X6004.

11.1.3 Before You Begin

Consider the following when making decisions on purchasing additional DSP modules or assigning the DSP channels on the X6004:

- A typical conversation uses two channels.
- A conference call uses one channel per participant.
- Unassigned DSP channels are shared among all services which require DSP resources.

11.2 Installing and Removing DSP Modules

This section describes how to install and remove the X6004's DSP modules.

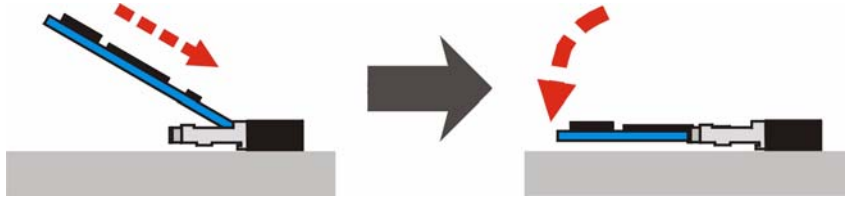
11.2.1 How to Install a DSP Module

Take the following steps to install a second Digital Signal Processor in your X6004.

- 1 Ensure the power is off and all cables are disconnected. Lay the X6004 upside down on a flat, dry surface. The DSP hatch is located on the base of the X6004.
- 2 Unscrew and remove the DSP hatch screw.
- 3 Remove the DSP hatch cover.
- 4 Insert the DSP module's contacts into the connector socket at an angle, as shown in the figure.

- 5 Gently press the DSP module downwards, until the two retaining arms click into place. Replace the hatch cover and the screw.

Figure 87 Installing a DSP module



11.2.2 How to Remove a DSP Module

Take the following steps to remove a DSP module from the X6004.

- 1 Ensure the power is off and all cables are disconnected. Lay the X6004 upside down on a flat, dry surface. The DSP hatch is located on the base of the X6004.
- 2 Unscrew and remove the DSP hatch retaining screw.
- 3 Remove the DSP hatch cover.
- 4 Gently press the retaining arms away from the module, as shown in the figure. When both retaining arms are disengaged from the module, the module springs up to its angled position.

DO NOT pull the DSP module up without first disengaging the retaining arms. This could damage the module or the connector on the X6004.

- 5 Remove the DSP module. Replace the hatch cover and the screw.

Figure 88 Removing a DSP Module



11.3 The DSP Management Screen

Use this screen to manage the DSP channels available on the X6004. To access this screen, click **Configuration > PBX > Server Configuration > DSP Management**.

Note: Your changes of DSP resource reservation will be applied after all ongoing calls are finished.

Figure 89 Server Configuration > DSP Management

Attributes	IPPBX_001	IPPBX_002	IPPBX_003	IPPBX_004	IPPBX_005
Total available	21	0	0	0	0
FXO	2	0	0	0	0
FXS	6	0	0	0	0
Conference	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
PRI	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
BRI	<input type="text" value="2"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Share	7	0	0	0	0

Each field is described in the following table.

Table 47 Server Configuration > DSP Management

LABEL	DESCRIPTION
Attributes	This column displays which features use the DSP channels on the X6004. If you have a ZyStack configured, each column identifies a single X6004 in the ZyStack.
Total available	The X6004 automatically detects the total available DSP channels available on the X6004 and displays them in this field. This value is based on the DSP modules you have installed on the X6004.
FXO	This field displays the total DSP channels assigned to the FXO ports on the X6004. The X6004 automatically assigns one DSP channel per FXO port on the X6004.
FXS	This field displays the total DSP channels assigned to the FXS ports on the X6004. The X6004 automatically assigns one DSP channel per FXS port on the X6004.
Conference	Specify the DSP channels you want to assign specifically for conference calls on the X6004.
PRI	Specify the DSP channels you want to assign specifically for the PRI port on the X6004.
BRI	Specify the DSP channels you want to assign specifically for the BRI ports on the X6004.

Table 47 Server Configuration > DSP Management (continued)

LABEL	DESCRIPTION
Share	This field displays the unassigned DSP channels on the X6004. Unassigned DSP channels are shared among all services which require DSP services on the X6004.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to set every field in this screen to its last-saved value.

Office Hours

12.1 Overview

This chapter shows you how to set the office hours for the X6004. You can use office hours to have the X6004 deal with incoming calls differently at different times of day and night.

12.1.1 What You Can Do in this Chapter

Use the **Office Hour** screen to configure the days of the week and times you are in the office. See [Section 12.2 on page 194](#).

12.1.2 What You Need To Know

The office hours you specify on the X6004 are used by the auto-attendant feature to determine how the X6004 handles incoming calls. For example, when calls come into your organization during office hours you may want to allow them to enter any extension they wish to call. However, when calls come into your organization after office hours you may want to direct them all to a single extension (a night clerk, for example).

12.1.3 Before You Begin

Before you configure office hours, you should know how to configure the auto-attendant. See [Chapter 19 on page 291](#) for more information.

Individuals can also specify their own office hours to deal with calls differently during various parts of the work week. See [Section 13.3.4 on page 209](#) for more information.

12.2 Office Hour Screen

Use this screen to specify office hours for the X6004. To access this screen, click **Configuration > PBX > Server Configuration > Office Hour**.

Note: The office hour configuration here is used as the default for all new extensions. To customize office hours on a per-extension or per-authority group basis, you must go to those specific screens. For more, see [Chapter 13 on page 197](#).

Figure 90 Server Configuration > Office Hour Setting

Office Hour Setting

Office Hours

Days of Week Sun Mon Tue Wed Thu Fri Sat

Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat
		08:00-12:00	08:00-12:00	08:00-12:00	08:00-12:00	08:00-12:00	
		13:00-17:30	13:00-17:30	13:00-17:30	13:00-17:30	13:00-17:30	

Holiday

Date	Description	
02/14	Lunar New Year	
01/01	New Years Day	
02/14	Lunar New Year	
07/04	July 4th	
10/10	Double 10 Day	
12/24	Christmas Eve	
12/25	Christmas Day	

Overwrite

Auto-Attendant
 Auto-Attendant + Authority Group
 Auto-Attendant + Authority Group + Extension

Apply Default

Each field is described in the following table.

Table 48 Server Configuration > Office Hour Setting

LABEL	DESCRIPTION
Office Hour Setting	Use this section to specify office hours on the X6004.
Days of Week	Select the days of the week which you want the X6004 to treat as working days.

Table 48 Server Configuration > Office Hour Setting (continued)

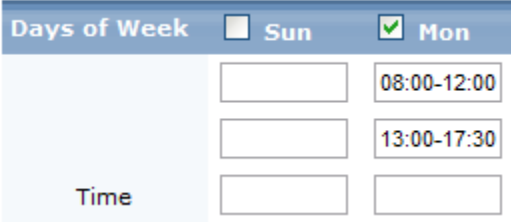

LABEL	DESCRIPTION
Time	<p>Specify the time range during the working days that you want the X6004 to treat as working hours.</p> <p>When entering a time range, the following conditions apply:</p> <ul style="list-style-type: none"> You can enter up to six time ranges, with each range consisting of a start time and an end time. The time entered in each field must be in 24 hr format (such as "08:00" for 8 AM or "24:00" for midnight). The start and end times must be separated by a hyphen. <p>For example, a standard work day may look like this:</p>  <p>In this example, the first time block is from 8 AM until 12 noon. The second time block is from 1 PM until 5:30 PM.</p>
Holiday	<p>This section allows you to set a specific day of the year as a holiday, which the X6004 will then treat as "after office hours".</p>
Date	<p>Enter a date in mm/dd format (double digit month / day; for example, 02/09 for February 9th.)</p> <p>You can also click the "... " icon to open the interactive calendar:</p>  <p>Click a day to select it.</p> <p>Use the < and > buttons to cycle through the years and months.</p> <p>Click the X button to close the calendar.</p>
Description	<p>Enter a description of the holiday using up to 63 alphanumeric characters (a-z, A-Z, 0-9, spaces, underscores and hyphens allowed).</p>
Add	<p>Click this to add the newly configured holiday to the list.</p> <p>You must fill out the Date and Description fields first.</p>
Delete	<p>Click this to remove a holiday from the list.</p>

Table 48 Server Configuration > Office Hour Setting (continued)

LABEL	DESCRIPTION
Overwrite	Select an auto-attendant policy to be used for office hours: <ul style="list-style-type: none">• Auto-Attendant - This applies the current system office hours to the auto-attendant.• Auto-Attendant + Authority Group - This applies the current system office hours to the auto-attendant and all authority groups.• Auto-Attendant + Authority Group + Extension - This applies the current system office hours to the auto-attendant, all authority groups, and all extensions.
Apply	Click Apply to save your changes.
Default	Click this button to set every field in this screen to factory default configuration.

Authority Group

13.1 Overview

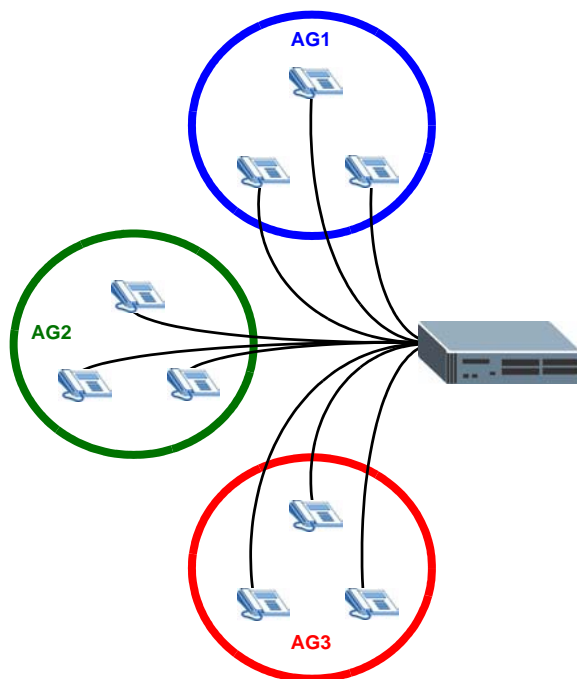
This chapter shows you how to create and manage SIP, FXS and ISDN BRI extensions on the X6004.

The X6004 allows you to manage individual SIP, FXS and ISDN BRI extensions.

Before you can create extensions, you need to create at least one authority group on the X6004. See the [How It Works](#) chapter on page 35 for an overall explanation of authority groups and extensions. This chapter focuses on how to create authority groups on the X6004. It also shows you how to configure settings for SIP, FXS and ISDN BRI on the X6004.

The following figure shows the X6004's extensions divided into three authority groups (**AG1**, **2** and **3**). Each authority group can have different settings and privileges.

Figure 91 Authority Group Overview



13.1.1 What You Can Do in this Chapter

- Use the **Authority Group** screen to set up, configure and manage the X6004's authority groups. See [Section 13.2 on page 200](#).
- Use the **Add SIP Peers** screen to configure a range of extensions for IP phones on your network. See [Section 13.3.1 on page 205](#).
- Use the **Add a SIP Extension** and **Configure SIP Extensions** screens to add a SIP extension to an authority group on the X6004, and configure its settings. See [Section 13.3.2 on page 207](#) and [Section 13.3.3 on page 208](#).
- Use the **SIP Extension Call Forward** screen to set up call forwarding and call blocking rules for your SIP extensions. See [Section 13.3.4 on page 209](#).
- Use the **SIP Extension Voice Mail** screen to configure voice mail settings for your SIP extensions. See [Section 13.3.8 on page 216](#).
- Use the **SIP Extension Advanced** screen to configure SIP advanced settings (for example, CODEC and DTMF mode settings) for your SIP extensions. See [Section 13.3.9 on page 217](#).
- Use the **SIP Extension Auto Provision** screen to configure auto provision settings to have VoIP devices periodically download new SIP extension settings from the X6004. See [Section 13.3.10 on page 219](#).
- Use the **Add an FXS Extension** and **Configure FXS Extensions** screens to add a regular telephone extension to an authority group on the X6004, and configure its settings. See [Section 13.3.11 on page 220](#) and [Section 13.3.12 on page 221](#).
- Use the **FXS Extension Call Forward** screen to set up call forwarding and call blocking rules for your regular telephone extensions. See [Section 13.3.13 on page 222](#).
- Use the **FXS Extension Voice Mail** screen to configure voice mail settings for your regular telephone extensions. See [Section 13.3.14 on page 222](#).
- Use the **FXS Extension Advanced** screen to configure advanced settings (for example, group pickup) for your FXS extensions. See [Section 13.3.9 on page 217](#).
- Use the **Add a BRI Extension** and **Configure BRI Extensions** screens to add an ISDN phone extension to an authority group on the X6004, and configure its settings. See [Section 13.3.16 on page 223](#) and [Section 13.3.12 on page 221](#).
- Use the **BRI Extension Call Forward** screen to set up call forwarding and call blocking rules for your ISDN phone extensions. See [Section 13.3.18 on page 226](#).
- Use the **BRI Extension Voice Mail** screen to configure voice mail settings for your ISDN phone extensions. See [Section 13.3.19 on page 226](#).
- Use the **BRI Extension Advanced** screen to configure advanced settings (for example, group pickup) for your BRI extensions. See [Section 13.3.9 on page 217](#).

13.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Authority Groups and Extensions

Basically, you can think of an authority group as a set of extensions. You use an authority group to assign equal rights to the entire set of extensions. Thus, an authority group is a group of extensions that all have the same authority. For example, if you create two authority groups, you can allow one group to make local calls and long distance calls and the second authority group to make local calls only.

Authority Group Guidelines

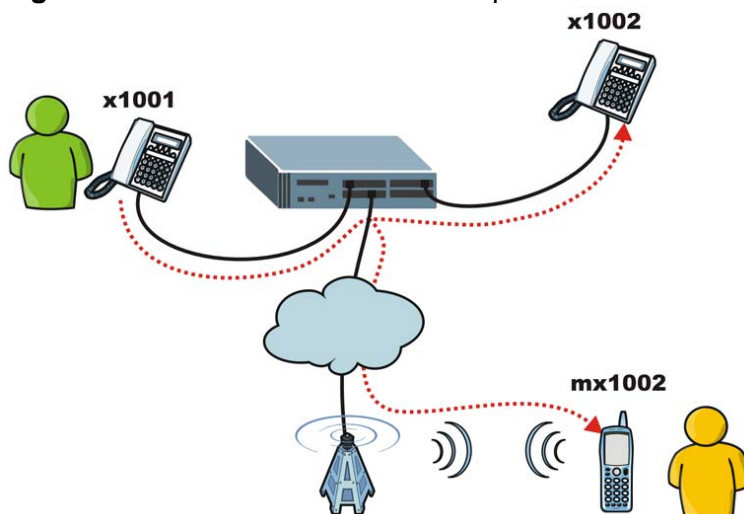
Authority groups and extensions follow these guidelines:

- You must create at least one authority group on the X6004.
- Each extension can be a member of only one authority group.
- SIP, FXS and ISDN BRI extensions are treated the same within an authority group.

Mobile Extensions

A mobile extension is essentially call forwarding to both your IP phone extension and another phone. When you set up a mobile extension and then activate it from your IP phone using a feature code ([Section 6.8 on page 141](#)), all calls sent to your IP phone extension are also sent at the same time to the phone that is designated as your mobile extension. When the call is picked up on one phone, the X6004 stops ringing the other.

Figure 92 A Mobile Extension Example



Finding Out More

- See [Section 13.3 on page 204](#) for more information on features related to individual extensions.
- See [Section 13.4 on page 227](#) for technical reference information on voice and video codecs.

13.2 The Authority Group Screen

Use this screen to set up authority groups on the X6004. To access this screen, click **Configuration > PBX > Extension Management > Authority Group**.

Figure 93 Extension Management > Authority Group

Machine ID	Group Name	Group ID	Description	
IPPBX_001	sales	0001		
IPPBX_001	General	002		

Each field is described in the following table.

Table 49 Extension Management > Authority Group

LABEL	DESCRIPTION
Authority Group	This screen allows you to see which authority groups are configured on the X6004 and it allows you to search extensions configured on the X6004.
Extension Number	Type an extension number and click Query to see if an extension number is already configured on the X6004 and to view its details. See Section 13.2.1 on page 201 for details.
Machine ID	This field indicates the Machine ID of the X6004 on which this authority group was created.
Group Name	This is the name of the authority group.
Description	This field displays the description for this authority group.
Add, Advanced, Edit, Office Hours, Delete	Click: <ul style="list-style-type: none"> • Add - to create a new authority group. • Advanced - to configure authority group settings. • Edit - to change the description of the authority group. • Office Hours - to change the authority group's designated office hours, or to create new ones. • Delete - to remove this authority group from the X6004.

13.2.1 The Extension Query Result Screen

The following screen appears when you click **Query** in the **Authority Group** screen. This screen displays a query result example.

Figure 94 Extension Query Result Example

Query Result	
Extension Number	2222
Group Name	default
SIP Auth. User Name	2222
Type	SIP
Description	2222
<input type="button" value="Edit"/> <input type="button" value="Back to Authority Group"/>	

Each field is described in the following table.

Table 50 Extension Query Result

LABEL	DESCRIPTION
Extension Number	This field displays the extension number that you searched for on the X6004.
Group Name	This field displays the authority group to which this extension belongs.
SIP Auth. User Name	This field displays the user name associated with the SIP account for this extension.
Type	This field displays SIP , if this extension is a SIP account or FXS , if this extension is associated with an analog phone connected to an FXS or BRI port, if this extension is associated with an ISDN phone connected to an BRI port on the X6004.
Description	This field displays the description given to this extension.
Edit	Click this to go to the configuration screen for this extension.
Back to Authority Group	Click this to go back to the main Authority Group screen.

The following screen appears if the X6004 cannot find the extension that you queried.

Figure 95 Extension Number Not Found

Extension Number 343343 Not Found!
<input type="button" value="Back to Authority Group"/>

13.2.2 The Add/Edit Authority Group Screen

Use the **Add Authority Group** screen to create a new authority group. Use the **Edit Authority Group** screen to change the description of an existing authority group. Only the screen used to add a new authority group is shown. Click the **Add** (or **Edit**) icon in the **Authority Group** screen to view the screen as shown.

Note: Only the **Add Authority Group** screen is shown in the following figure. In the **Edit Authority Group** screen, not all of the fields are available.

Figure 96 Add/Edit Authority Group

Each field is described in the following table.

Table 51 Add/Edit Authority Group

LABEL	DESCRIPTION
Machine ID	This field is only available when adding a new authority group. If you have configured ZyStack, select the X6004 on which you want to create this authority group.
Group Name	Type a new name or modify an existing name for this authority group. You can use 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Group ID	Type 1-8 digits to use as an ID for this authority group.
Description	Type a brief description for this authority group. You can use 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Add/Apply	If you are creating a new authority group, click Add to add this authority group to the X6004. If you are editing an existing authority group settings, click Apply to save your changes to the X6004.
Cancel	Click this to go back to the main Authority Group screen without saving your changes.

13.2.3 The Authority Group Configuration Screen

Use this screen to manage extensions in the authority groups. Click the **Advanced** icon in the **Authority Group** screen to view the screen as shown.

Figure 97 Authority Group Configuration

The screenshot displays the Authority Group Configuration screen, which is divided into three main sections: SIP Peer, FXS Peer, and BRI Peer. Each section has a header bar with a title and a set of action icons (Add, Edit, Delete). Below each header is a table with columns for User Name, Type, Extension Number, and Description. The SIP Peer section contains five rows of data for extensions 2001 through 2005, all of type SIP. The FXS Peer and BRI Peer sections are currently empty. There are 'Delete' buttons at the top left and bottom left of the SIP Peer section, and a 'Cancel' button at the bottom center of the entire screen.

SIP Peer						
<input type="checkbox"/> Delete		<input type="button" value="Batch Add"/>				:Add :Edit :Delete
<input type="checkbox"/>	User Name	Type	Extension Number	Description		
<input type="checkbox"/>	2001	SIP	2001			
<input type="checkbox"/>	2002	SIP	2002			
<input type="checkbox"/>	2003	SIP	2003			
<input type="checkbox"/>	2004	SIP	2004			
<input type="checkbox"/>	2005	SIP	2005			
<input type="button" value="Delete"/>						

FXS Peer					
		:Add :Edit :Delete			
	User Name	Type	Extension Number	Description	

BRI Peer					
		:Add :Edit :Delete			
	User Name	Type	Extension Number	Description	

Each field is described in the following table.

Table 52 Authority Group Configuration

LABEL	DESCRIPTION
Group Name	This field displays the name of the authority group you are configuring.
Description	This field displays the description given to the authority group you are configuring.
Batch Add	Click Batch Add if you want to configure multiple extensions for IP phones connected to the X6004.
SIP Peer / FXS Peer / BRI Peer	The screen is divided into three sections: the SIP Peer section shows you the extensions created for the IP phones connected to the X6004, the FXS Peer section shows you the extensions created for the analog phones connected to the X6004 and the BRI Peer section shows you the extensions created for the ISDN phones connected to the X6004.
Delete	Check the Delete box and click Delete to remove this extension from this authority group.
User Name	This is the username associated with an extension for SIP authentication.

Table 52 Authority Group Configuration (continued)

LABEL	DESCRIPTION
Type	<p>This field displays SIP, if this extension is a SIP account.</p> <p>This field displays FXS, if this extension is associated with an analog phone connected to an FXS port on the X6004.</p> <p>This field displays BRI, if this extension is associated with an ISDN phone connected to a BRI port on the X6004.</p>
Extension Number	This field displays the extension number.
Description	This field displays the description given to this extension.
Add, Edit, Delete	<p>Click:</p> <ul style="list-style-type: none"> • Add - to create a new extension on the X6004. • Edit - to edit an existing extension on the X6004. • Delete - remove an extension from the X6004.

13.3 Extension Features

You can configure the following features on a per extension basis:

- **Call Forwarding** - set up call forwarding rules for the individual extension based on the following criteria:
 - Your extension is busy.
 - You turn on DND (Do Not Disturb). You can set up a list of telephone numbers, referred to as the **White List** that ignore DND.
 - Unconditionally, forwards all calls to a specific extension or your voice mail.
 - There is no answer at your extension. This also allows you to set up a **Find Me List**, which is a list of phone numbers where you might be located.
- **Call Blocking** - set up a list of telephone numbers that you don't want to receive calls from. Or, stop calls without caller ID from reaching your extension.
- **Voice Mail Forwarding** - Configure the X6004 to forward your voice mail messages to your email account.

13.3.1 The Batch Add Screen

Use this screen to configure a range of extensions for IP phones on your network. To access this screen, click the **Batch Add** button in the **Authority Group** configuration screen.

Figure 98 Batch Add SIP Extensions

Each field is described in the following table.

Table 53 Batch Add SIP Extensions

LABEL	DESCRIPTION
Batch Add SIP Peers	
Group	Select the authority group you want these extensions to belong to.
Start Number	Type the first extension number for this range of extensions. Extensions can be 3-10 digits long.
Step/Interval	Type the value of the increment, which the X6004 uses to create this range of extensions.
Amount	Type the number of extensions you want to create. The number of extensions you can create is limited by the subscription service registered on the X6004 (see Section 36.4 on page 481).
SIP Auth. Password	<p>When you create multiple SIP extensions, you automatically create SIP accounts on the X6004. The user names for these SIP accounts are the extension numbers. The passwords for the SIP accounts are also the extension numbers. To make the passwords more secure you can add a prefix or a postfix to these extensions.</p> <p>For example type "1" in the Prefix field and the SIP account passwords for the SIP extensions you create become "1 + extension number".</p> <p>You can enter up to three letters, numbers or a combination of letters and numbers in the Prefix and Postfix fields.</p>

Table 53 Batch Add SIP Extensions (continued)

LABEL	DESCRIPTION
DTMF Mode	<p>Control how the X6004 handles the tones that the IP phones using these extensions make when they push their buttons. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number. You should use the same mode as your VoIP service provider. The choices are:</p> <ul style="list-style-type: none"> • rfc2833 - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • inband - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. • info - Send the DTMF tones in SIP messages.
Codec Setting	<p>Select the type of voice coder/decoder (codec) that you want this extension to use when communicating with the X6004. The following codecs are supported by the X6004:</p> <ul style="list-style-type: none"> • G.711 a-law (typically used in Europe) • G.711 u-law (typically used in North America and Japan) • G.729A • G.722 (pass-through) • G.722 AMR-WB (pass-through) • G.723.1 - you must activate support for this codec in the Configuration > PBX > Server Configuration > Server screen. • G.726 <p>See Voice Codecs on page 227 for more information.</p> <p>When two SIP devices start a SIP session, they must agree on a codec.</p> <p>If these SIP extensions are assigned to videophones, you must specify the video codecs used for video calls. The X6004 allows the following video codecs to passthrough:</p> <ul style="list-style-type: none"> • H.261 • H.263 • H.264 • MP4 <p>See Video Codecs on page 228 for more information.</p>
Codec Pool	<p>This column indicates the codec types not used for these extensions. You can add a codec type to be used for these extensions by highlighting it and clicking the Right button.</p>
Codec List	<p>This column indicates the codec types used by these extensions. You can organize the priority of the codecs by highlighting it and clicking the Up or Down buttons to move the codec higher or lower in priority. The SIP extensions attempt to use the higher priority codecs first and try the lower priority codecs next. You can remove a codec type from being used from these extension by highlighting it and hitting the Left button.</p>
Apply	<p>Click Apply to save your changes.</p>
Cancel	<p>Click Cancel to go back to Authority Group configuration page without saving your changes.</p>

13.3.2 Add a SIP Extension: The Basic Screen

Use this screen to add a SIP extension to an authority group on the X6004. To access this screen, click the **Add** icon in the **Authority Group** configuration screen.

Figure 99 Add a SIP Extension: Basic

The screenshot shows a web form titled "SIP Peer Basic Setting". It contains the following fields and controls:

- Group:** A dropdown menu with "sales" selected.
- Extension Number:** A text input field.
- Web/IVR/VM PIN Code:** A text input field.
- SIP Auth. User Name:** A text input field.
- SIP Auth. Password:** Two radio buttons: "Customization" (selected) and "Random". The "Random" option has a small input field containing the number "4".
- Description:** A text input field.
- Buttons:** "Apply" and "Cancel" buttons at the bottom right.

Each field is described in the following table.

Table 54 Add a SIP Extension: Basic

LABEL	DESCRIPTION
Group	Select the authority group you want this extension to belong to.
Extension Number	Type the extension number for this IP phone extension. The extension number can be 3-10 digits.
Web/IVR/VM PIN Code	Type the PIN code that allows the person with this extension to access the web portal, Interactive Voice Response system or Voice Mail. This value can be 3-10 digits.
SIP Auth. User Name	Type the SIP user name associated with this extension. The IP phone registering with the X6004 must provide this for authentication. The user name can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
SIP Auth. Password	Select Customization and type the SIP password associated with this extension. The IP phone registering with the X6004 must provide this for authentication. The password can be 4-32 alphanumeric characters (A-Z, a-z, 0-9). Spaces are not allowed. If you are using auto provisioning (see Chapter 7 on page 153), you can select Random and type the length of the password (4 - 32). The X6004 will assign a random SIP password to this extension. The password will be automatically sent to the IP phone client.

Table 54 Add a SIP Extension: Basic (continued)

LABEL	DESCRIPTION
Description	Type a brief description for this SIP extension. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means the field can be left blank.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to go back to the previous screen without saving your changes.

13.3.3 Configure SIP Extensions: The Basic Screen

After you create SIP extensions you can click on the **Edit** button in the **Authority Group** configuration screen to configure further settings. The **Basic** screen for a SIP extension appears as shown.

Figure 100 Configure SIP Extension: Basic

Each field is described in the following table.

Table 55 Configure SIP Extension: Basic

LABEL	DESCRIPTION
Group	Select the authority group you want this extension to belong to.
Extension Number	This field displays the extension number of this SIP extension.

Table 55 Configure SIP Extension: Basic (continued)

LABEL	DESCRIPTION
Web/IVR/VM PIN Code	Type the PIN code that allows the person with this extension to access the web portal, Interactive Voice Response (IVR) system or Voice Mail. This value can be 3-10 digits.
SIP Auth. User Name	Type the SIP user name associated with this extension. The IP phone registering with the X6004 must provide this for authentication. The user name can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
SIP Auth. Password	Type the SIP password associated with this extension. The IP phone registering with the X6004 must provide this for authentication. The password can be 4-32 alphanumeric characters long (A-Z, a-z, 0-9). Spaces are not allowed.
Department	Type the department for this SIP extension. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
First Name	Type the first name of the person this SIP extension is assigned to. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Last Name	Type the last name of the person this SIP extension is assigned to. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Description	Type a brief description for this SIP extension. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click Apply to save your changes.
Back to Peer List	Click Back to Peer List to go back to Authority Group configuration page without saving your changes.

13.3.4 The SIP Extension Call Forward Screen

Use this screen to set up call forwarding and call blocking rules for your extension.

Note: The X6004 checks any Auto-Attendant call forwarding (see [Chapter 19 on page 291](#)) and call blocking (see [Section 6.7 on page 139](#)) settings before applying any of the rules created for individual extensions.

To access this screen, click the **Call Forward** tab in any of the SIP extension configuration screens.

Figure 101 SIP Extension: Call Forward

Call Forward Setting

Office Hours
 Office Hours

DND(Do Not Disturb) Disable Enable () Voice Mail

Blind Forward Disable Enable (Extension Number:) Voice Mail

Busy Forward Disable Enable (Extension Number:) Voice Mail

No Answer Forward Disable Enable () Voice Mail

After Office Hours Disable Enable (Extension Number:) Voice Mail

Call Blocking Setting

Black list Disable Enable ()

Block the calls without Caller ID Disable Enable

Mobile Extension Setting

Mobile Extension Manually Force Enable

Number : Dial Rule : ▼

.....

Each field is described in the following table.

Table 56 SIP Extension: Call Forward

LABEL	DESCRIPTION
Call Forward Setting	Use this section to configure call forwarding settings for your extension.
Office Hours	<p>The X6004 has separate rules for call forwarding during office hours than after office hours. The settings you configure specify the office hours for this extension and affect call forwarding during those office hours.</p> <p>If a call is first handled by auto-attendant then it checks the system office hours settings first (and applies any forwarding rules), before checking the office hours configured in this screen.</p>

Table 56 SIP Extension: Call Forward (continued)

LABEL	DESCRIPTION
Office Hours	<p>Click this button to open the Office Hours screen, where you can configure an extension's individual office hour settings. The auto-attendant uses the system-wide office hour settings by default, then applies extension-specific office hour settings.</p> <p>This screen is almost identical to the one described in Chapter 12 on page 193 with only a few minor exceptions.</p>
Time	Specify the time range in 24 hour format for the office hours.
DND (Do Not Disturb)	<p>Select Disable to turn this feature off for this extension.</p> <p>Select Enable and the X6004 will not forward calls to your extension. Click on White List (see Section 13.3.5 on page 213) to configure telephone numbers which ignore whether you have DND turned on or off.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p>
Blind Forward	<p>Select Disable to turn this feature off for this extension.</p> <p>Select Enable and specify an extension 0-20 digits in length. The X6004 will forward all incoming calls to that extension.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p>
Busy Forward	<p>Select Disable to turn this feature off for this extension.</p> <p>Select Enable and specify an extension 0-20 digits in length. The X6004 will forward all incoming calls to that extension when your phone is off the hook. For FXS (analog phones) extensions incoming calls are put into a call waiting queue.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p>
No Answer Forward	<p>Select Disable to turn this feature off for this extension.</p> <p>Select Enable and the X6004 will forward all incoming calls to the extensions you specify when you do not answer the phone within the default ring time. The default ring time is configured in the Configuration > PBX > Server Configuration > Global Set screen. Click Find Me List (see Section 13.3.6 on page 214) to specify a list of extensions that the X6004 will forward incoming calls to.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p>
After Office Hours	<p>These fields specify how to treat calls to your extension that occur after office hours.</p> <p>Select Disable to turn this feature off for this extension.</p> <p>Select Enable and specify an extension 0-20 digits in length. The X6004 will forward all incoming calls to that extension.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p>

Table 56 SIP Extension: Call Forward (continued)

LABEL	DESCRIPTION
Call Blocking Setting	Use this section to configure call blocking settings for your extension.
Black List	<p>Select Disable to turn this feature off for this extension.</p> <p>Select Enable and the X6004 will block all incoming calls from extensions that you specify as blacklisted. Click the Black List (see Section 13.3.7 on page 215) button to configure phone numbers that you want to block from calling you.</p>
Block the calls without Caller ID	Select Enable and the X6004 will block all incoming calls from phone that do not send caller ID.
Mobile Extension	Use this section to configure your mobile extension settings.
Mobile Extension	<p>Select Disable to allow authority group members to turn this feature on and off using feature codes.</p> <p>Select Force Enable to override the authority group member settings and require that all calls to use this feature.</p> <p>For more information on feature codes, see Section 6.8 on page 141.</p>
Number	Enter the number to which you want the X6004 to forward any incoming calls to your extension.
Dial Rule	<p>Select a dial rule to be applied to the mobile extension. Dial rules correspond to the Least Cost Routing rules used in Configuration > PBX > Outbound Line Management > LCR. For more information, see Chapter 20 on page 309.</p> <p>Note: This option only works with digital outbound connections such as BRI. Analog outbound connections such as FXO cannot use this option.</p>
Apply	Click this to save your changes.
Back to Peer List	Click this to go back to the Authority Group configuration screen without saving your changes.

13.3.5 The DND White List Screen

Use this screen to edit the **DND White List** for your extension. This is a list of extensions that the X6004 will forward calls from even if you have DND enabled. To access this screen, click the **DND White List** button in the **Call Forward** screen.

Figure 102 DND White List

Each field is described in the following table.

Table 57 DND White List

LABEL	DESCRIPTION
Number	Enter the telephone number you want to allow to call you even if you DND turned on. Click Add and the number you entered displays in the field below. This field can be 1-20 digits and characters in length using only 0-9, [.] period, N, X, and Z.
Delete	Highlight an existing DND White List number and click the Delete icon to remove it from the list.
Apply	Click this to save your changes.
Cancel	Click this to return to the Call Forward screen.

13.3.6 The Find Me List Screen

Use this screen to edit the **Find Me List** for your extension. This is a list of extensions that the X6004 tries to call if you do not pick up a call. To access this screen, click the **Find Me List** button in the **Call Forward** screen.

Figure 103 Find Me List

Each field is described in the following table.

Table 58 Find Me List

LABEL	DESCRIPTION
Number	Enter the telephone extension you want the X6004 to forward calls to when you do not pick up a call. Click Add and the number you entered displays in the field below. This field can be 0-20 digits in length.
Priority	Highlight an existing Find Me List extension and use the up arrow to move it up in the list or use the down arrow to move it down in the list. The X6004 will try to forward the call to the extensions in the list in the order they appear from top to bottom. If the top extension does not pick up it tries the one below and so on. The X6004 attempts to forward calls to the top (highest priority) five phone numbers only.
Delete	Highlight an existing Find Me List extension and click the Delete icon to remove it from the list.
Apply	Click this to save your changes.
Cancel	Click this to return to the Call Forward screen.

13.3.7 The Blacklist Screen

Use this screen to edit the **Black List** for your extension. This is a list of phone numbers from which the X6004 will not forward calls to your extension. To access this screen, click the **Black List** button in the **Call Forward** screen.

Figure 104 Black List

Each field is described in the following table.

Table 59 Black List

LABEL	DESCRIPTION
Number	Enter the telephone number you want to block from calling you when you enable call blocking. Click Add and the number you entered displays in the field below. This field can be 1-20 digits and characters in length using only 0-9, [.] period, N, X, and Z.
Delete	Highlight an existing Black List number and click the Delete icon to remove it from the list.
Apply	Click this to save your changes.
Cancel	Click this to return to the Call Forward screen.

13.3.8 The SIP Extension Voice Mail Settings Screen

Use this screen to configure voice mail settings for this extension. To access this screen, click the **Voice Mail** tab in any of the SIP extension configuration screens.

Figure 105 SIP Extension: Voice Mail

Each field is described in the following table.

Table 60 SIP Extension: Voice Mail

LABEL	DESCRIPTION
Received E-mail Address	Specify the email address you want to forward your voice message notifications to. If you select the Attached Voice File option, then complete voice messages are sent to this email address.
Attached Voice File	Select this feature if you want complete voice messages to be sent to the email address you specified in the Received E-mail Address field.
Delete Voice Mail After Mailed	Check this box to delete voicemail messages stored on the X6004 after they have been emailed.
Apply	Click this to save your changes.
Back to Peer List	Click this to go back to the previous screen without saving your changes.

13.3.9 The SIP Extension Advanced Screen

Use this screen to configure advanced settings for this extension. Click the **Advanced** tab in any of the SIP extension configuration screens to view the screen as shown.

Figure 106 SIP Extension: Advanced

CODEC Setting

CODEC Pool	CODEC List
G.726	G.729
H.263	G.711 u-law
H.261	G.711 a-law
G.722 (pass-through)	
G.722 AMR-WB (pass-through)	

Extra Setting

DTMF Mode: info

MWI Enable

Group Pickup

Each field is described in the following table.

Table 61 SIP Extension: Advanced

LABEL	DESCRIPTION
Codec Setting	<p>Select the type of voice coder/decoder (codec) that you want this extension to use when communicating with the X6004. The following codecs (shown in highest quality to lowest quality order) are supported by the X6004:</p> <ul style="list-style-type: none"> • G.711 a-law (typically used in Europe) • G.711 u-law (typically used in North America and Japan) • G.729A • G.722 (pass-through) • G.722 AMR-WB (pass-through) • G.723.1 - you must activate support for this codec in the Configuration > PBX > Server Configuration > Server screen. • G.726 <p>See Voice Codecs on page 227 for more information.</p> <p>When two SIP devices start a SIP session, they must agree on a codec.</p> <p>If these SIP extensions are assigned to videophones, you must specify the video codecs used for video calls. The X6004 allows the following video codecs to passthrough:</p> <ul style="list-style-type: none"> • H.261 • H.263 • H.264 • MP4 <p>See Video Codecs on page 228 for more information.</p>
Codec Pool	<p>This column indicates the codec types not used by this extension. You can add a codec type to be used by this extension by highlighting it and hitting the Right button.</p>
Codec List	<p>This column indicates the codec types used by this extension. You can organize the priority of the codecs by highlighting it and clicking the Up or Down buttons to move the codec higher or lower in priority. The SIP extension attempts to use the higher priority codecs first and tries the lower priority codecs next. You can remove a codec type from being used from this extension by highlighting it and hitting the Left button.</p>
Extra Setting	
DTMF Mode	<p>Control how the X6004 handles the tones that the IP phone using this extension makes when you push its buttons. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number. You should use the same mode as your VoIP service provider. The choices are:</p> <ul style="list-style-type: none"> • rfc2833 - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • inband - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. • info - Send the DTMF tones in SIP messages.

Table 61 SIP Extension: Advanced (continued)

LABEL	DESCRIPTION
MWI Enable	Check this box to enable Message Waiting Indicator (MWI) mode for this extension. The X6004 sends a beeping tone to the IP phone when there is at least one voicemail for this extension.
Group Pickup	Check this box if you want to enable the group pickup feature for this extension. If this extension is added to a pickup group, then the phone at this extension rings when any extension that is part of this pickup group is called. See Chapter 15 on page 239 for more information on group pickup.
Apply	Click this to save your changes.
Back to Peer List	Click this to go back to the Authority Group configuration screen without saving your changes.

13.3.10 The Auto Provision Screen

Use this screen to generate the auto provision file for the SIP extension on the X6004. To access this screen, click the **Auto Provision** tab in any of the SIP extension configuration screen to view the screen as shown.

Figure 107 SIP Extension: Auto Provision

The screenshot shows the 'Provisioning Setting' screen for SIP extension auto-provisioning. It includes the following fields and controls:

- MAC Address:** Text input field containing '00134900000A'.
- Serial No.:** Text input field containing 'S4Z8012345'.
- Auto Provision Active:** Dropdown menu set to 'On'.
- Auto Provision Interval Time:** Text input field containing '43200', with '(seconds) <21600~604800>' to its right.
- Auto Provision Delay Time:** Dropdown menu set to 'Random', with '(seconds)' to its right.
- ATA device:** An unchecked checkbox.
- Port No.:** Dropdown menu set to '1'.

At the bottom of the screen, there are two buttons: 'Apply' and 'Back to Peer List'.

Each field is described in the following table.

Table 62 SIP Extension: Auto Provision

LABEL	DESCRIPTION
MAC Address	Type the MAC address of your SIP phone in this field. You can leave this field empty when your use a SIP softphone.
Serial No.	Type the serial number of your SIP phone in this field. You can leave this field empty when you use a SIP hand phone.
Auto Provision Active	Select On to activate auto provision or Off to deactivate it.

Table 62 SIP Extension: Auto Provision (continued)

LABEL	DESCRIPTION
Auto Provision Interval Time	Specify the amount of time in seconds to have the specified SIP client wait before the next time of provision file downloading from the X6004. Enter the time range between 21600 to 604800 seconds (between 6 to 168 hours). The default value is 43200 seconds (12 hours).
Auto Provision Delay Time	If many SIP clients download auto-provisioning files from the X6004 at the same time, the X6004 may be overloaded. The total interval between auto provisioning file downloads is the interval time plus the delay time. For example of SIP phone A has the interval time of 10 hours and delay time of 10 seconds, the next auto provisioning download will be 10 hours and 10 seconds later. Select 1~30 seconds or leave it as default, Random , which is to have a random delay time of between 1 to 30 seconds for the specified SIP client.
ATA device	Select this when your SIP client is a ZyXEL ATA (Analog Telephone Adapter) device. An ATA allows you to make VIP calls from a connected analog phone.
Port No.	This field is available when you select the ATA device field. An ATA device can have up to eight SIP numbers (for ports 1 to 8). Select an ATA port number to which you want to assign the SIP number.
Apply	Click this to save your changes and have the X6004 prepare the auto provisioning file for ZyXEL SIP phones downloading.
Back to Peer List	Click this to go back to the Authority Group configuration screen without saving your changes.

13.3.11 The Add an FXS Extension Screen

Use this screen to add an FXS extension to an authority group on the X6004. To access this screen, click the **Add** icon in the **Authority Group** configuration screen.

Figure 108 Add an FXS Extension

The screenshot shows a configuration window titled "Basic Setting". It contains the following fields and controls:

- Extension Number:** A text input field.
- Interface:** Labeled "Slot:" with a dropdown menu set to "Slot C", and "Port:" with a dropdown menu set to "Port 1".
- Web/IVR/VM PIN Code:** A text input field.
- Description:** A text input field.
- Buttons:** "Apply" and "Cancel" buttons are located at the bottom right of the form.

Each field is described in the following table.

Table 63 Add an FXS Extension

LABEL	DESCRIPTION
Extension Number	Type the extension number for this analog phone extension. The extension number can be from 3-10 digits in length.
Interface	Specify the location on the FXS interface card that the analog phone with this extension is connected to.
Web/IVR/VM PIN Code	Type the PIN code that allows the person with this extension to access the web portal, Interactive Voice Response system or Voice Mail. This value can be 4-8 digits in length.
Description	Type a brief description for this FXS extension. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to go back to Authority Group configuration page without saving your changes.

13.3.12 Configure FXS Extensions: the Basic Screen

After you create FXS extensions you can click on the **Edit** button in the **Authority Group** configuration screen to configure further settings associated with the extensions. The **Basic** screen for an FXS extension appears as shown.

Figure 109 FXS Extension: Basic

Basic Setting

Group	<input type="text" value="AG_EXAMPLE"/>
Extension Number	<input type="text" value="2002"/>
Interface	Slot: <input type="text" value="Slot D"/> Port: <input type="text" value="Port 2"/>
Web/IVR/VM PIN Code	<input type="text" value="****"/>
Department	<input type="text"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Description	<input type="text"/>

Each field is described in the following table.

Table 64 FXS Extension: Basic

LABEL	DESCRIPTION
Group	Select the authority group you want this extension to belong to.
Extension Number	This field displays the extension number for this analog phone extension.
Interface	Specify the location on the FXS interface card that the analog phone with this extension is connected to.
Web/IVR/VM PIN Code	Type the PIN code that allows the person with this extension to access the web portal, Interactive Voice Response system or Voice Mail. This value can be 4-8 digits in length.
Department	Type the department for this FXS extension. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
First Name	Type the first name of the person this FXS extension is assigned to. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Last Name	Type the last name of the person this FXS extension is assigned to. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Description	Type a brief description for this FXS extension. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click Apply to save your changes.
Back to Peer List	Click Back to Peer List to go back to Authority Group configuration page without saving your changes.

13.3.13 The FXS Extension Call Forward Screen

The fields in this screen are the same as the fields for SIP extension call forwarding screen. Refer to [Table 56 on page 210](#) for detailed field descriptions.

13.3.14 The FXS Extension Voice Mail Screen

The fields in this screen are the same as the fields for SIP extension voice mail screen. Refer to [Table 60 on page 216](#) for detailed field descriptions.

13.3.15 The FXS Extension Advanced Screen

Check the **Group Pickup** box in this screen if you want to enable the group pickup feature for this extension. If this extension is added to a pickup group, then this phone can be used to pick up calls to any extension that is part of a pickup group. See [Chapter 15 on page 239](#) for more information on group pickup.

Figure 110 FXS Extension: Advanced Screen

The screenshot shows a configuration window titled "Extra Setting". It contains two checked checkboxes: "MWI Enable" and "Group Pickup". Below the checkboxes, there are two buttons: "Apply" and "Back to Peer List".

13.3.16 The Add a BRI Extension Screen

Use this screen to add an BRI extension to an authority group on the X6004. To access this screen, click the **Add** icon in the **Authority Group** configuration screen.

Figure 111 Add a BRI Extension

The screenshot shows a configuration window titled "Basic Setting". It contains four input fields: "Extension Number", "Interface" (with sub-fields for Slot: Slot B, Port: Port 1, and MSN: 1), "Web/IVR/VM PIN Code", and "Description". At the bottom, there are two buttons: "Apply" and "Cancel".

Each field is described in the following table.

Table 65 Add a BRI Extension

LABEL	DESCRIPTION
Extension Number	Type the extension number for this ISDN phone extension. The extension number can be from 3-10 digits in length.
Interface	Specify the location on the BRI interface card and the multiple subscriber number (see Section 13.3.16.1 on page 224 for using MSNs for extensions) that the ISDN phone with this extension is connected to.
Web/IVR/VM PIN Code	Type the PIN code that allows the person with this extension to access the web portal, Interactive Voice Response system or Voice Mail. This value can be 4-8 digits in length.

Table 65 Add a BRI Extension (continued)

LABEL	DESCRIPTION
Description	Type a brief description for this BRI extension. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to go back to Authority Group configuration page without saving your changes.

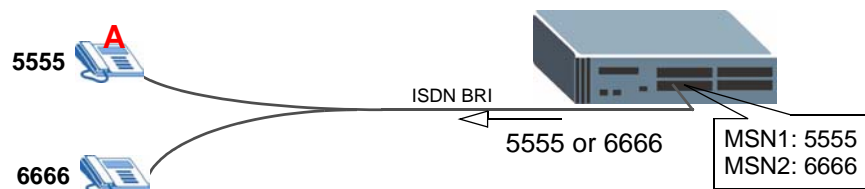
13.3.16.1 MSN

An MSN (Multiple Subscribe Number) is a phone line extension number that allows you to associate multiple phone numbers with an ISDN BRI line. You can configure two MSNs for each BRI line on the X6004. See the following example.

Table 66 MSN Example

INTERFACE / PORT	MSN	MAPPING EXTENSION NUMBER
BRI / Port 1	1	5555
	2	6666
BRI / Port 2	1	7777
	2	8888
...		

In the following example, two ISDN phones are connected to a single ISDN BRI port. Each phone has a unique MSN. These MSNs must correspond to those configured on the X6004. The phone **A** only answers the call dialing to **5555**.

Figure 112 Using MSNs for Extensions

Note: You should define the same extension number(s) in the connected ISDN phones. Otherwise, you cannot receive any calls.

13.3.17 Configure BRI Extensions: the Basic Screen

After you create BRI extensions you can click on the **Edit** button in the **Authority Group** configuration screen to configure further settings associated with the extensions. The **Basic** screen for an BRI extension appears as shown.

Figure 113 BRI Extension: Basic

The screenshot shows a web-based configuration form titled "Basic Setting". The form contains the following fields and controls:

- Group:** A dropdown menu with "AG_EXAMPLE" selected.
- Extension Number:** A text input field containing "6010".
- Interface:** Three dropdown menus: "Slot:" with "Slot B" selected, "Port:" with "Port 2" selected, and "MSN:" with "1" selected.
- Web/IVR/VM PIN Code:** A text input field containing "****".
- Department:** A text input field.
- First Name:** A text input field.
- Last Name:** A text input field.
- Description:** A text input field.

At the bottom of the form, there are two buttons: "Apply" and "Back to Peer List".

Each field is described in the following table.

Table 67 BRI Extension: Basic

LABEL	DESCRIPTION
Group	Select the authority group you want this extension to belong to.
Extension Number	Type the extension number for this ISDN phone extension.
Interface	Specify the location on the BRI interface card that the ISDN phone with this extension is connected to.
Web/IVR/VM PIN Code	Type the PIN code that allows the person with this extension to access the web portal, Interactive Voice Response system or Voice Mail. This value can be 4-8 digits in length.
Department	Type the department for this BRI extension. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
First Name	Type the first name of the person this BRI extension is assigned to. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Last Name	Type the last name of the person this BRI extension is assigned to. This field can be 0-40 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.

Table 67 BRI Extension: Basic (continued)

LABEL	DESCRIPTION
Description	Type a brief description for this BRI extension. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click Apply to save your changes.
Back to Peer List	Click Back to Peer List to go back to Authority Group configuration page without saving your changes.

13.3.18 The BRI Extension Call Forward Screen

The fields in this screen are the same as the fields for SIP extension call forwarding screen. Refer to [Table 56 on page 210](#) for detailed field descriptions.

13.3.19 The BRI Extension Voice Mail Screen

The fields in this screen are the same as the fields for SIP extension voice mail screen. Refer to [Table 60 on page 216](#) for detailed field descriptions.

13.3.20 The BRI Extension Advanced Screen

The fields in this screen are the same as the fields for FXS extension advanced screen. Refer to [Section 13.3.15 on page 223](#) for detailed field descriptions. See [Chapter 15 on page 239](#) for more information on group pickup.

13.4 Authority Group Technical Reference

This section contains technical background information about the **Authority Group** screens.

Voice Codecs

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The following table describes the codecs supported on the X6004

Table 68 Voice Codecs Supported

CODEC	DESCRIPTION
G.711	<p>This is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals (sampling) and converts them into digital bits (quantization). Quantization "reads" the analog signal and then "writes" it to the nearest digital value. For this reason, a digital sample is usually slightly different from its analog original (this difference is known as "quantization noise").</p> <p>G.711 provides excellent sound quality but requires 64kbps of bandwidth.</p> <p>There are two main algorithms defined in the G.711 standard, the μ-law algorithm (used in North America & Japan) and a-law algorithm (used in Europe and the rest of the world).</p>
G.722 (pass-through)	<p>G.722 is an ADPCM codec (see G.726) working at 48 ~ 64 Kbps, with an audio sample rate of 16 KHz. G.722 provides excellent sound quality.</p> <p>Note: The X6004 supports G.722 pass-through, meaning that devices communicating via the X6004 must support this codec.</p>
G.722 AMR-WB (pass-through) (also referred to G.722.2)	<p>G.722.2 is similar to G.722, but with a lower compression rate that can vary according to the amount of available bandwidth. When there is plenty of bandwidth, the compression ratio decreases, and when there is network congestion the compression ratio increases. This is also known as Adaptive Multi Rate - WideBand (AMR-WB).</p> <p>Note: The X6004 supports G.722.2 pass-through, meaning that devices communicating via the X6004 must support this codec.</p>
G.723.1	<p>This is an ITU (International Telecommunication Union) standard for voice coding. The G.723.1 codec compresses voice audio in 30 ms frames. The G.723.1 operates at two bitrates: 6.3 kbps when sampling at 24 bytes or 5.3 kbps when sampling at 20 bytes per 30 ms frame.</p>

Table 68 Voice Codecs Supported (continued)

CODEC	DESCRIPTION
G.726	This is an Adaptive Differential Pulse Code Modulation (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. G.726 operates at 16, 24, 32 or 40 kbps. Differential (or Delta) PCM is similar to PCM, but encodes the audio signal based on the difference between one sample and a prediction based on previous samples, rather than encoding the sample's actual quantized value. Many thousands of samples are taken each second, and the differences between consecutive samples are usually quite small, so this saves space and reduces the bandwidth necessary.
G.729	This is an Analysis-by-Synthesis (AbS) hybrid waveform codec. It uses a filter based on information about how the human vocal tract produces sounds. The codec analyzes the incoming voice signal and attempts to synthesize it using its list of voice elements. It tests the synthesized signal against the original and, if it is acceptable, transmits details of the voice elements it used to make the synthesis. Because the codec at the receiving end has the same list, it can exactly recreate the synthesized audio signal. G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

Video Codecs

Video codecs are used by video phones to compress the amount of information sent between two devices. Video codecs encode video signals into digital signals and decode the digital signals back into video signals. Although the X6004 does not perform any video coding, it does support the passthrough of the following video codecs.

Table 69 Video Codecs Supported

CODE C	DESCRIPTION
H.261	This is an ITU (International Telecommunication Union) video coding standard. H.261 was designed in 1990 and is considered the first practical video coding standard. The data rate of the coding algorithm is able to operate between 40 kbps and 2 Mbps. H.261 was targeted primarily to work over circuit-switched networks and has since been superseded by more efficient video coding standards.
H.263	This video codec is based closely on the H.261 standard, but as a general rule requires half the bandwidth to achieve the same quality video. H.263 is capable of streaming video at bandwidths as low as 20 kbps to 24 kbps.
H.264	This video codec is video compression technology that falls under the MPEG-4 standard, also known as MPEG-4 Part 10. H.264 can provide excellent video quality at bandwidth from 40 Kbps upwards.
MP4	MPEG-4 is an audio/video compression technology developed by the Motion Picture Experts Group. You need to enable MPEG-4 if you want SIP phones to make video calls via the X6004.

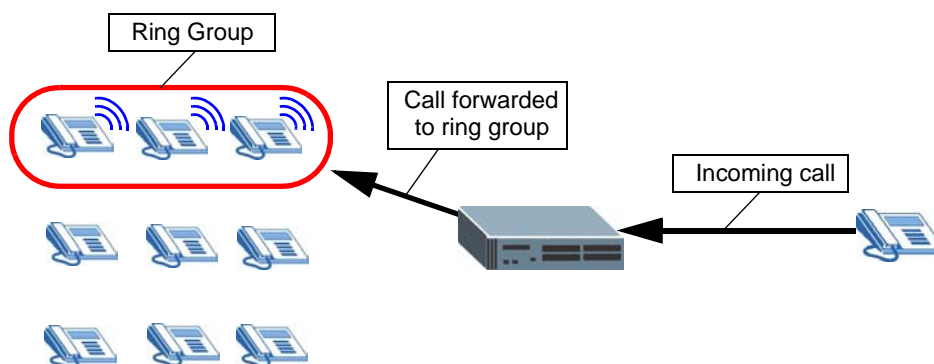
Ring Group

14.1 Overview

This chapter shows you how to create and manage ring groups on the X6004.

Each ring group consists of a number of extensions that work together when calls come in. For example, you can configure a number of extensions to all ring simultaneously when a call comes in.

Figure 114 Ring Group Overview



14.1.1 What You Can Do in this Chapter

Use the **Ring Group** screen to view and configure the X6004's ring groups. You can also add and edit page groups and hunt groups. See [Section 14.2 on page 233](#).

14.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Paging and Hunting

Ring groups on the X6004 control groups of extensions for two purposes:

- Paging - the caller can simply dial a number configured for a group of extensions. The telephones with the extensions in the group automatically pick up. It is similar to creating an automatic conference call.
- Hunting - the caller can simply dial a number to reach a group of extensions. The extensions ring based on a ringing method you configure. For example, all extensions can ring at the same time until the call is picked up or extensions in the group ring in a random order until the call is picked up.

14.1.3 Before You Begin

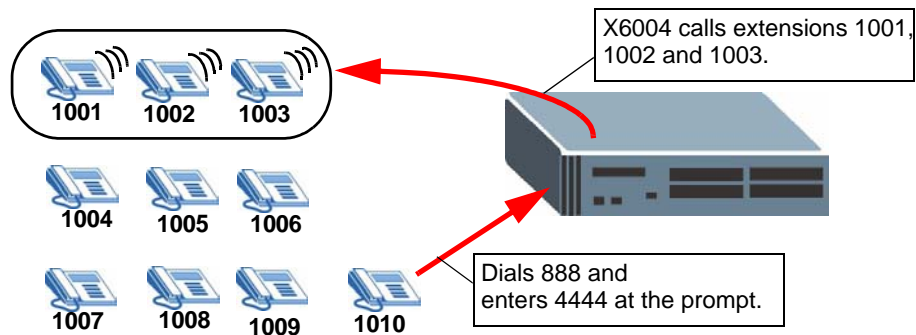
Before you configure the X6004's ring groups, you should decide exactly how you want to divide your extensions into groups, and consider exactly how you want the extensions to behave when calls come in.

14.1.3.1 Paging Group Example

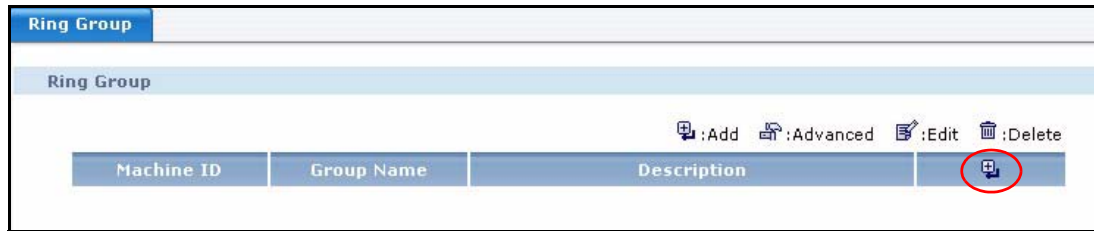
The following sections show you how to create page groups. Paging groups are sets of extensions that can all be called at the same time by dialing a single number (page group number). When a page group number is dialed, all of the extensions automatically pick up via speakerphone. One use of this feature can be to make announcements. A boss can dial the page group number to say "Meeting in five minutes!" or "Lunch time!!! It's on me".

This example shows you how to create a single page group. The paging group is for the marketing team and is made up of extensions **1001**, **1002** and **1003**. The example also gives the right to any member of authority group **Basic** (all extensions in our configuration) to call the page group. The page group number is **888**, it is also configured with a PIN code **4444** so that only the people who know the code can page the **Marketing** group.

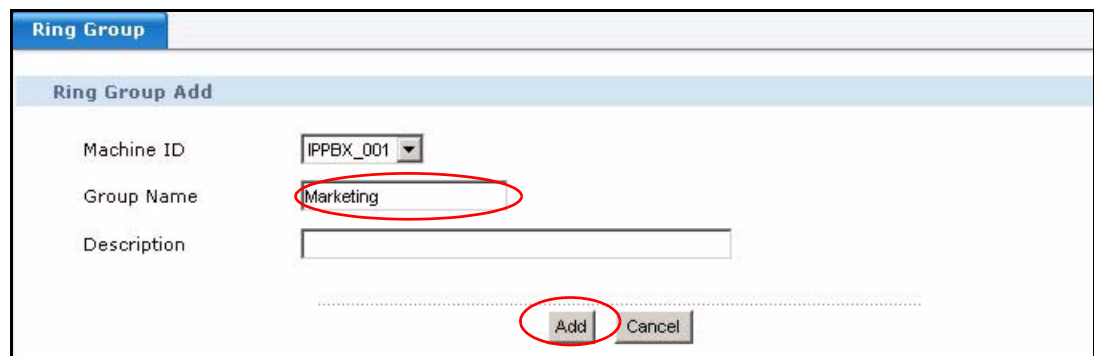
Figure 115 Paging Group Example



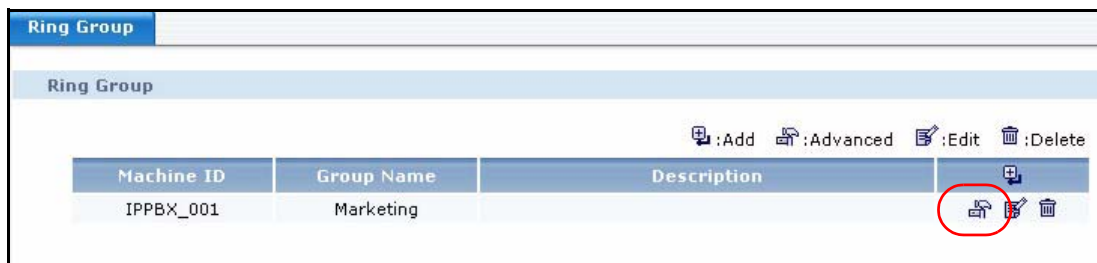
- 1 In the web configurator, click **Configuration > PBX > Extension Management > Ring Group** to open the following screen.



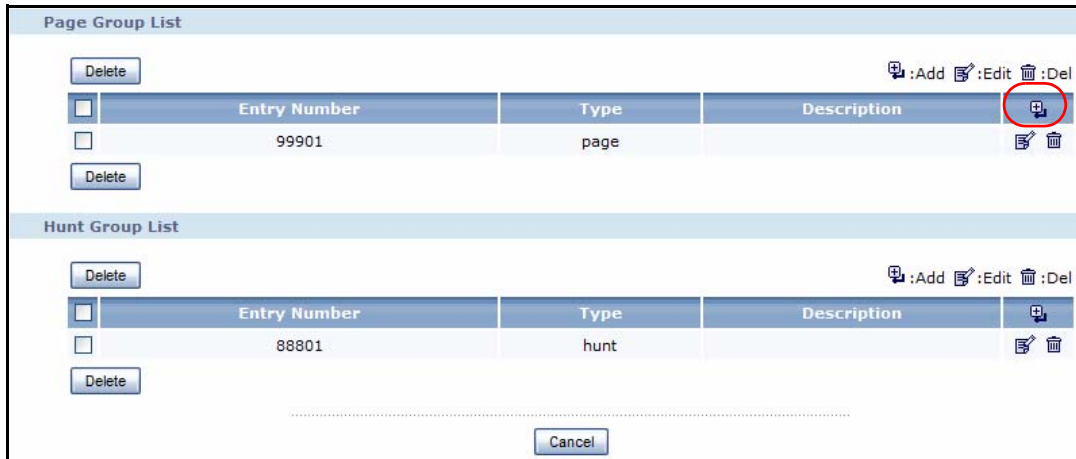
- 2 Click the **Add** icon to open the following screen. Type **Marketing** in the Group Name field and **Add** to save the ring group.



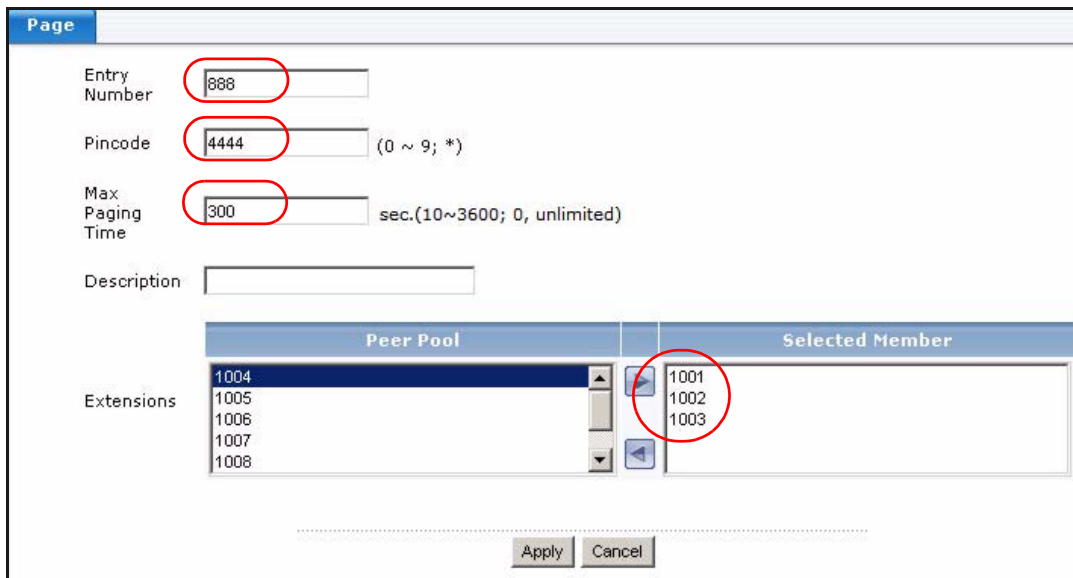
- 3 The **Ring Group** screen appears as shown. Click the **Advanced** icon next to the **Marketing** ring group entry.



- The configuration screen for the **Marketing** ring group opens up. Click **Add** in the **Page Group List** section.



- The **Page** screen opens up. Type **888** in the **Entry Number** field, **4444** in the **Pincode** field and **300** in the **Max Paging Time** field (this last entry keeps the paging time to a maximum of five minutes). Next, highlight the extensions you want to belong to the **Marketing** page group one at a time and use the **Right** icon to move them to the **Selected Member** column.



- Click **Apply** when you are done.

14.2 The Ring Group Screen

Use this screen to set up ring groups on the X6004. To access this screen, click **Configuration > PBX > Extension Management > Ring Group**.

Figure 116 Extension Management > Ring Group

Machine ID	Group Name	Description	
IPPBX_001	Sales	Sales	[Add] [Advanced] [Edit] [Delete]
IPPBX_001	RD	RD	[Add] [Advanced] [Edit] [Delete]

Each field is described in the following table.

Table 70 Extension Management > Ring Group

LABEL	DESCRIPTION
Machine ID	This field displays the ID of the X6004 on which a ring group is configured.
Group Name	This field displays the name assigned to this ring group.
Description	This field displays the description of the ring group.
Add, Advanced, Edit, Delete	Click: <ul style="list-style-type: none"> • Add - to create a new ring group. • Advanced - to configure the settings of a ring group. • Edit - to change the description of a ring group. • Delete - remove an existing ring group.

14.2.1 The New Ring Group Screen

Use this screen to create a new ring group. To access this screen, click **Configuration > PBX > Extension Management > Ring Group > Add**.

Figure 117 Ring Group > Add

Add Ring Group

Machine ID:

Group Name:

Description:

Each field is described in the following table.

Table 71 Ring Group > Add

LABEL	DESCRIPTION
Add Ring Group	
Machine ID	Select the ID of the X6004 on which you want to configure the ring group. This is an internal name (not configurable) of the X6004. Only one choice is shown if you have not configured ZyStack.
Group Name	Type the name of this ring group. You can use alpha-numeric characters and spaces are not allowed.
Description	Type the description for this ring group. You can use alpha-numeric characters and spaces are allowed.
Add	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

14.2.2 The Edit Ring Group Screen

Use this screen to change the description for a ring group. To access this screen, click **Configuration > PBX > Extension Management > Ring Group > Edit**.

Figure 118 Ring Group > Edit

Each field is described in the following table.

Table 72 Ring Group > Edit

LABEL	DESCRIPTION
Ring Group Edit	
Group Name	This field displays the name of this ring group.
Description	Type the description for this ring group. You can use alpha-numeric characters and spaces are allowed.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

14.2.3 The Configure Ring Group Screen

Use this screen to create paging groups, hunt groups or both. To access this screen, click **Configuration > PBX > Extension Management > Ring Group > Advanced**.

Figure 119 Ring Group > Advanced

The screenshot displays the 'Ring Group > Advanced' configuration interface. It is divided into two main sections: 'Page Group List' and 'Hunt Group List'. Each section features a 'Delete' button on the left and a set of icons (Add, Edit, Delete) on the right. Below these buttons is a table with three columns: 'Entry Number', 'Type', and 'Description'. In the 'Page Group List', there is one entry with 'Entry Number' 99901 and 'Type' 'page'. In the 'Hunt Group List', there is one entry with 'Entry Number' 88801 and 'Type' 'hunt'. A 'Cancel' button is located at the bottom center of the screen.

Each field is described in the following table.

Table 73 Ring Group > Advanced

LABEL	DESCRIPTION
Page Group List	Use this section to manage page groups.
Delete	Check the Delete box(es) and click Delete to remove page group(s).
Entry Number	This field displays the number you have to dial to call the extensions in this page group.
Type	This field displays "page".
Description	This field displays the description for this page group.
Add, Edit, Delete	Click: <ul style="list-style-type: none"> • Add - to create a new page group. • Edit - to configure the settings of a page group. • Delete - remove an existing page group.
Hunt Group List	Use this section to manage hunt groups.
Delete	Check the Delete box(es) and click Delete to remove hunt groups.
Entry Number	This field displays the number you have to dial to call the extensions in this hunt group.
Type	This field displays "hunt".

Table 73 Ring Group > Advanced (continued)

LABEL	DESCRIPTION
Description	This field displays the description for this hunt group.
Add, Edit, Delete	Click: <ul style="list-style-type: none"> • Add - to create a new hunt group. • Edit - to configure the settings of a hunt group. • Delete - remove an existing hunt group.

14.2.4 The Add/Edit Page Group Screen

The screens for editing or adding page groups on the X6004 contain the same fields. Only the screen used to add page groups is shown below. Click the **Add** (or **Edit**) icon in the **Paging** section of the **Ring Group** configuration screen to view the screen as shown.

Figure 120 Add/Edit Page Group

Each field is described in the following table.

Table 74 Add/Edit Page Group

LABEL	DESCRIPTION
Entry Number	Type the number you have to dial to call the extensions in this page group. This number can be from 3 to 10 digits long.
Pincode	Type the password you have to dial to call the extensions in this page group. This number can be 3-10 digits long. If you leave this field blank then callers do not have to dial a Pincode to call the extensions in this page group.
Max Paging Time	Type the maximum number of seconds that a person can page a group of extensions. Use 0 to set the paging time to "unlimited".
Description	Type a description for this page group.

Table 74 Add/Edit Page Group (continued)

LABEL	DESCRIPTION
Extensions	Move the extensions you want to be in this page group to the Selected Member column by highlighting them in the Peer Pool column and clicking the Right icon. Remove the extensions you don't want to be in this page group from the Selected Member column by highlighting them and clicking the Left icon.
Apply	Click Apply to save your changes and to apply them to the X6004.
Cancel	Click Cancel to go back to the Ring Group configuration page without saving your changes.

14.2.5 The Add/Edit Hunt Group Screen

The screens for editing or adding hunt groups on the X6004 contain the same fields. Only the screen used to add hunt groups is shown below. Click the **Add** (or **Edit**) icon in the **Hunt** section of the **Ring Group** configuration screen to view the screen as shown.

Figure 121 Add/Edit Hunt Group

Hunt Group Setting

Entry Number

Description

Ring Algorithm

Music on Hold Ring Tone System MOH

Time Out (sec.)

Office Hours

Peer Pool	Selected Member
5000	
5002	
5004	
5006	
5008	

Night Service

Peer Pool	Selected Member
5000	
5002	
5004	
5006	
5008	

Each field is described in the following table.

Table 75 Add/Edit Hunt Group

LABEL	DESCRIPTION
Entry Number	Type the number you have to dial to call the extensions in this hunt group. This number can be from 3-10 digits long.
Description	Type a description for this hunt group.
Ring Algorithm	<p>Select the method for the X6004 to decide the ring order of extensions in this hunt group.</p> <ul style="list-style-type: none"> • Ring All - ring all extensions at the same time until one answers. • Round Robin - take turns ringing each available (not engaged) extension in the hunt group. Start with the first extension (top in the Selected Member column) in this group. • Least Recent - ring the extension which was least recently called in this group. • Fewest Calls - ring the extension with fewest completed calls in this group. • Random - ring a random extension.
Music On Hold	<p>Select the Music on Hold a caller hears when being placed on hold with an extension from this hunt group.</p> <ul style="list-style-type: none"> • Ring Tone - The caller hears the system ring tone. • System MOH - The caller hears the music file selected from the associated menu.
Time Out	Set the duration in seconds for the call to be sent around the hunt group before the X6004 hangs up.
Office Hours	<p>Select the extensions that you want to be in this hunt group during the office hours period you configured for the X6004. (See Chapter 12 on page 193.)</p> <p>Move the extensions you want to be in this hunt group to the Selected Member column by highlighting them in the Peer Pool column and clicking the Right icon.</p> <p>Remove the extensions you don't want to be in this hunt group from the Selected Member column by highlighting them and clicking the Left icon.</p>
Night Service	<p>Select the extensions that you want to be in this hunt group in the off hours period (not during office hours) you configured for the X6004. (See Chapter 12 on page 193.)</p> <p>Move the extensions you want to be in this hunt group to the Selected Member column by highlighting them in the Peer Pool column and clicking the Right icon.</p> <p>Remove the extensions you don't want to be in this hunt group from the Selected Member column by highlighting them and clicking the Left icon.</p>
Apply	Click Apply to save your changes and to apply them to the X6004.
Cancel	Click Cancel to go back to the Ring Group configuration page without saving your changes.

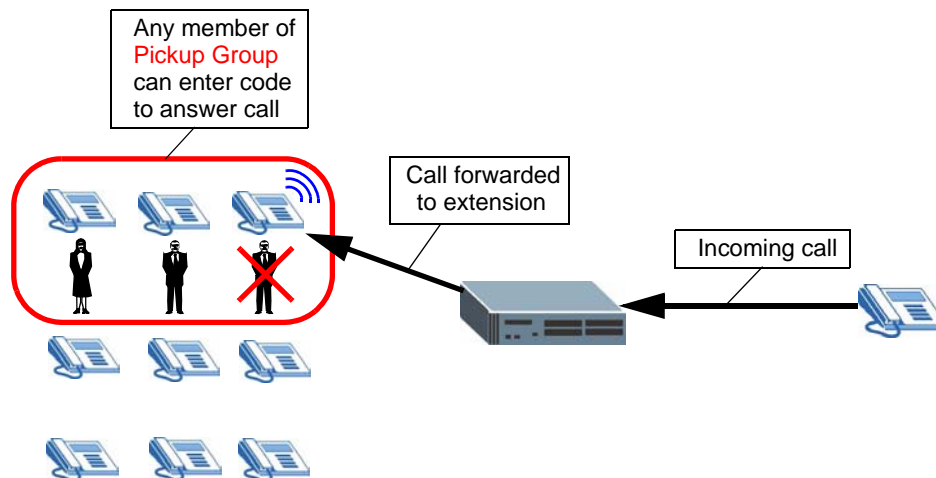
Pickup Group

15.1 Overview

This chapter shows you how to configure and manage pickup groups on the X6004.

The X6004 allows you to organize sets of extensions into pickup groups. All telephone users with extensions in the same pickup group can answer incoming calls for any member of that group. For example, you may want to configure a pickup group for your sales department. If a call comes in to one salesperson but they are not available to answer the call, then another member of the sales team can pick up the call. The members pick up the call by dialing the feature code for **Group Pickup**.

Figure 122 Group Pickup Overview



15.1.1 What You Can Do in this Chapter

Use the **Pickup Group** screen to create and edit the groups of extensions that can answer one another's calls. See [Section 15.2 on page 241](#).

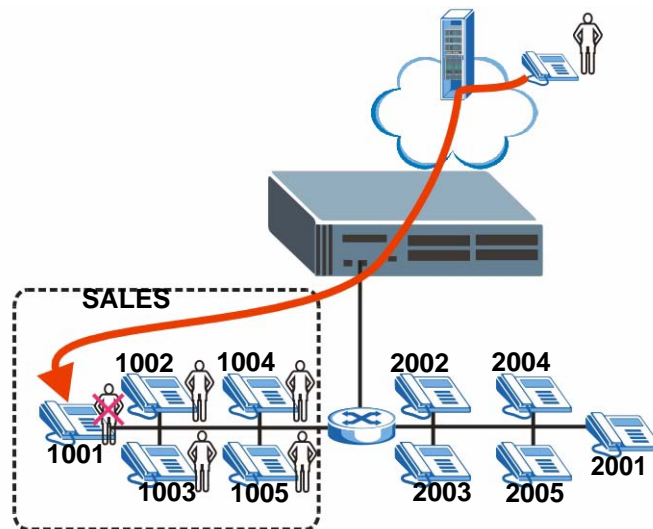
15.1.2 Before You Begin

When you configure the X6004's pickup groups, a group member needs to enter a specific feature code to pick up another group member's call. See [Section 6.8 on page 141](#) for information on how to configure the X6004's feature codes.

15.1.3 Pickup Group Example

The following figure shows a pickup group called **SALES**. Extensions 1001 - 1005 are in the **SALES** pickup group. When a call comes in to extension 1001, then people with extensions 1002, 1003, 1004 or 1005 can pickup the call by dialing the feature code for **Group Pickup** (for example ***94** is the default). Similarly, when a call comes in to any of the other extensions in this pickup group, then any of the group members can pick up that call.

Figure 123 Pickup Group Overview



When two calls come in at the same time, then the call that has rung the longest is picked up first when a group member dials the **Group Pickup** code.

When two group members try to pick up a call for someone in their pickup group, then the first person to dial the **Group Pickup** code answers the call.

15.2 The Pickup Group Screen

Use this screen to manage pickup groups on the X6004. To access this screen, click **Configuration > PBX > Extension Management > Pickup Group**.

Figure 124 Extension Management > Pickup Group

	Machine ID	Group name	Description	
<input type="checkbox"/>	IPPBX_001	pickupgroup	pickupgroup	

Each field is described in the following table.

Table 76 Extension Management > Pickup Group

LABEL	DESCRIPTION
Delete	Select the Delete box and click Delete to remove this pickup group from the X6004.
Machine ID	This field displays the Machine ID on which this pickup group is configured.
Group name	This field displays a pickup group name configured on the X6004.
Description	This field displays a description given to this pickup group.
Add, Edit, Delete	Click: <ul style="list-style-type: none"> • Add - to set up a new pickup group on the X6004. • Edit - to change the pickup group settings of an existing pickup group. • Delete - remove a pickup group from the X6004.

15.2.1 Add/Edit Pickup Groups

Use the **Add Group** screen to create a new pickup group. Use the **Edit Group** screen to add or remove extensions from a pickup group. To access this screen, click the **Add** or **Edit** icon in the **Configuration > PBX > Extension Management > Pickup Group** screen. Only the Add Group screen is shown.

Figure 125 Pickup Group > Add/Edit

Each field is described in the following table.

Table 77 Pickup Group > Add/Edit

LABEL	DESCRIPTION
Pickup Group	
Machine ID	Select the X6004 on which you want to configure this pickup group. This field is read-only when editing an existing pickup group.
Group name	Type a name for this pickup group. Use alpha-numeric characters. This field is read-only when editing an existing pickup group.
Description	Type a description for this pickup group. Use alpha-numeric characters. This field is read-only when editing an existing pickup group.
Extensions Select	Click on an extension in the Extensions Pool column to highlight it and use the Right icon to move it to the Extensions Select column. This adds this extension to the pickup group. Click on an extension in the Extensions Select column to highlight it and use the Left icon to move it to the Extensions Pool column. This removes this extension from the pickup group.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to go back to the previous screen.

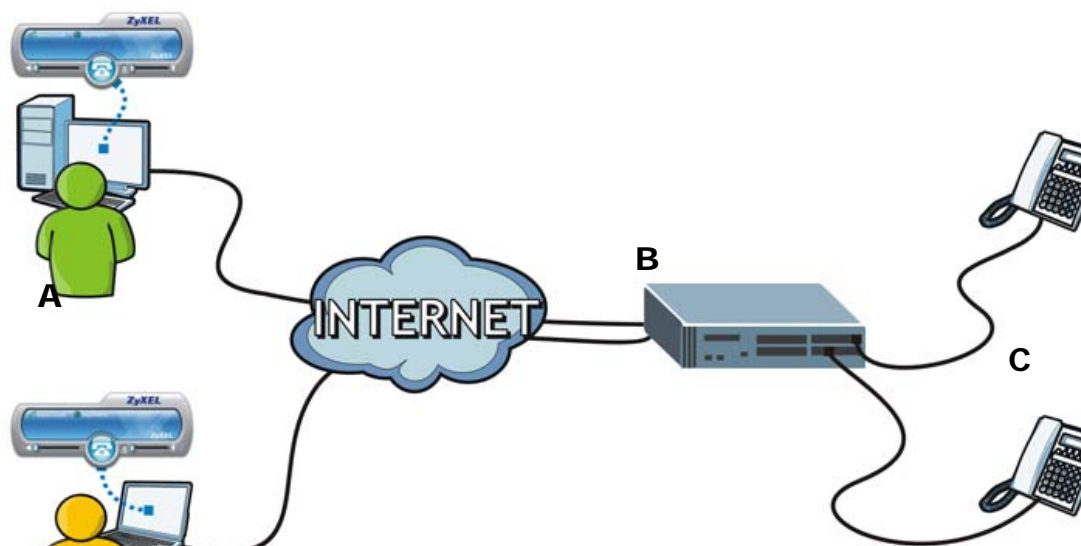
Click-To-Talk Group

16.1 Overview

This chapter shows you how to configure Click-To-Talk (CTT) groups to answer calls sent over the Internet with a web-based IP phone.

The CTT feature allows you to place a specially created HTML link on a Web page which a user can then click to connect directly to a live extension on the other end. This communication uses the SIP voice protocol with a web-based IP phone client handling the connection on the caller's side and the X6004 routing the connection to the recipient's phone on the other.

Figure 126 A Click-To-Talk Example



For example, when a user **A** clicks on an embedded Click-To-Talk link on a company's online ordering web page, the web-based IP phone opens. Next, the phone dials into X6004 **B**, which in turn routes the call to extension **C**. Both **A** and **C** can then talk to one another over the Internet as if they were talking by an actual phone. (The web phone only works if the caller's web browser supports it and they have a functional microphone attached to their computer.)

16.1.1 What You Can Do in this Chapter

Use the **Click-To-Talk** screen to set up CTT groups and their associated extensions. See [Chapter 16 on page 246](#).

16.1.2 Before You Begin

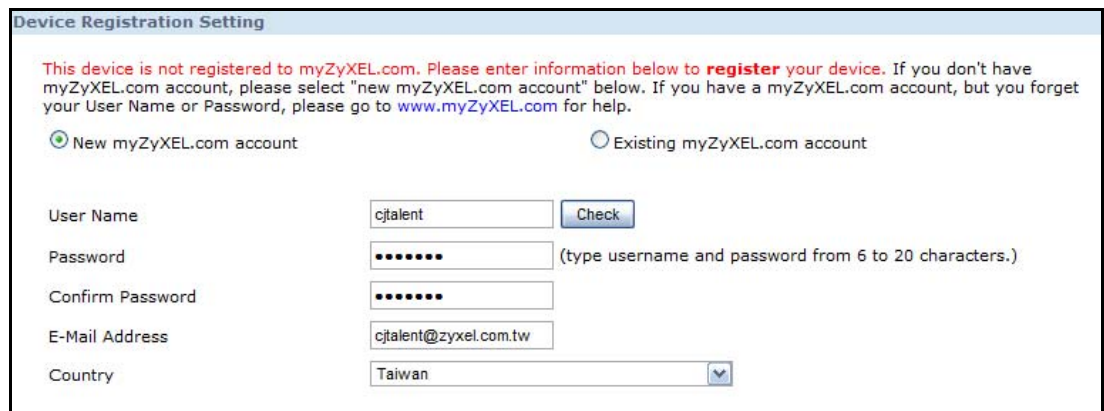
Be sure that you have purchased a license for the number of CTT extensions you want to use, and that your registration information on the License page is up to date. See [Chapter 16 on page 243](#) for more information on License management.

16.1.2.1 Registering Your Click-To-Talk License

To use the Click-To-Talk feature, you must have a valid license key for the number of CTT accounts that you wish to enable. You can get a license by purchasing a Click-To-Talk iCard from your local ZyXEL product vendor.

To register your license:

- 1 Log into the X6004, then click **Maintenance > License Control > Registration**.
- 2 On the **Configuration** tab select **New myzyxel.com account** then fill out all the required fields; click **Apply** when you are finished. You can skip this step if you already have a myzyxel.com account.



The screenshot shows the 'Device Registration Setting' form. At the top, there is a red warning message: 'This device is not registered to myZyXEL.com. Please enter information below to register your device. If you don't have myZyXEL.com account, please select "new myZyXEL.com account" below. If you have a myZyXEL.com account, but you forget your User Name or Password, please go to www.myZyXEL.com for help.' Below the message are two radio buttons: 'New myZyXEL.com account' (selected) and 'Existing myZyXEL.com account'. The form fields are: 'User Name' (cjtalent) with a 'Check' button; 'Password' (masked with dots) with a note '(type username and password from 6 to 20 characters.)'; 'Confirm Password' (masked with dots); 'E-Mail Address' (cjtalent@zyxel.com.tw); and 'Country' (Taiwan).

- 3 On the **Service** tab, enter your Click-To-Talk **License Key** then click **Update**. The X6004 checks to confirm it is valid. As soon as it completes this check, the Click-To-Talk **Quantity** updates, indicating the number of CTT accounts your license grants you.

The screenshot shows the 'Service Management' interface. It features a table with two columns: 'Service' and 'Quantity'. The 'Quantity' column is circled in red. Below the table is a 'License Upgrade' section with a 'License Key' field containing 'CT01-2212D37F2E0AE82' and an 'Update' button, both circled in red. A 'Service License Refresh' button is also visible.

Service	Quantity
Extension Number	32
Soft Phone Number	8
Click To Talk Number	0
Attendant Console Number	0

License Upgrade

License Key :CT01-2212D37F2E0AE82

(Sync with myZyXEL.com to download license info.)

- 4 You can check or update your license account at any time by logging into myzyxel.com.

The screenshot shows the myZyXEL.com login page. The 'Log In' section is circled in red. It includes fields for 'Username' and 'Password', a 'Remember Username' checkbox, and 'Login' and 'Cancel' buttons. The page also features a 'WELCOME' sidebar, a 'Spotlights' section with product images, and an 'Announcement' section with a list of updates.

myZyXEL.com

WELCOME

Log In /

Welcome to myZyXEL.com

myZyXEL.com provides an easy-to-use service management platform where you can manage your ZyXEL product registrations and services using your personal account.

The ZyXEL products which can be registered at myZyXEL.com are as follows:

ZyWALL Series	which support Content Filter, Anti-Virus, IDP, Anti-Spam and VPN
P662H series and P662HW series	which support Anti-Virus and Content Access Control
HS100/HS100W	which support Content Filter
Vantage series	which include Vantage CNM, Vantage Report and Vantage Access
NetAtlas Access EMS	which support device management

Please register your account at myZyXEL.com first.

Log In

Username: > Forget User Name / Password? [Click here](#)

Password:

Remember Username:

Spotlights

mySecurity Zone

Announcement More...

01/21/09 - AV/IDP iCard/E-iCard EOS and EOL

01/01/09 - P-662H/HW series Anti-Virus iCard EOS and EOL

09/23/08 - Anti-Spam iCard/E-iCard EOS and EOL

09/23/08 - IDP 10 iCard/E-iCard EOS and EOL

ZyXEL | Privacy Statement Version 3.3.02.60.00 (C) Copyright 1995-2008 by ZyXEL Communications Corp.

Note: Although you can embed as many of the web-based clients as you want in your web pages, the maximum number of unique numbers they can call is based on the number of clients allowed by your license.

16.2 The Click-To-Talk Group Screen

This screen allows you to set up CTT groups and their associated extensions. A CTT group is not related to an Authority Groups; it is created solely for the purpose of connecting calls placed with the web-based utility on a web page to the related extensions.

Click **Configuration > PBX > Extension Management > Click-To-Talk** to open this screen.

Figure 127 Extension Management > Click-To-Talk Group

Machine ID	Group Name	Description	
IPPBX_001	Customer_Support	Support for the XJ-20 Series	

Each field is described in the following table.

Table 78 Click-To-Talk Group List

LABEL	DESCRIPTION
Machine ID	This indicates the X6004 with which the group is associated.
Group Name	This indicates the name of the CTT group.
Description	This displays the description associated with the CTT group.
Delete	Click this button to remove any selected entries from the list.
Add	Click this to open the Click-To-Talk Group Setting screen, where you can add a CTT group to the list.
Edit	Click this to open the Click-To-Talk Group Setting screen, where you can modify an existing CTT group's information.

16.2.1 Add a Click-To-Talk Group

Use this screen to create a CTT group.

Click the **Add** icon in the **Click-To-Talk Group** screen to display the options as shown next.

Figure 128 Click-To-Talk Group Settings

Each field is described in the following table.

Table 79 Click-To-Talk Group Settings

LABEL	DESCRIPTION
Machine ID	Specify the X6004 for which you want to create a Click-To-Talk group.
Group Name	Enter a name for this CTT group, using up to 20 alphanumeric characters (a-z, A-Z, 0-9); underscores (_) are allowed while spaces and hypens are not.
Description	Enter a description for this CTT group, using up to 63 alphanumeric characters (a-z, A-Z, 0-9).
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

16.2.2 Edit a Click-To-Talk Group

Use this screen to edit a CTT group.

Click the **Edit** icon in the **Click-To-Talk Group** screen to display the options as shown next.

Figure 129 Click-To-Talk Group Settings

Each field is described in the following table.

Table 80 Click-To-Talk Group Settings

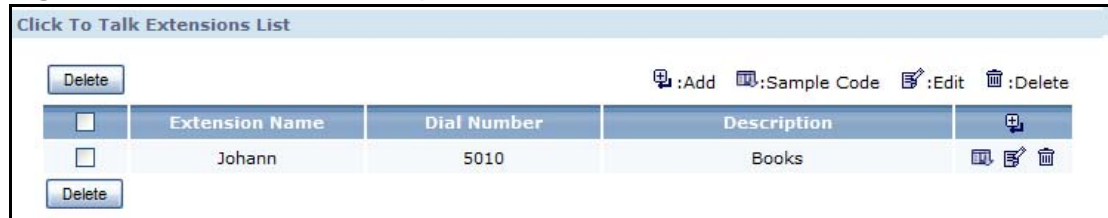
LABEL	DESCRIPTION
Group Name	This indicates the name of this CTT group.
Description	Enter a description for this CTT group, using up to 63 alphanumeric characters (a-z, A-Z, 0-9).
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

16.2.3 Manage Click-To-Talk Group Extensions

Use this screen to manage extensions belonging to a single CTT group.

Click the **Advanced** icon in the **Click-To-Talk Group** screen to display the options as shown next.

Figure 130 Click-To-Talk Group Extensions List



Each field is described in the following table.

Table 81 Click-To-Talk Group Extensions List

LABEL	DESCRIPTION
Delete	Click this button to remove any selected entries from the list.
Select	Check a box in an entry row to flag it for deletion.
Add	Click this to open the Click-To-Talk Extension Setting screen, where you can add an extension to this CTT list.
Edit	Click this to open the Click-To-Talk Extension Setting screen, where you can modify an existing extension's CTT information.
Sample Code	Click this to generate code for the extension which you can use to embed the ZyXEL web-based IP phone client in a web page.
Extension Name	This indicates the CTT extension name.
Dial Number	This indicates the extension associated with this CTT item. This extension must correspond to an existing authority group extension and the dialed number should be authorized in Group Management . For more information on extensions and authority groups, see Chapter 13 on page 197 .
Description	This displays the description associated with this CTT extension.
Cancel	Click this to go back to the previous screen.

16.2.3.1 Sample HTML for a Click-To-Talk Extension

This is the basic Javascript and HTML code used to embed the ZyXEL web-based IP phone client in a web page.

```
<script lang="JavaScript" src="http://WEB_SERVER_ADDR/ctt.js"></script>
<a href=
"javascript:Click_to_Talk('WEB_SERVER_ADDR','dicompjrwma7352)yshvpdgg@wm4rV
q[8&yuhvuhgrhx?zo3qTpZ:(vitvitltcghr@595246.542344<5483*fwqfypsfa5)uuhvkgAL
olcqr(wynqinlt?474165173.533*vxrnhprrvv@82)'">Click_to_Talk</a>
```

Note: You must replace both WEB_SERVER_ADDR strings in the sample code with your own company's website. For example, "www.zyxel.com".

Note: If you change your dial number or WAN IP address, then you must regenerate the sample code.

Note: Makes sure the following four files are in a single location: ctt.js, ctt.html, clicktotalk.cab and clicktotalk.swf.

Once you embed the link, a visitor to your website can then click it and open the web-based IP phone to speak directly to person at the other end.

Figure 131 Sample CTT Web Page



16.2.4 Click-To-Talk Extension Settings

Use this screen to create or edit extensions belonging to a single CTT group.

Click either the **Add** or **Edit** icons in the **Click-To-Talk Group Extensions** screen to display the options as shown next.

Figure 132 Edit a Click-To-Talk Extension

The screenshot shows a dialog box titled "Click To Talk Extension Setting". It has three input fields: "Extension Name" containing "abcde", "Dial Number" containing "1111", and "Description" which is empty. Below the fields, there are two buttons: "Apply" and "Cancel".

Each field is described in the following table.

Table 82 Edit a Click-To-Talk Extension

LABEL	DESCRIPTION
Extension	When you Add a new extension, enter the name for this item in the Click To Talk Group Extensions list. When you Edit an existing extension, this field displays the name of the extension and cannot be changed.
Dial Number	This indicates the extension associated with this CTT item. This extension must correspond to an existing authority group extension and the dialed number should be authorized in Group Management . For more information on extensions and authority groups, see Chapter 13 on page 197 .
Description	Enter a description for this CTT extension.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

Group Access Code

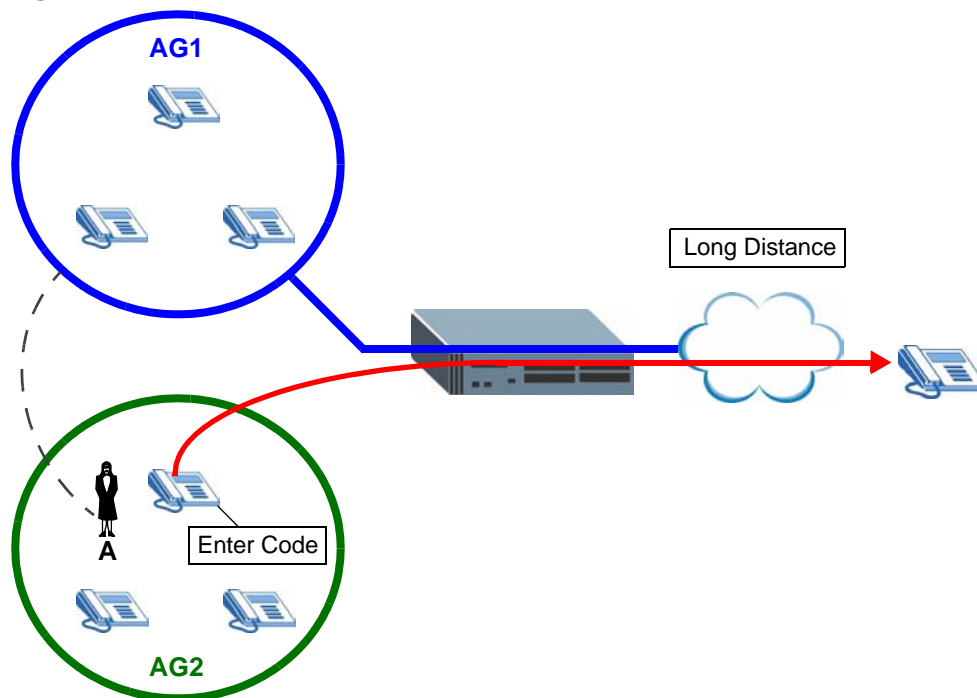
17.1 Overview

This chapter shows you how to configure a group access code for authority groups (see [Chapter 13 on page 197](#) for information on authority groups).

The group access code allows you to use the outbound dialing rules assigned to your authority group from extensions that do not have the same outbound dialing rules assigned to them.

The following figure shows user **A**, who is a member of authority group **AG1** (which has the ability to make long distance calls) moving to a phone belonging to authority group **AG2** (which cannot make long distance calls). She enters the code number and is able to place a call over the long distance connection.

Figure 133 Call Access Code Overview



17.1.1 What You Can Do in this Chapter

Use the **Group Access Code** screen to configure the codes that unlock access to each authority group's privileges. See [Section 17.2 on page 254](#).

17.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Group Access Codes

Group access codes allow your authority group members to use their group's privileges whichever extension they are using.

For example, you belong to an authority group allowed to make both local and long distance calls from your extension. Your secretary, however, belongs to a different authority group and can make only local calls. When you try to make a long distance call from your secretary's extension the X6004 does not allow it and prompts you to enter the access code associated with your authority group. After you enter the access code, your long distance call goes through.

17.2 The Group Access Code Screen

Use this screen to manage the access codes for authority groups on the X6004. To access this screen, click **Configuration > PBX > Extension Management > Group Access Code**.

Figure 134 Extension Management > Group Access Code

The screenshot shows the 'Group Access Code Setting' interface. At the top, there is a section titled 'Group Access Code Setting' with a checkbox labeled 'Enable Group Access Code' which is checked. Below this is an 'Apply' button. The main section is titled 'Group Access Code List' and contains a table with two columns: 'Group' and 'Access Code'. Above the table are buttons for 'Delete', 'Add', 'Edit', and 'Delete'. Below the table is another 'Delete' button.

Group	Access Code

Each field is described in the following table.

Table 83 Extension Management > Group Access Code

LABEL	DESCRIPTION
Enable Group Access Code	Select this to enable the group access code feature.
Apply	Click this to save your changes.
Delete	Check the Delete box and click Delete to remove this call access code setting.
Group	This field displays an authority group name that has been set up with an access code.
Access Code	This field displays the access code.
Add, Edit, Delete	Click one of the following options: <ul style="list-style-type: none"> • Add - to set up an access code for an authority group on the X6004. • Edit - to change the access code for an authority group. • Delete - remove an access code configured for an authority group.

17.2.1 The Group Access Code Screen

Use this screen to edit or create an access code on the X6004. To access this screen, click the **Edit** or **Add** icons in the **Group Access Code** screen.

Figure 135 Group Access Code > Edit/Add

The screenshot shows a form titled "GAC Setting for the Authority Group". It contains two main fields: "Group" and "Access Code". The "Group" field is a dropdown menu currently showing "Sales". The "Access Code" field is a text input box containing the number "12345", with a note "(5 ~ 10 digits)" to its right.

Each field is described in the following table.

Table 84 Access Code > Edit/Add

LABEL	DESCRIPTION
Group	Select the authority group you want to configure a call access code for. You can only create one call access code per authority group.
Access Code	Type the access code for this authority group.
Apply	Click this to save your changes.
Cancel	Click Cancel to return to Group Access Code screen without saving your changes.

Outbound Line Group

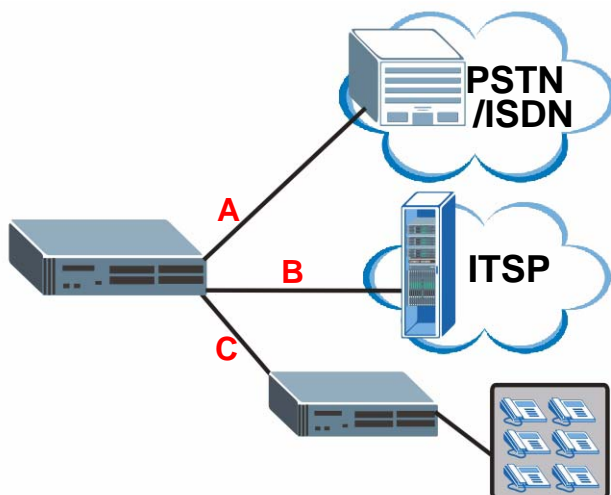
18.1 Overview

This chapter shows you how to manage outside lines on the X6004.

The following diagram shows the X6004 connected to the various types of outside connections:

- FXO/PRI/BRI Trunk (**A**): shows the X6004 connected to the PSTN (Public Switched Telephone Network) or ISDN (Integrated Service Digital Network) via an FXO/PRI/BRI port on the X6004. You can also use the FXO ports to connect to a traditional analog PBX, use the PRI port to connect to a primary rate interface, use the BRI port to connect to a basic rate interface, if your organization has one. You must have an FXO/PRI/BRI interface card installed on the X6004 to configure these connections.
- SIP Trunk (**B**): shows the X6004 connected to a SIP gateway at your VoIP service provider (ITSP: Internet Telephony Service Provider). You can use the SIP trunk to connect to a SIP gateway on which you have an existing SIP account.
- Trusted Peer (**C**): shows the X6004 connected to another X6004 (for example, at your branch office). You can establish a trusted peer connection with another SIP server that lists your X6004 as a trusted peer.

Figure 136 Outbound Line Overview



18.1.1 What You Can Do in this Chapter

Use the **Outbound Line Group** screen to configure settings for your outbound lines including FXO, PRI, BRI, SIP, Trusted Peer trunks. See [Section 18.2 on page 262](#).

18.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Outbound Trunk

The outbound lines define a connection between the X6004 and the PSTN, ISDN, ITSP or your trusted peer (another X6004). To make calls from extensions on your network you still have to define LCRs, which are outbound dialing rules (See [Chapter 20 on page 309](#)). You also have to configure an auto-attendant to handle the forwarding of incoming calls (See [Chapter 19 on page 291](#)).

FXO Trunk

FXO trunks allow you to connect to the PSTN (through your traditional analog telephone service provider) or a traditional analog PBX in your organization.

PRI Trunk

PRI trunk allows you to connect to the ISDN (through your ISDN telephone service provider) or an ISDN PBX in your organization. PRI trunk also allows you to connect to Channel Associated Signaling (CAS) also referred to as “Robbed Bit” or “in-band” Signaling. The X6004 supports “E&M” (Ear and Mouth) Immediate Start CAS signaling.

BRI Trunk

BRI trunks allow you to connect to the ISDN or an ISDN PBX in your organization.

SIP Trunk

SIP trunks allow you to connect to a VoIP service provider.

Trusted Peer Trunk

Trusted peers refer to connections to another SIP server (for example another X6004) that has configured your X6004 as a trusted peer. Your organization may want to use trusted peer connections between remote branch offices.

Using Multiple ISDN Numbers

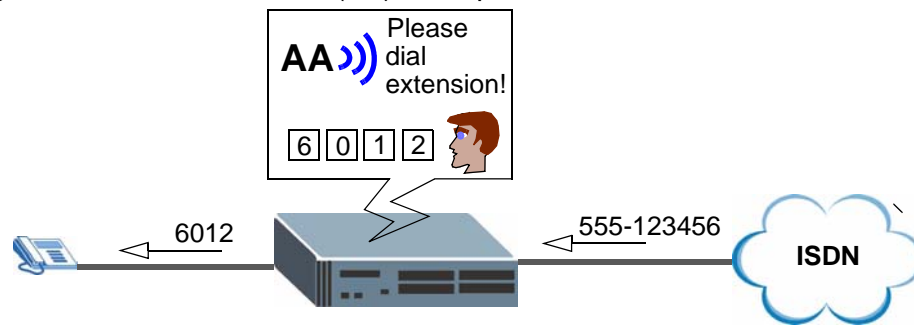
You may have multiple ISDN numbers from your ISDN service provider. You can map these numbers to the AA (Auto Attendant) and directly to extension numbers.

Note: Use AA if you do not have multiple ISDN numbers.

AA (Auto Attendant)

After calling the number, the caller is prompted to dial the extension number.

Figure 137 Auto Attendant (AA) Example



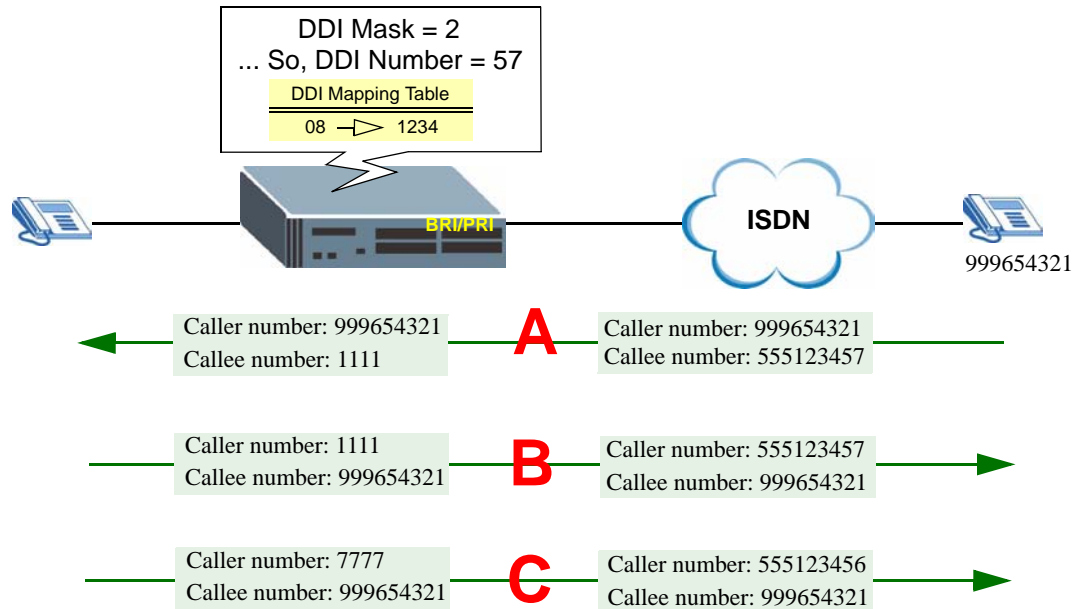
DDI (Direct Dial In)

DDI (also called DID, Direct Inward Dial) is a feature that maps a public number to an extension number. DDI enables a caller to call an extension number without going through an operator. When people give out their contact number and say it's a "direct line", often what they mean is that it's a DDI number.

For example, your company has 10 phone numbers (555-123456~555-123465). You can choose 555-123456 to be the directory number (the company's representative phone number) and map the others to extensions using DDI.

Define 2 digits (from right to left) for the DDI mask. Associate "57" to an extension number (for example, **1111**).

Figure 138 DDI Example



This example also shows three call examples.

A - When an outsider calls **555-123457**, the call is mapped to the extension **1111**.

B - When someone makes an outgoing call from the extension **1111**, the caller ID shown to the callee is **555-123457**.

C - When you make a call over this outbound line from an extension that is NOT listed in the DDI mapping table, the directory number (**555123456** in this example) is the number that displays on the callee's caller ID.

Note: Calls on incoming ISDN numbers that are not included in the DDI mapping table go to the AA.

Calling Directly to an Extension

ISDN calls can be made directly to an extension number from another PBX that is connected directly. In this example, all incoming calls are forwarded to the extension called.

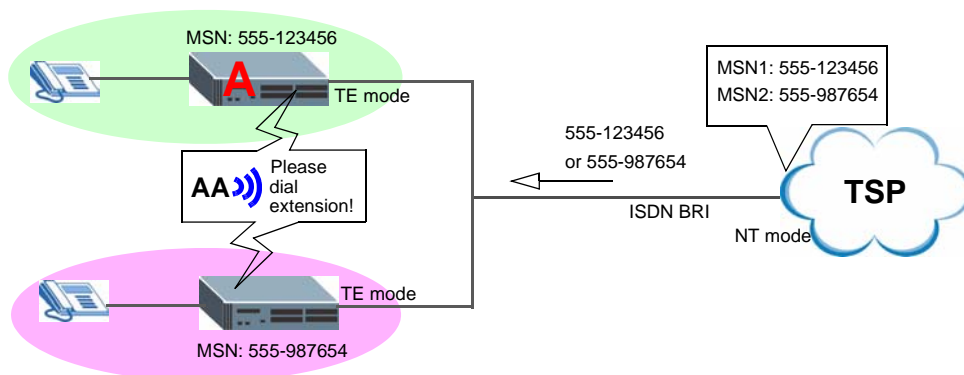
Figure 139 Direct Example



MSNs (Multiple Subscriber Numbers)

This feature is relevant to ISDN BRI (TE mode) only. In this example, two X6004s are connected through a single BRI line to one TSP (Telecommunications Service Provider). Each X6004 has a unique MSN. These MSNs must correspond to those configured on the connected ITSP's ISDN device. Device **A**'s auto-attendant system answers the incoming call only when the number matches the MSN configured on device **A**.

Figure 140 MSN Example



18.1.3 Before You Begin

Before you start to configure an outbound line group, please consider the following.

- In order to create an FXO/BRI/PRI trunk you must already have a corresponding interface card installed on the X6004. See the Quick Start Guide for information on installing your interface cards.

- In order to create a SIP trunk you must already have a SIP account and a network connection to your VoIP service provider.
- In order to create a Trusted Peer trunk you must already have a SIP server's information (for example, IP address) and a network connection to the peer device.

18.2 Outbound Line Group Screen

Use this screen to manage the outside lines on the X6004. To access this screen, click **Configuration > PBX > Outbound Line Management > Outbound Line Group**.

Figure 141 Outbound Line Management > Outbound Line Group

Outbound Line Group			
FXO Trunk			
:Add :Advanced :Edit :Delete :Auto-Attendant			
Machine ID	Group Name	Description	
IPPBX_001	OG_FXO_EXAMPLE		
PRI Trunk			
Machine ID	Group Name	Description	
IPPBX_001	OG_PRI_EXAMPLE		
BRI Trunk			
Machine ID	Group Name	Description	
IPPBX_001	OG_BRI_EXAMPLE		
SIP Trunk			
Machine ID	Group Name	Description	
IPPBX_001	OG_SIP_EXAMPLE		
Trusted Peer			
Machine ID	Group Name	Description	
IPPBX_001	OG_Trusted_EXAMPLE		

Each field is described in the following table.

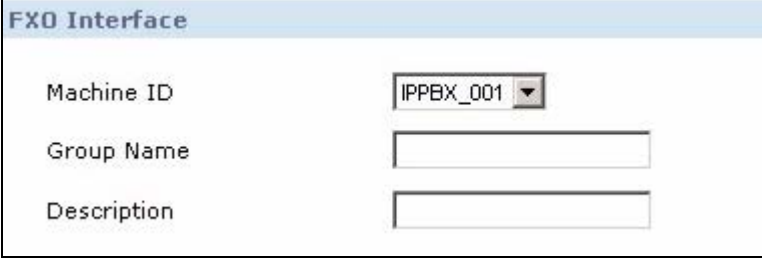
Table 85 Outbound Line Management > Outbound Line Group

LABEL	DESCRIPTION
FXO Trunk / PRI Trunk / BRI Trunk / SIP Trunk / Trusted Peer	<p>These headings divide the screen into sections based on the type of outside line you have configured:</p> <ul style="list-style-type: none"> • FXO Trunk - refers to a connection from the X6004 to the PSTN (your local telephone company) via the FXO port on the X6004. • PRI Trunk - refers to a connection from the X6004 to the ISDN T1 or E1 trunk line via the PRI port on the X6004. • BRI Trunk - refers to a connection from the X6004 to the basic rate ISDN trunk line via the BRI port on the X6004. • SIP Trunk - refers to a connection from the X6004 to a SIP server at your VoIP service provider. • Trusted Peer - refers to a connection to another SIP server (for example another X6004) that has configured your X6004 as a trusted peer.
Machine ID	This field displays the ID of the X6004 on which an outside line is configured.
Group Name	This field displays the name of an outside line.
Description	This field displays the description for an outside line.
Add, Advanced, Edit, Delete, Auto Attendant	<p>Select from one of the following choices:</p> <ul style="list-style-type: none"> • Add - to create a new outbound line group. • Advanced - to configure the settings of an outbound line group. • Edit - to change the description of an outbound line group. • Delete - to remove an existing outbound line group. • Auto Attendant - to assign an auto attendant to an outbound line group.

18.2.1 Add/Edit FXO Trunk

The screens for editing or adding FXO trunks on the X6004 contain the same fields. Only the screen used to add FXO trunks is shown below. Click the **Add** (or **Edit**) icon in the **FXO Trunk** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 142 Add/Edit FXO Trunk



The screenshot shows a web interface titled "FXO Interface". It contains three input fields:

- Machine ID:** A dropdown menu with "IPPBX_001" selected.
- Group Name:** An empty text input field.
- Description:** An empty text input field.

Each field is described in the following table.

Table 86 Add/Edit FXO Trunk

LABEL	DESCRIPTION
Machine ID	Select the ID of the X6004 on which you want to configure the FXO interface. This is an internal name (not configurable) of the X6004. Only one choice is shown if you have not configured ZyStack. This field is not available when editing an FXO configuration.
Group Name	Type the name of this FXO interface. This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Description	Type the description for this FXO interface. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click Apply to save your changes.
Back to Outbound Group/Cancel	Click this to go to the Outbound Line Group screen without saving your changes.

18.2.2 Configure an FXO Trunk

Use this screen to configure an FXO Trunk. Click the **Advanced** icon in the **FXO Trunk** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 143 Configure an FXO Trunk

Each field is described in the following table.

Table 87 Configure an FXO Trunk

LABEL	DESCRIPTION
Available Interface	This column displays the FXO ports available on the X6004. Highlight one of the FXO ports and click the Right icon if you want to add it to this outbound line group.
Used Interface	This column displays the FXO ports currently configured for this outbound line group. Highlight one of the FXO ports and click the Left icon if you want to remove it from the outbound line group. If you configure more than one interfaces in this outbound line group, the X6004 check and pick one of them available for an outgoing call.
Apply	Click this to save your changes.
Cancel	Click this to go to the Outbound Line Group screen without saving your changes.

18.2.3 Auto-Attendant for Incoming Analog Calls

Use this screen to select which auto-attendant should be used with this outbound line group. See [Chapter 19 on page 291](#) for information on configuring auto-attendant. Click the **Auto-Attendant** icon in the in the **FXO Trunk** section of the **Outbound Group** configuration screen to view the screen as shown.

Figure 144 AA for FXO Trunks

The screenshot shows a configuration window titled 'Apply AA'. It contains two main elements: a dropdown menu and a text input field. The dropdown menu is currently set to 'FAX'. Below it is a text input field labeled 'Extension Number for FAX' which is currently empty.

Each field is described in the following table.

Table 88 AA for FXO Trunks

LABEL	DESCRIPTION
Apply AA	Select the Auto-Attendant you want to use when calls come in on this outbound line group. Select FAX if you want to forward all incoming calls on this outbound line group to a fax machine located at a specific extension. Select Extension if you want to directly forward all incoming calls through this outbound line group to an extension or a hunting group number. Select Skill if you want to forward all incoming calls on this outbound line group to the group of agents associated with this skill name.
Extension Number for Fax	This field is only available if you select FAX in the Apply AA field. Type the extension of the Fax machine you want to forward calls to.

Table 88 AA for FXO Trunks (continued)

LABEL	DESCRIPTION
Extension Number	This field is only available if you select Extension in the Apply AA field. Type an extension or a hunting group number you want to forward calls to.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to go to the Outbound Group screen without saving your changes.

18.3 Add/Edit PRI Trunk

The screens for editing or adding a PRI trunk on the X6004 contain the same fields. Only the screen used to add a PRI trunk is shown below. Click the **Add** (or **Edit**) icon in the **PRI Trunk** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 145 Add/Edit PRI Trunk

Machine ID	IPPBX_001 ▼
Group Name	OG_PRI_EXAMPLE
Description	OG_PRI_EXAMPLE

Each field is described in the following table.

Table 89 Add/Edit PRI Trunk

LABEL	DESCRIPTION
Machine ID	Select the ID of the X6004 on which you want to configure the PRI interface. This is an internal name (not configurable) of the X6004. Only one choice is shown if you have not configured ZyStack. This field is not available when editing an PRI configuration.
Group Name	Type the name of this PRI interface. This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Description	Type the description for this PRI interface. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click Apply to save your changes.
Back to Outbound Group/Cancel	Click this to go to the Outbound Line Group screen without saving your changes.

18.3.1 Configure a PRI Trunk

Use this screen to configure a PRI Trunk. The fields in this screen vary depending on the application type you select in the **Option** field. Click the **Advanced** icon in the **PRI Trunk** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 146 Configure a PRI Trunk - DDI/DID

PRI Trunk Setting

PRI Signal ISDN CAS

Option DDI/DID AA Direct

Directory Number

Available Interface		Used Interface
Slot: <input style="width: 40px;" type="text"/> Port: <input style="width: 40px;" type="text"/>	<input type="button" value="▶"/> <input type="button" value="◀"/>	<input style="width: 100%; height: 30px;" type="text"/>

DDI/DID Mapping

DDI/DID Mask

DDI/DID Number	Extension Number
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>

Outgoing Calling Party Number

Type of Number

Calling Party Number Prefix

Calling Party Number (If not match DDI/DID) Directory Number User Defined

Hide Calling Party Number

Incoming Calling Party Number

Type of Number	Prefix
Unknown	<input style="width: 60px;" type="text"/>
National	<input style="width: 60px;" type="text"/>
International	<input style="width: 60px;" type="text"/>
Network Specific	<input style="width: 60px;" type="text"/>
Subscriber	<input style="width: 60px;" type="text"/>
Abbreviated	<input style="width: 60px;" type="text"/>

Figure 147 Configure a PRI Trunk - AA

PRI Trunk Setting

PRI Signal Option: ISDN CAS
 DDI/DID AA Direct

Available Interface		Used Interface
Slot: <input type="text"/> Port: <input type="text"/>	<input type="button" value="▶"/> <input type="button" value="◀"/>	<input type="text"/>

Incoming Calling Party Number

Type of Number	Prefix
Unknown	<input type="text"/>
National	<input type="text"/>
International	<input type="text"/>
Network Specific	<input type="text"/>
Subscriber	<input type="text"/>
Abbreviated	<input type="text"/>

Figure 148 Configure a PRI Trunk - Direct

PRI Trunk Setting

PRI Signal Option: ISDN CAS
 DDI/DID AA Direct

Available Interface		Used Interface
Slot: <input type="text"/> Port: <input type="text"/>	<input type="button" value="▶"/> <input type="button" value="◀"/>	<input type="text"/>

Calling Party Number

Length:

Trusted Peer:

Incoming Calling Party Number

Type of Number	Prefix
Unknown	<input type="text"/>
National	<input type="text"/>
International	<input type="text"/>
Network Specific	<input type="text"/>
Subscriber	<input type="text"/>
Abbreviated	<input type="text"/>

Each field is described in the following table.

Table 90 Configure a PRI Trunk

LABEL	DESCRIPTION
PRI Signal	Set whether the PRI trunk uses ISDN signaling or CAS (Channel Associated Signaling).
PRI Trunk Setting	Use this section to configure your PRI Trunk settings.
Option	<p>Specify the service type for this trunk.</p> <p>Select DDI/DID (Direct Dialing In) when you want people to use a “direct number” to dial an outgoing call. You can also specify a prefix number in the caller number that might be required by your telephone company for outgoing calls using DDI/DID. See DDI (Direct Dial In) on page 259 for more information.</p> <p>Select AA (Auto-Attendant) for all calls coming through this interface will be switched to the Auto-Attendant system first. See Section 19.1 on page 291 for more information.</p> <p>Select Direct for all calls coming through this interface and from trusted callers will be forwarded to extensions. See Calling Directly to an Extension on page 261 for more information.</p>
Directory Number	Enter one of your ISDN numbers registered to your telephone company. When you make a call over this outbound line from an extension that is NOT listed in the DDI mapping table, the Directory Number is the number that displays on the callee’s caller ID. This field can be 3-20 digits in length.
Available Interface	This column displays the available slots and ports on the X6004. Click one slot and port and then click the Right icon if you want to add it to this group.
Used Interface	<p>This column displays the ports currently configured for this outbound line group. Click one port and click the Left icon if you want to remove it from the group.</p> <p>If you configure more than one interfaces in this outbound line group, the X6004 check and pick one of them available for an outgoing call.</p>
DDI/DID Mapping	Use this section to configure your DDI/DID mapping table.
DDI/DID Mask	Enter a number (1~20) to identify the extension mapping digits from right to left, so a DDI/DID mask of 2 applied to the incoming ISDN number 555-123456 would identify the numbers 56.
DDI/DID Number, Extension Number	<p>Enter the DDI/DID number (like the example 56 above) and its associated extension number (for example, 6012).</p> <p>This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.</p>
Add	Click this to add a DDI/DID mapping rule.
Delete	Click this to delete a DDI/DID mapping rule.
Outgoing Calling Party Number	For a PRI trunk set to use an ISDN signal, use this section to configure your outgoing calling party numbers.

Table 90 Configure a PRI Trunk (continued)

LABEL	DESCRIPTION
Type of Number	Select the type for the prefix number which might be required by your telephone company to make outgoing calls. The options you can select are UNKNOWN , INTERNATIONAL , NATIONAL , NETWORK , SUBSCRIBER , ABBREVIATED .
Calling Party Number Prefix	Enter a number to add in the beginning of the outgoing caller's numbers using this trunk line. This field can be 0-20 digits in length.
Calling Party Number	Use this section to set your outgoing calling party numbers.
Directory Number	Select this to have the PRI trunk use the number defined in the Directory Number field.
User Defined	Select this to have the PRI trunk use another number. Enter the number in the field. This field can be 3-20 digits in length.
Hide Calling Party Number	Select this to not have your calling party number display on the callee's caller ID.
Incoming Calling Party Number	For a PRI trunk set to use an ISDN signal, use this section to configure your incoming calling party numbers.
Type of Number	This indicates the type of incoming call to which you can associate a dialing prefix.
Prefix	Assign a custom prefix to appended to this type of incoming call.
Apply	Click this to save your changes.
Cancel	Click this to go to the Outbound Line Group screen without saving your changes.

18.3.2 Auto-Attendant for Incoming PRI Calls

Use this screen to select which auto-attendant should be used with this outbound line group. See [Chapter 19 on page 291](#) for information on configuring auto-attendant. Click the **Auto-Attendant** icon in the in the **PRI Trunk** section of the **Outbound Group** configuration screen to view the screen as shown.

Figure 149 AA for Incoming PRI Calls

The screenshot shows a configuration window titled "Auto-Attendant". Inside the window, there is a label "Apply AA" on the left and a dropdown menu on the right. The dropdown menu currently displays "Default AA" with a downward-pointing arrow.

Each field is described in the following table.

Table 91 AA for Incoming PRI Calls

LABEL	DESCRIPTION
Apply AA	Select an Auto-Attendant or ACD skill profile used for the calls incoming through this PRI trunk.

Table 91 AA for Incoming PRI Calls (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to go to the Outbound Group screen without saving your changes.

18.4 Add/Edit BRI Trunk

The screens for editing or adding BRI trunks on the X6004 contain the same fields. Only the screen used to add BRI trunks is shown below. Click the **Add** (or **Edit**) icon in the **BRI Trunk** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 150 Add/Edit BRI Trunk

Machine ID	<input type="text" value="IPPBX_001"/>
Group Name	<input type="text"/>
Description	<input type="text"/>

Each field is described in the following table.

Table 92 Add/Edit BRI Trunk

LABEL	DESCRIPTION
Machine ID	Select the ID of the X6004 on which you want to configure the BRI interface. This is an internal name (not configurable) of the X6004. Only one choice is shown if you have not configured ZyStack. This field is not available when editing an BRI configuration.
Group Name	Type the name of this BRI interface. This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Description	Type the description for this BRI interface. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click Apply to save your changes.
Back to Outbound Group/Cancel	Click this to go to the Outbound Line Group screen without saving your changes.

18.4.1 Configure a BRI Trunk

Use this screen to configure a BRI Trunk. The fields vary depending on how the X6004 handles incoming and outgoing calls you configured in the **Option** field. Click the **Advanced** icon in the **BRI Trunk** section of the **Outbound Line Group** configuration screen to view the screen as shown. See [Figure 137](#), [138](#) and [139](#) for similar screens with AA, DDI/DID, Direct additional options when you click AA, DDI/DID or Direct in the Option field in this screen.

Figure 151 Configure a BRI Trunk - AA

The screenshot shows the 'BRI Trunk Setting' configuration screen for the AA option. The 'Option' field is set to AA, with radio buttons for DDI/DID, AA (selected), Direct, and MSN. Below this, there are three columns: 'Available Interface', a central column with two arrow buttons, and 'Used Interface'. The 'Available Interface' column contains 'Slot: Slot D' and 'Port: Port 1' dropdown menus. Below the interface selection is the 'Incoming Calling Party Number' section, which is a table with two columns: 'Type of Number' and 'Prefix'. The 'Type of Number' column lists: Unknown, National, International, Network Specific, Subscriber, and Abbreviated. The 'Prefix' column contains six empty input boxes corresponding to each type.

BRI Trunk Setting	
Option	<input type="radio"/> DDI/DID <input checked="" type="radio"/> AA <input type="radio"/> Direct <input type="radio"/> MSN
Available Interface	Used Interface
Slot: Slot D Port: Port 1	
Incoming Calling Party Number	
Type of Number	Prefix
Unknown	<input type="text"/>
National	<input type="text"/>
International	<input type="text"/>
Network Specific	<input type="text"/>
Subscriber	<input type="text"/>
Abbreviated	<input type="text"/>

Figure 152 Configure a BRI Trunk - MSN

The screenshot shows the 'BRI Trunk Setting' configuration screen for the MSN option. The 'Option' field is set to MSN, with radio buttons for DDI/DID, AA, Direct, and MSN (selected). Below this, there are three fields: 'Number' (empty), 'Used Interface' (empty), and 'Slot: Slot D', 'Port: Port 1', 'MSN: MSN 1' dropdown menus. Below the interface selection is the 'Incoming Calling Party Number' section, which is a table with two columns: 'Type of Number' and 'Prefix'. The 'Type of Number' column lists: Unknown, National, International, Network Specific, Subscriber, and Abbreviated. The 'Prefix' column contains six empty input boxes corresponding to each type.

BRI Trunk Setting	
Option	<input type="radio"/> DDI/DID <input type="radio"/> AA <input type="radio"/> Direct <input checked="" type="radio"/> MSN
Number	<input type="text"/>
Used Interface	Slot: Slot D Port: Port 1 MSN: MSN 1
Incoming Calling Party Number	
Type of Number	Prefix
Unknown	<input type="text"/>
National	<input type="text"/>
International	<input type="text"/>
Network Specific	<input type="text"/>
Subscriber	<input type="text"/>
Abbreviated	<input type="text"/>

Figure 153 Configure a BRI Trunk - DDI/DID

BRI Trunk Setting

Option DDI/DID AA Direct MSN

Directory Number

Available Interface		Used Interface
Slot: Slot D Port: Port 1	▶ ◀	▶ ◀

DDI/DID Mapping

DDI/DID Mask

DDI/DID Number	Extension Number	
<input type="text"/>	<input type="text"/>	+

Outgoing Calling Party Number

Type of Number

Calling Party Number Prefix

Incoming Calling Party Number

Type of Number	Prefix
Unknown	<input type="text"/>
National	<input type="text"/>
International	<input type="text"/>
Network Specific	<input type="text"/>
Subscriber	<input type="text"/>
Abbreviated	<input type="text"/>

Figure 154 Configure a BRI Trunk - Direct

BRI Trunk Setting

Option DDI/DID AA Direct MSN

Directory Number

Available Interface		Used Interface
Slot: Slot D Port: Port 1	▶ ◀	▶ ◀

Trusted Peer List

Length

Trusted Peer	
<input type="text"/>	+

Incoming Calling Party Number

Type of Number	Prefix
Unknown	<input type="text"/>
National	<input type="text"/>
International	<input type="text"/>
Network Specific	<input type="text"/>
Subscriber	<input type="text"/>
Abbreviated	<input type="text"/>

Each field is described in the following table.

Table 93 Configure a BRI Trunk

LABEL	DESCRIPTION
BRI Trunk Setting	
Option	<p>Specify the service type for this BRI trunk.</p> <p>Select DDI/DID (Direct Dialing In) when you want people to use a "direct number" to dial an outgoing call. You can also specify a prefix number in the caller number that might be required by your telephone company for outgoing calls using DDI/DID. See DDI (Direct Dial In) on page 259 for more information.</p> <p>Select AA (Auto-Attendant) for all calls coming through this interface will be switched to the Auto-Attendant system first. See Section 19.1 on page 291 for more information.</p> <p>Select Direct for all calls coming through this interface and from trusted callers will be forwarded to extensions. See Calling Directly to an Extension on page 261 for more information.</p> <p>Select MSN (Multiple Subscribe Number) for all the calls to MSNs coming through this interface will be switched to the Auto-Attendant system first. See Using Multiple ISDN Numbers on page 259 for more information.</p>
Directory Number	<p>Enter your ISDN number registered to your telephone company. This number is used for the caller number when you make an outgoing call through the trunk from the extension which cannot be found in the DDI mapping table. This field can be 3-20 digits in length.</p>
Available Interface	<p>This column displays the available slots and ports on the X6004. Click one slot and port and then click the Right icon if you want to add it to this outbound group.</p>
Used Interface	<p>This column displays the ports currently configured for this outbound line group. Click one port and click the Left icon if you want to remove it from the outbound group.</p> <p>If you configure more than one interfaces in this outbound line group, the X6004 check and pick one of them available for an outgoing call.</p>
DDI/DID Mapping	<p>Use this section to configure your DDI mapping table.</p>
DDI/DID Mask	<p>Enter a number (1~20) to identify the extension mapping digits from right to left, so a DDI mask of 2 applied to the incoming ISDN number 555-123456 would identify the numbers 56.</p>
DDI/DID Number, Extension Number	<p>Enter the DDI number (like the example 56 above) and its associated extension number (for example, 6012).</p> <p>This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.</p>
Add	<p>Click this to add a DDI mapping rule.</p>
Delete	<p>Click this to delete a DDI mapping rule.</p>

Table 93 Configure a BRI Trunk (continued)

LABEL	DESCRIPTION
Outgoing Calling Party Number	
Type of Number	Select the type for the prefix number which might be required by your telephone company to make outgoing calls. The options you can select are UNKNOWN, INTERNATIONAL, NATIONAL, NETWORK, SUBSCRIBER, ABBREVIATED.
Calling Party Number Prefix	Enter a number to add in the beginning of the outgoing caller's numbers using this trunk line. This field can be 0-20 digits in length.
Calling Party Number	The settings in this section are optional. Leave them empty to allow all incoming calls. Alternatively, you can define trusted caller number(s) to filter incoming callers. Then the X6004 only forwards the calls that their caller numbers are listed in the trusted caller table.
Length	Enter a number (1~10) to identify the phone number length for trusted callers.
Trusted Peer	Enter a phone number you accept the caller to dial extensions using this outbound group. Click the Add icon to add a number into the trusted caller table. Click the Delete icon to remove a number. This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.
Incoming Calling Party Number	
Type of Number	This indicates the type of incoming call to which you can associate a dialing prefix.
Prefix	Assign a custom prefix to appended to this type of incoming call.
Apply	Click this to save your changes.
Cancel	Click this to go to the Outbound Line Group screen without saving your changes.

18.4.2 Auto-Attendant for Incoming BRI Calls

Use this screen to select which auto-attendant should be used with this outbound line group. The fields in this screen are the same as the fields in the PRI trunk auto-attendant screen. Refer to [Section 18.3.2 on page 270](#) for detailed field descriptions.

18.5 Add/Edit SIP Trunk

The screens for editing or adding SIP trunks on the X6004 contain the same fields. This section uses the screen “adding a SIP truck” for an example. Click the **Add** (or **Edit**) icon in the **SIP Trunk** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 155 Add/Edit SIP Trunk

Machine ID	IPPBX_001 ▾
Group Name	<input type="text"/>
Description	<input type="text"/>

Each field is described in the following table.

Table 94 Add/Edit SIP Trunk

LABEL	DESCRIPTION
Machine ID	Select the ID of the X6004 on which you want to configure the SIP trunk. This is an internal name (not configurable) of the X6004. Only one choice is shown if you have not configured ZyStack. This field is not available when editing a SIP trunk configuration.
Group Name	Type the name of this SIP trunk. This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Description	Type the description for this SIP interface. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click this to save your changes.
Back to Outbound Group/Cancel	Click this to go to the Outbound Line Group screen without saving your changes.

18.5.1 Configure a SIP Trunk

Use this screen to configure a SIP trunk. Click the **Advanced** icon in the **SIP Trunk** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 156 Configure a SIP Trunk

SIP Trunk Setting

Representative Num	<input type="text"/>
Proxy Server Address	<input type="text"/>
SIP Server Port	<input type="text" value="5060"/>
REGISTER Server Address	<input type="text"/>
REGISTER Server Port	<input type="text" value="5060"/>
Service Domain	<input checked="" type="radio"/> Disable <input type="radio"/> Define service domain: <input type="text"/>
Outbound Proxy	<input checked="" type="radio"/> Disable <input type="radio"/> Define outbound proxy: <input type="text"/>
Outbound Proxy Port	<input type="text" value="5060"/>
DTMF Mode	<input type="text" value="info"/>
Privacy	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Specific Support	<input checked="" type="radio"/> None <input type="radio"/> Nortel (MCS 5100/5200) <input type="radio"/> Huawei <input type="radio"/> Siemens early media support
Proxy Require	<input type="text"/> (Optional.)
Channel-limit	<input type="text" value="8"/> Range (1~128)

Session Timer

<input type="checkbox"/> Enable Session Timer	
Minimum SE :	<input type="text" value="90"/> sec. (90 ~ 1800)
Session Expires :	<input type="text" value="1800"/> sec. (90 ~ 86400, must ≥ Minimum SE)

CallerID Setting

CallerID Viewer	From: "Extension" <Extension@server IP>
CallerID Name & Number	<input checked="" type="radio"/> Extension + Extension <input type="radio"/> Extension + Representative Num <input type="radio"/> Representative Num + Representative Num <input type="radio"/> Extension + Representative Num (DDI/DID mapped) <input type="radio"/> Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped)
The Extension Prefix	<input type="checkbox"/> <input type="text"/>

Authentication

User Name	<input type="text"/>
Password	<input type="text"/>

CODEC Setting

<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">CODEC Pool</div> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> G.728 H.263 H.261 H.264 MP4 </div>	<input type="button" value="▶"/> <input type="button" value="◀"/>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">CODEC List</div> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> G.729 G.711 u-law G.711 a-law </div>	<input type="button" value="↕"/> <input type="button" value="↕"/>
--	--	--	--

Each field is described in the following table.

Table 95 Configure a SIP Trunk

LABEL	DESCRIPTION
SIP Setting	
Representative Num	Enter the phone number that displays to called party if outgoing calls through this outbound line group don't match configured rules associated with the SIP account for this SIP trunk. In the full SIP URI, this is the part before the @symbol. You can use up to 127 printable ASCII characters.
Proxy Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 127 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 127 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field.
Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters. If you choose not to use a service domain, select Disable .
Outbound Proxy	Enter the IP address or domain name of the outbound proxy server provided by your VoIP service provider. You can use up to 127 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server. If you choose not to use an outbound proxy server, select Disable .
Outbound Proxy Port	Enter the outbound proxy's listening port number, if your VoIP service provider gave you one. Otherwise, leave it as the default '5060'. If the outbound proxy is disabled, then this port will be ignored.
DTMF Mode	Control how the X6004 handles the tones that the IP phones on your network make when they push their buttons. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number. You should use the same mode as your VoIP service provider. The choices are: <ul style="list-style-type: none"> • rfc2833 - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • inband - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. • info - Send the DTMF tones in SIP messages.
Privacy	Select Disable to display caller ID as displayed in this screen's CallerID Viewer field. Select Enable to replace the caller's name and number with "Anonymous". For example, "Anonymous" <Anonymous@172.1.1.253>.

Table 95 Configure a SIP Trunk (continued)

LABEL	DESCRIPTION
Specific Support	<p>Select None if you do not need any of the following options:</p> <p>Select Nortel (MCS 5100/5200) to support the specified Nortel SIP server.</p> <p>Select Huawei to support Huawei SIP servers.</p> <p>Select Siemens early media support to turn on support for Siemens early media.</p>
Proxy Require	Enter this (0~127 alphanumeric characters) to inform the SIP server that this device is behind a firewall or NAT device. Fill this field in only if you were given information by your SIP service provider.
Channel-limit	Specify the maximum number of SIP calls (1~128) allowed to be made through this trunk connection at one time.
Session Timer	
Enable Session Timer	Select this activate the X6004's session timer. If you encounter connectivity issues with your network or Internet, then it is suggested that you use the session timer.
Minimum SE	<p>Enter the minimum session expiry time in seconds. The allowable range is 90~1800 seconds.</p> <p>When an incoming call requests a session expiry time that is lower than this, the X6004 uses this value instead.</p>
Session Expires	<p>Enter the session expiry time in seconds for all phone connections on this trunk The allowable range is 90~86400 seconds. This value cannot be lower than the Minimum SE.</p> <p>This allows the X6004 to automatically disconnect any phone calls on this trunk after a certain period of inactivity.</p>
CallerID Setting	<p>Configure this section to change the format of identification you want to send when you make VoIP phone calls.</p> <p>The default format is "From: "Extension"<Extension@Server IP>".</p>
CallerID Viewer	This field displays the caller ID format shown to the callees depending on the setting you configure in the CallerID Name & Number and The Extension Prefix fields.

Table 95 Configure a SIP Trunk (continued)

LABEL	DESCRIPTION
CallerID Name & Number	<p>Select the caller ID display format you want to use when you make calls.</p> <p>A caller ID consists of a call ID name (A), a caller ID number (B) and a SIP server IP address (C). The caller ID has the following format: "A" <B@C>.</p> <p>The choices are:</p> <p>(In the following examples, we assume a company representative number is 12345678, their SIP server IP is 10.1.1.1, a caller extension number is 1111 and DDI/DID number 12345555 can map to the extension 1111.)</p> <ul style="list-style-type: none"> • Extension + Extension: Displays the caller's extension number in A and B. For example, "1111" <1111@10.1.1.1>. • Extension + Representative Num: Displays the caller's extension number in A and the SIP trunk's representative number in B. For example, "1111" <12345678@10.1.1.1>. • Representative Num + Representative Num: Displays the SIP trunk's representative number in A and B. For example, "12345678" <12345678@10.1.1.1>. Select this format if you don't want callees to know the caller's extension number. • Extension + Representative Num (DDI/DID mapped): Displays the caller's extension number in A and the SIP trunk's DDI/DID mapped representative number in B. For example, "1111" <12345555@10.1.1.1>. • Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped): Displays the SIP trunk's DDI/DID mapped representative number in both A and B. For example, "12345555" <12345555@10.1.1.1>.
The Extension Prefix	<p>Specify whether to add a prefix number in the callerID name when you make calls through this trunk connection. The availability of this setting varies depending on the format of CallerID Name & Number you selected.</p> <p>This field can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), colons (:), periods (.), hyphens (-) and plusses (+)</p>
Authentication	
Username	<p>Type the SIP user name associated with this extension. The IP phone registering with the X6004 must provide this for authentication.</p> <p>This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9).</p>
Password	<p>Type the SIP password associated with this extension. The IP phone registering with the X6004 must provide this for authentication.</p> <p>This field can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), plusses (+), periods (.), and "at" symbols (@).</p>

Table 95 Configure a SIP Trunk (continued)

LABEL	DESCRIPTION
Codec Setting	<p>Select the type of voice coder/decoder (codec) that you want this extension to use when communicating with the X6004. The following codecs (shown in highest quality to lowest quality order) are supported by the X6004:</p> <ul style="list-style-type: none"> • G.711 a-law (typically used in Europe) • G.711 u-law (typically used in North America and Japan) • G.729 • G.723.1 - you must activate support for this codec in the Configuration > PBX > Server Configuration > Server > Global screen. • G.726 <p>See Voice Codecs on page 227 for more information on voice codecs.</p> <p>When two SIP devices start a SIP session, they must agree on a codec.</p> <p>If these SIP extensions are assigned to videophones, you must specify the video codecs used for video calls. The X6004 allows the following video codecs to passthrough:</p> <ul style="list-style-type: none"> • H.261 • H.263 • H.264 • MP4 <p>See Video Codecs on page 228 for more information on video codecs.</p>
Codec Pool	<p>This column indicates the codec types not used for these extensions. You can add a codec type to be used for these extensions by highlighting it and clicking the Right button.</p>
Codec List	<p>This column indicates the codec types used by these extensions. You can organize the priority of the codecs by highlighting it and clicking the Up or Down buttons to move the codec higher or lower in priority. The SIP extensions attempt to use the higher priority codecs first and try the lower priority codecs next. You can remove a codec type from being used from these extension by highlighting it and clicking the Left button.</p>
Apply	<p>Click this to save your changes.</p>
Cancel	<p>Click this to set every field in this screen to its last-saved value.</p>

18.5.2 Auto-Attendant for SIP Trunks

Use this screen to select which auto-attendant should be used with this outbound line group. See [Chapter 19 on page 291](#) for information on configuring auto-attendant. You can also configure your DID (Direct Inward Dialing) settings. Click the **Auto-Attendant** icon in the in the **SIP Trunk** section of the **Outbound Group** configuration screen to view the screen as shown.

Figure 157 AA for SIP Trunks

Each field is described in the following table.

Table 96 AA for SIP Trunks

LABEL	DESCRIPTION
Auto-Attendant	
Apply AA	<p>Select the Auto-Attendant you want to use when calls come in on this outbound line group.</p> <p>Select FAX if you want to forward all incoming calls on this outbound line group to a fax machine located at a specific extension.</p> <p>Select Extension if you want to directly forward all incoming calls through this outbound line group to an extension or a hunting group number.</p> <p>Select Skill if you want to forward all incoming calls on this outbound line group to the group of agents associated with this skill name.</p>
Extension Number for Fax	This field is only available if you select FAX in the Apply AA field. Type the extension of the Fax machine you want to forward calls to.
Extension Number	This field is only available if you select Extension in the Apply AA field. Type an extension or a hunting group number you want to forward calls to.
DDI/DID Mapping Setting	

Table 96 AA for SIP Trunks (continued)

LABEL	DESCRIPTION
Representative Number	This field displays the representative number of the SIP trunk if you have configured one in the SIP trunk setting (see Section 18.5.1 on page 277).
Routing by SIP "To" Header	<p>Select Enable if this auto-attendant interacts with a SIP server that uses the SIP To header to do the DDI/DID mapping. If this SIP trunk outbound line group has DDI/DID mode enabled, using this deletes all of the this SIP trunk outbound line group's DDI/DID mapping settings and sets the DDI/DID Mask to 0.</p> <p>Select Disable to use the SIP request URI to do the DDI/DID mapping.</p>
DDI/DID Mask	Enter a number (0~10) to decide the number of digits you want to enter for the next DDI/DID number(s). 0 means you can enter any number of digits for the next DDI/DID number(s).
DDI/DID Number	<p>Enter a DDI/DID number which allows outsiders to call and reach an extension directly. The number of digits you can enter in this field depends on what you set in the Representative Number DDI/DID Mask field.</p> <p>This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.</p>
Extension Number	<p>Select the first radio box and enter the extension number to which the DDI/DID number maps. Alternatively, select Auto-Attendant to forward the matched DDI calls to auto-attendant.</p> <p>This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.</p>
Add	Click this to add a new DDI/DID-to-extension mapping rule.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to go to the Outbound Group screen without saving your changes.

18.6 Add/Edit Trusted Peer

The screens for editing or adding trusted peers on the X6004 contain the same fields. Only the screen used to add a trusted peer is shown below. Click the **Add** (or **Edit**) icon in the **Trusted Peer** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 158 Add/Edit Trusted Peer

Each field is described in the following table.

Table 97 Add/Edit Trusted Peer

LABEL	DESCRIPTION
Machine ID	Select the ID of the X6004 on which you want to configure the trusted peer. This is an internal name (not configurable) of the X6004. Only one choice is shown if you have not configured ZyStack. This field is not available when editing a Trusted Peer configuration.
Group Name	Type the name of this trusted peer connection. This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Description	Type the description for this trusted peer connection. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Apply	Click this to save your changes.
Back to Outbound Group	Click this to go to the Outbound Line Group screen without saving your changes.

18.6.1 Configure a Trusted Peer

Use this screen to configure a trusted peer. Click the **Advanced** icon in the **Trusted Peer** section of the **Outbound Line Group** configuration screen to view the screen as shown.

Figure 159 Trusted Peer Configuration

Trusted Peer Setting

SIP Server Address:

SIP Server Port:

Service Domain: Disable Define service domain:

Outbound Proxy: Disable Define outbound proxy:

Outbound Proxy Port:

DTMF Mode:

Privacy: Disable Enable

Specific Support: None Nortel (MCS 5100/5200) Huawei Siemens early media support

Proxy Require: (Optional.)

Channel-limit: Range (1~128)

Session Timer

Enable Session Timer

Minimum SE : sec. (90 ~ 1800)

Session Expires : sec. (90 ~ 86400, must ≥ Minimum SE)

CallerID Setting

CallerID Viewer: From: "Extension" <Extension@server IP>

Representative Number:

CallerID Name & Number:

- Extension + Extension
- Extension + Representative Num
- Representative Num + Representative Num
- Extension + Representative Num (DDI/DID mapped)
- Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped)

The Extension Prefix:

CODEC Setting

CODEC Pool	CODEC List
G.726	G.729
H.263	G.711 u-law
H.261	G.711 a-law
H.264	
MP4	

Apply Cancel

Each field is described in the following table.

Table 98 Trusted Peer Configuration

LABEL	DESCRIPTION
SIP Server Address	Enter the IP address or domain name of the trusted peer. You can use up to 127 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number. Keep the default value, if you are not sure of this value.

Table 98 Trusted Peer Configuration (continued)

LABEL	DESCRIPTION
Service Domain	Select Disable to not use a SIP service domain or select Define service domain and enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Outbound Proxy	Enter the IP address or domain name of the outbound proxy server provided by your VoIP service provider. You can use up to 127 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server. If you choose not to use an outbound proxy server, select Disable .
Outbound Proxy Port	Enter the outbound proxy's listening port number, if your VoIP service provider gave you one. Otherwise, leave it as the default '5060'. If the outbound proxy is disabled, then this port will be ignored.
DTMF Mode	Control how the X6004 handles the tones that the IP phones on your network make when they push their buttons. One use of the tones is to distinguish between numbers when trying to dial a PSTN phone number. You should use the same mode as your trusted peer. The choices are: <ul style="list-style-type: none"> • rfc2833 - Follow the RFC 2833 standard and send the DTMF tones in RTP packets. • inband - Send the DTMF tones in the voice data stream. This works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) can distort the tones. • info - Send the DTMF tones in SIP messages.
Privacy	Select Disable to display caller ID as displayed in this screen's CallerID Viewer field. Select Enable to replace the caller's name and number with "Anonymous". For example, "Anonymous" <Anonymous@172.1.1.253>.
Specific Support	Select None if you do not need any of the following options: Select Nortel (MCS 5100/5200) to support the specified Nortel SIP server. Select Huawei to support Huawei SIP servers. Select Siemens early media support to turn on support for Seimens early media.
Proxy Require	Enter this (0~127 alphanumeric characters) to inform the SIP server that this device is behind a firewall or NAT device. Fill this field in only if you were given information by your SIP service provider.
Channel-limit	Specify the maximum number of SIP calls (1~128) allowed to be made through this trunk connection at one time.
Session Timer	
Enable Session Timer	Select this activate the X6004's session timer. If you encounter connectivity issues with your network or Internet, then it is suggested that you use the session timer.
Minimum SE	Enter the minimum session expiry time in seconds. The allowable range is 90~1800 seconds. When an incoming call requests a session expiry time that is lower than this, the X6004 uses this value instead.

Table 98 Trusted Peer Configuration (continued)

LABEL	DESCRIPTION
Session Expires	<p>Enter the session expiry time in seconds for all phone connections on this trunk. The allowable range is 90~86400 seconds. This value cannot be lower than the Minimum SE.</p> <p>This allows the X6004 to automatically disconnect any phone calls on this trunk after a certain period of inactivity.</p>
CallerID Setting	
CallerID Viewer	<p>This field displays the caller ID format shown to the callees depending on the setting you configure in the CallerID Name & Number and The Extension Prefix fields.</p>
Representative Number	<p>Specify the representative number shown as source caller ID to the callees when you make external calls through this trunk connection. The default is "zyxel".</p>
CallerID Name & Number	<p>Select the caller ID display format you want to use when you make calls.</p> <p>A caller ID consists of a call ID name (A), a caller ID number (B) and a SIP server IP address (C). The caller ID has the following format: "A"<B@C>.</p> <p>The choices are:</p> <p>(In the following examples, we assume a company representative number is 12345678, their SIP server IP is 10.1.1.1, a caller extension number is 1111 and DDI/DID number 12345555 can map to the extension 1111.)</p> <ul style="list-style-type: none"> • Extension + Extension: Displays the caller's extension number in A and B. For example, "1111"<1111@10.1.1.1>. • Extension + Representative Num: Displays the caller's extension number in A and the SIP trunk's representative number in B. For example, "1111"<12345678@10.1.1.1>. • Representative Num + Representative Num: Displays the SIP trunk's representative number in A and B. For example, "12345678"<12345678@10.1.1.1>. Select this format if you don't want callees to know the caller's extension number. • Extension + Representative Num (DDI/DID mapped): Displays the caller's extension number in A and the SIP trunk's DDI/DID mapped representative number in B. For example, "1111"<12345555@10.1.1.1>. • Representative Num (DDI/DID mapped) + Representative Num (DDI/DID mapped): Displays the SIP trunk's DDI/DID mapped representative number in both A and B. For example, "12345555"<12345555@10.1.1.1>.
The Extension Prefix	<p>Specify whether to add a prefix number in the callerID name when you make calls through this trunk connection. The availability of this setting varies depending on the format of CallerID Name & Number you selected.</p> <p>This field can be 0-20 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), colons (:), periods (.), hyphens (-) and plusses (+)</p>

Table 98 Trusted Peer Configuration (continued)

LABEL	DESCRIPTION
Codec Setting	<p>Select the type of voice coder/decoder (codec) that you want to use when communicating with the trusted peer. The following codecs (shown in highest quality to lowest quality order) are supported by the X6004:</p> <ul style="list-style-type: none"> • G.711 a-law (typically used in Europe) • G.711 u-law (typically used in North America and Japan) • G.729 • G.723.1 - you must activate support for this codec in the Configuration > PBX > Server Configuration > Server screen. • G.726 <p>See Voice Codecs on page 227 for more information.</p> <p>When two SIP devices start a SIP session, they must agree on a codec.</p> <p>If the trusted peer uses videophones, you must specify the video codecs used for video calls. The X6004 allows the following video codecs to passthrough:</p> <ul style="list-style-type: none"> • H.261 • H.263 • H.264 • MP4 <p>See Video Codecs on page 228 for more information.</p>
Codec Pool	<p>This column indicates the codec types not used for this trusted peer connection. You can add a codec type to be used for these extensions by highlighting it and hitting the Right button.</p>
Codec List	<p>This column indicates the codec types used for this trusted peer connection. You can organize the priority of the codecs by highlighting it and clicking the Up or Down buttons to move the codec higher or lower in priority. The SIP extensions attempt to use the higher priority codecs first and try the lower priority codecs next. You can remove a codec type from being used from these extension by highlighting it and hitting the Left button.</p>
Apply	<p>Click this to save your changes and to apply them to the X6004.</p>
Cancel	<p>Click this to set every field in this screen to its last-saved value.</p>

18.6.2 Auto-Attendant for Trusted Peer

Use this screen to select which auto-attendant should be used with this outbound line group. See [Chapter 19 on page 291](#) for information on configuring auto-attendant. Click the **Auto-Attendant** icon in the in the **Trusted Peer** section of the **Outbound Group** configuration screen to view the screen as shown.

Figure 160 AA for Incoming Trusted Peer Calls

Each field is described in the following table.

Table 99 AA for Incoming Trusted Peer Calls

LABEL	DESCRIPTION
Auto-Attendant	
Apply AA	Select an Auto-Attendant or ACD skill profile used for the calls incoming through this outbound line trunk.
DDI/DID Mapping Setting	Select DDI/DID if you want to map a dialed number through this outbound line group to an extension or direct it to auto attendant for incoming calls. Select Direct if you want to forward all incoming calls through this outbound line group directly to their called numbers.
Representative Number	This field displays the representative number of the trusted peer if you have configured one in the trusted peer setting (see Section 18.6.1 on page 285).
Routing by SIP "To" Header	Select Enable if this auto-attendant interacts with a SIP server that uses the SIP To header to do the DDI/DID mapping. If this trusted peer outbound line group has DDI/DID mode enabled, using this deletes all of the this trusted peer outbound line group's DDI/DID mapping settings and sets the DDI/DID Mask to 0. Select Disable to use the SIP request URI to do the DDI/DID mapping.
DDI/DID Mask	Enter a number (1~10) to decide the number of digits you want to enter for the next DDI/DID number(s).

Table 99 AA for Incoming Trusted Peer Calls (continued)

LABEL	DESCRIPTION
DDI/DID Number	<p>Enter a DDI/DID number which allows outsiders to call and reach an extension directly. The number of digits you can enter in this field depends on what you set in the Representative Number DDI/DID Mask field.</p> <p>This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.</p>
Extension Number	<p>Select the first radio box and enter the extension number to which the DDI/DID number maps. Alternatively, select Auto-Attendant to forward the matched DDI calls to auto-attendant.</p> <p>This field can be 1-10 digits or 1-10 digits - 1-10 digits (two sets of up to ten digits separated by a hyphen). For example, 5783900 or 5783900-5783999.</p>
Add	Click this to add a new DDI/DID-to-extension mapping rule.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to go to the Outbound Group screen without saving your changes.

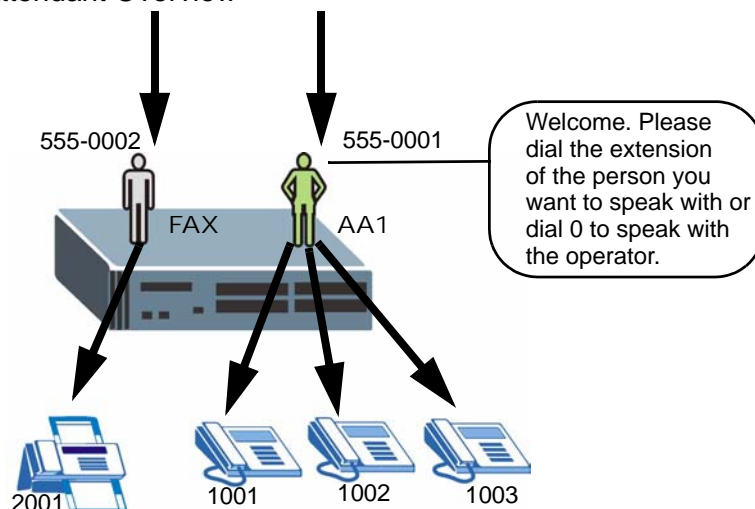
Auto-Attendant

19.1 Overview

This chapter shows you how to configure auto-attendant on the X6004.

An auto-attendant is software which acts as an automatic switchboard operator. auto-attendants help route incoming calls to their proper extension. An auto-attendant is assigned to each outbound line group and it services incoming calls on those lines. If your organization has two outbound line groups, each with a specific telephone number for incoming calls, then you can assign a different auto-attendant for each incoming line. Assign one auto-attendant for general calls to your organization (for example, **AA1**) and one auto-attendant (for example **FAX**) for direct routing to a fax machine.

Figure 161 Auto-Attendant Overview



19.1.1 What You Can Do in this Chapter

- Use the **Default** screen to configure the default auto-attendant used by all trunks when a custom auto-attendant does not exist or apply. See [Section 19.2 on page 294](#).
- Use the **Customized** screen to view, add, edit or delete auto-attendants from the X6004. See [Section 19.2 on page 294](#).

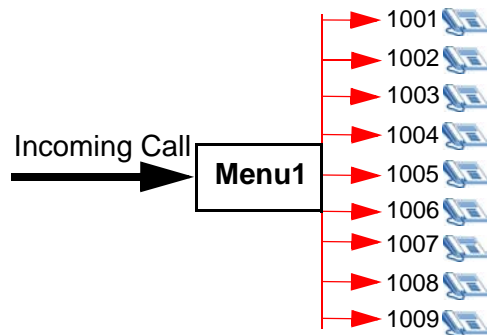
19.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Default Auto-Attendant Structure

The X6004 comes with a default auto-attendant. The default auto-attendant simply prompts callers to enter the extension they wish to reach. There is only one time when a caller has to make a decision. The following figure shows the default auto-attendant structure.

Figure 162 Auto-Attendant Default Structure Example

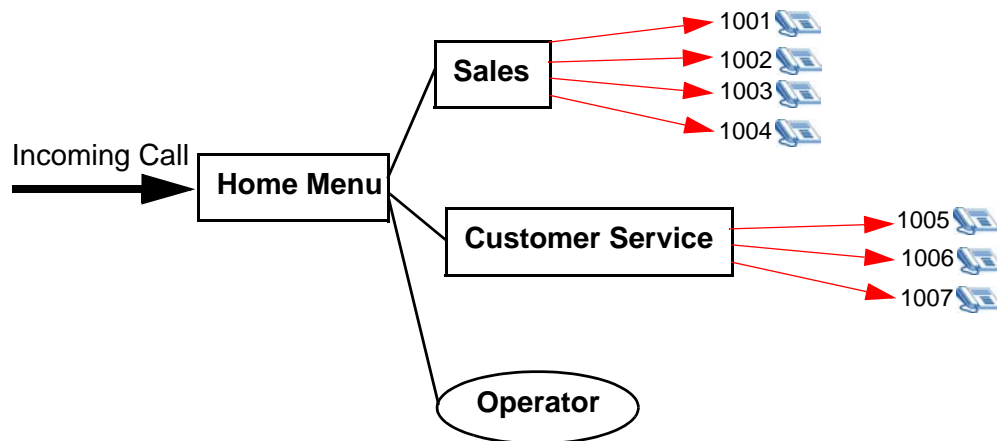


Custom Auto-Attendant Structure

You can configure a more complex auto-attendant structure to fit your organization's needs. An auto-attendant can contain several more complex menus that can guide an incoming call to a specific extension or a group of extensions. In the following example, an incoming caller is prompted to specify whether they want to talk to a sales representative, customer service representative or the operator. Once the caller reaches the **Sales** menu, the auto-attendant can prompt

them to specify which product they are interested in. The caller then dials a number to reach the appropriate sales representative.

Figure 163 Auto-Attendant Custom Structure Example



Configuring Menus

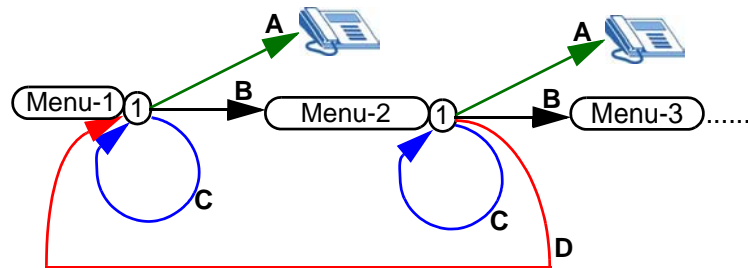
Configuring an auto-attendant requires you to set up menus. In [Figure 163 on page 293](#) there are three menus. The **Home Menu** and two sub menus: **Sales** and **Customer Service**. Each menu should have an accompanying audio file which informs the callers of their options. In each menu you can allow or disallow the dialing of extensions. You can also assign the following options to each menu based on the action performed by the caller. Each option is followed by example content for the accompanying audio file.

- Direct a call to an extension. “Dial 1 to reach the operator.”
- Direct a caller to the next menu. “Dial 2 to reach the sales department.”
- Allow the caller to listen to the current menu again. “Dial 3 to listen to this menu again.”
- Allow the caller to go back to the previous menu. “Dial 4 to go back to the previous menu.” (Not available for the first menu.)

The caller dials the number specified in the prompt to navigate through the auto-attendant’s menus. When configuring auto-attendant, you must choose a number that the caller should dial and an associated function for that option. The following

example shows the options you can assign when the caller dials 1 as he or she moves through your customized auto-attendant.

Figure 164 Auto-Attendant Menus



When a caller dials **1** in **Menu-1**, you can direct them to an extension (**A**), move them to the next menu (**B**) or allow them to hear the menu again (**C**). The same options are available in **Menu-2** with the addition of going back to **Menu-1** (**D**).

19.2 The Default Screen

Use this screen to configure the default auto-attendant used by all trunks when a custom auto-attendant does not exist or apply. These settings are used if a custom auto-attendant is not assigned.

Click **Configuration > PBX > Outbound Line Management > Auto-Attendant** to view the screen as shown next.

Figure 165 Auto-Attendant > Default

Greeting	
Audio File Upload	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Audio File State	Uploaded <input type="button" value="Playback"/>
Operator	
Key	<input type="text" value="0"/> <input type="button" value="v"/>
Extension	<input type="text"/>
Action for Time Out	
<input checked="" type="radio"/>	Hang up
<input type="radio"/>	Extension <input type="text"/>
<input type="radio"/>	ACD <input type="text" value="55555 / South_America"/> <input type="button" value="v"/>

Each field is described in the following table.

Table 100 Auto-Attendant > Default

LABEL	DESCRIPTION
Greeting	
Audio File Upload	Click Browse to locate an audio file to be used as the auto-attendant greeting message, and Upload to copy it to the X6004. The audio file you upload must meet the following criteria: <ul style="list-style-type: none"> • G.711 format voice file (*.wav), μ-law 8-bit mono mode. • Size limit of a single announcement cannot exceed 1 MB. • Size limit of all voice files is 10 Mb per X6004 (or per ZyStack).
Audio File State	This indicates whether an audio file has been uploaded to the X6004 or not. You can also Playback the audio file to hear how it sounds.
Operator	
Key	Select either 0 or 9 to be the default operator key. When a caller presses the operator key, his calls is routed to the associated Extension .
Extension	Enter an extension number to associate with the operator Key . When that key is pressed, the call is routed to this extension.
Action for Time Out	These options indicate how the auto-attendant should proceed if no key is pressed for 5 seconds or the caller inputs an incorrect key code three times in a row.
Hang Up	The auto-attendant disconnects the call.
Extension	The auto-attendant routes the call to the specified extension.
ACD	The auto-attendant engages the ACD system. See Chapter 24 on page 365 for details on this feature.
Apply	Click this to save your changes.
Reset	Click this to clear the fields on this screen and begin anew.

19.3 The Customized Screen

Use this screen to view, add, edit or delete auto-attendants from the X6004. To access this screen, click **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized**.

Figure 166 Auto-Attendant > Customized

Auto-Attendant List			
ID	Name	Description	
2	Research		

Each field is described in the following table.

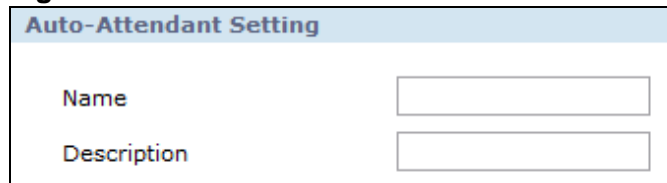
Table 101 Outbound Line Management > Auto-Attendant

LABEL	DESCRIPTION
ID	This field displays the ID assigned to an auto-attendant.
Name	This field displays the name assigned to an auto-attendant.
Description	This field displays the description for an auto-attendant.
Add, Advanced, Edit, Delete	Click: <ul style="list-style-type: none"> • Add - to create a new auto-attendant. • Advanced - to configure an auto-attendant. • Edit - to change the description of an auto-attendant. • Delete - remove an existing auto-attendant.

19.3.1 The Add/Edit Auto-Attendant Screen

Use this screen to add or edit an auto-attendant. To access this screen, click the **Add** or **Edit** icon in the **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized** screen to view the screen as shown.

Figure 167 Auto-Attendant > Add/Edit



The screenshot shows a form titled "Auto-Attendant Setting". It contains two input fields: "Name" and "Description".

Each field is described in the following table.

Table 102 Auto-Attendant > Add/Edit

LABEL	DESCRIPTION
Name	Type a name for this auto-attendant. This field can be 1-20 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_).
Description	Type a description for this auto-attendant. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Add/Edit	Click Add to save your changes.
Cancel	Click Cancel to go back to the previous screen without saving your changes.

19.3.2 Advanced Settings: Office Hours

Use this screen to edit auto-attendant menu settings. Click the **Advanced** icon in the **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized** screen to view a screen as shown next. The **Office Hours** screen displays by default.

Figure 168 Office Hours Setting

Key	Description	Action	Extension	
1	North American Sales	Forward to skill	55556/North_America	

Each field is described in the following table.

Table 103 Office Hours Setting

LABEL	DESCRIPTION
Office Hour Setting [Auto-Attendant Name]	
Audio File Upload	Click Browse to locate an audio file to be used as the auto-attendant greeting message, and Upload to copy it to IP-PBX. The audio file you upload must meet the following criteria: <ul style="list-style-type: none"> • G.711 format voice file (*.wav), μ-law 8-bit mono mode. • Size limit of a single announcement cannot exceed 1 MB. • Size limit of all voice files is 10 Mb per X6004 (or per ZyStack).
Audio File State	This indicates whether an audio file has been uploaded to the X6004 or not. You can also Playback the audio file to hear how it sounds.

Table 103 Office Hours Setting (continued)

LABEL	DESCRIPTION
Dial Extension Number	Select Enable if you want to allow incoming calls to dial extensions that are not associated with specific key codes on the Options list below. Select Disable if you want to limit all input to the key codes listed on the Options table below.
Forward to a specific extension directly	Select this option and then input an Extension number if you want all incoming calls to this auto-attendant to bypass the auto-attendant options and go straight to the specified extension.
Play audio file before forward to a specific extension	Select this option to play the uploaded audio file before forwarding the call to the specified extension.
Operator	
Key	Select either 0 or 9 to be the default operator key. When a caller presses the operator key, his calls is routed to the associated Extension .
Extension	Enter an extension number to associate with the operator Key . When that key is pressed, the call is routed to this extension.
Action for Time Out	These options indicate how the auto-attendant should proceed if no key is pressed for 5 seconds or the caller inputs an incorrect key code three times in a row.
Hang Up	The auto-attendant disconnects the call.
Extension	The auto-attendant routes the call to the specified extension.
ACD	The auto-attendant routes the call to the specified ACD skill group.
Options	This section displays the actions configured for this auto-attendant menu.
Key	This field displays the digits a caller must dial to perform an action.
Description	This field displays the description for this action.
Action	This field displays the function of an action.
Extension	This field displays either the extension, hunting group or ACD number that this call is forwarded to or it displays Next Menu , if the action for this auto-attendant option is set to Forward to a sub menu . Click Next Menu to configure the settings for a sub menu.
Add/Edit/Delete	Click: <ul style="list-style-type: none">• Add to create a new option for this auto-attendant menu.• Edit to change the settings for an auto-attendant option.• Delete to remove this option from this menu.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

Auto-Attendant Audio Files

You can record your own custom auto-attendant messages. The audio files you record must meet the following criteria:

- G.711 format voice file (*.wav), μ -law 8-bit mono mode.
- Size limit of a single auto-attendant message cannot exceed 1 MB.
- Size limit of all auto-attendant voice files is 10 Mb per X6004 (or per ZyStack).

19.3.3 The Add/Edit Office Hours Auto-Attendant Screen

Use this screen to configure an option for an auto-attendant menu. To access this screen, click the **Add** or **Edit** icon for an item in the auto-attendant list.

Figure 169 Add/Edit Option Setting

Each field is described in the following table.

Table 104 Add/Edit Option Setting

LABEL	DESCRIPTION
Key	Type the digit(s) a caller should dial to execute this option. This field can be 1-5 digits in length.
Description	Type a description for this auto-attendant option. This field can be 0-63 alphanumeric characters (A-Z, a-z, 0-9), underscores (_), hyphens (-) and spaces. 0 means this field can be left blank.
Action	Specify the action for this auto-attendant option. The choices are: <ul style="list-style-type: none"> • Forward to an extension - to forward a call to a specific extension. • Forward to a sub menu - to forward a call to the next menu. • Forward to a skill - to route the call to an ACD skill. See Chapter 24 on page 365 for details on using this feature. • Repeat menu - to replay the auto-attendant audio file for this menu.
Extension	Specify the extension or a hunting group number you want to forward this call to. This field is only applicable if you select Forward to an extension in the Action field. This field can be 3-20 digits in length.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

19.3.4 The Auto-Attendant Sub Menu Screen

Use this screen to configure an option for an auto-attendant sub menu. To access this screen, click the **Next Menu** button for an item in the auto-attendant list.

Figure 170 Auto-Attendant Sub Menu

Each field is described in the following table.

Table 105 Auto-Attendant Sub Menu

LABEL	DESCRIPTION
Audio File Upload	Click Browse to locate an audio file to be used as the auto-attendant greeting message, and Upload to copy it to IP-PBX. The audio file you upload must meet the following criteria: <ul style="list-style-type: none"> • G.711 format voice file (*.wav), μ-law 8-bit mono mode. • Size limit of a single announcement cannot exceed 1 MB. • Size limit of all voice files is 10 Mb per X6004 (or per ZyStack).
Audio File State	This indicates whether an audio file has been uploaded to the X6004 or not. You can also Playback the audio file to hear how it sounds.
Dial Extension Number	Select Enable if you want to allow incoming calls to dial extensions that are not associated with specific key codes on the Options list below. Select Disable if you want to limit all input to the key codes listed on the Options table below.
Key	This field displays the digits a caller must dial to perform an action.
Description	This field displays the description for this action.
Action	This field displays the function of an action.
Extension	This field displays either the extension, hunting group or ACD number that this call is forwarded to or it displays Next Menu , if the action for this auto-attendant option is set to Forward to a sub menu . Click Next Menu to configure the settings for a sub menu.
Add/Edit/Delete	Click: <ul style="list-style-type: none"> • Add to create a new option for this auto-attendant menu. • Edit to change the settings for an auto-attendant option. • Delete to remove this option from this menu.

Table 105 Auto-Attendant Sub Menu (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

19.3.5 Advanced Settings: Night Service

Use this screen to configure **Night Service** settings for this auto-attendant. You only need to configure this screen if you want the auto-attendant to perform different actions outside of regular office hours.

Click the **Advanced** icon in the **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized** screen then select the **Night Service** tab to view a screen as shown next.

Figure 171 Night Service Setting

Night Service Setting [Advertising]

Night Service Enable Disable

Audio File Upload

Audio File State

Dial Extension Number Enable Disable

Forward to a specific extension directly (Extension)

Play audio file before forward to a specific extension

Operator

Key

Extension

Action for Time Out

Hang up

Extension

ACD

Options

Key	Description	Action	Extension	
1	Night Clerk	Forward to an extension	1001	<input type="button" value="+"/> <input type="button" value="edit"/> <input type="button" value="trash"/>

Each field is described in the following table.

Table 106 Night Service Setting

LABEL	DESCRIPTION
Night Service Setting [Auto-Attendant Name]	
Night Service	<p>Select Enable to activate the night service settings for this auto-attendant.</p> <p>Select Disable to turn them off.</p>
Audio File Upload	<p>Click Browse to locate an audio file to be used as the auto-attendant greeting message, and Upload to copy it to IP-PBX.</p> <p>The audio file you upload must meet the following criteria:</p> <ul style="list-style-type: none"> • G.711 format voice file (*.wav), μ-law 8-bit mono mode. • Size limit of a single announcement cannot exceed 1 MB. • Size limit of all voice files is 10 Mb per X6004 (or per ZyStack).
Audio File State	This indicates whether an audio file has been uploaded to the X6004 or not. You can also Playback the audio file to hear how it sounds.
Dial Extension Number	<p>Select Enable if you want to allow incoming calls to dial extensions that are not associated with specific key codes on the Options list below.</p> <p>Select Disable if you want to limit all input to the key codes listed on the Options table below.</p>
Forward to a specific extension directly	Select this option and then input an Extension number if you want all incoming calls to this auto-attendant to bypass the auto-attendant options and go straight to the specified extension.
Play audio file before forward to a specific extension	Select this option to play the uploaded audio file before forwarding the call to the specified extension.
Operator	
Key	Select either 0 or 9 to be the default operator key. When a caller presses the operator key, his calls is routed to the associated Extension .
Extension	Enter an extension number to associate with the operator Key . When that key is pressed, the call is routed to this extension.
ACD	The auto-attendant routes the call to the specified ACD skill group.
Action for Time Out	These options indicate how the auto-attendant should proceed if no key is pressed for 5 seconds or the caller inputs an incorrect key code three times in a row.
Hang Up	The auto-attendant disconnects the call.
Extension	The auto-attendant routes the call to the specified extension.
Options	This section displays the actions configured for this auto-attendant menu.
Key	This field displays the digits a caller must dial to perform an action.
Description	This field displays the description for this action.
Action	This field displays the function of an action.

Table 106 Night Service Setting (continued)

LABEL	DESCRIPTION
Extension	This field displays either the extension, hunting group or ACD number that this call is forwarded to or it displays Next Menu , if the action for this auto-attendant option is set to Forward to a sub menu . Click Next Menu to configure the settings for a sub menu.
Add/Edit/Delete	Click: <ul style="list-style-type: none"> • Add to create a new option for this auto-attendant menu. • Edit to change the settings for an auto-attendant option. • Delete to remove this option from this Menu.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

19.3.5.1 The Add/Edit Night Service Auto-Attendant Screen

Use this screen to configure an option for an auto-attendant menu. To access this screen, click the **Add** or **Edit** icon for an item in the auto-attendant list.

Note: This screen is identical to the Add/Edit Office Hours Auto-Attendant screen. See [Section 19.3.3 on page 299](#) for details.

19.3.6 Advanced Settings: Greetings

Use this screen to set up custom auto-attendant messages.

The **Temporary Greeting** can be played before the normal auto-attendant greeting. This can be used to broadcast special messages, such as special operating hours for the office building (“We’re sorry but the Acme Mail Order Company is closed today to observe the holiday.”)

The **Scheduled Greeting** can be played during specific time range every day. This can be used to broadcast to highlight certain information only at certain hours, such as lunch time hours for the office building (“Thank you for calling the Acme Mail Order Company. As it is currently lunch time, representatives may be unavailable until 1 PM.”)

Click the **Advanced** icon in the **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized** screen then select the **Greetings** tab to view a screen as shown next.

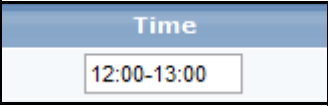
Figure 172 Greeting Setting

Each field is described in the following table.

Table 107 Greetings Setting

LABEL	DESCRIPTION
Temporary Greeting Setting [Auto-Attendant Name]	
Temporary Greeting	Select Enable to play this greeting immediately before playing the auto-attendant's normal greeting. Select Disable to turn this feature off.
Audio File Upload	Click Browse to locate an audio file to be used as the temporary auto-attendant greeting message, and Upload to copy it to IP-PBX. The audio files you upload must meet the following criteria: <ul style="list-style-type: none"> • G.711 format voice file (*.wav), μ-law 8-bit mono mode. • Size limit of a single announcement cannot exceed 1 MB. • Size limit of all voice files is 10 Mb per X6004 (or per ZyStack).
Audio File State	This indicates whether an audio file has been uploaded to the X6004 or not. You can also Playback the audio file to hear how it sounds.
Schedule Greeting Setting [Auto-Attendant Name]	
Index	This indicates the position of the item in the list.

Table 107 Greetings Setting (continued)

LABEL	DESCRIPTION
Time	<p>Enter the time range in one of six available fields for this scheduled greeting to be played. Time should be entered using 24-hr notation and the two times separated by a hyphen (hh:mm-hh:mm).</p> <p>For example:</p> 
Audio File Upload	<p>Click Browse to locate an audio file to be used as the temporary auto-attendant greeting message, and Upload to copy it to IP-PBX.</p> <p>The audio files you upload must meet the following criteria:</p> <ul style="list-style-type: none"> • G.711 format voice file (*.wav), μ-law 8-bit mono mode. • Size limit of a single announcement cannot exceed 1 MB. • Size limit of all voice files is 10 Mb per X6004 (or per ZyStack).
Audio File State	<p>This indicates whether an audio file has been uploaded to the X6004 or not. You can also Playback the audio file to hear how it sounds.</p>
Apply	<p>Click this to save your changes.</p>
Cancel	<p>Click this to go back to the previous screen without saving your changes.</p>

19.4 Technical Reference

The following section contains additional technical information about the X6004 features described in this chapter.

Recording Auto-Attendant Audio Files

Follow the steps in this section to record audio files for use by an auto-attendant.

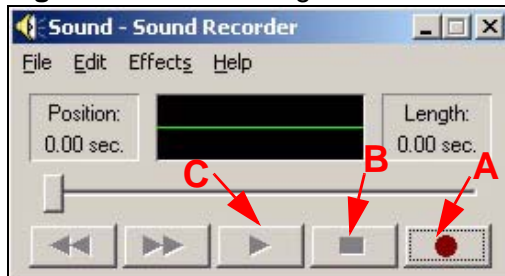
Note: The example shown here uses the components available in the Microsoft Windows 2000 operating system to create the audio files. Use this section as a guideline only.

Note: Make sure you have a microphone connected to your computer or that your system has an internal microphone (and that it is enabled).

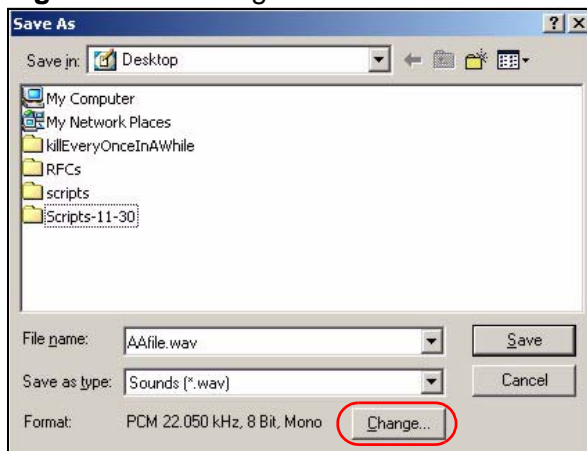
- 1 Open your sound recording software (**Sound Recorder** on Windows 2000). From your desktop, click **Start > Programs > Accessories > Entertainment > Sound Recorder**.

Figure 173 Sound Recorder

- 2 Record your audio file. When you are ready to record, press the **Record** button (A). When you are finished recording, press the **Stop** button (B). Press the **Play** button (C) to review your recording.

Figure 174 Recording Audio

- 3 Save your audio file. In **Sound Recorder**, press **File > Save As**. Type a name for the audio file in the **File name:** field and then click **Change** to make sure that the file is saved in correct format.

Figure 175 Saving Audio Files

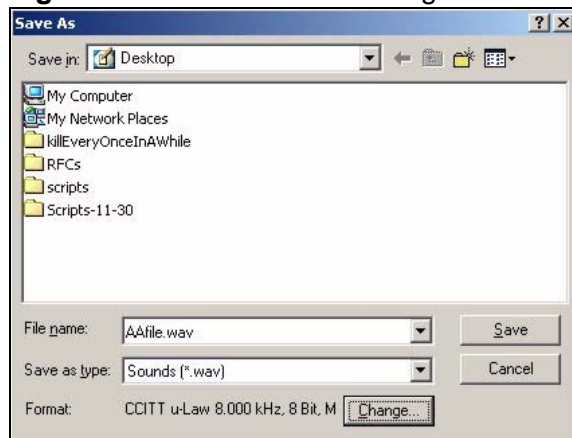
- Specify the file format. In the **Sound Selection** window. Choose **CCITT μ -Law** in the **Format** field. Next, select the playback sound quality by choosing the frequency of the playback audio file. Higher frequency results in better sound but larger file size. Typically the setting **8.000 kHz, 8 Bit, Mono 7 kb/sec** is sufficient for auto-attendant recordings. Press **OK** when you are done.

Figure 176 Audio File Settings



- Confirm your settings. Specify a location for the audio file by browsing to a suitable location on your file system. Click **Save** when you are finished.

Figure 177 Confirm File Settings

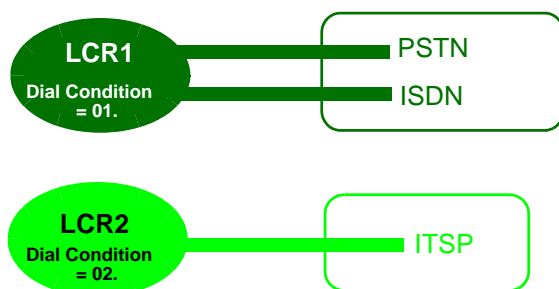


20.1 Overview

This chapter shows you how to configure dialing rules, also referred to as LCR (Least Cost Routing) on the X6004.

The following figure shows an example of two LCRs. **LCR1** is composed of outbound line groups **PSTN** and **ISDN** along with the dial condition **01**. (the period (.) is part of the dial condition). **LCR2** is composed of outbound line group **ITSP** along with the dial condition **02**.. When a user calls "021234" the call is routed through the outbound line group defined in **LCR2**.

Figure 178 LCR Components Example

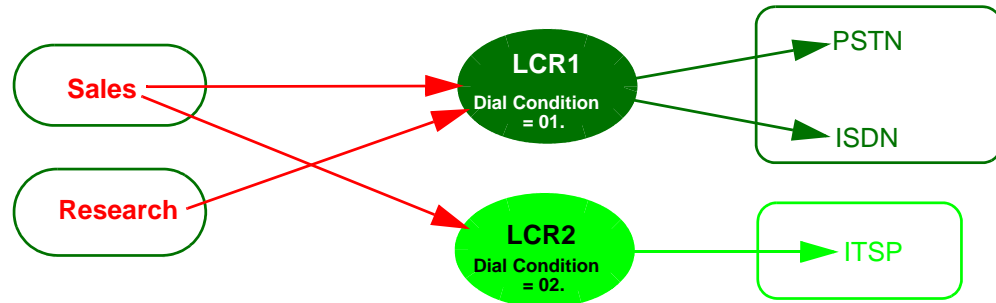


When an LCR contains more than one outbound line group, as in the **LCR1** example, the administrator can prioritize the outbound line groups in the LCR. When a call is made using an LCR with multiple outbound line groups, the X6004 tries to use the higher priority outbound line group first and, if the line is not available, then it tries a lower priority outbound line group.

The following figure shows a possible assignment of LCRs to authority groups. In our example, the **Sales** authority group has been associated with both **LCR1** and **LCR2**, so extensions that are part of **Sales** can use any outbound line group they

choose. The second authority group - **Research**, only has **LCR1** assigned to it, so extensions that are part of **Research** cannot use outbound line group **ITSP**.

Figure 179 LCR Components Example



20.1.1 What You Can Do in this Chapter

Use the **LCR List** screen to configure settings for your dialing rules for outbound calls routing. See [Section 20.2 on page 311](#).

20.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

LCR

LCRs are made up of two components. The first part of an LCR is a set of 1 or more outbound line groups (see [Chapter 18 on page 257](#)). The second part of an LCR is a set of dial conditions, or a set of pattern of digits that distinguish each individual LCR.

LCRs define which outbound line group(s) that authority groups, trusted SIP peers or outbound line groups can use to make an outgoing call. This is done via group management, see [Chapter 21 on page 317](#). Once you create an LCR, you can associate it with:

- **Authority Groups** - give all the extensions contained in an authority group the right to use the outbound line groups configured in the LCR.
- **Trusted SIP Peers** - give the telephones connected to the SIP peer the right to call the X6004 and then dial out from the X6004 using the outbound line groups configured in the LCR.
- **Outbound Line Groups** - give anyone calling in via the associated outbound line group the right to use the X6004 to make calls via the outbound line groups configured in the LCR.

Outbound Line Group

The outbound lines define a connection between the X6004 and PSTN, ISDN, ITSP or your trusted peer. See [Section 18.1 on page 257](#) for more information.

20.1.3 Before You Begin

Before you start to configure an LCR, please consider the following.

- You have to define your outbound dialing plan. For example, dial a number starting with “0” is for local calls, “200” is for international calls, “3” is a call to branch office, etc.
- You should define at least one outbound line group. See [Section 18.2 on page 262](#).

20.2 LCR List

Use this screen to view outbound dialing rules (LCRs) configured on the X6004. To access this screen, click **Configuration > PBX > Outbound Line Management > LCR**.

Figure 180 Outbound Line Management > LCR

LCR Name	Description
<input type="checkbox"/> ezout	easy to call out
<input type="checkbox"/> local_call	local call LCR
<input type="checkbox"/> long_distance_call	long distance call LCR
<input type="checkbox"/> international_call	international call LCR

Each field is described in the following table.

Table 108 Outbound Line Management > LCR

LABEL	DESCRIPTION
Delete	Select the LCRs that you want to remove in the Delete column and then click the Delete button.
LCR Name	This is the name of the LCR.
Description	This text describes the LCR.
Move Up/Down	Use these arrows to re-arrange the LCR sequence.

Table 108 Outbound Line Management > LCR (continued)

LABEL	DESCRIPTION
Apply LCR Sequence	Click this button to save your LCR sequence after re-arranging it.
Add/Edit/Delete	Click Add to create a new LCR. Click Edit to change the settings of an existing LCR. Click Delete to remove an existing LCR.

20.2.1 LCR Configuration

Use this screen to choose the outbound line groups and create dialing conditions for an LCR. To access this screen, click the **Add** or **Edit** icon in the **Dial Condition List** section of the **LCR** screen to view the screen as shown.

Note: Only the **Add LCR** screen is shown. In the **Edit LCR** screen, some of the fields are read-only.

Before you configure any dial conditions for an LCR, you must first configure the **LCR Setting** section of this screen and click **Apply**.

Figure 181 LCR > ezout

The screenshot shows the 'LCR Setting' section with the following fields:

- LCR Name: ezout
- Description: easy to call out
- Max Call Time: [] sec.
- Outbound Line Group: A list box with 'Pool' and 'Selected' columns, and arrows for moving items between them.

Below the settings are 'Apply' and 'Cancel' buttons.

The 'Dial Condition List' section shows a table with one row:

Dial Condition	Actions
XXXXXXX.	[Delete] [Add] [Edit] [Delete]

Each field is described in the following table.

Table 109 LCR > ezout

LABEL	DESCRIPTION
LCR Setting	
LCR Name	Type a short name to identify this outbound dialing rule (LCR). You can use letters "a-z", "A-Z", numbers "0-9" and the underscore "_" character. Spaces are not allowed.

Table 109 LCR > ezout (continued)

LABEL	DESCRIPTION
Description	Type a short description for this outbound dialing rule (LCR). You can use printable ASCII characters; spaces are allowed.
Max Call Time	<p>Leave this field blank, if you don't want to limit the duration of outgoing calls that use this outbound dialing rule (LCR).</p> <p>Alternatively, enter the number of seconds (1-99999) to which you want to limit the duration of outgoing calls that use this outbound dialing rule (LCR).</p>
Outbound Line Group	<p>Use this section to add or remove outbound line groups from this outbound dialing rule (LCR).</p> <ul style="list-style-type: none"> • Add an outbound line group to this LCR: Highlight an outbound line group in the Pool column by clicking on it and then click the Right button to move it to the Selected column. • Remove an outbound line group from this LCR: Highlight an outbound line group in the Selected column by clicking on it and then click the Left button to move it to the Pool column. <p>If the LCR contains multiple outbound line groups, you can use the Up and Down buttons to specify the priority of the outbound line groups.</p> <ul style="list-style-type: none"> • Highlight an outbound line group in the Selected column by clicking on it and then click the Up button to raise its priority. • Highlight an outbound line group in the Selected column by clicking on it and then click the Down button to lower its priority.
Apply	Click this to save your changes.
Cancel	Click this to go back to the LCR List screen without saving changes.
Dial Condition List	
Delete	Select the dial conditions that you want to remove in the Delete column and then click the Delete button.
Dial Condition	This field displays the dial conditions (string of digits) that are used by this outbound dialing rule (LCR).
Add/Edit/Delete	<p>Click Add to create a new dial condition for this outbound dialing rule (LCR).</p> <p>Click Edit to change the settings of an existing dial condition for this outbound dialing rule (LCR).</p> <p>Click Delete to remove an existing dial condition from this outbound dialing rule (LCR).</p>

20.2.2 Add/Edit LCR Dial Condition

Use this screen to set up a dialing condition for an LCR. To access this screen, click the **Add** or **Edit** icon in the **Dial Condition List** section of the **LCR** screen you are configuring to view a screen as shown.

Note: Only the **Add Dial Condition** screen is shown. In the **Edit Dial Condition** screen, some of the fields are read-only.

When creating a new LCR, you must first configure the **LCR Setting** portion of the LCR configuration screen and press **Apply** before you can add a dial condition.

Figure 182 LCR > Dial Condition

Each field is described in the following table.

Table 110 LCR > Dial Condition

LABEL	DESCRIPTION
Dial Condition	
LCR Name	This field displays the name of the outbound dialing rule that this dialing condition applies to.

Table 110 LCR > Dial Condition (continued)

LABEL	DESCRIPTION
Dial Condition	<p>Create the criteria for using this outbound dialing rule. The criteria can be</p> <ul style="list-style-type: none"> • a specific number - for example "55555555"; in this case the number dialed by users must match this string exactly. • any number starting with a specified pattern of digits - for example "0.", "555.", "011." and so on; in this case the number dialed must match the digits before the period "." and it doesn't matter what follows. For example dialing "0222-2222" matches the dialing condition "0." <p>You can also specify a range for digits within a dial condition. You can:</p> <ul style="list-style-type: none"> • use the letters X, Z, N to specify a range of numbers to match. X represents the range 0-9, Z represents the range 1-9 and N represents the range 2-9. • use brackets to specify an allowed range for a dialed digit. For example [0-8] or [0-46-9], in the second example 5 is not allowed. <p>Use the Right button to test if the dial condition is in acceptable format.</p> <p>Note: You should make sure to create unique dial conditions for each LCR. The X6004 is not able to distinguish between LCRs if they have the same dial condition.</p>
Number Pattern Test	<p>This field allows you to test whether a number dialed from one of the extensions meets the criteria specified in the Dial Condition field.</p> <p>Type a number you want to test and click the Right button. An O appears, if the number you typed matches the dial condition. An X appears, if the number you typed does not match the dial condition.</p>
Dial Number Viewer	<p>This field displays the phone number sent from the X6004 to this outbound line group. You must click on an outbound line group in the Channel column of this screen to view the number sent from the X6004 to the outside line.</p>
Channel	<p>This column identifies the outbound line groups for this outbound dialing rule (LCR).</p>
Offset	<p>Specify how many initial digits of the dialed number should not be included in the number going out of the X6004.</p>
Length	<p>Specify whether the number dialed should be limited in length. If you set a limit, the numbers which extend beyond the limit will be cut off by the IPPBX.</p>
Prefix	<p>Specify a number which should be inserted at the beginning of the dialed number before it is sent out from the X6004. Use a "p" to have a 0.5 second pause between dialing numbers. For example, enter "Op5" to have the X6004 wait 0.5 second after dialing 0 and then dial 5.</p>
Postfix	<p>Specify a number which should be appended to the end of the dialed number before it is sent out from the X6004. Use a "p" to have a 0.5 second pause between dialing numbers. For example, enter "Op5" to have the X6004 wait 0.5 second after dialing 0 and then dial 5.</p>
Apply	<p>Click this to save your changes.</p>
Cancel	<p>Click this to set every field in this screen to its last-saved value.</p>

Group Management

21.1 Overview

This chapter shows you how to manage the X6004's authority groups and outbound line groups.

Group management allows you to control the types of calls made via the X6004. See the following figure for what you can configure in the group management.

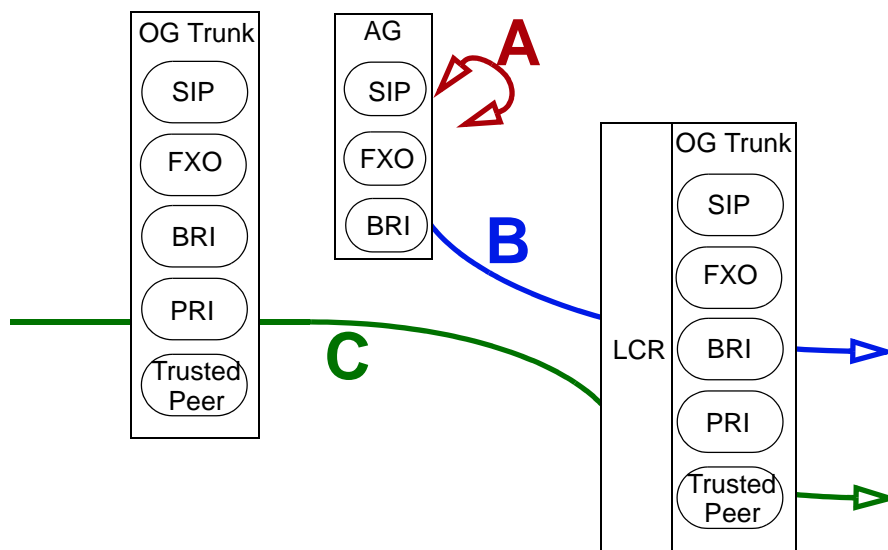
A - You can allow or disallow an extension group (defined in the authority group, AG) to call extensions in other extension group(s).

B - You can manage the types of outgoing calls that extensions within authority groups can make.

C - You can manage incoming calls that callers from outside your organization can make using different interfaces.

You grant calling rights by creating associations or links between the various logical entities configured on the X6004.

Figure 183 Group Management Example



The following sections give an overview of granting calling rights to authority groups (see [Managing Authority Groups on page 318](#)), followed by granting calling rights to outbound line groups (see [Managing Outbound Line Groups on page 320](#)).

21.1.1 What You Can Do in this Chapter

Use the **LCR List** screen to configure settings for your outbound call dialing rules. See [Section 21.2 on page 322](#).

21.1.2 What You Need to Know

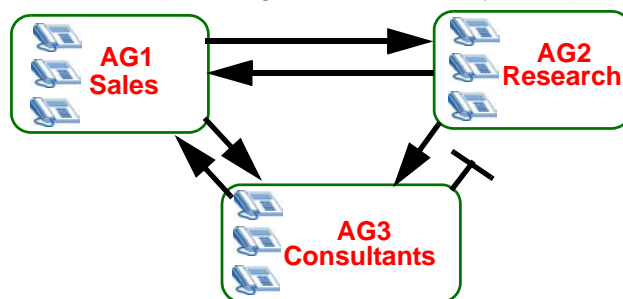
The following terms and concepts may help you as you read through the chapter.

Managing Authority Groups

You control extensions within an authority group by associating (linking) authority groups with:

- **Other Authority Groups** - When you create an authority group it is by default linked to all other authority groups created on the X6004 and all the other authority groups are also linked to it. This means that any extension created on the X6004 can call any other extension created on the X6004 regardless if they are part of the same authority group. You can, however, stop extensions within one authority group from calling extensions in another authority group. An example is shown below. You have an organization with three authority groups (AG1-AG3). You can remove the link from one authority group (for example AG3) to another authority group (for example AG2) to stop extensions in AG3 from calling AG2 (AG2 can still call AG3).

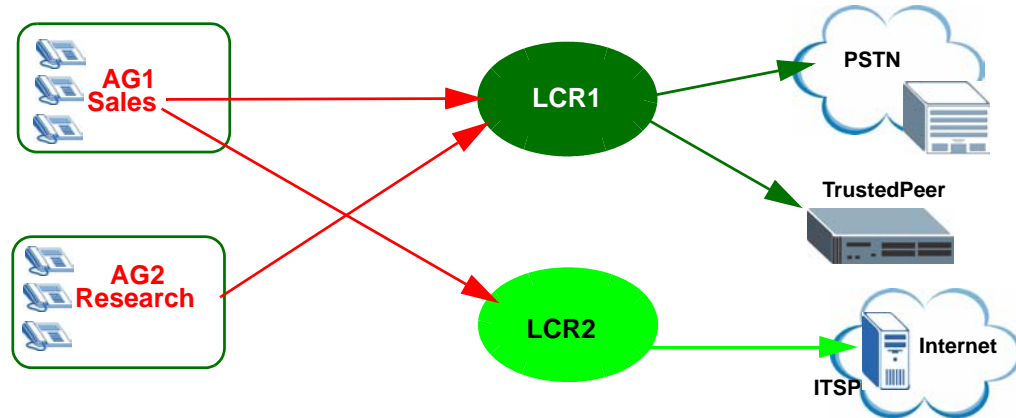
Figure 184 Group Management - Authority Group to Authority Group



- **LCRs** - An LCR is an outbound dialing rule. When you create links from an authority group to an LCR, you allow the extensions in that authority group to make outbound calls via the outbound line groups configured in the LCR. The following figure shows **AG1**, which is an authority group for the sales department, associated with LCR1 (this could be an LCR allowing calls through your local telephone service provider - **PSTN** and calls via a link to your branch office - **TrustedPeer**) and LCR2 (this could be an LCR for long distance calls via

your VoIP service provider **ITSP**). **AG2** is associated with **LCR1** only. In this case extensions belonging to **AG1** can make calls via all outbound line groups, whereas extensions in **AG2** are limited to calls to your local telephone company and your branch office.

Figure 185 Group Management - Authority Group to LCR



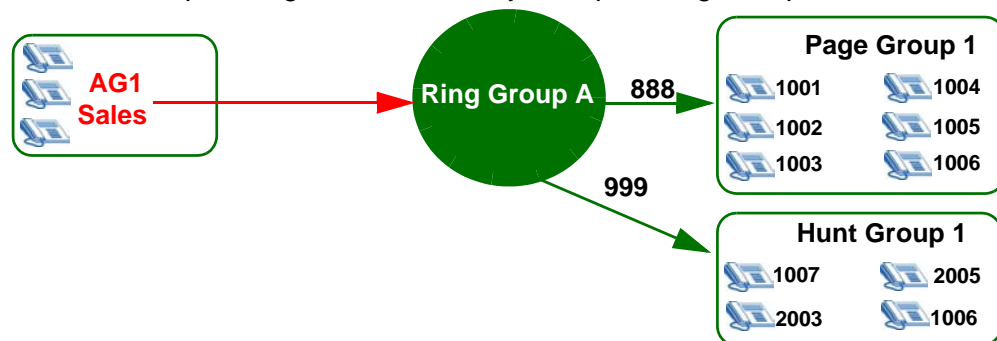
- **Ring Groups** - When a set of extensions are linked to a page group or a hunt group this is known by the generic term 'ring group'. Extensions which are linked to the page or hunt groups do not need to come from the same authority group. See [Chapter 14 on page 229](#) for more information on ring groups and see [Paging and Hunting on page 229](#).

In the following example, authority group **Sales** is associated to **Ring Group A**. **Ring Group A** consists of:

- **Page Group 1**: allows you to call all the extensions within **Page Group 1** simply by dialing the page group number (**888**).
- **Hunt Group 1**: allows you to call extensions within **Hunt Group 1** based on the algorithm defined in the hunt group setup simply by dialing the hunt group number (**999**).

All the extensions in the authority group **Sales** can call **Page Group 1** or **Hunt Group 1**.

Figure 186 Group Management - Authority Group to Ring Group



Managing Outbound Line Groups

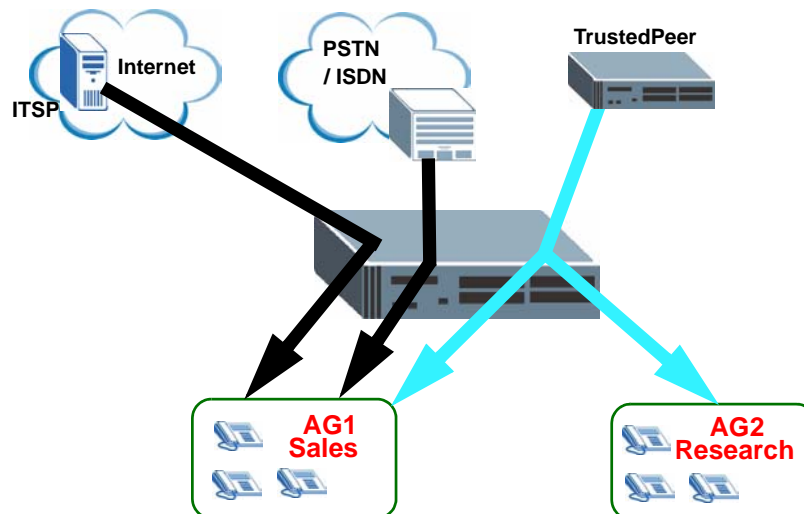
Outbound line groups include SIP, FXO, ISDN PRI/BRI Trunks and Trusted Peers as defined in [Chapter 18 on page 257](#). For management purposes the X6004 grants rights to calls coming in via these channels based on the outbound line group they are part of. You can manage incoming calls by associating (linking) outbound line groups with:

- **Authority Groups** - When you create an outbound line group it is by default linked to all authority groups created on the X6004. This means that calls coming in via this outbound line group are authorized to call any extension created on the X6004. You can remove the link from an outbound line group to an authority group to stop incoming calls from an outbound line group from going to a specific authority group.

Note: You must also configure auto-attendant settings before calls coming in from outside lines can call the extensions created on the X6004. See [Chapter 19 on page 291](#).

The following example shows a configuration with three outbound line groups. **ITSP** represents a SIP trunk to your VoIP service provider. **PSTN** represents a link to your local traditional telephone service provider and **TrustedPeer** is a connection to your branch office. Incoming calls from **ITSP** and from **PSTN** are allowed to only reach extensions of your sales team (**AG1**). Calls coming in from **TrustedPeer** are allowed to reach the extensions of both the sales (**AG1**) and research (**AG2**) departments. This configuration is accomplished by removing the association to **AG2** from the **ITSP** and **PSTN** outbound line groups.

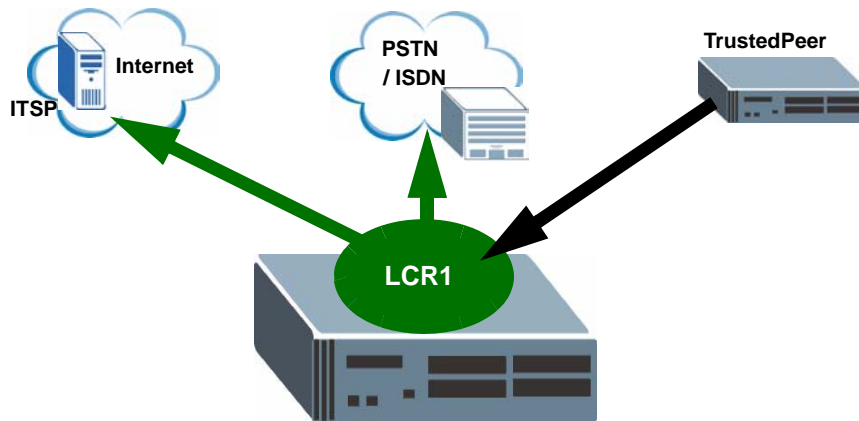
Figure 187 Group Management - Outbound Line Group to Authority Group



- **LCRs** (LCR is the outbound dialing rule) - When you create links from an outbound line group to an LCR, you allow incoming calls from that outbound line group to make outbound calls via the outbound line groups configured in the LCR. For example, someone calling from outside your organization can use the X6004 to forward their call to another outside line.

In the following example, outbound line group **TrustedPeer** is associated with **LCR1**. **LCR1** is comprised of two outbound line groups: a SIP trunk to your VoIP service provider - **ITSP** and a connection to your local traditional telephone company - **PSTN/ISDN**. Calls coming in via the **TrustedPeer** connection can use the **ITSP** and **PSTN/ISDN** connections to complete their calls.

Figure 188 Group Management - Outbound Line Group to LCR



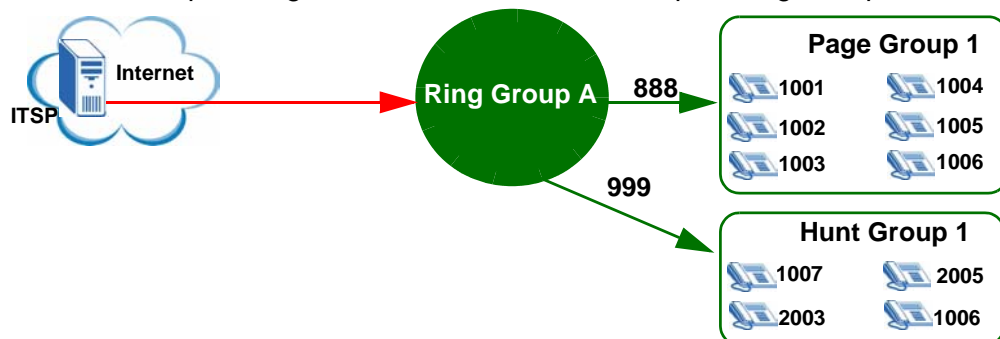
- **Ring Groups** - Links from an outbound line group to a page or hunt group are known as a 'ring group'. You can allow calls coming in via that outbound line group to call the page or hunt group configured within the ring group.

In the following example, outbound line group **Sales** is associated to **Ring Group A**. **Ring Group A** consists of:

- **Page Group 1**: allows you to call all the extensions within **Page Group 1** simply by dialing the page group number (**888**).
- **Hunt Group 1**: allows you to call extensions within **Hunt Group 1** based on the algorithm defined in the hunt group setup simply by dialing the hunt group number (**999**).

All calls coming in via the outbound line group **ITSP** can call **Page Group 1** or **Hunt Group 1**.

Figure 189 Group Management - Outbound Line Group to Ring Group



21.1.3 Before You Begin

Before you start to configure a group management, you need to do the following.

- Configure authority group(s). See [Section 13.2 on page 200](#).
- Configure outbound line group(s) and the corresponding auto-attendant settings. See [Section 18.2 on page 262](#).
- Configure ring groups, page groups, hunt groups. See [Chapter 14 on page 229](#).

21.2 Group Management Screen

Use this screen to view and manage the associations for the authority and outbound line groups configured on the X6004. To access this screen, click **Configuration > PBX > Group Management**.

Figure 190 PBX > Group Management

Overview			
Authority Group			
Machine ID	Group Name	Description	Associations
IPPBX_001	sales		
IPPBX_001	General		
FXO Trunk			
Machine ID	Group Name	Description	Associations
IPPBX_001	Sales		
BRI Trunk			
Machine ID	Group Name	Description	Associations
IPPBX_001	Nifleheim		
PRI Trunk			
Machine ID	Group Name	Description	Associations
IPPBX_001	Hodir		
SIP Trunk			
Machine ID	Group Name	Description	Associations
IPPBX_001	Brunnhildr		
Trusted Peer			
Machine ID	Group Name	Description	Associations
IPPBX_001	Dalaran		
Click To Talk Group			
Machine ID	Group Name	Description	Associations
IPPBX_001	sales		
IPPBX_001	General		

Each field is described in the following table.

Table 111 PBX > Group Management

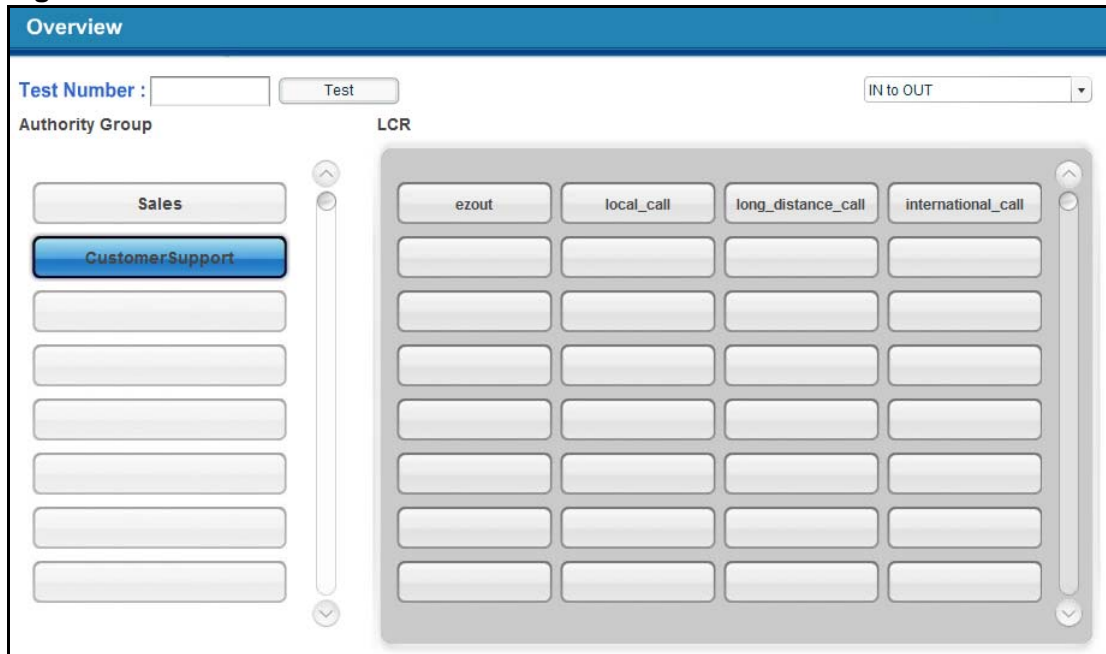
LABEL	DESCRIPTION
Overview	Click this to open the Overview screen.
Authority Group, FXO Trunk, BRI Trunk, PRI Trunk, SIP Trunk, Trusted Peer, Click to Talk	<p>These headings separate the group types you can manage on the X6004:</p> <ul style="list-style-type: none"> • Authority Group - These are the authority groups containing extensions on the X6004. • FXO Trunk - These are outside lines via the FXO ports on the X6004. • PRI Trunk - This refers to a connection from the X6004 to the ISDN T1 or E1 trunk line via the PRI port on the X6004. • BRI Trunk - This refers to a connection from the X6004 to the basic rate ISDN trunk line via the BRI port on the X6004. • SIP Trunk - These are outside lines to a SIP server at your VoIP service provider. • Trusted Peer - These are outside lines to another SIP server (for example another X6004) that has configured your X6004 as a Trusted Peer. • Click to Talk Group - These are Click To Talk groups on the X6004.
Machine ID	This field displays the ID of the X6004 on which a group is configured.
Group Name	This field displays the name of a group (authority group or an outbound line group).
Description	This field displays the description of this group.
Associations	Click the Advanced icon to configure links for an authority or an outbound line group.

21.2.1 The Overview Screen

This screen provides a graphical overview of group management in the X6004 and a means to examine outgoing call routes. Rather than having to go from one authority group setting screen to the next as you review and compare settings, you can instead use this screen to immediately see how they relate to each other. Moreover, you can test a number to more easily identify call-related problems.

To access this screen, click **Configuration > PBX > Group Management** then click the **Overview** button. The following screen opens in its own window.

Figure 191 The Overview Screen



Each field is described in the following table.

Table 112 Group Management > Overview

LABEL	DESCRIPTION
Test Number	Enter a number to test with the selected Authority Group and then click the Test button.
Direction	<p>Select a call Direction from this menu. This indicates the direction from the source number to the destination number you want to test.</p> <p>The direction that you select determines which items appear in the call Source columns and the call Destination columns.</p> <ul style="list-style-type: none"> • IN to IN - Calls tested are internal to internal. • IN to OUT - Calls tested are internal to external. • OUT (FXO Trunk) to IN - Calls tested are external on the FXO trunk to an internal connection. • OUT (PRI Trunk) to IN - Calls tested are external on the PRI trunk to an internal connection. • OUT (BRI Trunk) to IN - Calls tested are external on the BRI trunk to an internal connection. • OUT (SIP Trunk) to IN - Calls tested are external on the SIP trunk to an internal connection. • OUT (Trusted Peer) to IN - Calls tested are external from a Trusted Peer to an internal connection. • OUT (FXO Trunk) to OUT - Calls tested are external on the FXO trunk to another external connection. • OUT (PRI Trunk) to OUT - Calls tested are external on the PRI trunk to another external connection. • OUT (BRI Trunk) to OUT - Calls tested are external on the BRI trunk to another external connection. • OUT (SIP Trunk) to OUT - Calls tested are external on the SIP trunk to another external connection. • OUT (Trusted Peer) to OUT - Calls tested are external from a Trusted Peer to another external connection.
Source	<p>This table displays available call sources based on the selected Call Scenario.</p> <p>For example, if your call scenario is IN to OUT, then this column displays the call sources for any configured authority groups.</p>
Destination	<p>This table displays available call destinations. based on the selected Call Scenario.</p> <p>For example, if your call scenario is IN to OUT, then this column displays the available call destinations.</p>
Description	<p>This popup window appears when you click an item in either the Source or Destination columns. It displays the description that is associated with the item.</p>

21.2.2 Edit Group Management Associations

Use this screen to configure links from an authority group or an outbound line group to authority groups, LCRs or ring groups configured on the X6004. To access this screen, click the **Advanced** icon next to the group you want to configure in the **Configuration > PBX > Group Management** screen.

Figure 192 Advanced > (Group Type) > (Group Name)

Accessible Group List			
Group Name		default	
Group Name	Description	Group Type	Associations
ezout	easy to call out	LCR	<input checked="" type="checkbox"/>
local_call	local call LCR	LCR	<input type="checkbox"/>
long_distance_call	long distance call LCR	LCR	<input type="checkbox"/>
international_call	international call LCR	LCR	<input type="checkbox"/>

Each field is described in the following table.

Table 113 Advanced > (Group Type) > (Group Name)

LABEL	DESCRIPTION
Accessible Group List	The table below shows which links you can create from the group (authority group or outbound line group) identified in the Group Name field above the table.
Group Name	This field displays the name of an authority group, LCR or ring group to which you can configure a link.
Description	This field displays the description of the group to which you can create a link.
Group Type	This field identifies whether you are creating a link to: Authority Group - another set of extensions on the X6004. LCR - an outbound dialing rule containing outbound line groups.
Associations	Select this checkbox to link a group you are configuring to another group. Clear this checkbox to remove a link between the group you are configuring and another group.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen.

Call Services

22.1 Overview

This chapter shows you how to configure and use call services on the X6004. There are a variety of call services that can be configured.

22.1.1 What You Can Do in this Chapter

- Use the **Call Emergency** screen to configure emergency numbers, which the X6004 treats with the highest priority. Even if all outbound lines from the X6004 are busy, the X6004 will drop an existing FXO channel and allow an emergency call to complete. See [Section 22.2 on page 329](#).
- Use the **Meet-me Conference** screen to configure conference room extensions. Callers from within and outside your organization can join conference calls by dialing a conference room extension. See [Section 22.3 on page 331](#).
- Use the **Music on Hold** screen to upload your choice of audio to play while callers are placed on hold. See [Section 22.4 on page 333](#).
- Use the **Distinctive Ring** screen to configure different ring tones for incoming calls. This allows you to differentiate where the call is coming from (within or outside your organization, for example). See [Section 22.5 on page 337](#).
- Use the **Auto Callback** screen to configure the X6004 to automatically call an extension once it becomes available (ends an existing conversation). This eliminates the need for you to keep trying to call a busy extension. See [Section 22.6 on page 338](#).
- Use the **Call Parking** screen to configure the X6004 to allow users to put a call on hold at one extension and pick up the call from another extension in your organization. See [Section 22.7 on page 339](#).
- Use the **Call Waiting** screen to configure the X6004 to allow users to put a call on hold at one extension and pick up another incoming call. See [Section 22.8 on page 341](#).
- Use the **Call Transfer** screen to configure the X6004 to allow users to transfer an incoming call that they have answered to another extension in your organization. See [Section 22.9 on page 345](#).
- Use the **Call Recording** screens to record all the calls going to or from specific extensions or trunks. See [Section 22.10 on page 345](#).

- Use the **TAPI** screen to download the server version of the TAPI driver. See [Section 22.11 on page 349](#).

22.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

About Emergency Calls and VoIP

In the past, many commercial VoIP phone services have lacked the ability to deal correctly with emergency calls. Such VoIP services have been unable either to connect emergency calls to an emergency dispatcher (at a Public Safety Answering Point, or PSAP), or to adequately provide information on the caller's whereabouts to the dispatcher.

For this reason, the FCC (the Federal Communications Commission of the United States) has imposed "Enhanced 911" (E911) obligations on providers of "interconnected VoIP" services. Interconnected VoIP services are those that, in addition to making calls over the Internet, also connect to the regular public telephone network. E911 systems not only route emergency calls made from VoIP accounts to emergency dispatchers, but also provide information on the call's originating number and, usually, location information.

However, this system still has disadvantages over traditional emergency call service. For example, the physical location provided to the PSAP is usually the account-holder's address as registered with the VoIP provider; this is not necessarily the location from which the VoIP account is being used. Furthermore, VoIP emergency calls are subject to the limitations of the Internet connection over which they are made, which may be unreliable. Also, VoIP services that do not directly connect to the public telephone network are not required to adhere to the FCC's E911 regulations. Lastly, the E911 service is available only in North America. Similar systems exist elsewhere in the world, but regulation and implementation may vary.

For these reasons, the X6004 routes all calls made to the emergency numbers you configure via its FXO interface whenever possible. The X6004 drops an ongoing FXO call if necessary.

22.1.3 Before You Begin

Emergency Calls

Before you configure emergency calling, ensure that you are aware of all local emergency call numbers used in the location where the X6004 is to operate. Bear in mind that emergency calls may be made to phone numbers other than the

standard public emergency services number (to a private security company or medical facility, for example).

Music on Hold

Before you configure music on hold, ensure that the audio file you want to use is compatible with the standards described in [Section 22.4 on page 333](#).

22.2 The Emergency Call Screen

The X6004 allows you to specify and give higher priority to emergency calls to emergency services. You can configure a list of emergency phone numbers, for example police or fire department, on the X6004. The X6004 recognizes when an emergency number is dialed and tries to send the call to the configured destination number. If all the lines on the X6004 are busy, the X6004 frees up a line by hanging up an existing conversation and then passing the emergency call to the destination number.

22.2.1 Configuring the Emergency Call Screen

Use this screen to manage emergency call numbers on the X6004. Click **Configuration > PBX > Call Services > Call Emergency** to view the following screen.

Figure 193 Call Services > Call Emergency

The screenshot shows the 'Call Services > Call Emergency' configuration screen. It is divided into two main sections:



- Outbound Line List:** This section contains two columns: 'Outbound Line Pool' and 'Selected Outbound Line'. The 'Outbound Line Pool' column lists five entries: 'IPPBX_001:itSP', 'IPPBX_001:SlotB_Port1', 'IPPBX_001:SlotB_Port2', 'IPPBX_001:SlotB_Port3', and 'IPPBX_001:SlotB_Port4'. The 'Selected Outbound Line' column is currently empty. There are navigation arrows between the columns and 'Apply' and 'Cancel' buttons below.
- Emergency Numbers:** This section has a 'Delete' button on the left and '+Add', 'Edit', and 'Del' icons on the right. Below this is a table with the following data:

<input type="checkbox"/>	Emergency Numbers	<input type="checkbox"/>
<input type="checkbox"/>	911	<input type="checkbox"/>

 There is another 'Delete' button at the bottom left of this section.

The following table describes the labels in this screen.

Table 114 Call Services > Call Emergency

LABEL	DESCRIPTION
Outbound Line List	Use this section to specify which outside line groups should be used for emergency calls.
Outbound Line Pool/ Selected Outbound Line	<p>Highlight an outside line group in the Outbound Line Pool column and click the right arrow to select this outside line group for emergency call use.</p> <p>Highlight an outside line group in the Selected Outbound Line column and click the left arrow to remove this outside line group from emergency call use.</p>
Edit	<p>Highlight an outside channel and click the edit icon to add a prefix which should be appended to emergency calls when using this outside line.</p>  <p>The prefix is what allows callers to simply dial the well known emergency number for their region. For example, in the United States the emergency number is 911, so you want users to simply dial 911 in case of an emergency. Since extensions usually have to dial a prefix to dial out via the X6004, this might make it confusing for callers within your organization.</p> <p>Type the prefix number necessary to connect users to an emergency number by simply dialing the emergency number you configure in the Emergency Number section of this screen.</p>
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to set every field in this screen to its last-saved value.
Emergency Numbers	Use this section to add, edit or remove emergency numbers.
Delete	Select this checkbox and click Delete to remove this emergency number from the X6004.
Emergency Numbers	This column displays the emergency numbers currently configured on the X6004.
Add/Edit/ Delete	<p>Use the Add icon to configure a new emergency number. A window opens up and prompts you to enter the emergency number.</p> <p>Use the Edit icon to change an existing emergency number. A window opens up and prompts you to change the emergency number.</p>  <p>Use the Delete icon to remove an existing emergency number from the X6004.</p>

22.3 The Conference Calling Screen

The X6004 allows you to set up specific extension numbers which callers can dial to join a conference call. This type of extension is referred to as a conference room number. You can restrict the number of callers that can join the conference call. You can also specify a PIN (Personal Identification Number) for the conference room. Callers must enter the PIN before they can enter the conference room.

If you have multiple X6004s working together (ZyStack), then you can specify which one should hold the conference room. This allows you choose which X6004s resources are being used for the conference call. The resources used up include DSP channels and outside lines coming into your organization.

Callers within your organization simply call the conference room number to join the conference call. Callers from the outside dial the conference room number after they are prompted by auto-attendant to dial the extension they wish to call.

22.3.1 Configuring the Conference Calling Screen

Use this screen to manage conference calling on the X6004. Click **Configuration > PBX > Call Services > Meet-me Conference** to view the following screen.

Figure 194 Call Services > Meet-me Conference

DSP Resource		
Machine ID	Conference	Share
IPPBX_001	0	88

Conference Room List				
Room	Machine ID	Max. Members	Description	
45405	IPPBX_001	15	Sales Calls from Europe	

The following table describes the labels in this screen.

Table 115 Call Services > Meet-me Conference

LABEL	DESCRIPTION
DSP Resource	This section displays the DSP resources available for each X6004 in a ZyStack. It only displays one X6004 if you have not implemented ZyStacking.
Machine ID	This field displays the name of the X6004 in the ZyStack.
Conference	This field displays the number of DSP channels reserved for conference calls. You can reserve DSP channels in the Configuration > PBX > Server Configuration > DSP Management screen.

Table 115 Call Services > Meet-me Conference (continued)

LABEL	DESCRIPTION
Share	This field displays the unassigned DSP channels on the X6004. Unassigned DSP channels are shared among all services which require DSP services on the X6004.
Conference Room List	This section allows you to view conference room details as well as add or delete conference rooms.
Delete	Select this checkbox and click Delete to remove this conference room from the X6004.
Room	This field displays the conference room number. This is the extension callers should dial to enter this conference room.
Machine ID	This is the system name of the X6004.
Max. Members	This is the number of participants that can join this conference call at any one time.
Description	This field displays the description you enter to identify this conference room.
Add/Edit/Delete	Click the Add icon to create a new conference room. Click the Edit icon to change the settings of an existing conference room on the X6004. Click the Delete icon to remove an existing conference room from the X6004.

22.3.2 The Conference Calling Edit and Add Screen

Use this screen to configure a new conference room. Click the **Add** icon to see the screen as shown.

Note: The screen for editing an existing conference room has the same fields as the screen shown below. You can access the **Conference Room Edit** screen by clicking the **Edit** icon in the **Conference Room List** screen.

Figure 195 Conference Room Add

Conference Room Setting	
Conference Number	<input type="text"/> (4 to 7 digits)
Machine ID	IPPBX_001 <input type="button" value="v"/>
Max. Members	<input type="text"/>
PIN Number	<input type="text"/> (Empty is no authentication)
Confirm PIN Number	<input type="text"/>
Description	<input type="text"/>

The following table describes the labels in this screen.

Table 116 Conference Room Add

LABEL	DESCRIPTION
Conference Number	Enter the extension (4 to 7 digits in length) callers should dial to enter this conference room. If you are editing an existing conference room entry, this field is read-only.
Machine ID	Select the X6004 you want to use for this conference call. If you are editing an existing conference room entry, this field is read-only.
Max. Members	Specify the maximum number of participants for this conference room. The minimum number of participants for a conference call is three and the maximum number you can configure is 99. Once the maximum number of participants join this conference call, the conference room will be closed until an existing participant leaves the conference room. If you allow too many participants into a single conference room, you may use up all of the DSP resources on the X6004 and callers will not be able to make calls.
PIN Number	Type the numeric password callers need to enter to join a conference room. If this field is left blank, then callers can enter this conference room without entering a PIN.
Confirm PIN Number	Retype the PIN.
Description	Enter a brief description to identify this conference room.
Add/Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its last-saved value.

22.4 The Music on Hold Screen

The X6004 allows you to specify a music file to play when callers are placed on hold. This lets the callers know that they are still connected. Use the following guidelines for the music file:

Table 117 Music on Hold File Guidelines

SPECIFICATION	DESCRIPTION
Format	The music file must be a G.711 format audio file (*.wav), μ -law.
Size	The music file should be less than 1 MB in size. The X6004 will play the file in a loop.

22.4.1 Global Setting Screen

Use this screen to customize the default music callers will hear when placed on hold. If you create any custom profiles then they can override this setting.

Click **Configuration > PBX > Call Services > Music On Hold** to open the screen as shown.

Figure 196 Music on Hold: Global Setting

The following table describes the labels in this screen.

Table 118 Music On Hold Global Setting

LABEL	DESCRIPTION
System Default	Select a music on hold profile to use as the system default. You can create new profiles on the Customized MOH screen (Section 22.4.2 on page 334).
Apply	Click this to save your changes.
Reset	Click this to restore the options on this page back to their last saved values so you can begin configuring anew.

22.4.2 Custom Music On Hold

Use this screen to manage your music on hold profiles.

Click **Configuration > PBX > Call Services > Music On Hold** then click the **Customized MOH** tab to open the screen as shown.

Figure 197 Customized Music on Hold

	Name	Description of the MOH	
<input type="checkbox"/>	Rush	TomSawyer	
<input type="checkbox"/>			

The following table describes the labels in this screen.

Table 119 Custom Music on Hold

LABEL	DESCRIPTION
Delete	Click this button to remove any selected entries from the list.
Select	Check a box in an entry row to flag it for deletion.
Name	This indicates the name of the music on hold profile.
Description of the MOH	This displays the description associated with the music on hold profile.
Add	Click this to open the Music on Hold Setting screen, where you can add a new agent to the list.
Edit	Click this to open the Music on Hold Setting screen, where you can modify an existing agent's information.

22.4.3 Add or Edit a Music On Hold Profile

Use this screen to create or edit a music on hold profile. Once you create a profile, you can upload an audio file to it on the **Upload the Music File** screen ([Section 22.4.4 on page 336](#)).

Click the **Add** or **Edit** icons on the **Customized MOH** screen to display these options.

Figure 198 Add a Music on Hold Profile

The following table describes the labels in this screen.

Table 120 Add a Music on Hold Profile

LABEL	DESCRIPTION
Name	Enter a name for the music on hold profile.
Description	Enter a description for the music on hold profile.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

22.4.4 Upload a Music On Hold Profile

Use this screen to upload an audio file to associated music on hold profile. You can create the profile on the **Music on Hold Setting** screen ([Section 22.4.3 on page 335](#)).

Click the **Advanced** icon on the **Customized MOH** screen to display these options.

Figure 199 Upload a Music on Hold File

The following table describes the labels in this screen.

Table 121 Add a Music on Hold Profile

LABEL	DESCRIPTION
Upload Music File	Click Browse to locate an audio file to be used as the auto-attendant greeting message, and Upload to copy it to IP-PBX. The audio files you upload must meet the following criteria: <ul style="list-style-type: none"> • G.711 format voice file (*.wav), μ-law 8-bit mono mode. • Size limit of a single announcement cannot exceed 1 MB. • Size limit of all voice files is 10 Mb per X6004 (or per ZyStack).
Audio File State	This indicates whether an audio file has been uploaded to the X6004 or not. You can also Playback the audio file to hear how it sounds.
Cancel	Click this to go back to the previous screen without saving your changes.

22.5 The Distinctive Ring Screen

The X6004 allows you to select different ring tones based on the origins of calls routed through the X6004.

Click **Configuration > PBX > Call Services > Distinctive Ring** to configure the distinctive ring feature.

Note: This function works only when the callee uses an analog phone connected to X6004's FXS port, a ZyXEL softphone such as V100 or a ZyXEL IP phone such as V500.

Figure 200 Distinctive Ring

The following table describes the labels in this screen.

Table 122 Distinctive Ring

LABEL	DESCRIPTION
Active	Select this to activate the distinctive ring feature.
Ring Tone	Select a ring tone (1~12) and press Playback to listen to the ring tone on the computer that you are using to configure the X6004.
Internal Call	Select the ring tone for internal calls (calls from one X6004's extension to another X6004's extension).
SIP Trunk	Select the ring tone for calls coming in from the SIP trunk (for example your connection to the ITSP).
FXO	Select the ring tone for calls coming in from the FXO trunk (for example your connection to the PSTN).
PRI	Select the ring tone for calls coming in from the PRI trunk (for example your connection to an ISDN T1/E1 line).
BRI	Select the ring tone for calls coming in from the BRI trunk (for example your connection to an ISDN BRI line).
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

22.6 The Auto Callback Screen

The auto callback feature is used when a caller encounters a busy signal when dialing one of the extensions. The caller can then request the X6004 to automatically call both parties when both of the extensions are free.

Click **Configuration > PBX > Call Services > Auto Callback** to configure the auto callback feature.

Figure 201 Auto Callback



The following table describes the labels in this screen.

Table 123 Auto Callback

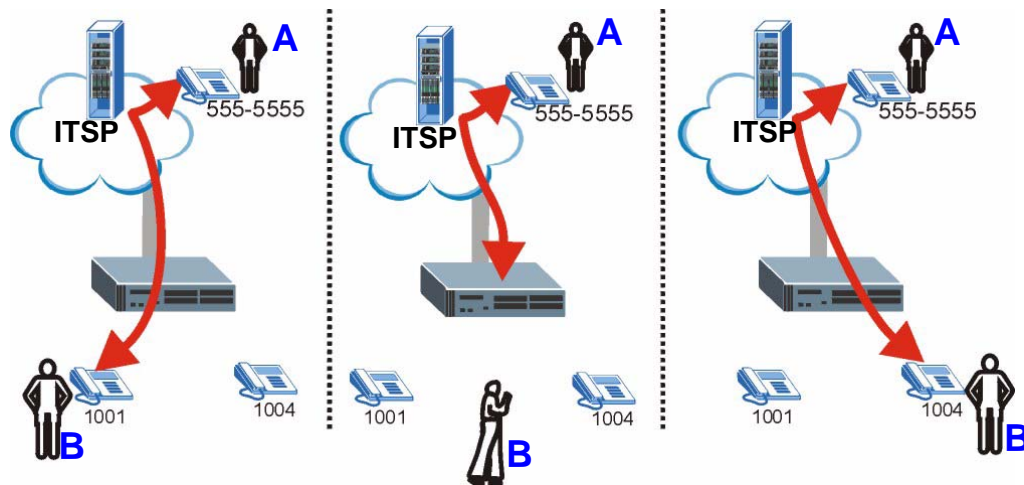
LABEL	DESCRIPTION
Active	Select this to activate the auto callback feature.
Queue Size	Select a limit to the number of auto callback requests for the X6004.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

22.7 The Call Park Screen

Call parking is similar to placing a call on hold. The difference is that you can pick the call up again from another telephone extension in your organization.

The X6004 allows you to configure an extension for a call parking lot. The parking lot places a call in parking slot and informs you of the parking slot number that you can use to reconnect to the parked call. You can reconnect to the call from any extension within your organization. The following figure shows the progression of call parking.

Figure 202 Call Parking Overview



A step by step progression is the following

Table 124 Call Parking Progression

CALLER A	X6004	CALLER B
1. Caller A makes a call to caller B.	2. The X6004 routes the call to caller B at extension 1001.	3. Caller B picks up the call.
Conversation between caller A and B		
		4. Caller B transfers the call to the call parking lot. (This is done by dialing # followed by the parking lot number.
	5. The X6004 parks the call and informs caller B of the number to call to reconnect to the call. This is called the parking slot number.	

Table 124 Call Parking Progression

CALLER A	X6004	CALLER B
		6. Caller B walks to another extension and reconnects to the call with A by dialing # followed by the parking slot number.
Conversation between caller A and B continues		

22.7.1 Configuring the Call Parking Screen

Use this screen to configure call parking on the X6004. Click **Configuration > PBX > Call Services > Call Park** to open the screen.

Figure 203 Call Parking Configuration

Call Park Setting	
Representative Number	<input type="text" value="700"/>
Amount of Parking Position / ZyStack	<input type="text" value="16"/>
Parking Time	<input type="text" value="180"/> (sec.)

The following table describes the labels in this screen.

Table 125 Call Parking Configuration

LABEL	DESCRIPTION
Call Parking Setting	
Representative Number	Enter the telephone number users should dial to park a telephone call. You can use 3-10 digits.
Amount of Parking Position / ZyStack	Enter the number of call parking extensions available. This also establishes the range of numbers that users will have to dial to retrieve a parked call. You can use 1-99 positions.
Parking Time	Enter the maximum number of seconds that a call can be parked. After a parked call exceeds this amount of time, it will hang up. The range you can use is 60-300 seconds.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to set every field in this screen to its last-saved value.

22.8 The Call Waiting Screen

Call waiting allows you to put a present call on hold and answer a new call. When a second call comes in, the X6004 sends a beep tone to you. You can decide to ignore it or to switch to the second call using one of the following methods.

- press the flash button on your telephone
- very quickly press and release the on-hook switch on your telephone

You can switch back to the first call using the same methods above. When you hang up one call, the X6004 sends you a ring tone if another call is still waiting.

Note: This feature only applies to extension receivers which use SIP or analog phones.

The following figure shows how call waiting works.

Figure 204 Call Waiting Overview

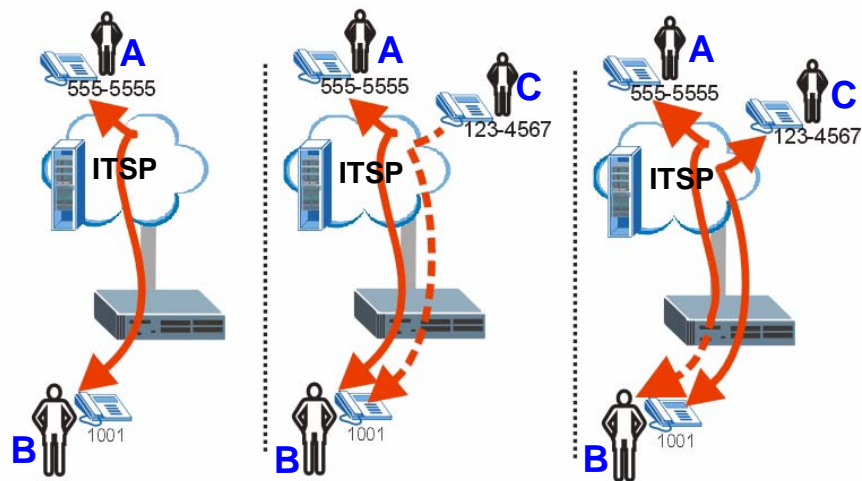


Table 126 Call Waiting Example

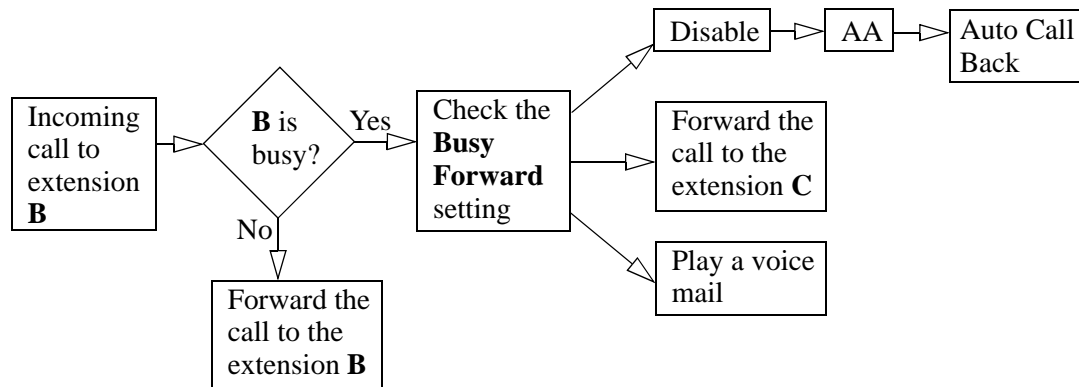
CALLER A	CALLER C	X6004	RECEIVER B
1. Caller A makes a call to caller B .		2. The X6004 routes the call to B at extension 1001.	3. B picks up the call.
4. Conversation established between caller A and B			
	5. Caller C makes a call to caller B .	6. The X6004 routes the call to B at extension 1001.	7. B hears a beep tone and decides to answer the second call. B then presses the flash button on his telephone).
8. Conversation established between caller C and B . Caller A is on hold. B is busy.			

However, if you DISABLE the call waiting feature, the following happens.

Table 127 No Call Waiting Example

CALLER A	CALLER C	X6004	RECEIVER B
1. Caller A makes a call to caller B.		2. The X6004 routes the call to B at extension 1001.	3. B picks up the call.
4. Conversation between caller A and B. Then B is busy.			
	5. Caller C makes a call to caller B.	6. The X6004 routes the call to B at extension 1001.	7. B replies with a busy tone.
		8. The X6004 handles the call (from C) by following extension B's Busy Forward setting.	

Figure 205 The Flow to Check Whether The Receiver Is Busy Or Not



When **B** is busy, additional calls will hear a busy tone and then the X6004 will handle the calls according to what you configured in the **Busy Forward** setting configured in the **Extension Management > Authority Group > Advanced > SIP Peer or FXS Peer > Call Forward** screen for the extension number (see [Figure 101 on page 210](#) and [Figure 110 on page 223](#)).

22.8.1 Configuring the Call Waiting Screen

Use this screen to configure call waiting on the X6004. Click **Configuration > PBX > Call Services > Call Waiting** to open the screen as following.

Figure 206 Call Waiting Setting

The following table describes the labels in this screen.

Table 128 Call Waiting Setting

LABEL	DESCRIPTION
Call Waiting	Select Enable or Disable to turn this feature on or off. If you enable this feature, then call waiting will apply to all extensions except the disable list below and ISDN extensions. If you disable this feature, then call waiting will only apply to the extensions in the enable list below.
Disable/Enable List	To add one extension, select an available one in the Extension List field, click the Right button (to add it into the Setting List field). You can remove extensions from the list by selecting one extension in the Setting List field and click the Left button.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to set every field in this screen to its last-saved value.

22.8.2 Call Waiting Example - 1

This example enables call waiting on extensions 9000, 9001, and 9002. Select **Disable** in the **Call Waiting** field and add those extensions into the enable extension list. Click **Apply**.

Figure 207 Call Waiting Example1

Call Waiting Setting

Call Waiting Enable **Disable**
(BRI phone does not support this feature!)

Enable List

Extension List		Setting List
1111	▶ ◀	9000 9001 9002

Apply Reset

22.8.3 Call Waiting Example - 2

This example enables call waiting for all extensions in the company except extensions 1111 and 1112. Select **Enable** in the **Call Waiting** field and add those extensions into the disable extension list. Click **Apply**.

Figure 208 Call Waiting Example2

Call Waiting Setting

Call Waiting **Enable** Disable
(BRI phone does not support this feature!)

Disable List

Extension List		Setting List
9000	▶ ◀	1111 1112

Apply Reset

22.9 The Call Transfer Screen

Call Transfer allows you to transfer an incoming call (that you have answered) to another phone by doing the following.

- 1 Dial a predefined feature code (for example, ***96** by default) followed by the number to which you want to transfer the call to operate the intercom. See more feature code information in [Section 6.8 on page 141](#).
- 2 After you hear the ring signal or the second party answers it, hang up the phone.

22.9.1 Configuring the Call Transfer Screen

Use this screen to configure call transfer on the X6004. Click **Configuration > PBX > Call Services > Call Transfer** to open the screen as following.

Figure 209 Call Transfer Settings

The following table describes the labels in this screen.

Table 129 Call Transfer Settings

LABEL	DESCRIPTION
Interdigit timeout	Enter the maximum number of seconds the X6004 waits for each digit input of a complete callee number after you press the flash key on the phone. If the X6004 cannot receive the next digit entered within this time period, the X6004 processes digits you have dialed.
Call transfer local handling	Select Enable to allow a caller to transfer a current external call (via an outbound line group) to another extension. Otherwise, select Disable to not allow this.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to set every field in this screen to its last-saved value.

22.10 Call Recording

Use the call recording feature to record all the calls going to or from specific extensions or trunks. This is useful if you need to monitor certain individuals' calls. It is also useful for conference call recording, the administrator may configure the

X6004 to record a Meetme conference room and use the recording as the meeting minutes.

Supported Extension Types:

- SIP
- FXS
- Meetme

Supported Trunk Types:

- FXO
- SIP trunk
- Trusted Peer

Note: Other important call recording details:

- You must have the X6004's hard drive installed to record calls.
- The X6004 plays a beep at a regular interval to remind the call participants about the recording. The default interval is 10 seconds although you can use the commands to change it.
- Once the X6004 is recording 4 channels, it does not record additional concurrent calls.
- An individual call record can only go up to 24 hours.
- The X6004 generates a warning log when the remaining call recording time goes below five days and an alert if it goes below 24 hours. The X6004 stops recording calls once the hard drive is full.
- Calls recordings are saved in .wav format files.

22.10.1 Configuring the Call Recording Screen

Use this screen to configure call recording on the X6004. Click **Configuration > PBX > Call Services > Call Recording** to open the screen as following.

Figure 210 Call Recording

The following table describes the labels in this screen.

Table 130 Call Recording

LABEL	DESCRIPTION
Trunk Peer Pool/ Recorded Peer	Use this section to specify for which trunks the X6004 should record all outgoing and incoming calls. Select a trunk in the Peer Pool column and click the right arrow to select it for recording. Select a trunk in the Recorded Peer column and click the left arrow to not record this trunk's calls.
Extension Peer Pool/ Recorded Peer	Use this section to specify for which extensions the X6004 should record all outgoing and incoming calls. Select an extension in the Peer Pool column and click the right arrow to select it for recording. Select an extension in the Recorded Peer column and click the left arrow to not record this extension's calls.
Apply	Click this to save your changes and to apply them to the X6004.

22.10.2 Querying Call Recordings

Use this screen to search for call recordings on the X6004. Click **Configuration > PBX > Call Services > Call Recording > Query** to open the screen as following.

Figure 211 Call Recording Query

The following table describes the labels in this screen.

Table 131 Call Recording Query

LABEL	DESCRIPTION
Record Time	Select the first option to look for call recordings from the past day, week, or month. Select the line to not specify a time period. Select the second option to be able to specify an exact time period for which to find call recordings. Enter the starting and ending year, month, day, hour, minute, and seconds look for call recordings from the past day, week, or month. Click the button to open a calendar for entering the date.
Peer Type	Specify whether you want to find call recordings for trunks, extensions, or both.
Peer Name	Select the trunk or extension for which you want to find call recordings.
Report	Click this to display a list of call recordings that match your specified criteria.

22.10.3 Call Recordings File List

This screen lists the call recordings that matched your specified criteria. Use this screen to listen to or delete individual call recordings. Click **Configuration > PBX > Call Services > Call Recording > Query** to open the screen as following.

Figure 212 Call Recordings File List

<input type="checkbox"/>	#	Recorded Time	Caller	Callee
<input type="checkbox"/>	1	2009-12-14 18:16:39	511	512
<input type="checkbox"/>	2	2010-02-23 10:57:12	5131	5132
<input type="checkbox"/>	3	2010-02-23 10:57:25	5131	5133
<input type="checkbox"/>	4	2010-02-23 10:57:49	5132	5133
<input type="checkbox"/>	5	2010-02-23 10:58:05	5133	5131
<input type="checkbox"/>	6	2010-02-23 10:58:17	5133	5132

The following table describes the labels in this screen.

Table 132 Call Recordings File List

LABEL	DESCRIPTION
Total Record Files	This is how many call recordings matched your specified criteria. You can select how many recordings to display on the page at a time.
Delete	Select checkboxes for individual call recordings (or use the heading row's checkbox to select all entries) and click Delete to remove the entries from the X6004.
#	This is the number of the entry in the list.
Recorded Time	This is the time that the call recording started. Right-click an entry to be able to save the call recording to your computer.
Caller	This is the number that initiated the call. This cell is highlighted if the number is for a peer in the recording list.
Callee	This is the number that received the call. This cell is highlighted if the number is for a peer in the recording list.

22.11 TAPI

Microsoft Windows Telephony Application Programming Interface (TAPI) integrates the X6004's telephone services with user computers. ZyXEL's TAPI driver allows you to use Microsoft Outlook from a Windows 2000 or later computer to issue an invite to any person in your address book. When the invite is sent out, the X6004 rings both your extension and the extension of the invited person. For a snom phone, you can also click to answer a call.

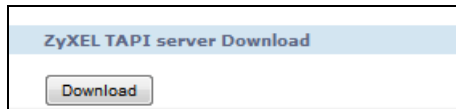
You can download a server version of ZyXEL's TAPI driver from the administrator Web Configurator screens. The server version can control all of the X6004's SIP and FXS extensions. Users can download a client version of ZyXEL's TAPI driver

from the administrator Web Configurator screens that applies to the user's own extension only.

22.11.1 Setting Up the TAPI Server Driver

ZyXEL's TAPI driver is called the ZyXEL TSP (Telephony Service Provider). Your computer needs to be on the X6004's LAN. To download and install the server version:

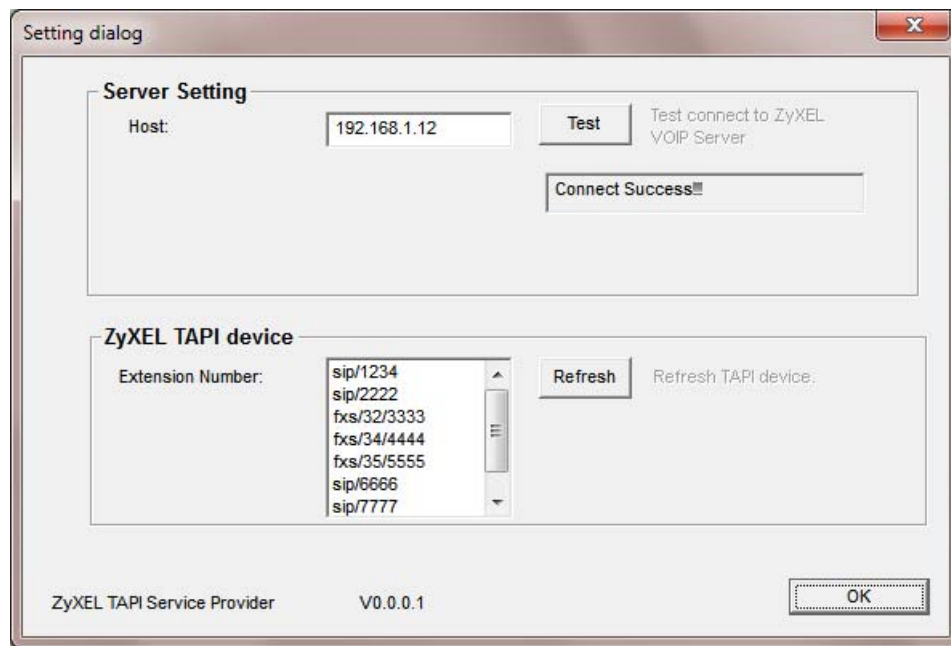
- 1 Click **Configuration > PBX > Call Services > TAPI**. Click **Download** and save the file to your computer.



- 2 Unzip the file and run it, following the on-screen instructions to install it.



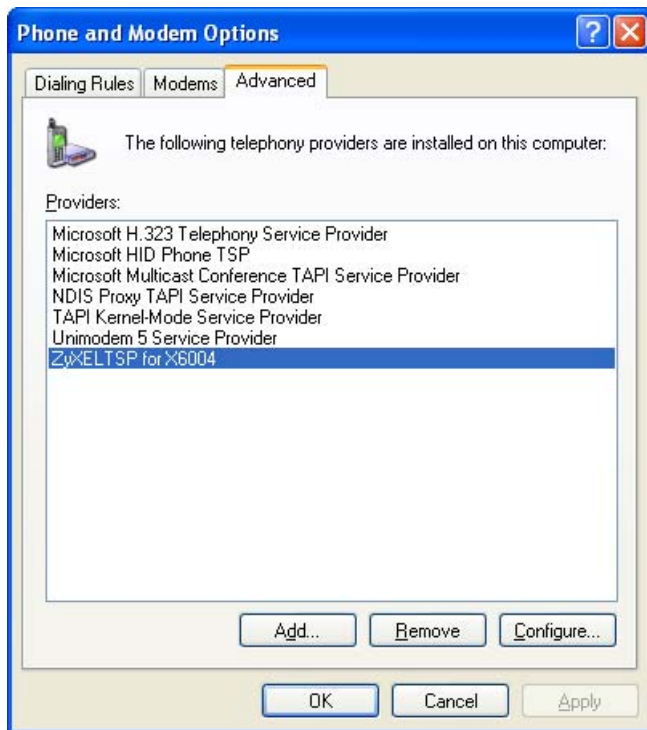
- 3 In the **Setting dialog** window: enter the X6004's host name or IP address in the **Host** field and click **Test** to make sure you can connect to it. The X6004's extensions display in the **Extension Number** list. Click **OK**.



- 3a Enter the X6004's host name or IP address in the **Host** field and click **Test** to make sure you can connect to it.
- 3b After "Connect Success" displays, click **Refresh** to update the list of the X6004's extensions in the **Extension Number** list.
- 3c Click **OK**.

To confirm that the driver is installed, click **Start > Control Panel > Phone and Modem Options**. If you haven't configured your modem settings, you'll need to do

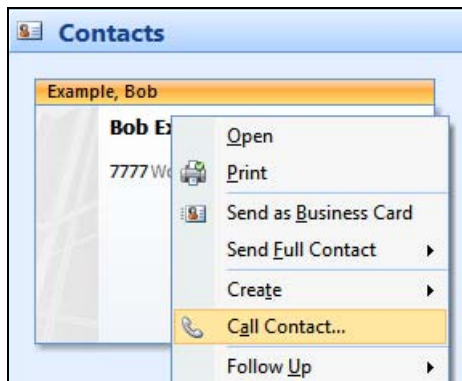
so. Then click the **Advanced** tab and make sure a ZyXEL TSP entry appears in the list of providers.

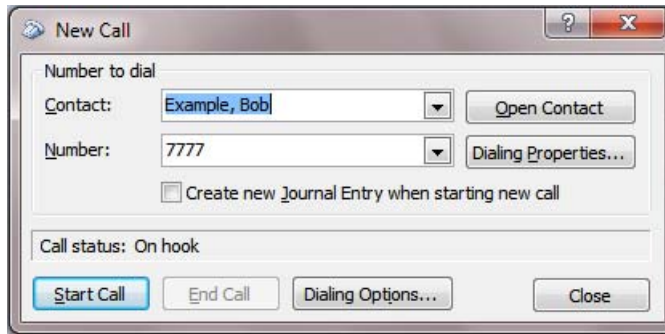
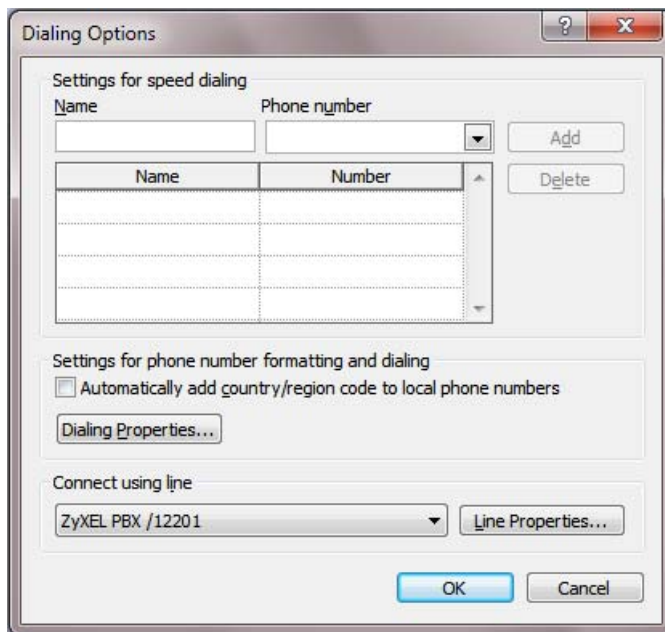


22.11.2 Sending Call Invites from Microsoft Outlook

This section shows you how to use the server version of ZyXEL's TAPI driver in Microsoft Outlook.

- 1 In Outlook, right-click a contact and select **Call Contact**.



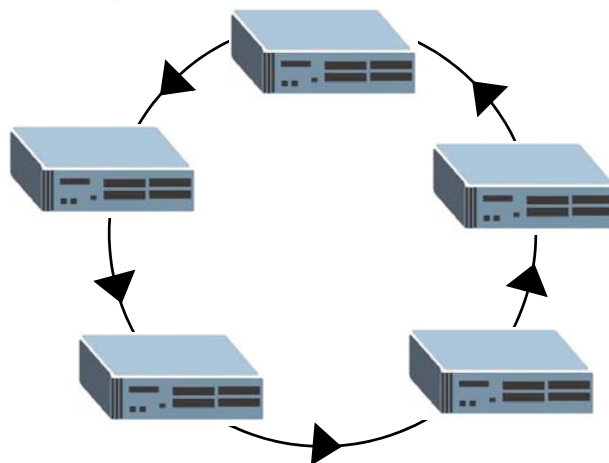
2 Click Dialing Options.**3 Use Connect using line to select the X6004 extension you want to call the contact and click OK.****4 Both extensions ring.**

23.1 Overview

This chapter shows you how to combine two or more X6004s to expand your IP PBX capabilities and utilize a failsafe mechanism in case of a breakdown.

A ZyStack is the aggregation of multiple X6004s under a single management IP address. A ZyStack provides two major advantages. Firstly, it allows you to pool the resources of individual X6004s.

Figure 213 ZyStack Example



23.1.1 What You Can Do in this Chapter

- Use the **Configuration** screen to view and configure ZyStack settings. See [Section 23.2 on page 357](#).
- Use the **Intranet** screen to configure local subnets from which IP phones connect to the X6004s in the ZyStack. See [Section 23.3 on page 360](#).
- Use the **Status** screen to view ZyStack members' status and perform network connectivity test(s) between ZyStack members. See [Section 23.4 on page 362](#).

23.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Master/Slave in ZyStack

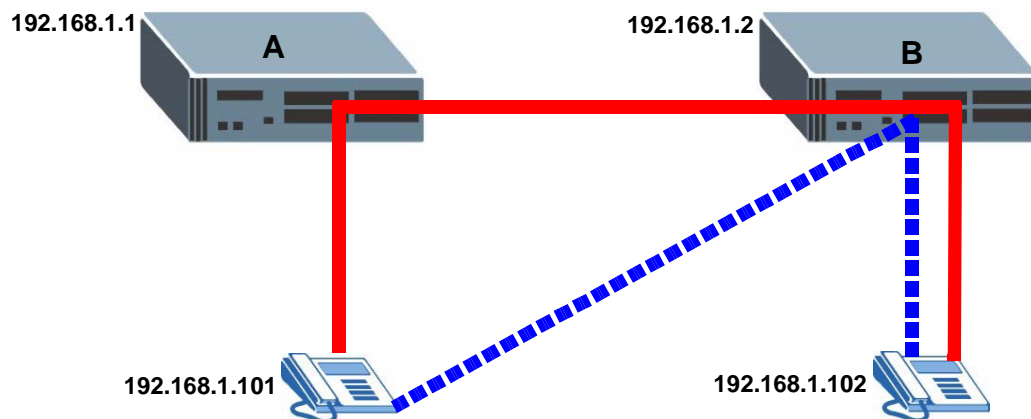
When you create a ZyStack, the X6004s can take on a role of a master or a slave. There can only be one master X6004 per ZyStack. You can manage the configuration of the master and slave X6004s by logging into the LAN or WAN IP address of the master X6004.

ZyStack Internal Call Routing

When an IP phone is a SIP client of one X6004 (**A** in the figure) and it calls a telephone that is a SIP client of another X6004 (**B** in the figure). The default behavior of the X6004 (**A**) is to process the call and connect it to the X6004 (**B**) on which the SIP client is configured. This telephone call is illustrated by the solid line in the following figure. Note that the processing resources of both X6004s are being utilized throughout the duration of the call.

The X6004s can handle internal calls more efficiently if you specify the local subnets which can connect to other ZyStack members. The dotted line shows the same phone call after it has been redirected to X6004 **B**. In this scenario the subnet **192.168.1.0/24** was configured as a local subnet. When **A** receives a call from a SIP client that matches the local subnet and the destination of the client's request is a phone connected to another X6004 (**B**), it then redirects the call to **B**.

Figure 214 Internal Call Routing

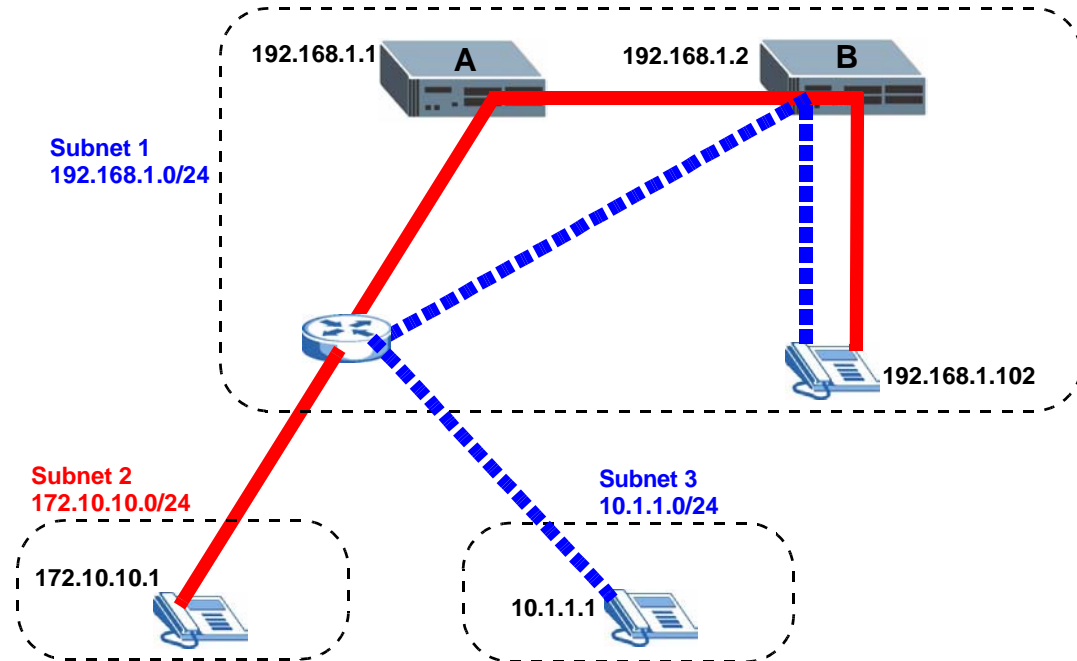


In this first example all the devices reside on the same subnet. A single subnet configuration is recommended for ease of use and management. This, however, is not always possible in your network.

The following example shows an example where your IP phones are located in different subnets on your network. The X6004s are still on the same subnet (**Subnet 1**). IP phones in **Subnet 2** and **Subnet 3** are both SIP clients of X6004 **A**. In this example, **Subnet 3** has been configured as a local subnet. When X6004 **A** receives a call from a phone on **Subnet 3** that is directed to a SIP client of X6004 **B**, it is then able to redirect the call directly to X6004 **B**. **Subnet 2**,

however, has not been configured as a local subnet. Calls that originate from **Subnet 2** must go through X6004 **A** and **B** in order to reach SIP clients connected to **B**.

Figure 215 Internal Call Routing



23.1.3 Before You Begin

Before you start to configure a ZyStack, please do the following:

All the X6004s should use the same interface, either LAN or WAN, to create a ZyStack. The setting on the master X6004 determines which interface the X6004s should use.

23.2 ZyStack Configuration

Use this screen to view and manage your ZyStack settings. Click **Configuration** > **ZyStack** > **Configuration** in the navigation panel to view the screen as shown.

Figure 216 ZyStack > Configuration

Machine ID	Description	WAN IP	LAN IP	Z_Interface	Type	
IPPBX_001	Localhost	172.2.2.201	192.168.1.13	LAN	Master	
IPPBX_002	secondary	172.2.2.234	192.168.1.12	LAN	Slave	

The following table describes the labels in this screen.

Table 133 ZyStack > Configuration

LABEL	DESCRIPTION
Machine ID	This field displays the system name of the X6004. The system name is automatically assigned to the X6004 based on when it was added to the ZyStack. IPPBX_001 is always the master followed by slaves IPPBX_002 , IPPBX_003 and so on.
Description	This field displays the description of this ZyStack member.
WAN IP	This field displays the WAN IP address of the X6004.
LAN IP	This field displays the LAN IP address of the X6004.
Z_Interface	This field displays the interface (LAN or WAN) which the X6004s use to form the ZyStack. This interface is the same for all X6004 in the ZyStack.
Type	This field displays the role this X6004 performs in the ZyStack. The options are: <ul style="list-style-type: none"> • Master - controls configuration on all the other X6004s. • Slave - all configuration is done on the slave from the master X6004.
Add / Edit / Reboot / Delete	Click the Add icon to create or expand a ZyStack by configuring a new member. Click Edit to change the settings of an existing ZyStack member. Click Reboot to shut down and restart a specific member of the ZyStack. Click Delete to remove an existing member from a ZyStack.

23.2.1 ZyStack Add Screen

Use this screen to add an X6004 to your ZyStack. Click the **Add** icon in the **Configuration > ZyStack > Configuration** screen to view the screen as shown.

Figure 217 ZyStack Add

ZyStack Setting


Serial

Description

WAN IP

LAN IP

Z_Interface

 **Note:** If codec G723.1 is enabled or there is any ISDN card in this slave machine, please reboot the slave machine after adding to the ZyStack.

The following table describes the labels in this screen.

Table 134 ZyStack Add

LABEL	DESCRIPTION
Serial	Type the serial number of the X6004 you want to add to the ZyStack. You can get the serial number by clicking on the edit icon in the Configuration > ZyStack > Setting screen of an X6004 that is not part of a ZyStack.
Description	Type a description for this ZyStack member.
WAN IP	Type the WAN IP address of the X6004 you want to add to the ZyStack.
LAN IP	Type the LAN IP address of the X6004 you want to add to the ZyStack.
Z_Interface	This field is only configurable for the ZyStack master. It displays whether the interface on the master X6004 is LAN or WAN for the ZyStack.
Add	Click Add to save your changes to the X6004.
Cancel	Click Cancel to go back to the previous screen without saving your changes.
Reset	Click Reset to clear the fields and begin configuring anew.

23.2.2 ZyStack Edit Screen

Use this screen to edit the serial number or description of an existing ZyStack member. Click the **Edit** icon in the **Configuration > ZyStack > Setting** screen to view the screen as shown.

Figure 218 ZyStack Edit

ZyStack Setting	
Machine ID	IPPBX_001
Serial	b0dbeea3
Description	<input type="text" value="Localhost"/>
WAN IP	172.23.31.1
LAN IP	192.168.1.12
Z_Interface	<input type="button" value="WAN"/> ▼
Type	Master
WAN MAC	200902181606
LAN MAC	200902181607

The following table describes the labels in this screen.

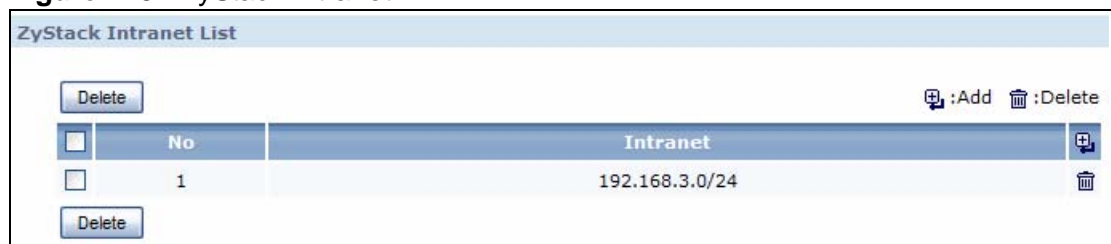
Table 135 ZyStack Edit

LABEL	DESCRIPTION
Machine ID	This field displays the system name of the X6004. The system name is automatically assigned to the X6004 based on when it was added to the ZyStack. IPPBX_001 is always the master (or a stand-alone IPPBX) followed by slaves IPPBX_002 , IPPBX_003 and so on.
Serial	Type the serial number of the X6004 you want to add to the ZyStack. You can get the serial number by clicking on the edit icon in the Configuration > ZyStack > Setting screen of an X6004 that is not part of a ZyStack.
Description	Type a description for this ZyStack member.
WAN IP	This field displays the WAN IP address of the X6004.
LAN IP	This field displays the LAN IP address of the X6004.
Z_Interface	This field displays the interface (LAN or WAN) which the X6004s use to form the ZyStack. This interface is the same for all X6004 in the ZyStack.
Type	This field displays whether the X6004 is a Master or a Slave member of the ZyStack.
WAN MAC	This field displays the MAC address of the WAN interface of this X6004.
LAN MAC	This field displays the MAC address of the LAN interface of this X6004.
Set	Click Set to save your changes.
Cancel	Click Cancel to go back to the previous screen without saving your changes.
Reset	Click Reset to reset the screen to the last saved configuration.

23.3 ZyStack Intranet Setup

Use this screen to manage local subnets from which IP phones connect to the X6004s in the ZyStack. Click **Configuration > ZyStack > Intranet** to view the following screen.

Figure 219 ZyStack Intranet



The following table describes the labels in this screen.

Table 136 ZyStack Intranet

LABEL	DESCRIPTION
Delete	Select the check boxes of the intranets you want to remove and click the Delete button to remove them.
No	This field displays the index number of an intranet configured for this ZyStack.
Intranet	This field displays the intranet configured for this ZyStack. It is displayed in CIDR (Classless Inter-Domain Routing) format. The CIDR format is displayed as follows: "IP address/number of matching initial bits in the IP address". For example, 192.168.1.0/24 indicates the range of IP addresses 192.168.1.0 - 192.168.1.255 with the subnet mask 255.255.255.0 . See Appendix A on page 529 for more information on IP addresses and subnet masks.
Add / Delete	Click the Add button to add an intranet for this ZyStack. Click the Delete button to remove an existing intranet from this ZyStack.

23.3.1 ZyStack Add Intranet

Use this screen to add local subnets from which IP phones connect to the X6004s in the ZyStack. Adding network subnets helps to increase the efficiency of call routing. Click **Add** in the **Configuration > ZyStack > Intranet** screen to view the following screen.

Figure 220 ZyStack Add Intranet

The following table describes the labels in this screen.

Table 137 ZyStack Add Intranet

LABEL	DESCRIPTION
IPv4 subnet in CIDR format	Type the IP address which identifies this network and specify how many initial bits in the IP address of a host must match. The subnet is specified via CIDR (Classless Inter-Domain Routing) format. The CIDR format is displayed as follows: "IP address/number of matching initial bits in the IP address". For example, 192.168.1.0/24 indicates the range of IP addresses 192.168.1.0 - 192.168.1.255 with the subnet mask 255.255.255.0 . See Appendix A on page 529 for more information on IP addresses and subnet masks.
Add	Click Add to save your changes.
Cancel	Click Cancel to go back to the previous screen without saving your changes.

23.4 ZyStack Status

Use this screen to view the status of the ZyStack as well as perform network connectivity tests between X6004s. Click **Configuration > ZyStack > Status** to view the following screen.

Figure 221 ZyStack Status

Machine ID	Description	Type	Update Update All	Ping Ping All	Delete
IPPBX_001	Localhost	Master	N/A	N/A	N/A

Refresh

Machine ID	Serial	Fail Reason	Clear Log
------------	--------	-------------	-----------

The following table describes the labels in this screen.

Table 138 ZyStack Status

LABEL	DESCRIPTION
ZyStack Status List	This table displays the X6004s participating in the ZyStack and their current status.
Machine ID	This field displays the system name of the X6004. The system name is automatically assigned to the X6004 based on when it was added to the ZyStack. IPPBX_001 is always the master followed by slaves IPPBX_002 , IPPBX_003 and so on.
Description	This field displays the description of this ZyStack member.
Type	This field displays the role this X6004 performs in the ZyStack. The options are: <ul style="list-style-type: none"> • Master - controls configuration on all the other X6004s. • Slave - all configuration is done on the slave from the master X6004.
Update/ Update All	Click an Update button refresh the item's information on this screen, or click Update All to refresh all of the information.
Ping	Click a Ping button to test IP connectivity with one member of the ZyStack or click Ping All to test IP connectivity with all members of the ZyStack. This field displays N/A when this function is not available for a specified X6004. This field displays Ok if you have a network connection from the master to the slave X6004.

Table 138 ZyStack Status (continued)

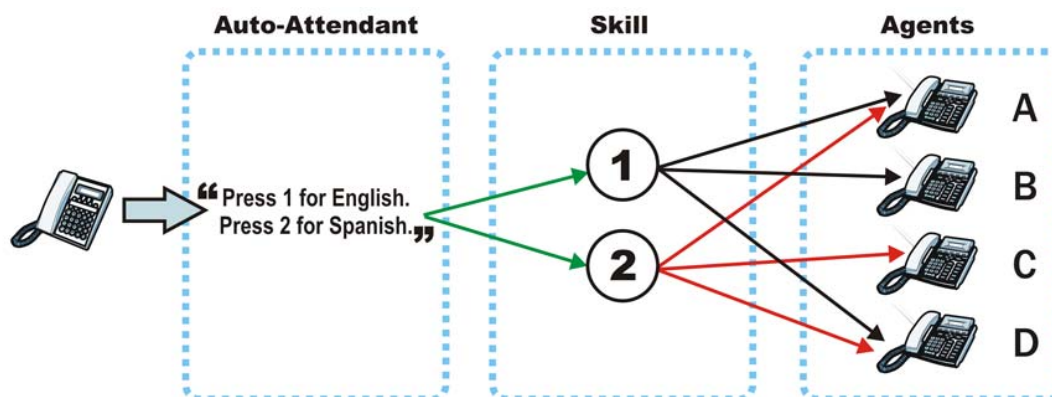
LABEL	DESCRIPTION
Delete	<p>This field displays the reason for not being able to delete an X6004 from the ZyStack. The field displays as the following followed by hyphen and a ZyStack X6004 serial number. For example, "timeout-b471c385" where b471c385 is a serial number.</p> <ul style="list-style-type: none"> • timeout displays if the master X6004 was unable to establish a connection with the X6004 that you wanted to remove from the ZyStack. • wrong master displays if the X6004 is already a member of another ZyStack. • wrong serial displays if the serial number did not match when removing this X6004 from the ZyStack. • N/A displays when the delete function was not performed or X6004(s) were successfully deleted from the ZyStack.
ZyStack Add Failure Log	This table is a list of log entries regarding successful and unsuccessful attempts to add X6004s to the ZyStack.
Machine ID	This field displays the system name of the X6004. The system name is automatically assigned to the X6004 based on when it was added to the ZyStack. IPPBX_001 is always the master followed by slaves IPPBX_002 , IPPBX_003 and so on.
Serial	This field displays the serial number that was entered when trying to add this X6004 to the ZyStack.
Fail Reason	<p>This field displays the reason for not being able to add an X6004 to the ZyStack. The field displays:</p> <ul style="list-style-type: none"> • timeout - if the master X6004 was unable to establish a connection with the X6004 that wanted to join the ZyStack. • wrong master - if the X6004 is already a member of another ZyStack. • wrong serial - if an incorrect serial number was entered when adding this X6004 to the ZyStack.
Clear Log	Click the Clear button to erase a ZyStack failure log.

24.1 Overview

This chapter shows you how to configure Automatic Call Distribution (ACD). ACD utilizes Skill-Based Routing (SBR), which allows you to distribute incoming calls to specific groups of phones based on assigned skills.

When the X6004 receives an incoming call, the auto-attendant presents the caller with a list of available skills and the key codes to access them. Each skill is linked to a specific group of agents. One agent from the group can be selected to answer the incoming call based on the rules defined by the associated skill.

Figure 222 ACD Example



For example, a call comes in and the X6004 prompts the caller with an auto-attendant greeting, asking him to choose which “skill” he requires: an English-speaking (1) or Spanish-speaking (2) representative. In this case, the auto-attendant’s message may say something to the effect of “Thank you for calling Acme Mail Order Company. Press 1 for English service, o selecciones el número 2 para Español.” Once the caller makes his selection, the call is routed to an agent according to the skill rule set. If the caller presses the 1 key for English then, the X6004 routes the call to 1 of 3 available agents (A, B, and D) whose IDs appear in the English skill’s associated agent list and based upon their current availability.

24.1.1 What You Can Do in this Chapter

- Use the **ACD Global** screen to set the global “wrap up” time for each extension in the ACD system. See [Section 24.2 on page 368](#).
- Use the **Agent** screen to manage the ACD agent identities. See [Section 24.3 on page 369](#).
- Use the **Skill** screen to manage the ACD skills. See [Section 24.4 on page 371](#).
- Use the **Skill Menu** screen to create menus that a caller can use while in the queue waiting for an agent to respond. See [Section 24.5 on page 377](#).

24.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Agent

An agent is a member of an Automated Call Distribution system who receives incoming calls. Agents are usually classified according to “skills”. For example, a customer support representative in an automotive parts company may be classified as a member of the “Brakes and Tires” skill. As such, the X6004 auto attendant would only route calls to him related to those two topics.

Agent Feature Code

The agent-specific feature code is: ****03**. This allows an agent to get a login prompt and log into the X6004 to notify the device that his extension is a member of the Automated Call Distribution system. This code is also used to log out.

When logged in as an agent, you can put your phone on “pause” status so it temporarily cannot receive incoming calls from the X6004. To do so, type: ****04**. Type it a second time to un-pause your phone.

Note: This feature code cannot be modified. For more information on feature codes and how to use them, see [Section 6.8 on page 141](#).

Skill

In the context of ACD, a skill is a set of rules that bridge the auto-attendant on one side and the agents on the other. The rules tell the X6004 exactly how to route calls to specific agents based on the input it receives from the caller interacting with the auto-attendant.

Auto-Attendant




The X6004's auto-attendant feature is an integral part of the ACD system. When a caller first dials in, the auto-attendant receives the call. The auto-attendant then passes the call to the ACD system.

To link the ACD system with the auto-attendant feature:

- 1 Create at least 2 agent identities in the ACD system ([Section 24.3 on page 369](#)) to ultimately receive incoming calls after they have been routed by the X6004. You can click **Configuration > ACD > Agent** to open this screen.

Agent List					
Delete					
Add : Edit : Delete					
<input type="checkbox"/>	Agent ID	Agent Name	Description	Create Time	
<input type="checkbox"/>	6000	Charles	South American Sales	2009/04/13 11:32:21	 
<input type="checkbox"/>	6002	Theresa	South American Sales	2009/04/13 11:32:37	 

- 2 Define at least 1 skill in the ACD system ([Section 24.4 on page 371](#)). The rules defined here will help the X6004 properly route calls to the agent identities created in step 1. You can click **Configuration > ACD > Skill** to open this screen.

Skill List					
Delete					
Add : Edit : Delete					
<input type="checkbox"/>	Number	Skill Name	Description	Create Time	
<input type="checkbox"/>	55556	North_America	English	2009/04/13 14:41:32	 

- Finally, link the skill with your auto-attendant by forwarding calls from it to the skill you created in step 2 ([Section 19.3.2 on page 297](#)). You can click the **Advanced** icon in the **Configuration > PBX > Outbound Line Management > Auto-Attendant > Customized** to open this screen.

Office Hour Setting [Advertising]

Audio File Upload

Audio File State Uploaded

Dial Extension Number Enable Disable

Forward to a specific extension directly (Extension)

Operator

Key

Extension

Action for Time Out

Hang up

Extension

ACD

Options

Key	Description	Action	Extension	
1	North American Sales	Forward to skill	55556/North_America	<input type="button" value="edit"/> <input type="button" value="delete"/>

24.2 The ACD Global Screen

Use this screen to set the global “wrap up” time for each extension in the ACD system. This is how long the X6004 waits before sending new calls to the agent.

Click **Configuration > ACD > ACD Global** to open this screen.

Figure 223 ACD > ACD Global Setting

ACD Global Setting

Wrap Up Time second(s)

Each field is described in the following table.

Table 139 ACD > ACD Global Setting

LABEL	DESCRIPTION
Wrap Up Time	Enter a number of seconds here that the X6004 waits before re-queuing the agent to receive new incoming calls. You can enter a number between 1 and 86400.
Apply	Click this to save your changes.

24.3 The Agent Screen

This screen allows you to manage the X6004's agent identities. It can also serve as a jumping off point for creating new ones or editing ones previously created.

Click **Configuration > ACD > Agent** to open this screen.

Figure 224 ACD > Agent List

Agent List					
<input type="checkbox"/>	Agent ID	Agent Name	Description	Create Time	
<input type="checkbox"/>	6000	Charles	South American Sales	2009/04/13 11:32:21	
<input type="checkbox"/>	6002	Theresa	South American Sales	2009/04/13 11:32:37	
<input type="checkbox"/>	6004	Guiseppe	Riviera Sales (EU)	2009/04/13 11:33:59	
<input type="checkbox"/>	6006	Evangeline	Riviera Sales (EU)	2009/04/13 11:34:34	
<input type="checkbox"/>	6008	Sue	North American Sales	2009/04/13 11:34:56	

Each field is described in the following table.

Table 140 ACD > Agent List

LABEL	DESCRIPTION
Delete	Click this button to remove any selected entries from the list.
Select	Check a box in an entry row to flag it for deletion.
Agent ID	This indicates the identification number of the agent.
Agent Name	This indicates the name of the agent.
Description	This displays a brief description about the agent.
Create Time	This indicates when this agent identity was created.
Add	Click this to add a new agent to the list.
Edit	Click this to modify an existing agent's information.

24.3.1 The Agent Settings Screen

Use this screen to create or edit an agent's settings.

Click either the **Add** or **Edit** icons in the **Agent List** screen to display the options as shown next.

Figure 225 Agent List > Agent Setting

Agent Setting	
Agent ID	<input type="text" value="6010"/>
Password	<input type="password" value="••••"/>
Agent Name	<input type="text" value="Fieval"/>
Description	<input type="text" value="Central European Sales"/>
Create Time	

Each field is described in the following table.

Table 141 Agent List > Agent Setting

LABEL	DESCRIPTION		
Agent ID	<p>Enter an identification number for this agent. It can be any combination of 3~20 digits (0-9). No spaces, underscores, or hyphens are allowed.</p> <p>An agent must use this ID to log into the ACD system.</p> <p>Note: To get a login prompt, enter the feature code ***03 on your phone's keypad. You can also use this code to log out later.</p>		
Password	<p>Enter a password for this agent. It can be any combination of 1~32 digits (0-9). No spaces, underscores, or hyphens are allowed.</p> <p>An agent must use this password to log into the ACD system.</p> <p>Note: To get a login prompt, enter the feature code ***03 on your phone's keypad. You can also use this code to log out later.</p>		
Agent Name	<p>Enter the name of the agent associated with this ID. It can be any combination of 1~32 alphanumeric characters (a-z, A-Z, 0-9). No asterixes (*) or exclamation points (!) allowed.</p>		
Description	<p>Enter a description for this agent ID. It can be any combination of 0~64 alphanumeric characters (a-z, A-Z, 0-9). No asterixes (*) or exclamation points (!) allowed.</p>		
Create Time	<p>When you create a new agent identity, this field is blank.</p> <p>However, when you edit an existing agent identity, this field indicates the date and time when the ID was created.</p> <table border="1" data-bbox="553 1787 1179 1839"> <tr> <td>Create Time</td> <td>2009/04/13 14:07:03</td> </tr> </table>	Create Time	2009/04/13 14:07:03
Create Time	2009/04/13 14:07:03		

Table 141 Agent List > Agent Setting (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

24.4 The Skill Screen

This screen allows you to manage the ACD skills. It can also serve as a jumping off point for creating new ones or editing ones previously created.

Click **Configuration > ACD > Skill** to open this screen.

Figure 226 ACD > Skill List

Skill List						
Delete						:Add :Edit :Delete
<input type="checkbox"/>	Number	Skill Name	Description	Create Time	<input type="checkbox"/>	
<input type="checkbox"/>	55555	South_America	Portuguese and Spanish	2009/04/13 11:52:34	<input type="checkbox"/>	
<input type="checkbox"/>	55556	North_America	English	2009/04/13 14:41:32	<input type="checkbox"/>	
<input type="checkbox"/>	55557	Riviera_EU	French and Italian	2009/04/13 14:42:28	<input type="checkbox"/>	
<input type="checkbox"/>	55558	Central_Europe	Czech	2009/04/13 14:43:11	<input type="checkbox"/>	
Delete						

Each field is described in the following table.

Table 142 ACD > Skill List

LABEL	DESCRIPTION
Delete	Click this button to remove any selected entries from the list.
Select	Check a box in an entry row to flag it for deletion.
Number	This indicates the phone number dialed to reach the agents associated with this particular skill.
Skill Name	This indicates the name of the skill.
Description	This displays the description associated with this skill.
Create Time	This indicates the time and date the skill was created.
Add	Click this to add a new skill to the list.
Edit	Click this to modify an existing skill's information.

24.4.1 The Skill Settings Screen

Use this screen to create or edit a skill.

A skill allows you to create rules for routing calls to a specific group of agents. You can also manage how calls to those agents are handled in the event that one or more of them is not logged on, or engaged in a conversation, and so on. Skills work in tandem with the auto-attendant. When a call comes in, the auto-attendant presents an automated menu system that guides the caller to a specific skill and from there to an agent.

Click either the **Add** or **Edit** icons in the **Skill List** screen to display the options as shown next.

Figure 227 Skill > Skill Setting

Skill Setting

Number	55555		
Skill Name	South_America		
Description	Portuguese and Spanish		
Skill Menu	-----		
Ring Strategy	Least Recent		
No Login Action	Hang Up		
No Available Action	Join		
Timeout Action	No Timeout		
Waiting Music	default		
Max. Waiting Calls	64		
Waiting Timeout	180	sec.	
Ring Agent Timeout	15	sec.	
Service Level	30	sec.	
Position Report Frequency	60	sec.	(0:disable)
Periodic Announce Frequency	60	sec.	(0:disable)
Announce	x	Playback	Browse... Upload
Periodic Announce	x	Playback	Browse...
Create Time	2009/04/13 11:52:34		

Skill Member

Priority : 1

Available Exten.	Member
6004/Giuseppe 6006/Evangeline 6008/Sue 6010/Fieval	6000/Charles:1 6002/Theresa:1

Each field is described in the following table.

Table 143 Skill > Skill Setting

LABEL	DESCRIPTION
Skill Setting	
Number	<p>Enter the number to be dialed that uses this skill. It can be any combination of 3~20 digits (0-9). No spaces, underscores, or hyphens are allowed.</p> <p>When this screen is in Edit mode, this number cannot be changed.</p>
Skill Name	<p>Enter a name for this skill. It can be any combination of 1~32 alphanumeric characters (a-z, A-Z, 0-9). No asterixes (*) or exclamation points (!) allowed.</p>
Description	<p>Enter a description for this skill. It can be any combination of 0~64 alphanumeric characters (a-z, A-Z, 0-9). No asterixes (*) or exclamation points (!) allowed.</p>
Skill Menu	<p>Associate this skill with a skill menu. For more on skill menus, see Section 24.5.1 on page 378.</p>
Ring Strategy	<p>Select the method for the X6004 to decide the ring order of extensions associated with this skill.</p> <ul style="list-style-type: none"> • Least Recent - This action rings the agent associated with this skill who was least recently called. • Round Robin with Memory - This strategy takes turns ringing each available agent associated with this skill. Once an extension picks up, it is put at the end of the queue for the next ring cycle; the next agent in the list is then rung first when a new call comes in. • Round Robin - This strategy takes turns ringing each available agent associated with this skill. • Fewest Calls - This strategy rings the agents who have received the fewest number of calls, in order, from lowest to highest. • Ring All - This strategy rings all extensions at the same time until one answers. • Random - This strategy rings a random extension.

Table 143 Skill > Skill Setting (continued)

LABEL	DESCRIPTION
No Logon Action No Available Action Timeout Action	<p>Available fields:</p> <ul style="list-style-type: none"> • No Logon Action - If all agents associated with a skill do not log in or log off, then this item defines how the X6004 responds when calls are sent to them. • No Available Action - If no agent associated with this skill is available to take a call, then this item defines how the X6004 responds when calls are sent to that agent. • Timeout Action - If a call to an agent associated with this skill times out, then this item defines how the X6004 responds when calls are sent to that agent. <p>Possible actions are:</p> <ul style="list-style-type: none"> • Join - This action puts the call back in the queue for other extensions within this skill. (No Available Action only.) • No Timeout - This action keeps the caller on the line indefinitely while the extension is rung. (Timeout Action only.) • Hang Up - This action disconnects the call. • Backup Skill - This action sends the call to the next skill if one is associated with this one. When you select this option and you have already configured more than 1 skill, a submenu with all available skill appears. <div data-bbox="597 905 1076 947" style="border: 1px solid black; padding: 2px;"> Backup Skill <input type="text"/> </div> <ul style="list-style-type: none"> • Auto Attendant - This action routes the call back to the auto attendant system that first greeted the caller. • Extension - This action forwards the call to the specified extension. When you select this option, a field allowing you to input a destination extension appears to the right of it. <div data-bbox="597 1123 1068 1171" style="border: 1px solid black; padding: 2px;"> Extension <input type="text"/> </div> <ul style="list-style-type: none"> • Voice Mail - This action engages the extension owner's voice mail.
Waiting Music	Select the music to play while a caller waits for an agent to pick up. For more on Music On Hold, see Section 22.4 on page 333 .
Max. Waiting Calls	Enter the maximum number of calls (up to 999) to be put on hold while calling the agents associated with this skill.
Waiting Timeout	<p>Enter the duration in seconds (up to 99999) that the call to the agents associated with the skill rings before timing out.</p> <p>Once a call times out, the action defined in Timeout Action applies. This timeout only applies to calls in the queue that have not yet been routed to a particular agent.</p>
Ring Agent Timeout	<p>Enter the duration in seconds (up to 99999) that a call to a specific agent associated with this skill rings before timing out.</p> <p>Once a call times out, it is routed to a different agent.</p>
Service Level	Enter the duration in seconds (up to 99999) in which the agent associated with this skill has to pick up for it to be considered 'good service'. You can view skill-related service reports in Monitor > Status Observation > ACD Queue . See Chapter 26 on page 385 for details.

Table 143 Skill > Skill Setting (continued)

LABEL	DESCRIPTION
Position Report Frequency	<p>Enter the duration in seconds (up to 99999) that the X6004 waits before informing the caller on hold what their current position in the queue is. This report occurs periodically and continues until either the caller hangs up or the agent answers.</p> <p>For example, if a caller is second in the queue then the X6004 may say, "You are currently call number 2" every 60 seconds.</p> <p>If you enter a "0" for this field, the option is disabled.</p>
Periodic Announce Frequency	<p>Enter the duration in seconds (up to 99999) that the X6004 waits before playing a previously uploaded audio file. This announcement occurs periodically and continues until either the caller hangs up or the agent answers.</p> <p>For example, a caller to the Acme Mail Order Company may hear, "Thank you for calling us. A service representative will be with you momentarily" every 240 seconds.</p> <p>If you enter a "0" for this field, the option is disabled.</p>
Announce Periodic Announce	<p>Available fields:</p> <ul style="list-style-type: none"> • Announce - The X6004 plays this file first when the agent answers the phone, then it connect his phone to the call. It can be used to announce which skill the incoming caller requires, which is especially useful when one agent is associated with multiple skills. For example, if an agent is associated with the skills "English" and "Spanish", then the announce audio file played before receiving a call sent to him by way of the English skill may say "This caller speaks English." • Periodic Announce - The X6004 plays this file to a caller on hold every X number of seconds and can be used to keep the caller apprised of their status. For example, a caller may hear the following every 30 seconds: "Thank you for your patience. Please continue holding." <p>Possible actions are:</p> <ul style="list-style-type: none"> • Click the Browse button to find an audio file on your computer that you want to upload. • Click the Upload button to upload the selected file to the X6004. • Click the Playback button to listen to the audio file once it has been uploaded. • Click the X button to delete an uploaded audio file. <p>The audio files you upload must meet the following criteria:</p> <ul style="list-style-type: none"> • G.711 format voice file (*.wav), μ-law 8-bit mono mode. • Size limit of a single announcement cannot exceed 1 MB. • Size limit of all voice files is 10 Mb per X6004 (or per ZyStack).
Create Time	<p>This indicates when a skill was created. If you are creating a new skill, then this field remains blank until you click the Apply button.</p>
Skill Member	

Table 143 Skill > Skill Setting (continued)

LABEL	DESCRIPTION
Priority	<p>Select an agent from the Available Exten. list, then choose a priority. The priority indicates to whom the incoming calls are routed first.</p> <p>The highest priority is 1 while the lowest priority is 5.</p> <p>If multiple agents share the same priority, then the Ring Strategy applies first to the highest priority group, then if all those agents are engaged it applies to the next group, and so on.</p>
Available Exten.	This list indicates all available agents in the X6004.
Member	This list indicates all members who are assigned to this skill.
< and >	Use the arrow buttons to add from the Available Exten. list to the Members list. You can also remove agents from the Members list.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

24.5 The Skill Menu Screen

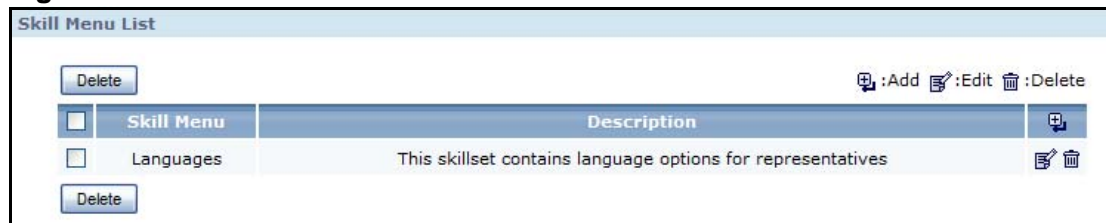
This screen allows you to create menus that a caller can use while in the queue waiting for an agent to respond. Skill menus are self-contained auto-attendants limited to the ACD system.

For example, if a caller enters the queue for the “English” skill but an English-speaking sales representative hasn’t yet picked up, he will periodically hear “Press 0 to exit. Press 3 for a Spanish-speaking representative. Press 4 for a French-speaking representative. Press 5 for a Russian-speaking representative.”

The **Periodic Announce** settings for a skill menu can be configured in the **Skill Settings** screen. See [Section 24.4.1 on page 372](#) for more details.

Click **Configuration > ACD > Skill Menu** to open this screen.

Figure 228 ACD > Skill Menu



Each field is described in the following table.

Table 144 ACD > Skill Menu

LABEL	DESCRIPTION
Skill Menu	This indicates the name for this skill menu.
Description	This indicates the description for this skill menu.
Delete	Click this to remove any selected entries from the list.
Select	Check a box in an entry row to flag it for deletion.
Add	Click this to add a new skill menu to the list.
Edit	Click this to modify an existing skill menu's information.

24.5.1 The Skill Menu Settings Screen

Use this screen to create or edit a skill menu.

Click either the **Add** or **Edit** icons in the **Skill Menu** screen to display the options as shown next.

Figure 229 The Skill Menu Screen

Code	Action
0	exit
1	goto 55556/North_America
2	goto 55555/South_America
4	goto 55557/Riviera_EU
5	goto 55558/Central_Europe

Each field is described in the following table.

Table 145 Skill Menu

LABEL	DESCRIPTION
Skill Menu	Enter a name for this skill menu. It can be any combination of 3~20 alphanumeric characters (a-z, A-Z, 0-9). Spaces, underscores, and hyphens are allowed. You cannot begin the name with a digit.
Description	Enter a description for this skill menu. It can be any combination of 0~64 alphanumeric characters (a-z, A-Z, 0-9). Spaces, underscores, and hyphens are allowed.
Delete	Click this button to remove any selected entries from the list.
Select	Check a box in an entry row to flag it for deletion.
Code	Select a keypad code that a caller can press to engage the associated action. A single code can only be used once within a skill menu. This column in the list indicates the code for a list item.
Action	Select an action that happens when a caller presses an associated keypad code. The action is linked to the skills created on the Configuration > ACD > Skill screen. This column in the list indicates the action for a list item.
Add	Click this to add an associated Code and Action pair to the list.
Apply	Click this to save your changes.
Cancel	Click this to go back to the previous screen without saving your changes.

Monitor

25.1 Overview

This chapter shows you how to view system information and configure SNMP settings via the **Monitor** screens.

25.2 The System Information Screen






The **System Information** screen allows you to view essential information about the X6004. Click **Monitor > System Information** in the web configurator to view the screen as shown.

Figure 230 Monitor > System Information

System Information									
#	IP Address		ZyStack	Status	F/W Version				
	WAN	LAN							
1	172.23.31.1	192.168.1.12	Master	On	1.11(AVA.0)b3				

Hardware Information								
#	CPU(MIPS):	Memory(MB):	File System:	Trunk(port#)				DSP
				FXO	FXS	BRI	PRI	
1	627.50	257	256MB	4	4	4	1	96

IPPBX Information									
#	Outbound Line					License			
	FXO Trunk	SIP Trunk	Trusted Peer	PRI	BRI	Extension	softphone	Attendant Console	Click-to-talk
1	4	0	0	1	0	32	8	0	0

Device Monitor						
#	File System:			Extension		
	Flash	HDD		SIP	FXS	BRI
1	 59%	 N/A		 46%	 0%	 0%

Each field is described in the following table.

Table 146 Monitor > System Information

LABEL	DESCRIPTION
System Information	
#	This field displays the index number of the X6004. If you have a ZyStack configured then this screen displays information about all the X6004 in the ZyStack.
IP Address	These two fields display the IP addresses of the WAN and LAN interfaces on the X6004.
ZyStack	This field displays: Master - if the X6004 is the master for all of the X6004s in a ZyStack. This field also displays Master if this X6004 is set up as a stand alone IP PBX. Slave - if this X6004 is a slave in a ZyStack.
Status	This field displays: On - If the X6004 is powered on. Off - If this X6004 is not receiving power.
F/W Version	This field displays the firmware version currently installed on the X6004.
Hardware Information	
#	This field displays the index number of the X6004. If you have a ZyStack configured then this screen displays information about all the X6004 in the ZyStack.
CPU(MIPS)	This field displays the speed of the processing chip on the X6004 in MIPS (Millions of Instructions Per Second).
Memory(MB)	This field displays the total RAM memory available on the X6004. This is the memory available for processing functions on the X6004.
File System	This field displays the total memory available for the files system on the X6004. The file system stores information such as configuration settings, CDR and voice mail. This number is the sum of the built in flash memory and the optional hard disk (if installed).
Trunk(port#)	These fields display the number of FXO ports (ports leading to the PSTN), FXS ports (ports leading to analog phones on your network), ISDN BRI or PRI ports (ports leading to the ISDN) installed on the X6004.
DSP	This field displays the capacity of the DSP (Digital Signal Processing) modules installed on the X6004. The capacity is displayed in the number of channels the X6004 can process at any one time.
IPPBX Information	
#	This field displays the index number of the X6004. If you have a ZyStack configured then this screen displays information about all the X6004 in the ZyStack.

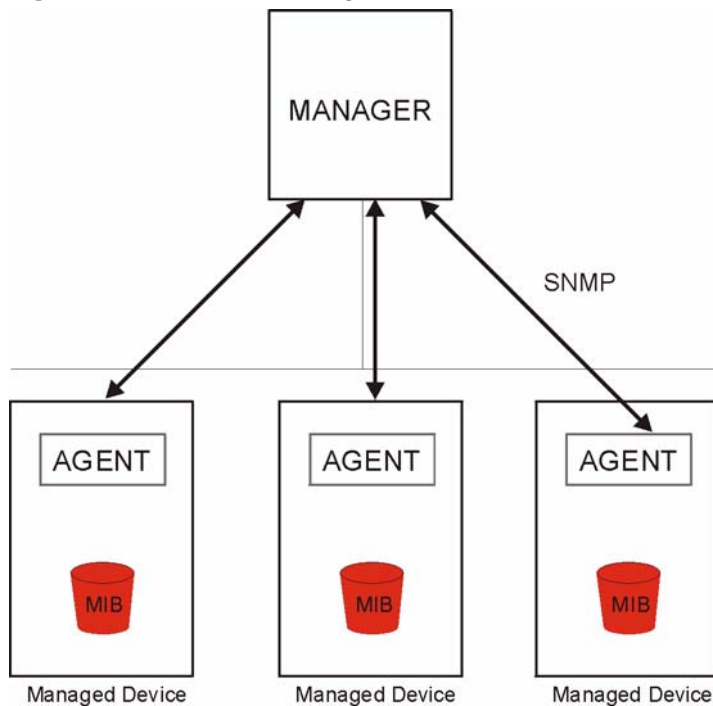
Table 146 Monitor > System Information (continued)

LABEL	DESCRIPTION
Outbound Line	<p>These fields display the number of outside lines configured on the X6004. They are divided into the following categories:</p> <ul style="list-style-type: none"> • FXO Trunk - the available connections via the FXO ports to your local telephone company. • SIP Trunk - the number of SIP connections you have configured to SIP server(s) at your VoIP provider. • Trusted Peer lines - the number of connections you have configured to peer SIP device(s). A peer SIP device could be another X6004 or another SIP server that allows you to use its services. • PRI lines - the number of PRI ports available on the X6004. • BRI lines - the number of BRI ports you have configured for outbound lines on the X6004.
License	<p>These fields display the number of licenses you have for subscription services via myZyXEL.com website. The services are divided into the following categories:</p> <ul style="list-style-type: none"> • Extension - This is the number of SIP extensions you can configure on the X6004. • softphone - This is the number of ZyXEL's V100 softphones you can register with the X6004. • Attendant Console - This is the number of attendant consoles you can configure on the X6004. • Click-to-Talk - This is the number of CTT extension you can configure on the X6004.
Device Monitor	
#	<p>This field displays the index number of the X6004. If you have a ZyStack configured then this screen displays information about all the X6004 in the ZyStack.</p>
File System	<p>These fields display the current utilization of the available memory on the X6004. They are divided into the following categories:</p> <ul style="list-style-type: none"> • Flash - This field displays the percentage of the total built in memory currently being used up on the X6004. • HDD - If an external hard disk is installed, this field displays the percentage of your hard disk memory currently used up on the X6004. Otherwise, it displays N/A.
Extension	<p>These fields display the utilization percentage of your available SIP extensions and FXS extension. An extension is considered to be utilized as soon as it is created.</p> <p>The number of SIP extensions you are allowed to create on the X6004 is limited by the subscription service on the X6004.</p> <p>The number of FXS extensions you are allowed to create on the X6004 is limited by the number of FXS ports you have installed on the X6004. The FXS ports are used to connect analog phones to the X6004.</p> <p>The number of BRI extensions you are allowed to create on the X6004 is limited by the number of BRI MSNs available on the X6004. The BRI extensions are configured to BRI ports which connect to ISDN phones.</p>

25.3 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your X6004 supports SNMP agent functionality, which allows a manager station to manage and monitor the X6004 through the network. The X6004 supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 231 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the X6004). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

25.3.1 Supported MIBs

The X6004 supports MIB II that is defined in RFC-1213 and RFC-1215. The X6004 also supports private MIBs (pbx.mib and zyxel-pbx-Common.mib) to collect current call count, SIP peer and SIP trunk information. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the X6004's MIBs from www.zyxel.com.

25.3.2 SNMP Traps

The X6004 will send traps to the SNMP manager when any one of the following events occurs.

Table 147 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the X6004 is turned on or an agent restarts.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.

25.3.3 Configuring SNMP

To change your X6004's SNMP settings, click **Monitor > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings.

Figure 232 Monitor > SNMP

The following table describes the labels in this screen.

Table 148 Monitor > SNMP

LABEL	DESCRIPTION
Enable	Select or clear the check box to enable or disable SNMP service.
Get Community	Enter the password for the incoming Get and GetNext requests from the management station. The default is "public" and allows all requests.
Set Community	Enter the password for incoming Set requests from the management station. The default is "private" and allows all requests.
SNMP Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Trap Port	You may change the port number the X6004 uses for sending traps to the SNMP manager if needed.
Apply	Click Apply to save your changes back to the X6004.
Reset	Click Reset to return the screen to its last-saved settings.

Status Observation

26.1 Overview

This chapter shows you how to view detailed status information about SIP and FXS extensions as well as the FXO and SIP trunks configured on the X6004.

26.2 What You Can Do in this Chapter

- Use the **SIP Peer Status** screen to view status information about the X6004's SIP extensions. See [Section 26.3 on page 386](#).
- Use the **FXS Peer Status** screen to view status information about the X6004's FXS extensions. See [Section 26.4 on page 388](#).
- Use the **BRI Peer Status** screen to view status information about the X6004's ISDN extensions. See [Section 26.5 on page 389](#).
- Use the **CTI Peer Status** screen to view status information about the X6004's Computer Telephony Integration (CTI) connections. See [Section 26.6 on page 390](#).
- Use the **FXO Trunk** screen to view status information about external connections via FXO interface cards. See [Section 26.7 on page 391](#).
- Use the **SIP Trunk** screen to view status information about external connections to other SIP servers. See [Section 26.8 on page 392](#).
- Use the **BRI Trunk** screen to view status information about external connections via ISDN BRI interface cards. See [Section 26.9 on page 393](#).
- Use the **PRI Trunk** screen to view status information about external connections via ISDN PRI interface cards. See [Section 26.10 on page 394](#).
- Use the **ACD Queue** screen to monitor phone call activity for Automatic Call Distribution (ACD) agents. See [Section 26.11 on page 396](#).

26.2.1 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Interface Types

The **Status Observation** screens allow you to check the current status of several types of interface.

- **SIP Peers** refer to the X6004's VoIP extensions, whereas **SIP Trunk** interfaces are links to other VoIP servers (these may be located locally, or anywhere else in the world).
- FXO and FXS interfaces refer to regular analog telephone connections. In the acronym FXO (Foreign eXchange Office) the term "Office" refers to the connection's final destination (the telephone company's central office). Thus, **FXO Trunk** interfaces lead to the public telephone network. Likewise, in the acronym FXS (Foreign eXchange Station) the term "Station" refers to the connection's final destination (the user's analog telephone set). Thus, **FXS Peer** interfaces lead to the X6004's analog telephone extensions.
- BRI and PRI are types of ISDN. BRI refers to Basic Rate Interface. Basic Rate Interface connections are used for connections to the ISDN phone network (**BRI Trunk**) and also for connections to user's ISDN telephone sets (**BRI Peer**). PRI refers to Primary Rate Interface, which has a much higher capacity than standard BRI. PRI connections are therefore used only for connections to the ISDN phone network (**PRI Trunk**).

26.3 The SIP Peer Screen

Use the **SIP Peer** screen to view status information about the X6004's SIP extensions. Click **Monitor > Status Observation > SIP Peer** in the web configurator to view the screen as shown.

Figure 233 Status Observation > SIP Peer

Query							
Machine ID	all	Query	Refresh interval : 0 sec.		Apply		
SIP Peer							
Machine ID	Group Name	User Name	Extension Number	Registration Status	Call Status	Mobile Extension Status	P2P Status
IPPBX_001	Sales	1000	1000	offline	idle	No Specified	
IPPBX_001	Sales	1001	1001	offline	idle	No Specified	
IPPBX_001	Sales	1002	1002	offline	idle	No Specified	
IPPBX_001	Sales	1003	1003	offline	idle	No Specified	
IPPBX_001	Sales	1004	1004	offline	idle	No Specified	
IPPBX_001	Sales	1005	1005	offline	idle	No Specified	
IPPBX_001	Sales	1006	1006	offline	idle	No Specified	
IPPBX_001	Sales	1007	1007	offline	idle	No Specified	
IPPBX_001	Sales	1008	1008	offline	idle	No Specified	
IPPBX_001	Sales	1009	1009	offline	idle	No Specified	
IPPBX_001	CustomerSupport	2000	2000	offline	idle	No Specified	
IPPBX_001	CustomerSupport	2001	2001	offline	idle	No Specified	
IPPBX_001	CustomerSupport	2002	2002	offline	idle	No Specified	
IPPBX_001	CustomerSupport	2003	2003	offline	idle	No Specified	
IPPBX_001	CustomerSupport	2004	2004	offline	idle	No Specified	
IPPBX_001	CustomerSupport	2005	2005	offline	idle	No Specified	
IPPBX_001	CustomerSupport	2006	2006	offline	idle	No Specified	
IPPBX_001	CustomerSupport	2007	2007	offline	idle	No Specified	

Each field is described in the following table.

Table 149 Status Observation > SIP Peer

LABEL	DESCRIPTION
Query	<p>Use this section to specify your query criteria. You can select an attribute-value pair for your search. You can choose to query by:</p> <ul style="list-style-type: none"> • Machine ID - choose the X6004 (if you have a ZyStack configured) for which you want to view status details of SIP extensions. • Authority Group - select a specify authority group for which you want to view status details of SIP extensions. • Registration Status - select to view status details about SIP extension with which SIP devices have registered (online) or view status details about SIP extensions with which no SIP device is currently registered (offline). • Call Status - select whether you want to view status details about extensions that are currently busy or idle. <p>Click Query to update the status detail table in the SIP Peer section of the screen.</p>
Refresh interval	<p>Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately.</p> <p>If you do not want this screen to update periodically, enter 0.</p>
SIP Peer	This section displays the status detail table.
Machine ID	This field displays the auto-configured name of the X6004.
Group Name	This field displays the authority group name to which an extension belongs.
User Name	This field displays the user name associated with a SIP extension.
Extension Number	<p>This field displays the SIP extension number. For each SIP extension there is also a web phone extension listed in the following format web + extension number. For example, extension 1001 also has a web phone extension web1001 listed in this table. The web phone extensions allow you to see whether a web phone is being used for a specific SIP extension.</p>
Registration Status	<p>This field displays online, if an IP phone is registered with the X6004. It displays offline if no IP phone is registered with the X6004 for a specific extension.</p> <p>For the web phone feature, it displays online, if a user has logged in the web phone feature, otherwise it displays offline.</p>
Call Status	This field displays busy if a SIP extension is currently engaged, otherwise it displays idle .
Mobile Extension Status	This indicates whether the connection's mobile extension is activated or not, or if it is unspecified.
P2P Status	This indicates whether the connection is a peer-to-peer connection.
Disconnect	This icon appears when a connection is off-hook and allows you to disconnect that connection by clicking it.

26.4 The FXS Peer Status Screen

Use the **FXS Peer** screen to view status information about the X6004's FXS extensions. Click **Monitor > Status Observation > FXS Peer** in the web configurator to view the screen as shown.

Figure 234 Status Observation > FXS Peer

Machine ID	Slot	Port	Number	Call Status	Mobile Extension Status
IPPBX_001	A	1	N/A	idle	No Specified
IPPBX_001	A	2	N/A	idle	No Specified
IPPBX_001	A	3	N/A	idle	No Specified
IPPBX_001	A	4	N/A	idle	No Specified

Each field is described in the following table.

Table 150 Status Observation > FXS Peer

LABEL	DESCRIPTION
Query	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: <ul style="list-style-type: none"> • Machine ID - choose the X6004 (if you have a ZyStack configured) for which you want to view status details of FXS extensions. • Call Status - select whether you want to view status details about extensions that are currently busy or idle. Click Query to update the status detail table in the FXS Peer section of the screen.
Refresh interval	Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately. If you do not want this screen to update periodically, enter 0 .
FXS Peer	This section displays the status detail table.
Machine ID	This field displays the auto-configured name of the X6004.
Slot	This field displays the slot (A - D) where the FXS interface card is installed.
Port	This field displays the port number on the FXS interface card.
Number	This field displays the extension number associated with an FXS port or it displays N/A , if no FXS extension has been configured for an FXS port.
Call Status	This field displays busy if an FXS extension is currently engaged, otherwise it displays idle .
Mobile Extension Status	This indicates whether the connection's mobile extension is activated or not, or if it is unspecified.

26.5 The BRI Peer Status Screen

Use the **BRI Peer** screen to view status information about the X6004's ISDN extensions. Click **Monitor > Status Observation > BRI Peer** in the web configurator to view the screen as shown.

Figure 235 Status Observation > BRI Peer

Each field is described in the following table.

Table 151 Status Observation > BRI Peer

LABEL	DESCRIPTION
Query	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: <ul style="list-style-type: none"> • Machine ID - choose the X6004 (if you have a ZyStack configured) for which you want to view status details of ISDN extensions. • Call Status - select whether you want to view status details about extensions that are currently busy or idle. Click Query to update the status detail table in the BRI Peer section of the screen.
Refresh interval	Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately. If you do not want this screen to update periodically, enter 0 .
BRI Peer	This section displays the status detail table.
Machine ID	This field displays the auto-configured name of the X6004.
Slot	This field displays the slot (A - D) where the ISDN BRI interface card is installed.
Port	This field displays the port number on the ISDN BRI interface card.
MSN	This field displays the index number of MSN (Multiple Subscriber Number) which an ISDN extension number associates with.
Group	This field displays the authority group name which an ISDN extension number associates with.
Number	This field displays the extension number associated with an ISDN BRI port or it displays N/A , if no ISDN extension has been configured for a BRI port.
Call Status	This field displays busy if an ISDN extension is currently engaged, otherwise it displays idle .
Mobile Extension Status	This indicates whether the connection's mobile extension is activated or not, or if it is unspecified.

26.6 The CTI Peer Status Screen

Use the **CTI Peer** screen to view status information about the X6004's Computer Telephony Integration (CTI) connections. There are three types of CTI connection client: Outlook Plugin, TAPI, and V120. This screen displays which clients are registered through CTI.

Click **Monitor > Status Observation > CTI Peer** in the web configurator to view the screen as shown.

Figure 236 Status Observations > CTI Peer

Each field is described in the following table.

Table 152 Status Observation > CTI Peer

LABEL	DESCRIPTION
Query	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: Connected Type - choose the type of CTI connection to filter for and display. If you select all then all CTI connections display. Click Query to update the status detail table in the CTI Peer section of the screen.
Refresh interval	Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately. If you do not want this screen to update periodically, enter 0 .
CTI Peer	This section displays the status detail table.
Username	This displays the username that is making the connection.
IP Address	This displays the originating IP address of the connection.
Connected Type	This displays the type of CTI connection.

26.7 The FXO Trunk Status Screen

Use the **FXO Trunk** screen to view status information about external connections via FXO interface cards. Click **Monitor > Status Observation > FXO Trunk** in the web configurator to view the screen as shown.

Figure 237 Status Observation > FXO Trunk

Machine ID	Slot	Port	Group Name	Call Status
IPPBX_001	B	1	N/A	idle
IPPBX_001	B	2	N/A	idle
IPPBX_001	B	3	N/A	idle
IPPBX_001	B	4	N/A	idle

Each field is described in the following table.

Table 153 Status Observation > FXO Trunk

LABEL	DESCRIPTION
Query	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: <ul style="list-style-type: none"> • Machine ID - choose the X6004 (if you have a ZyStack configured) for which you want to view status details of FXO connections. • Call Status - select whether you want to view status details about FXO lines that are currently busy or idle. Click Query to update the status detail table in the FXO Trunk section of the screen.
Refresh interval	Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately. If you do not want this screen to update periodically, enter 0 .
FXO Trunk	This section displays the status detail table.
Machine ID	This field displays the auto-configured name of the X6004.
Slot	This field displays the slot (A - D) where the FXO interface card is installed.
Port	This field displays the port number on the FXO interface card.
Group Name	This field displays the outbound line group name to which an FXO line is assigned.
Call Status	This field displays busy if an FXO line is currently engaged. Otherwise, it displays idle .
Disconnect	This icon appears when a connection is off-hook and allows you to disconnect that connection by clicking it.

26.8 The SIP Trunk Status Screen

Use the **SIP Trunk** screen to view status information about external connections to other SIP servers. Click **Monitor > Status Observation > SIP Trunk** in the web configurator to view the screen as shown.

Figure 238 Status Observation > SIP Trunk

Query						
Machine ID	all	Query	Refresh interval : 0	sec.	Apply	
SIP Trunk						
Machine ID	Group Name	Rep. Number	Host	Port	Registration Status	Call Status
IPPBX_001	st01	3604	172.23.49.36	5060	online	idle

Each field is described in the following table.

Table 154 Status Observation > SIP Trunk

LABEL	DESCRIPTION
Query	<p>Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by:</p> <ul style="list-style-type: none"> • Machine ID - choose the X6004 (if you have a ZyStack configured) for which you want to view status details of SIP trunks. • Registration Status - select to view status details about SIP trunks which have successfully registered with a SIP server (online), SIP trunks which are in the process of registering with a SIP server (Auth. Sent) or SIP trunks that have failed to register with a SIP server (offline). • Call Status - select whether you want to view status details about SIP trunks that are currently busy or idle. <p>Click Query to update the status detail table in the SIP Trunk section of the screen.</p>
Refresh interval	<p>Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately.</p> <p>If you do not want this screen to update periodically, enter 0.</p>
SIP Trunk	This section displays the status detail table.
Machine ID	This field displays the auto-configured name of the X6004.
Group Name	This field displays the outbound line group name of this SIP trunk.
Rep. Number	This field displays the caller number of an active call which its callee need use to call back.
Host	This field displays the IP address of the SIP server for the SIP server associated with this SIP trunk.
Port	This field displays the port number used for SIP communication with a SIP server.

Table 154 Status Observation > SIP Trunk (continued)

LABEL	DESCRIPTION
Registration Status	This field displays online if the X6004 successfully registered with the SIP server for this SIP trunk, offline if the X6004 failed to register with the SIP server for this SIP trunk or Auth. Sent if the X6004 is in the process of registering with the SIP server associated with this SIP trunk.
Call Status	This field displays busy if a SIP line is currently engaged, otherwise it displays idle .

26.9 The BRI Trunk Status Screen

Use the **BRI Trunk** screen to view status information about external connections via BRI interface cards. Click **Monitor > Status Observation > BRI Trunk** in the web configurator to view the screen as shown.

Figure 239 Status Observation > BRI Trunk

BRI Trunk						
Machine ID	Slot	Port	Group Name	Caller ID	Called Num.	Direction
IPPBX_001	B	3	bri01	9102	2222222	Out

Each field is described in the following table.

Table 155 Status Observation > BRI Trunk

LABEL	DESCRIPTION
Query	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: <ul style="list-style-type: none"> • Machine ID - choose the X6004 (if you have a ZyStack configured) for which you want to view status details of ISDN BRI connections. • Direction - select which direction of calls you want to view status details about ISDN BRI lines. Select In for incoming calls, Out for outgoing calls or all for both incoming and outgoing calls. Alternatively, select N/A to display configured BRI trunk(s) without any calls over it. Click Query to update the status detail table in the BRI Trunk section of the screen.
Refresh interval	Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately. If you do not want this screen to update periodically, enter 0 .
BRI Trunk	This section displays the status detail table.
Machine ID	This field displays the auto-configured name of the X6004.

Table 155 Status Observation > BRI Trunk (continued)

LABEL	DESCRIPTION
Slot	This field displays the slot (A - D) where the ISDN BRI interface card is installed.
Port	This field displays the port number on the ISDN BRI interface card.
Group Name	This field displays the outbound line group name to which an ISDN BRI line is assigned.
Caller ID	This field displays the caller identifier of a call or N/A for configured BRI trunk(s) without any calls over it.
Called Num.	This field displays the dialed number of a call or N/A for configured BRI trunk(s) without any calls over it.
Direction	This field displays In for an incoming call, Out for an outgoing call, N/A for configured BRI trunk(s) without any calls over it.

26.10 The PRI Trunk Status Screen

Use the **PRI Trunk** screen to view status information about external connections via PRI interface cards. Click **Monitor > Status Observation > PRI Trunk** in the web configurator to view the screen as shown.

Figure 240 Status Observation > PRI Trunk

Query						
Machine ID	IPPBX_001	Query	Refresh interval : 0 sec. <input type="button" value="Apply"/>			
PRI Trunk						
Machine ID	Slot	Port	Group Name	Caller ID	Called Num.	Direction
IPPBX_001	D	1	PRI1	9102	2222222	Out

Each field is described in the following table.

Table 156 Status Observation > PRI Trunk

LABEL	DESCRIPTION
Query	<p>Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by:</p> <ul style="list-style-type: none"> • Machine ID - choose the X6004 (if you have a ZyStack configured) for which you want to view status details of ISDN PRI connections. • Direction - select which direction of calls you want to view status details about ISDN PRI lines. Select In for incoming calls, Out for outgoing calls or all for both. Alternatively, select N/A to display configured PRI trunk(s) without any calls over it. <p>Click Query to update the status detail table in the PRI Trunk section of the screen.</p>
Refresh interval	<p>Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately.</p> <p>If you do not want this screen to update periodically, enter 0.</p>
PRI Trunk	This section displays the status detail table.
Machine ID	This field displays the auto-configured name of the X6004.
Slot	This field displays the slot (A - D) where the ISDN PRI interface card is installed.
Port	This field displays the port number on the ISDN PRI interface card.
Group Name	This field displays the outbound line group name to which an ISDN PRI line is assigned.
Caller ID	This field displays the caller identifier of a call or N/A for configured PRI trunk(s) without any calls over it.
Called Num.	This field displays the dialed number of a call or N/A for configured PRI trunk(s) without any calls over it..
Direction	This field displays In for an incoming call, Out for an outgoing call or N/A for configured PRI trunk(s) without any calls over it.

26.11 The ACD Queue Screen

Use this screen to monitor phone call activity for Automatic Call Distribution (ACD) agents. Click **Monitor** > **Status Observation** > **ACD Queue** in the web configurator to view the screen as shown.

Figure 241 Status Observations > ACD Queue

The screenshot shows the ACD Queue screen with the following elements:

- Query Section:** A dropdown menu for "Skill Number/Name" set to "55555/South_America" and a "Refresh interval" field set to "0" seconds with an "Apply" button.
- ACD Queue Statistics:**
 - Number of Agents: 2
 - Agents Login: 0
 - Agents Available: 0
 - Agents on Call: 0
 - Waiting Calls: 0
 - Service Level Rate: 0.0%
 - Accepted Service Level: 30
 - Completed Calls: 0
 - Abandon Calls: 0
- Agents Table:**

Agent Name	Agent ID	Login	Extension	State	Priority	Caller ID
Charles	6000			Logoff	1	
Theresa	6002			Logoff	1	
- ACD Queue: Waiting Calls Table:**

Caller ID	Enterd Time	Waiting Time

Each field is described in the following table.

Table 157 Status Observation > ACD Queue

LABEL	DESCRIPTION
Query	Use this section to specify your query criteria. You can select an attribute, value pair for your search. You can choose to query by: Skill Number/Name - Select the ACD skill number/name for which you want to view the statistics.
Refresh interval	Enter how often (seconds) you want the X6004 to update this screen. Click Apply to update the screen immediately. If you do not want this screen to update periodically, enter 0 .

Table 157 Status Observation > ACD Queue (continued)

LABEL	DESCRIPTION
ACD Queue	<p>This section displays the current statistics for the queue on the selected Skill/Number. The following statistics are monitored:</p> <ul style="list-style-type: none"> • Number of Agents - This indicates the total number of agents associated with the selected skill. • Agents Login - This indicates how many of the agents associated with this skill are currently logged in. • Available Agents - This indicates how many of the currently logged in agents associated with this skill are available. • Agents on Call - This indicates how many of the currently logged in agents associated with this skill are engaged in phone calls. • Waiting Calls - This indicates how many calls are still in the queue for the selected skill. • Service Level Rate - This indicates the average service level score of all the agents associated with this skill who login within a single 24-period. • Accepted Service Level - This number corresponds to the Service Level setting on the Skill screen (Section 24.4 on page 371). • Completed Calls - This indicates the total number calls received and completed by all agents associated with the skill. • Abandon Calls - This indicates the total number of calls that were never answered by all agents associated with this skill. <p>Note: All of these statistics reset everyday at midnight, or if you make any changes to the associated skill/number, or if you restart the X6004. Once the statistics reset then they begin calculating anew.</p>
Agent Name	This displays the name of an agent associated with the selected skill/number.
Agent ID	This displays the ID numbers of an agent associated with the selected skill/number.
Login	This indicates the time of the agent's last login.
Extension	This displays the extension of an agent associated with the selected skill/number.
State	<p>This displays the current state of an agent associated with the selected skill/number.</p> <ul style="list-style-type: none"> • Idle - This indicates the agent associated with the selected skill/number is logged in and idle. • Busy(skill_XXXXX) - This indicates the agent associate with the selected skill/number is logged and busy. The skill that appears in parentheses indicates the skill with which he is currently occupied, if he belongs to multiple skills. • Pause - This indicates the agent associated with the selected skill/number is logged in and his account is currently paused (not receiving or making calls). • Logoff - This indicates the agent associated with the selected skill/number is not logged in.
Priority	This indicates the priority rating of the agent associated with the selected skill/number.
Caller ID	This indicates the caller ID of the most recent call to the agent associated with the selected skill/number.

Table 157 Status Observation > ACD Queue (continued)

LABEL	DESCRIPTION
ACD Queue Waiting Calls	This table displays a list all calls currently waiting in the queue for the selected skill/number.
Caller ID	This indicates the caller ID of the call.
Entered Time	This indicates the time the caller entered the queue.
Waiting Time	This indicates how long the caller has been waiting in the queue.

System Log

27.1 Overview

This chapter contains information about configuring log settings and viewing the X6004's logs.

The X6004 monitors different aspects of its operations and can be configured to record events based on the source of the event. The following are sources of events for which the X6004 can create logs:

- **IPPBX** - activities related to the PBX functions of the X6004. Some examples include: an FXS interface card failure, the setup of a new SIP extension or a ZyStack member failure.
- **User** - activities related to administrator account activities. Some examples include: a successful login of an administrator or a failure to login by an administrator.
- **myZyXEL.com** - activities related to services registered via myZyXEL.com. Some examples include: registration of additional SIP extensions or registration of ZyXEL's V100 softphones.
- **Default** - all other activities related to the functions of the X6004. Some examples include: failure to reach a DNS server or a new IP address received from a DHCP server.

27.1.1 What You Can Do in this Chapter

- Use the **View Log** screen to view current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen. See [Section 27.2 on page 402](#).
- Use the **Log Setting** screen to specify which log messages are e-mailed, where they are stored, and where they are e-mailed. See [Section 27.3 on page 405](#).

27.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Log Severity

The X6004 can also be configured to send email alerts to an administrator based on the severity of the event recorded. The following table outlines the severity levels of the logs on the X6004.

Table 158 Log Severity

SEVERITY LEVEL	DESCRIPTION	ALERT SENT?
EMERG	Emergency logs are created when the X6004 is unusable, for example a power failure.	YES
ALERT	Alert logs are created when administrative action must be taken immediately, for example the backup power supply has been activated.	YES
CRIT	Critical logs are created when a critical condition occurs on the X6004, for example the system is running low on memory.	YES
ERR	Error logs are created when an error occurs on the X6004, for example a login failure by an administrator.	NO
WARNING	Warning logs are created when a warning condition occurs on the X6004, for example when the X6004 fails to register an extension.	NO
NOTICE	Notice logs are created when normal but significant events occur on the X6004. For example, a new administrator account is created on the X6004.	NO
INFO	Information logs are created when normal events occur. For example, a successful creation of a SIP extension.	NO
DEBUG	Debugging logs are used by service and development engineers to monitor the operations of the X6004. It is recommended not to turn these logs on unless it is instructed by support technicians.	NO

27.2 The View Log Screen

The web configurator allows you to look at all of the X6004's logs in one location.

Click **Report > LOGS > System Log > View Log** to open the **View Log** screen. Use this screen to see the logs for the categories that you select in the **Log Setting** screen (see [Section 27.3 on page 405](#)). Options include logs about system errors and administrator logins.

The log records wrap around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 242 System Log > View Log

Each field is described in the following table.

Table 159 System Log > View Log

LABEL	DESCRIPTION
Logs	
Show Filter	Click this button to filter the logs you want to view. The screen changes to the one shown in Section 27.2.1 on page 404 .
Display	Select a category of logs to view; select All Logs to view logs from all of the log categories that you selected in the Log Setting page. Refer to Section 27.1 on page 401 for more information on log categories.
Email Log Now	Click Email Log Now to send the log screen to the e-mail address specified in the Log Setting page (see Section 27.3 on page 405).
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all logs.
Total logging entries	This field displays the total number of log entries on the X6004.
entries per page	Select the total number of messages that you want to display on one page.
Page	This field displays which page of the log you are currently viewing. It is in "current page/total pages" format. In other words "1/4" means that you are viewing the first page of a four page log file.
Left / Right	Click the Left button to view the previous log page or click the Right button to view the next log page.
#	This field displays a sequential number of the log.
Time	This field displays the time the log was recorded. See Section 5.5 on page 119 to configure the X6004's time and date. Click the column header to sort search results by Time .
Priority	This field displays the priority of the log. Priorities are described in Log Severity on page 402 .
Category	This field shows the category to which the log belongs.
Message	This field states the reason for the log. Click the column header to sort search results by Message .

Table 159 System Log > View Log (continued)

LABEL	DESCRIPTION
Source	This field lists the source IP address of the incoming packet. Click the column header to sort search results by Source .
Destination	This field lists the destination IP address of the incoming packet. This is typically the LAN or WAN IP address of the X6004. Click the column header to sort search results by Destination .
Note	This field displays additional information about the log entry. Click the column header to sort search results by Note .

27.2.1 Filter Log Results Screen

Use this screen to filter the logs you want to view. Click the **Show Filter** button in the **View Log** screen to bring up the log filter.

Figure 243 System Log > View Log: Show Filter

Each field is described in the following table.




Table 160 System Log > View Log: Show Filter

LABEL	DESCRIPTION
Display	Select a category of logs to view; select All Logs to view logs from all of the log categories that you selected in the Log Setting page. Refer to Section 27.1 on page 401 for more information on log categories.
Keyword	You can filter the logs to only display log entries that match a string you enter in this field. A string can be a word, a number or a combination of words and numbers. Type the string you want to search the logs for.
Priority	Select a log priority with which to filter your query results. Only logs matching the selected priority are shown. Priorities are described in Log Severity on page 402 .
Source Address	You can filter the logs to only display log entries that are created as a result of some action originating at a particular IP address. For example, an administrator logging into the X6004 from a computer with a particular IP address on your network. Type the IP address you want to search for as the source IP address of the X6004.
Destination Address	You can filter the logs to only display log entries that are created as a result of some action terminating at a particular IP address. This is typically the X6004s LAN or WAN IP address. Type the IP address you want to search for as the destination IP address of the X6004.
Search	Click Search to show the filtered results of your logs. Only the logs that match the criteria you specified are displayed.

27.3 The Log Setting Screen

The log setting screen lets you view the settings configured for the internal system log and the remote syslog servers. Use this screen to access the configuration pages for internal and external log servers. Click **Report > Logs > System Log > Log Setting** to view the screen as shown next.

Figure 244 System Log > Log Setting

Log Setting				
#	Name	Log Format	Summary	Modify
1	System Log	Internal	Mail Server : Mail Subject : Send From : Send Log to : Send Alert to : Schedule : When Full	
			Mail Server : Mail Subject : Send From : Send Log to : Send Alert to : Schedule : When Full	
2	Remote Server 1	Syslog	Server Address : Log Facility : Local 1	

Each field is described in the following table.

Table 161 System Log > Log Setting

LABEL	DESCRIPTION
#	This is an index number identifying the system and remote log servers.
Name	This field displays the name of the log servers. System Log is the name of the internal log server and Remote Server 1 through 4 are the external syslog servers.
Log Format	This field displays: Internal for the system log and Syslog for the remote log servers.
Summary	This field summarizes the settings you configured for the log servers. Click the Edit icon in the Modify column to change any of the settings that are displayed.
Modify	<p>The light bulb in this field is displayed as glowing green when the corresponding log server is activated. The light bulb is displayed as grayed out when the corresponding log server is not activated.</p> <p>Click the Edit icon to configure log settings for the system log or one of the external syslog servers.</p>
Active Log Summary	Click the Active Log Summary button to view and edit the categories the X6004 logs in the internal and external log servers.
Apply	Click the Apply button to save your changes to the X6004.

27.3.1 Active Log Summary Screen

The **Active Log Summary** screen allows you to view and edit the categories the X6004 logs in the internal and external log servers. Click the **Active Log Summary** button in the **Report > LOGS > System Log > Log Setting** screen to view the screen as shown next.

Figure 245 Log Setting > Active Log Summary

Each field is described in the following table.

Table 162 Log Setting > Active Log Summary

LABEL	DESCRIPTION
Log Category	<p>This column displays the source of log events that you can record on the X6004. The categories are:</p> <ul style="list-style-type: none"> • All Logs - All logs generated on the X6004. • IPPBX - All activities related to the PBX functions of the X6004. For example, a an FXS card failure. • User - Administrator activity, such as a successful login. • myZyXEL.com - Service registration with the myZyXEL.com website • Default - All other logs generated by the X6004. For example, failure to reach a DHCP server.
System Log	<p>Select whether you want to enable logging and the types of logs to record for each source of logs as described in the Log Category field. The choices are:</p> <ul style="list-style-type: none"> • Disable All Logs - Select this if you do not log any events. • Enable Error Logs - Select this if you want to enable error logs. • Enable Warning Logs - Select this if you want to enable warning and error logs. • Enable Notice Logs - Select this if you want to enable warning, error and notice logs. • Enable Info Logs - Select this if you want to enable warning, error, notice and info logs. • Enable All Logs - Select this to log all events.

Table 162 Log Setting > Active Log Summary (continued)

LABEL	DESCRIPTION
E-mail Server 1/2	<p>Select whether you want to send logs to the e-mail address of an administrator you specify in the Log Setting screen.</p> <ul style="list-style-type: none"> • Enable Logs - Select this to send logs to an administrator at the time interval you specify in the Log Setting screen. • Enable Alert Log - Select this to send e-mail alerts to an administrator when emergency, alert or critical level logs are created on the X6004.
Remote Server	<p>Select whether you want to send logs to the syslog servers you configure in the Log Setting screen. For each syslog server choose one of the following options:</p> <ul style="list-style-type: none"> • Disable All Logs - Select this if you do not log any events. • Enable Error Logs - Select this if you want to enable error logs. • Enable Warning Logs - Select this if you want to enable warning and error logs. • Enable Notice Logs - Select this if you want to enable warning, error and notice logs. • Enable Info Logs - Select this if you want to enable warning, error, notice and info logs. • Enable All Logs - Select this to log all events.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click Cancel to go back to the Log Setting screen without saving your changes.

27.3.2 System Log Configuration Screen

To change your X6004's log settings, click the edit icon of the **System Log** entry in the **Report > LOGS > System Log > Log Setting** screen. The screen appears as shown.

Use the **Log Settings** screen to configure to where the X6004 is to send logs; the schedule for when the X6004 is to send logs and which logs and/or immediate alerts the X6004 is to send.

Figure 246 Log Setting > Internal Log

Active Log and Alert Setting

⊗ :Disable All Logs ⊙ :Enable Logs ⊙ :Enable All Logs ⚠ :Enable Alert Log

Log Category	System Log	E-mail Server 1	E-mail Server 2
		⊗ ⊙ ⊙ ⊙ ⊙ ⊙	⊙ ⊚
All Logs	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
IPPBX	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
User	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
myZyXEL.com	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
Default	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

E-mail Server

Active

Mail Server (Outgoing SMTP Server Name or IP Address)
 Mail Subject
 Send From (E-Mail Address)
 Send Log to (E-Mail Address)
 Send Alerts to (E-Mail Address)
 Sending Log
 Day for Sending Log
 Time for Sending Log (Hour) (Minute)

SMTP Authentication
 User Name
 Password

Log Consolidation

Active
 Log Consolidation Period (seconds) (10-600)

Each field is described in the following table.

Table 163 Log Setting > Internal Log

LABEL	DESCRIPTION
Active Log and Alert Setting	
Log Category	<p>This column displays the source of log events that you can record on the X6004. The categories are:</p> <ul style="list-style-type: none"> • All Logs - all logs generated on the X6004. • IPPBX - all activities related to the PBX functions of the X6004. For example, a an FXS card failure. • User - administrator activity, such as a successful login. • myZyXEL.com - service registration with the myZyXEL.com website • Default - All other logs generated by the X6004. For example, failure to reach a DHCP server.
System Log	<p>Select whether you want to enable logging and the types of logs to record for each source of logs as described in the Log Category field. The choices are:</p> <ul style="list-style-type: none"> • Disable All Logs - Select this if you do not log any events. • Enable Error Logs - Select this if you want to enable error logs. • Enable Warning Logs - Select this if you want to enable warning and error logs. • Enable Notice Logs - Select this if you want to enable warning, error and notice logs. • Enable Info Logs - Select this if you want to enable warning, error, notice and info logs. • Enable All Logs - Select this to log all events.
E-mail Server	<p>Select whether you want to send logs to the e-mail address of an administrator you specify in the Log Setting screen.</p> <ul style="list-style-type: none"> • Enable Logs - Select this to send logs to an administrator at the time interval you specify in the Log Setting screen. • Enable Alert Log - Select this to send e-mail alerts to an administrator when emergency, alert or critical level logs are created on the X6004.
E-mail Server	
Active	Select this to activate sending logs to this E-Mail server.
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the X6004 sends.
Send From	Enter the e-mail address that you want to be in the from/sender line of the log e-mail message that the X6004 sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.

Table 163 Log Setting > Internal Log (continued)

LABEL	DESCRIPTION
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> • Daily • Weekly • Hourly • When Log is Full • None. <p>If you select Weekly or Daily, specify a time of day when the E-mail should be sent. If you select Weekly, then also specify which day of the week the E-mail should be sent. If you select When Log is Full, an alert is sent when the log fills up. If you select None, no log messages are sent.</p>
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
SMTP Authentication	<p>SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.</p> <p>Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.</p>
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Consolidation	
Active	Some logs may be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log.
Log Consolidation Period	Specify the time interval during which the X6004 merges logs with identical messages into one log.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click Cancel to go back to the Log Setting screen without saving your changes.

27.3.3 Edit Syslog Server Settings Screen

Use this screen to edit the remote syslog server settings. To access this screen, click the **Edit** icon of one of the **Remote Server** columns in the **Report > LOGS > System Log > Log Setting** screen.

Figure 247 Log Setting > Remote Log

Log Setting for Remote Server 1

Active

Server Address

Log Facility

⊗ :Disable All Logs ⊕ :Enable Logs ⊕ :Enable All Logs

Log Category	Remote Server 1					
All Logs	⊗	⊕	⊕	⊕	⊕	⊕
IPPBX	⊕	⊕	⊕	⊕	⊕	⊕
User	⊕	⊕	⊕	⊕	⊕	⊕
myZyXEL.com	⊕	⊕	⊕	⊕	⊕	⊕
Default	⊕	⊕	⊕	⊕	⊕	⊕

Each field is described in the following table.

Table 164 Log Setting > Remote Log

LABEL	DESCRIPTION
Active	Click Active to enable syslog logging.
Server Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Log Category	Select the categories of logs that you want to record. The categories are: <ul style="list-style-type: none"> • All Logs - all logs generated on the X6004. • IPPBX - all activities related to the PBX functions of the X6004. • User - administrator activity, such as a successful login. • myZyXEL.com - service registration with the myZyXEL.com website • Default -

Table 164 Log Setting > Remote Log (continued)

LABEL	DESCRIPTION
Remote Server	<p>Select which logs to send to this syslog server. Choose one of the following options:</p> <ul style="list-style-type: none">• Disable All Logs - Select this if you do not log any events.• Enable Error Logs - Select this if you want to enable error logs.• Enable Warning Logs - Select this if you want to enable warning and error logs.• Enable Notice Logs - Select this if you want to enable warning, error and notice logs.• Enable Info Logs - Select this if you want to enable warning, error, notice and info logs.• Enable All Logs - Select this to log all events.
Apply	Click Apply to save your changes back to the X6004.
Cancel	Click Cancel to go back to the Log Setting screen without saving your changes.

Call Detail Record (CDR)

28.1 Overview

This chapter shows you how to collect and manage Call Detail Records (CDRs) on the X6004.

Call Detail Records (CDRs) are telephone records containing details such as the time of call, duration of call, source telephone number and so on. The X6004 has a built in CDR database that automatically stores calls made to or from its extensions. You can search the CDR database to find out details about your organization's calls. You can also use an external database to store CDRs.

28.1.1 What You Can Do in this Chapter

- Use the **Configuration** screen to configure where to store CDR information, an administrator e-mail address to send alerts and CDR backup files for later viewing. See [Section 28.2 on page 414](#).
- Use the **Backup** screen to manage CDR backup files. See [Section 28.3 on page 417](#).
- Use the **Query** screen to query and create CDR reports. See [Section 28.4 on page 418](#).

28.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Local CDR Database

The local CDR database has limited capacity and when it is full it empties its contents into a compressed file of the call records. This file is referred to as an "Aged File". You can delete an "Aged File" or forward it to an e-mail address where it can be reviewed at a later time. The CDR database is then emptied. Whether you delete the aged file or send to an administrator, the X6004 continues to record telephone call details in an empty CDR database.

Another way to deal with the limited capacity on the local CDR database of the X6004 is to actively manage the CDR database. This requires you to create backups of the CDR database and send them to an administrator via e-mail.

Viewing Aged Files

An "Aged File" is a compressed file with the extension ".tgz". ".tgz" files can be decompressed with data compression utilities for example WinRAR or WinZIP. The result of decompressing this file are three files which can then be managed via a MySQL Database Management System (DBMS). The three files are:

- **cdr.MYD** - a MySQL data file.
- **cdr.MYI** - a MySQL index file.
- **cdr.frm** - a MySQL format file.

CDR Database Management via MySQL

MySQL is a database management system based on SQL (Structured Query Language). You can configure a MySQL server to collect CDRs from the X6004 and expand the capacity of telephone records you can collect and review.

28.2 The Configuration Screen

Use this screen to set up an external server to collect CDR information. You can also configure an administration e-mail address to which to send alerts and CDR files for later viewing.

Note: You should use a MySQL server 5.0 or above for the remote server.

You must execute the SQL script downloaded from this screen on your MySQL server before the X6004 starts to work with the remote server.

Click **Report > LOGS > CDR > Configuration** to view the screen as shown next.

Figure 248 Report > LOGS > CDR > Configuration

Each field is described in the following table.

Table 165 CDR > Configuration

LABEL	DESCRIPTION
CDR Setting	
Database Usage	This field indicates the percentage of records currently held by the database. When the local database is full, the X6004 removes all the CDRs from the local database and creates an "Aged File" (a compressed file containing all the CDRs). Use the Aged File field to specify how to deal with the compressed file containing the CDRs.
Generate CDR	Select this to record internal calls. Internal calls are calls from one extension to another extension configured on the X6004. Unselect this box if you do not want the X6004 to record internal calls.
Alert	Select this to have the X6004 send an email alert to the e-mail address specified in the E-mail Address field when the CDR database is half full.
Aged File	Specify how to deal with CDR files when the CDR database is full. Choose mail to admin. to send the CDR file to the e-mail address specified in the E-mail Address field and then delete it or drop to delete the file from the system.
Backup File Type	Select whether you want the X6004 to send a MySQL database file or a CSV file.
E-mail Address	Type the e-mail address to which you want to send the alerts indicating that the CDR file is half full. This is also the e-mail address to which complete CDR files are sent when they are full (reach approximately 20000 records).

Table 165 CDR > Configuration (continued)

LABEL	DESCRIPTION
Database Location	Use this section to specify the location and login credentials for a MySQL server that collects the CDR information from the X6004.
Use built-in server	Select this to have the X6004 use the built-in MySQL server to collect CDR information.
Use remote server	Select this to have the X6004 send a record of each call to the remote MySQL server you specify in the Server field.
Server	Type the IP address or the domain name of the server to which you want to send your CDR files. Then type the port number on which the remote server receives records of telephone calls from the X6004.
Username	Type the username of the account set up on a remote server to which you want to send your CDR files.
Password	Type the password of the account set up on a remote server to which you want to send your CDR files.
Schema script	Click Download to download a SQL script (cdr.sql). Execute the script in your external database server to establish a database to work with your X6004.
Apply	Click the Apply button to save your changes.

28.2.1 Configure your remote server

The procedure to configure your remote server is as follows:

- 1 Fill in all fields in the **Report > LOGS > CDR > Configuration** screen and then click **Download**.
- 2 Save the **cdr.sql** file to your computer.
- 3 Make sure the MySQL service is ready on the remote server.
- 4 Upload the **cdr.sql** file to your remote server (in the same directory of your installed MySQL server) and execute the file using the command shown in the first line of the **cdr.sql** file. For example, `"mysql -u sqlzyxel -p123456 < cdr.sql"` where `sqlzyxel` is the username and `123456` is the password.
- 5 After the script is successfully applied, your MySQL server can work with the X6004.

28.3 The Backup Screen

Use this screen to backup CDR files, delete existing backups of CDR files and mail CDR files to an administrator email address.

Figure 249 CDR > Backup List



Each field is described in the following table.

Table 166 CDR > Backup List

LABEL	DESCRIPTION
Backup File List	If you have a ZyStack configured using multiple X6004s, then specify the X6004 for which you want to create a backup file of the CDRs.
Filename	<p>This column displays the names of the backup CDR files currently stored on the X6004. Use the check box on the left to specify which files you want to forward or delete. The filename of the CDR takes the following format: "cdr.YYYYMMDDHHMMSS.tgz"</p> <p>Where:</p> <ul style="list-style-type: none"> • cdr - indicates this is a Call Detail Record file. • YYYYMMDD - is the year, month, and day indicating when the backup file was created. • HHMMSS - is the time of the day indicating when the backup file was created in hour, minute, second format. • tgz - indicates that this is a compressed. That can be decompressed using a compression utility such as WinRAR. The resulting decompressed files are MySQL database files that can be managed via a MySQL DBMS (Database Management System). See CDR Database Management via MySQL on page 414. <p>Note: The X6004 can store only three CDR backup files at a time. If you create a new backup file when you already have three files created, then the oldest backup file is deleted from the system.</p>
Forward	Check the boxes next to the files you want to forward to the administrator email address and click the Forward button. The files you forward to an administrator are deleted from the X6004.
Delete	If you no longer want to store a CDR file on the X6004 then check the boxes next to the files you want to delete from the X6004 and click the Delete button.
Backup Now	Click the Backup Now button to save a CDR backup file on the X6004.

28.4 The Query Screen

Use this screen to configure search criteria for call records on the X6004. You also use this screen to execute your query and create CDR reports. Click **Report > LOGS > CDR > Query** to view the screen as shown next.

Figure 250 The Query Screen

Query Condition

Start Time : [Dropdown] From : [] / [] / [] 0 : 0 [...]
 To : [] / [] / [] 0 : 0 [...]

Direction : extension / extension extension / outbound
 outbound / extension outbound / outbound

Call Time : [] ~ [] seconds [...]
 Talk Time : [] ~ [] seconds [...]

Caller Group : [] Totally Match [...]
 Channel : [] Totally Match [...] Either [...]
 Caller Number : [] Totally Match [...]
 Dialed Number : [] Totally Match [...]

Displayed Item Setting

Call Date Caller ID Caller Number
 Called Number Caller Group Src. Channel
 Dst. Channel Call Time Talk Time
 Call Result

Each field is described in the following table.

Table 167 Query

LABEL	DESCRIPTION
Query Condition	Use this section to specify your query details.
Start Time	Specify the time period for your query. Choose a specific time period from the drop down list box or fill in the From and To fields with the time range you want to search the call detail record. You can use the pop-up calendar to fill in the date fields for the To and From fields by clicking the [...] buttons and selecting the date.

Table 167 Query (continued)

LABEL	DESCRIPTION
Direction	<p>Specify the types of calls you want to view based on the source and destination of the calls. You can choose one or more of the available source - destination combinations:</p> <ul style="list-style-type: none"> • extension / extension - to view internal calls; those made from one extension to another extension on the X6004. • extension / outbound - to view calls from within your organization made to the outside world via one of the outbound lines. • outbound / extension - to view calls from the outside world to extensions configured on the X6004. • outbound / outbound - to view calls that come in from an outbound line and are routed back to the outside world via another outbound line.
Call Time	<p>Call time is the time from when a caller finishes dialing a number until one of the parties hangs up.</p> <p>Enter the range of seconds, minutes or hours to specify the length of calls that you want to search for. If you leave this field blank, then the length of the call will not be considered as a search criterion, in other words calls of all length duration are displayed unless limited by other search criteria.</p>
Talk Time	<p>Talk time is the time from when a callee picks up an incoming call until one of the parties hangs up.</p> <p>Enter the range of seconds, minutes or hours to specify the length of calls that you want to search for. If you leave this field blank, then the length of the call will not be considered as a search criterion, in other words calls of all length duration are displayed unless limited by other search criteria.</p>
Caller Group	<p>Type the name of the authority group or outbound line group for which you want to search the call detail record. Use the drop down listbox to choose Totally Match, if you want to display only call records that exactly match the criteria you type or select Partially Match, if you want to enter only a part of the group name that you want to search for. Alternatively, use the <input type="button" value="..."/> button to select the outbound line group or authority group configured on the X6004 that you want to use as your search criterion.</p>
Channel	<p>Type the name of the type of channel for which you want to search the call detail record. The channels can be either FXS extensions, FXO outbound channels, or SIP based connections. Use the drop down listbox to choose Totally Match, if you want to display only call records that exactly match the criteria you type in or select Partially Match if you want to enter only a part of the group name that you want to search for. Alternatively, use the <input type="button" value="..."/> button to select the channel configured on the X6004 that you want to use as your search criterion.</p> <p>Next use the drop down list box to select whether you want to search calls originating from this channel (SRC.), terminating via this channel (Dest.) or both (Both).</p>
Caller Number	<p>Type the telephone number of the caller for which you want to search the call detail record. Use the drop down listbox to choose Totally Match, if you want to display only call records that exactly match the criteria you type in or select Partially Match, if you want to enter only a part of the telephone number to search for.</p>

Table 167 Query (continued)

LABEL	DESCRIPTION
Dialed Number	Type the dialed telephone number of the callee for which you want to search the call detail record. Use the drop down listbox to choose Totally Match , if you want to display only call records that exactly match the criteria you type in or select Partially Match , if you want to enter only a part of the telephone number to search for.
Displayed Item Setting	Use this section to specify which details you want to display in the CDR report for each telephone call record displayed. You can choose to display the following details: <ul style="list-style-type: none"> • Call Date - The date and time the call took place (start time). • Called Number - The telephone number of a callee. • Dst. Channel - The type of outbound line group, if the callee is outside your organization or the extension type (SIP or FXS) if the callee is within your organization. • Call Result - "Answered" if the call was completed successfully, "Not Answered" if the call was not answered. • Caller ID - The username associated with the extension that partook in the call. • Caller Group - The authority group of the extension that partook in the call or the outbound line group used to make the call. • Call Time - The total duration of the call from the time the ringing started until one of the parties hung up. • Caller Number - The telephone number from which the call originated from. • Src. Channel - the interface type (FXS, FXO or SIP) and name from which this call originated. • Talk Time - The total time of the call from the time the callee picked up the call until one of the parties hung up.
Report	Click the Report button to display your query results in a report window. Your Internet browser opens up a new window with the query results.

28.4.1 The Report Screen

The **CDR Report** screen displays the results of the searches you make in the **CDR Query** screen. Specify your search criteria and click the **Report** button in the **CDR Query** screen to view the screen as shown next.

Figure 251 CDR Query > Report

#	Call Date ▲	Caller ID	Caller Number	Called Number	Caller Group
1	2007-03-06 17:40:15	"1004" <1004>	1004	h	ag_default

Each field is described in the following table.

Table 168 CDR Query > Report

LABEL	DESCRIPTION
Left / Right	Use the Left and Right icons to change the page you want to view (if the report has more than one page). Alternatively, use the drop down list box to select the page you want to view.
Lines/Page	Specify how many lines you want to display on each page of the report.
Total	This field displays the total records created by this report.
Report Output Fields	The format of your report depends on the criteria you select in the Report > LOGS > CDR > CDR Query page. See Section 28.4 on page 418 for explanation of all criteria.

28.5 CDR Technical Reference

This is a sample of cdr.sql file content.

```
-- mysql -u sqlzyxel -p123456 < cdr.sql

CREATE DATABASE cdr;

GRANT ALL PRIVILEGES ON cdr.* TO sqlzyxel IDENTIFIED BY '123456';

USE cdr;

-- create cdr table
CREATE TABLE IF NOT EXISTS `cdr` (
  `calldate` datetime NOT NULL default '0000-00-00 00:00:00',
  `clid` varchar(80) NOT NULL default '',
  `src` varchar(80) NOT NULL default '',
  `dst` varchar(80) NOT NULL default '',
  `dcontext` varchar(80) NOT NULL default '',
  `channel` varchar(80) NOT NULL default '',
  `dstchannel` varchar(80) NOT NULL default '',
  `lastapp` varchar(80) NOT NULL default '',
  `lastdata` varchar(80) NOT NULL default '',
  `duration` int(11) NOT NULL default '0',
  `billsec` int(11) NOT NULL default '0',
  `disposition` varchar(45) NOT NULL default '',
  `amaflags` int(11) NOT NULL default '0',
  `accountcode` varchar(20) NOT NULL default '',
  `userfield` varchar(255) NOT NULL default ''
);

ALTER TABLE `cdr` ADD INDEX ( `calldate` );
ALTER TABLE `cdr` ADD INDEX ( `dst` );
ALTER TABLE `cdr` ADD INDEX ( `accountcode` );
```


ACD Logs

29.1 Overview

This chapter shows you how to collect and manage Automatic Call Distribution (ACD) logs on the X6004.

For a detailed explanation of how ACD works, see [Chapter 24 on page 365](#).

29.1.1 What You Can Do in this Chapter

- Use the **Configuration** screen to configure where to store ACD information, an administrator e-mail address to send alerts and ACD backup files for later viewing. See [Section 29.2 on page 423](#).
- Use the **Backup** screen to manage ACD backup files. See [Section 29.3 on page 426](#).
- Use the **Query** screen to query and create ACD reports. See [Section 29.4 on page 427](#).

29.1.2 Before You Begin

Familiarize yourself with the terms and concepts in [Chapter 28 on page 413](#) as many of the principles that apply there also apply here.

29.2 The Configuration Screen

Use this screen to set up an external server to collect ACD information. You can also configure an administration e-mail address to which to send alerts and ACD files for later viewing.

Note: You should use a MySQL server 5.0 or above for the remote server.

You must execute the SQL script downloaded from this screen on your MySQL server before the X6004 starts to work with the remote server.

Click **Report > LOGS > ACD > Configuration** to view the screen as shown next.

Figure 252 ACD > Configuration

Each field is described in the following table.

Table 169 ACD > Configuration

LABEL	DESCRIPTION
ACD Setting	
Database Usage	This field indicates the percentage of records currently held by the database. When the local database is full, the X6004 removes all the ACD logs from the local database and creates an "Aged File" (a compressed file containing all the ACD logs). Use the Aged File field to specify how to deal with the compressed file containing the ACDs.
Alert	Select this to have the X6004 send an email alert to the e-mail address specified in the E-mail Address field when the ACD log files database is half full.
Aged File	Specify how to deal with ACD log files when the ACD log files database is full. Choose mail to admin. to send the log file to the e-mail address specified in the E-mail Address field and then delete it or drop to delete the file from the system.
E-mail Address	Type the e-mail address to which you want to send the alerts indicating that the ACD log file is half full. This is also the e-mail address to which complete log files are sent when they are full (reach approximately 20000 records).
Database Location	Use this section to specify the location and login credentials for a MySQL server that collects the ACD information from the X6004.

Table 169 ACD > Configuration (continued)

LABEL	DESCRIPTION
Use built-in server	Select this to have the X6004 use the built-in MySQL server to collect ACD information.
Use remote server	Select this to have the X6004 send a record of each call to the remote MySQL server you specify in the Server field.
Server	Type the IP address or the domain name of the server to which you want to send your ACD files. Then type the port number on which the remote server receives records of telephone calls from the X6004.
Username	Type the username of the account set up on a remote server to which you want to send your ACD files.
Password	Type the password of the account set up on a remote server to which you want to send your ACD files.
Schema script	Click Download to download a SQL script (acd.sql). Execute the script in your external database server to establish a database to work with your X6004.
Apply	Click the Apply button to save your changes.

29.2.1 Configure your remote server

The procedure to configure your remote server is as follows:

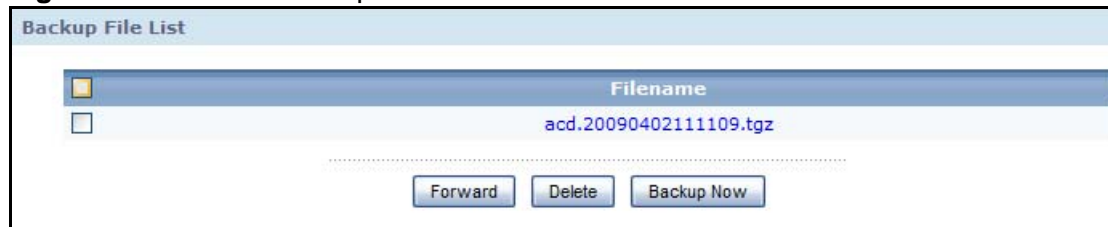
- 1 Fill in all fields in the **Report > LOGS > ACD > Configuration** screen and then click **Download**.
- 2 Save the **acd.sql** file to your computer.
- 3 Make sure the MySQL service is ready on the remote server.
- 4 Upload the **acd.sql** file to your remote server (in the same directory of your installed MySQL server) and execute the file using the command shown in the first line of the **acd.sql** file. For example, `mysql -u sqlzyxel -p123456 < acd.sql` where `sqlzyxel` is the username and `123456` is the password.
- 5 After the script is successfully applied, your MySQL server can work with the X6004.

29.3 The Backup Screen

Use this screen to backup ACD files, delete existing backups of ACD files and mail ACD files to an administrator email address.

Click **Report > LOGS > ACD > Backup** to view the screen as shown next.

Figure 253 ACD > Backup



Each field is described in the following table.

Table 170 ACD > Backup

LABEL	DESCRIPTION
Backup File List	If you have a ZyStack configured using multiple X6004s, then specify the X6004 for which you want to create a backup file of the ACDs.
Filename	<p>This column displays the names of the backup ACD files currently stored on the X6004. Use the check box on the left to specify which files you want to forward or delete. The filename of the ACD takes the following format: "acd.YYYYMMDDHHMMSS.tgz"</p> <p>Where:</p> <ul style="list-style-type: none"> • acd - indicates this is a Automatic Call Distribution file. • YYYYMMDD - is the year, month, and day indicating when the backup file was created. • HHMMSS - is the time of the day indicating when the backup file was created in hour, minute, second format. • tgz - indicates that this is a compressed. That can be decompressed using a compression utility such as WinRAR. The resulting decompressed files are MySQL database files that can be managed via a MySQL DBMS (Database Management System). <p>Note: The X6004 can store only three ACD backup files at a time. If you create a new backup file when you already have three files created, then the oldest backup file is deleted from the system.</p>
Forward	Check the boxes next to the files you want to forward to the administrator email address and click the Forward button. The files you forward to an administrator are deleted from the X6004.
Delete	If you no longer want to store a ACD file on the X6004 then check the boxes next to the files you want to delete from the X6004 and click the Delete button.
Backup Now	Click the Backup Now button to save a ACD backup file on the X6004.

29.4 The Query Screen

Use this screen to configure search criteria for ACD call records on the X6004. You also use this screen to execute your query and create ACD reports. Click **Report > LOGS > ACD > Query** to view the screen as shown next.

Figure 254 ACD > Query

Each field is described in the following table.

Table 171 ACD > Query

LABEL	DESCRIPTION
Query Condition	Use this section to specify your query details.
Call In Time	Call in time is the time a caller dials into a skill. Select a time frame (such as Last 24 Hours or Last 7 Days) from the drop down menu or enter a range From a starting date (yyyy/mm/dd) and time (hh:mm:ss) To an ending date and time.
Skill	Select the skill group for which you want to run the query.
Agent	Select an agent. Only agent names that are associated with the skill selected in the Skill query option appear here.
Wait Time	If you want to search only for calls based on how long they waited before an agent answered, use this query option. Enter a starting wait range and an ending wait range. You can enter up to 99999 seconds, minutes or hours per field. Wait Time : <input type="text" value="20"/> ~ <input type="text" value="60"/> <input type="text" value="seconds"/>

Table 171 ACD > Query (continued)

LABEL	DESCRIPTION
Talk Time	<p>If you want to search only for calls based on how long an agent talked, use this query option.</p> <p>Enter a starting talk range and an ending talk range. You can enter up to 99999 seconds, minutes or hours per field.</p> <p>Talk Time : <input type="text" value="2"/> ~ <input type="text" value="5"/> <input type="text" value="minutes"/> <input type="button" value="v"/></p>
Displayed Item Setting	<p>Use this section to specify which details you want to display in the CDR report for each telephone call record displayed. You can choose to display the following details:</p> <ul style="list-style-type: none"> • Call in Time - This is time it takes for a caller to call into a skill. • Caller ID - This is the username associated with the extension that partook in the call. • Status - This is the status of the agent who fielded the call. • Skill - This is the skill with which the agent is associated. • Wait Time - This is the total time the caller waited in the queue until the time the agent picked up the call. • Agent - This is the agent who fielded the call. • Talk Time - This is the total time of the call from the time the agent picked up the call until one of the parties hung up.
Report	<p>Click the Report button to display your query results in a report window. Your Internet browser opens up a new window with the query results.</p>

29.4.1 ACD Report Screen

The **ACD Report** screen displays the results of the searches you make in the **Query** screen. Specify your search criteria and click the **Report** button in the **Query** screen to view the screen as shown next.

Figure 255 ACD > Report

#	Call in Time	Skill	Agent	Caller ID	Wait Time	Talk Time	Status
1	2009-04-13 16:19:10	11111		3601	57	0	ABANDON
2	2009-04-13 16:20:11	11111		3601	100	0	ABANDON
3	2009-04-13 17:00:56	11111		3601	42	0	ABANDON
4	2009-04-13 17:01:41	11111		3601	43	0	ABANDON
5	2009-04-13 17:02:26	11111		3601	17	0	ABANDON
6	2009-04-13 17:10:42	11111		3601	37	0	ABANDON
7	2009-04-13 17:11:25	11111		3601	13	0	ABANDON
8	2009-04-13 17:12:01	11111		3601	73	0	ABANDON
9	2009-04-15 17:11:44	11111		3601	62	0	ABANDON
10	2009-04-15 17:13:14	11111		3601	38	0	ABANDON
11	2009-04-16 11:09:33	11111		3612	3	0	ABANDON
12	2009-04-16 11:09:50	11111		3601	3	0	ABANDON
13	2009-04-17 10:17:54	11111	2222	3601	11	103	COMPLETECALLER
14	2009-04-24 10:06:32	11111	1111	3611	10	51	COMPLETEAGENT
15	2009-04-24 14:24:20	11111	1111	3611	2	31	COMPLETEAGENT
16	2009-04-24 14:33:57	11111	1111	3611	8	106	COMPLETECALLER
17	2009-04-24 15:33:25	11111	1111	3611	4	17	COMPLETEAGENT
18	2009-04-24 15:37:26	11111	1111	3611	3	14	COMPLETEAGENT
19	2009-04-24 15:45:37	11111	1111	3611	3	118	COMPLETEAGENT
Σ					00:08:49	00:07:20	

Each field is described in the following table.

Table 172 ACD > Report

LABEL	DESCRIPTION
Left / Right	Use the Left and Right icons to change the page you want to view (if the report has more than one page). Alternatively, use the drop down list box to select the page you want to view.
Lines/Page	Specify how many lines you want to display on each page of the report.
Total	This field displays the total records created by this report.
Report Output Fields	The format of your report depends on the criteria you select in the Report > LOGS > ACD > Query page. See Section 29.4 on page 427 for explanation of all criteria.

Administrator Accounts

30.1 Overview

This chapter shows you how to create and manage administrator accounts on the X6004.

The X6004 has a default administrator account, named “admin”. You can also configure up to four additional accounts on the X6004.

30.1.1 What You Can Do in this Chapter

- Use the **Logged-In Administrator** screen to change the password of the currently logged in administrator account you are using. See [Section 30.2 on page 432](#).
- Use the **Administrator List** screen to view and manage administrator accounts. See [Section 30.3 on page 433](#).

30.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Administrator Account Types

The X6004 supports the following types of accounts:

- **Full admin** - This account can perform all configuration changes.
- **Debug admin** - This account has the same privilege level as the read only account. This type of account may be assigned to service technicians to perform additional diagnostics on the X6004.
- **Read only** - This account can only view settings on the X6004.

Only one person of the same account type can log in at one time.

30.2 The Logged-In Administrator Screen

Use the **Logged-In Administrator** screen to change the password of the currently logged in administrator. Click **Maintenance > Logged-In Administrator** to view the screen as shown next.

Figure 256 Maintenance > Logged-In Administrator

The screenshot shows a web form with the following elements:

- Old Password :
- Username
- Password
- Confirm Password
- Buttons:

Each field is described in the following table.

Table 173 Maintenance > Logged-In Administrator

LABEL	DESCRIPTION
Old Password	Type the existing password for the currently logged in administrator account.
Username	Type the new username of the currently logged in administrator account. You can use up to 20 alphanumeric characters. Spaces are not allowed and the first character must be a letter.
Password	Type a new password for the currently logged in administrator account. You can use up to 32 alphanumeric characters and spaces are not allowed.
Confirm Password	Retype the new password for the currently logged in administrator account.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to begin configuring the fields again.

30.3 The Administrator List Screen

Use this screen to manage administrator accounts on the X6004. To access this screen, click **Maintenance > Administrator List**.

Figure 257 Maintenance > Administrator List

Administrator list				
<input type="checkbox"/>	Username	Description	Rank	
<input type="checkbox"/>	Jeffrey	Jeffrey	Debug admin	
<input type="checkbox"/>	admin	1234	Full admin	
<input type="checkbox"/>	john	john	Debug admin	
<input type="checkbox"/>	rick	rick	Debug admin	
<input type="checkbox"/>	steve	steve	Debug admin	

Each field is described in the following table.

Table 174 Maintenance > Administrator List

LABEL	DESCRIPTION
Administrator List	
Delete	Check the Delete box and click Delete to remove this account from the X6004.
Username	This field displays the username of an administrator account on the X6004.
Description	This field displays the description of an administrator account on the X6004.
Rank	This field displays the rank of an administrator account on the X6004. This field displays: <ul style="list-style-type: none"> • Full admin - if this account is allowed to perform all configuration changes on the X6004. • Debug admin - if this account has the same privilege level as the read only account. This type of account is reserved for use by service technicians to perform additional diagnostics. • Read only - if this account is only able to view configuration details on the X6004.
Add / Edit / Delete	Click Add to configure a new administrator account on the X6004. Click Edit to edit an existing administrator account on the X6004. Click Delete to remove an administrator account from the X6004.

30.3.1 Add an Administrator

Use this screen to create new administrator accounts. To access this screen, click **Maintenance > Administrator List > Add**.

Figure 258 Administrator List > Add

Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Description	<input type="text"/>
Rank	Level : <input type="text" value="Read only"/> ▼

Each field is described in the following table.

Table 175 Administrator List > Add

LABEL	DESCRIPTION
Create a new administrator	
Username	Type a username for this administrator. You can use up to 20 alphanumeric characters. Spaces are not allowed. The first character must be a letter.
Password	Type a password for this administrator account. You can use up to 32 alphanumeric characters and spaces are not allowed.
Confirm Password	Retype the new password for this administrator account.
Description	Type a short description for this administrator account. You can use up to 63 alphanumeric characters. Spaces are allowed.
Rank	Select the rank you want this administrator account to have. You can select: <ul style="list-style-type: none"> • Full admin - to allow this account to perform all configuration changes on the X6004. • Debug admin - if this account has the same privilege level as the read only account. This type of account is reserved for use by service technicians to perform additional diagnostics. • Read only - to allow this account to only be able to view configuration details on the X6004.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving your changes.

30.3.2 Edit an Administrator Account

Use this screen to change the password, description or rank of an existing administrator account. To access this screen, click **Maintenance > Administrator List > Edit**.

Figure 259 Administrator List > Edit

The screenshot shows a web form for editing an administrator account. It includes the following elements:

- Password:** A text input field containing four asterisks (****).
- Confirm Password:** A text input field containing four asterisks (****).
- Description:** A text input field containing the word 'admin'.
- Rank:** A dropdown menu with the text 'Level : Full admin' and a downward arrow.
- Buttons:** Two buttons labeled 'Apply' and 'Cancel' are positioned at the bottom right of the form area.

Each field is described in the following table.

Table 176 Administrator List > Edit

LABEL	DESCRIPTION
Edit administrator profile	
Password	Type a new password for this administrator account. You can use up to 32 alphanumeric characters. Spaces are not allowed.
Confirm Password	Retype the new password for this administrator account.
Description	Type a short description for this administrator account. You can use up to 63 alphanumeric characters. Spaces are allowed.
Rank	Select the rank you want this administrator account to have. You can select: <ul style="list-style-type: none"> • Full admin - to allow this account to perform all configuration changes on the X6004. • Debug admin - to allow this account to have the same privilege level as the read only account. This type of account is reserved for use by service technicians to perform additional diagnostics. • Read only - to allow this account to only be able to view configuration details on the X6004.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving your changes.

Diagnostics

31.1 Overview

The X6004 comes with advanced diagnostic tools to help a service technician troubleshoot problems or simply to ensure that everything is running smoothly on the X6004.

This chapter shows you how to collect diagnostic information and capture network traffic for analysis from the X6004.

31.1.1 What You Can Do in this Chapter

- Use the **Information Collect** screen to capture running configuration details for troubleshooting. See [Section 31.2 on page 438](#).
- Use the **Packet Capture** screen to capture network traffic flowing through X6004's LAN or WAN interface for troubleshooting. See [Section 31.3 on page 440](#).
- Use the **Voice Sniffer** screen to capture running VoIP details for individual telephone extensions. See [Section 31.3 on page 440](#).

31.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Privilege to Use Diagnostics

Diagnostics is for a debug administrator and full administrator only. You can use an account with "debug admin" or "full admin" privilege rank to log into the X6004 first. (see [Administrator Account Types on page 431](#)).

Information Collection via Diagnostics

You can collect the following information from the X6004:

- Current status information - the X6004 executes debugging commands and saves the results in a compressed file. You can then submit the results to a service technician or view some of the results via a spreadsheet application (for example, Excel or WordPad). See the CLI Reference Guide for more information on the commands executed to collect current status information. The resulting file can be decompressed with data compression utilities, for example, WinRAR. The resulting decompressed files are:
 - **diag.ezsh.dbg** - contains the results of executing diagnostic and debug log commands on the X6004. This file can be opened using a spreadsheet application such as Excel or a text editor such as WordPad.
 - **system.bin** - contains encrypted information which can only be diagnosed by a service engineer. Customer support may ask you to submit this file for diagnostic purposes.
- Network traffic information - the X6004 logs traffic passing through its interfaces. You can specify the interface, protocol or a specific host from which to capture the traffic. The logs are saved in a Generic Network Capture Document (.cap file extension) and can be viewed via a network analyzer such as Ethereal. These files can diagnose communication problems between the X6004 and other network devices. A service technician may ask you to perform a packet capture when troubleshooting connectivity problems on your network.

31.2 The Information Collect Screen

Use this screen to capture running configuration details on the X6004 and save them in compressed file format on your computer. A service technician may request that you send this file for troubleshooting. This feature is for a debug administrator and full administrator only (see [Section 30.3 on page 433](#)).

Click **Maintenance > Administration > Diagnostics > Information Collect** to view the screen as shown.

Figure 260 Diagnostics > Information Collect

The screenshot displays the 'Information Collect' web interface. It features a 'Machine ID' dropdown menu with 'IPPBX_001' selected, followed by a 'Collect Now' button. Below this is a 'File Download' section showing the filename 'diaginfo-20070725.tar.gz', the last modified date '2007-07-25 10:50:06', and the file size '186KB', with a 'Download' button at the bottom.

Information Collect	
Machine ID:	IPPBX_001
Collect Now	
File Download	
Filename:	diaginfo-20070725.tar.gz
Last Modified:	2007-07-25 10:50:06
Size:	186KB
Download	

Each field is described in the following table.

Table 177 Diagnostics > Information Collect

LABEL	DESCRIPTION
Machine ID	If you have more than one X6004 configured in a ZyStack, select the one from which you want to collect information.
Collect Now	Click Collect Now to capture the configuration details of the X6004. Note: It takes about 1 minute to perform the data collection. Do not try to browse to other screens while the capture is in progress.
Filename	This field displays the name of the compressed file which holds the running configuration details. The file naming convention is: diaginfo-YYYYMMDD.tar.gz , where YYYY is the year, MM is the month and DD is the day of the month on which the capture took place. The file can be decompressed with variety of data compression utilities, for example, WinRAR.
Last Modified	This field displays the date and time when the information was retrieved from the X6004.
Size	This field displays the size of the file.
Download	Click Download to save the file to your computer.

31.3 The Packet Capture Screen

Use this screen to log network traffic going through the X6004 LAN or WAN interface. This feature is for a debug administrator and full administrator only (see [Section 30.3 on page 433](#)). Click **Maintenance > Administration > Diagnostics > Packet Capture** to view the screen as shown.

Figure 261 Diagnostics > Packet Capture

Each field is described in the following table.

Table 178 Diagnostics > Packet Capture

LABEL	DESCRIPTION
Machine ID	If you have more than one X6004 configured in a ZyStack, select the one from which you want to collect information.
Interface	Choose the interface for which you want to log network traffic.
Host	Optionally, limit the capture of information to communication with a specific network device. Enter the IP address of the network device that the X6004 is communicating with. You can also enter the IP address of the X6004 itself, in which case, the X6004 only collects information where the destination or source IP matches that of the X6004.
Protocol	Specify the protocol type which you want to capture information on. You can choose TCP , UDP , ICMP or select All to capture all IP traffic going through the X6004.

Table 178 Diagnostics > Packet Capture (continued)

LABEL	DESCRIPTION
Stop capture after.. Packets	<p>Specify how many packets you want to collect before ending the packet capture. If you select to limit the capture by the number of packets and by total time of the capture, then the capture session will end when the time limit is reached.</p> <p>Note: You must specify either a time limit or a total number of packets limit for the data capture.</p>
Stop capture after.. Sec.	<p>Specify how long a packet capture session should last. If you select to limit the capture by the number of packets and by total time of the capture, then the capture session will end when the time limit is reached.</p> <p>If you do not specify any limits for the capture, then the capture will last for the maximum time allowed (600 seconds).</p> <p>Note: You must specify either a time limit or a total number of packets limit for the data capture.</p>
Capture Now / Stop Capture	<p>Click Capture Now to start collecting network traffic information going through the X6004. The Stop Capture button appears after you successfully start a network traffic collection. You can click it to stop the collection any time.</p> <p>Note: It may take several minutes to perform the data collection. Do not try to browse to other screens while the capture is in progress.</p>
Filename	<p>This field displays the name of the .cap file which holds the packet capture data. The file naming convention is: X6004-YYYYMMDD.cap, where YYYY is the year, MM is the month and DD is the day of the month on which the capture took place.</p>
Last Modified	<p>This field displays the date and time when the information was collected from the X6004.</p>
Size	<p>This field displays the size of the file.</p>
Download	<p>Click Download to save the file to your computer.</p>

31.4 The Voice Sniffer Screen

Use this screen to capture running Voice over Internet Protocol (VoIP) details for individual telephone extensions and save them in compressed file format on your computer. A service technician may request that you send this file for troubleshooting. This feature is for a debug administrator and full administrator only (see [Section 30.3 on page 433](#)).

Click **Maintenance > Administration > Diagnostics > Voice Sniffer** to view the screen as shown.

Figure 262 Diagnostics > Voice Sniffer

The screenshot shows the 'Voice Sniffer' interface. It is divided into two main sections: 'Packet Capture' and 'File Download'.

Packet Capture Section:

- Machine ID:** A dropdown menu with 'IPPBX_001' selected.
- Channel Type:** A dropdown menu with 'SIP' selected.
- Sniffed Line:** A dropdown menu with '5000' selected.
- A horizontal dotted line separates the selection fields from a 'Capture Now' button.

File Download Section:

- Filename:** sip_5000_diag_20090504014823.tgz
- Last Modified:** 2009/05/04 01:48:23
- Size:** 37.1 KB

Each field is described in the following table.

Table 179 Diagnostics > Voice Sniffer

LABEL	DESCRIPTION
Machine ID	If you have more than one X6004 configured in a ZyStack, select the one from which you want to collect information.
Channel Type	Select an available channel to be sniffed if you have configured extensions for BRI, FXS, FXO, PRI or SIP.
Sniffed Line	Select an extension number to be sniffed. The extensions that appear in this list correspond directly to the Channel Type . For example, if you select the SIP channel type, then only the SIP extensions appear here.
Capture Now	Click Capture Now to capture the configuration details of the X6004. Note: It takes about 1 minute to perform the packet capture. Do not try to browse to other screens while the capture is in progress.

Table 179 Diagnostics > Voice Sniffer (continued)

LABEL	DESCRIPTION
Filename	<p>This field displays the name of the packet capture data file.</p> <p>File naming convention is channel_line/port_diag_date.tgz, where:</p> <ul style="list-style-type: none"> • channel - This is based on the selected Channel Type. For example, if you choose 'SIP' in the channel type menu then the file name begins with the word sip. • line/port - This indicates the line or port that was sniffed. • diag - This word is non-variable and indicates the file is diagnostic. • date - The date is expressed as a 14-digit string: yyymmddhhmiss, where yyyy is the year ('2009'), mm is the month ('05'), dd is the day ('15'), hh is the hour (1-24), mi is the minute (1-60) and ss is the seconds (1-60). In this example, the string 20090515 equates to the year 2009, the month of May, and the 15th day. • tgz - This is the Unix TAR filetype.
Last Modified	This field displays the date and time when the information was collected from the X6004.
Size	This field displays the size of the file.
Download	Click Download to save the file to your computer.

Inactivity Timer

32.1 Overview

There is a default system management idle timeout of ten minutes (six hundred seconds) defined in the **Maintenance > Administration > Inactivity Timer** screen. The X6004 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

32.2 The Inactivity Timer Screen

Use this screen to set the maximum time period allowed before an idle session expires. To access this screen, click **Maintenance > Administration > Inactivity Timer**.

Figure 263 Administration > Inactivity Timer

Each field is described in the following table.

Table 180 Administration > Inactivity Timer

LABEL	DESCRIPTION
Web Configurator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 10 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to set every field in this screen to its last-saved value.

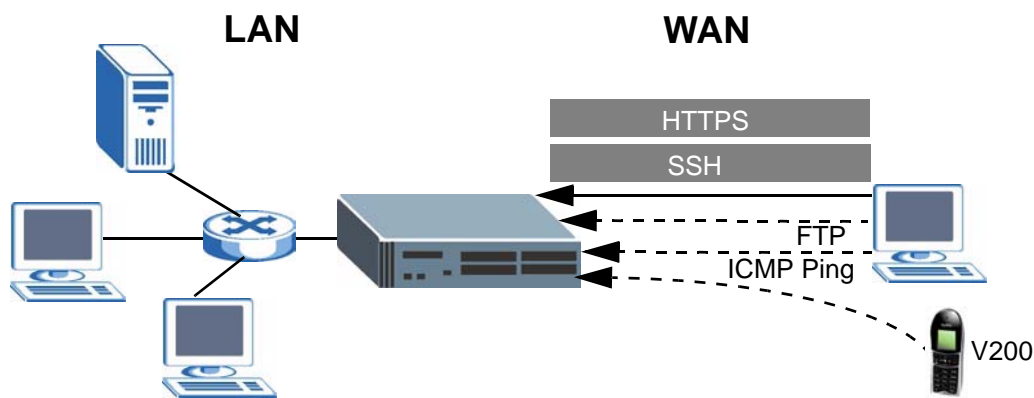
Remote Management

33.1 Overview

This chapter provides information on configuring remote management.

Remote management allows you to determine which computer(s) can access which X6004 interface. The following figure shows remote management of the X6004 coming in from the WAN. Use HTTPS or SSH to access the X6004 more securely than FTP and a ZyXEL V200 SIP phone.

Figure 264 Secure and Insecure Remote Management From the WAN



33.1.1 What You Can Do in this Chapter

- Use the **WWW** screen to configure which computers can access the X6004's web configurator. See [Section 33.2 on page 449](#).
- Use the **SSH** screen to configure which computers can access the X6004 via SSH protocol. See [Section 33.4 on page 451](#).
- Use the **FTP** screen to configure which computers can access the X6004 via FTP protocol. See [Section 33.6 on page 453](#).
- Use the **ICMP** screen to configure to which computers' ping test the X6004 responses. See [Section 33.8 on page 455](#).
- Use the **CTI** screen to configure which ZyXEL V200 SIP phones can access the X6004. See [Section 33.10 on page 457](#).

33.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Access Interface

You may manage your X6004 from a remote location via:

- WAN only
- ALL (LAN and WAN)
- LAN only

X6004 allows multiple remote management sessions running at a time if you login using different administrator accounts with different ranks. See [Chapter 40 on page 521](#) for the maximum number of remote management session the X6004 supports.

Remote Management Limitations

Remote management does not work when:

- You have disabled that service in one of the remote management screens.
- The IP address in the **Address** field (in the service's white list) does not match the client IP address. If it does not match, the X6004 refuses the login session.
- There is already another remote management session with the same rank running.

WWW (HTTPS)

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

HTTPS on the X6004 is used so that you may securely access the X6004 using the web configurator. The SSL protocol specifies that the SSL server (the X6004) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the X6004).

HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the X6004's web server.

SSH

You can use SSH (Secure SHell) to securely access the X6004's command line interface. Specify which interfaces and from which IP address(es) users are allowed to access the device through SSH.

Unlike FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

SSH Implementation on the X6004

Your X6004 supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the X6004 for remote SMT management and file transfer on port 22. Multiple SSH connections are allowed at a time.

Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the X6004 over SSH.

ICMP

Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and are directly apparent to the application user.

33.2 The WWW Screen

Use this screen to configure trusted computers which is allowed to access your X6004's World Wide Web. Click **Maintenance** > **Administration** > **Remote Management** to display the **WWW** screen.

Figure 265 Remote Management > WWW

#	Access Interface	Address
1	LAN	0.0.0.0

The following table describes the labels in this screen.

Table 181 Remote Management > WWW

LABEL	DESCRIPTION
Activate WWW Remote Management White List	Select this to allow only computers which use IP addresses listed in this screen to access your X6004 via an HTTPS connection.
#	This field displays the index number of records in this table.
Access Interface	This field displays the interface(s) through which a computer may access the X6004 using this service.
Address	This field displays trusted computers' IP addresses that is allowed to communicate with the X6004 using this service. 0.0.0.0 displayed means all computers are allowed to access the X6004 using this service. An IP address displayed (for example, a.b.c.d) means only the computer is allowed to access the X6004 using this service. An IP address with a subnet mask displayed (for example, a.b.c.d/255.255.255.0) means only the computers in the subnet network are allowed to access the X6004 using this service.
Add	Click Add to add a new trusted computer record.
Edit	Click Edit to modify a trusted computer record.
Delete	Click the Delete icon to delete a single record in this table. Alternatively, select one or multiple records and click the Delete button to delete record(s) at one time.

33.3 The WWW > Add/Edit Screen

Use this screen to add trusted computer(s) which is allowed to access your X6004's World Wide Web. Click the add or edit icon in the **Maintenance > Administration > Remote Management > WWW** screen.

Figure 266 WWW > Add/Edit

Access Interface	<input type="text" value="ALL"/>
Address Type	<input type="text" value="ALL"/>

The following table describes the labels in this screen.

Table 182 WWW > Add/Edit

LABEL	DESCRIPTION
Access Interface	Select the interface(s) through which computer(s) may access the X6004 using this service. Select ALL to allow the specified computer(s) to access the X6004 through either LAN or WAN interface.
Address Type	Select ALL to allow any computers to access the X6004 using this service. Select Host and specify the IP address of a trusted computer to allow the computer to access the X6004 using this service. Select Subnet and specify the IP addresses of a trusted subnet to allow all computers from the subnet network to access the X6004 using this service.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to begin configuring the fields again.

33.4 The SSH Screen

You can use SSH to access the X6004's command line interface. Specify which interfaces allow SSH access and from which IP address the access can come. Click **Advanced > Remote Management > SSH** tab to display the screen as shown.

Figure 267 Remote Management > SSH

The following table describes the labels in this screen.

Table 183 Remote Management > SSH

LABEL	DESCRIPTION
Activate SSH Remote Management White List	Select this to allow only computers which use IP addresses listed in this screen to access your X6004 via an SSH connection.
#	This field displays the index number of records in this table.
Access Interface	This field displays the interface(s) through which a computer may access the X6004 using this service.

Table 183 Remote Management > SSH (continued)

LABEL	DESCRIPTION
Address	<p>This field displays trusted computers' IP addresses that is allowed to communicate with the X6004 using this service.</p> <p>0.0.0.0 displayed means all computers are allowed to access the X6004 using this service.</p> <p>An IP address displayed (for example, a.b.c.d) means only the computer is allowed to access the X6004 using this service.</p> <p>An IP address with a subnet mask displayed (for example, a.b.c.d/255.255.255.0) means only the computers in the subnet network are allowed to access the X6004 using this service.</p>
Add	Click Add to add a new trusted computer record.
Edit	Click Edit to modify a trusted computer record.
Delete	Click the Delete icon to delete a single record in this table. Alternatively, select one or multiple records and click the Delete button to delete record(s) at one time.

33.5 The SSH > Add/Edit Screen

Use this screen to add trusted computer(s) which is allowed to access your X6004 using SSH. Click the add or edit icon in the **Maintenance > Administration > Remote Management > SSH** screen.

Figure 268 SSH > Add/Edit

The screenshot shows a form with two dropdown menus. The first is labeled 'Access Interface' and has a dropdown arrow pointing to 'ALL'. The second is labeled 'Address Type' and also has a dropdown arrow pointing to 'ALL'.

The following table describes the labels in this screen.

Table 184 SSH > Add/Edit

LABEL	DESCRIPTION
Access Interface	Select the interface(s) through which computer(s) may access the X6004 using this service. Select ALL to allow the specified computer(s) to access the X6004 through either LAN or WAN interface.
Address Type	<p>Select ALL to allow any computers to access the X6004 using this service.</p> <p>Select Host and specify the IP address of a trusted computer to allow the computer to access the X6004 using this service.</p> <p>Select Subnet and specify the IP addresses of a trusted subnet to allow all computers from the subnet network to access the X6004 using this service.</p>

Table 184 SSH > Add/Edit (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to begin configuring the fields again.

33.6 The FTP Screen

You can use FTP (File Transfer Protocol) to upload and download the X6004's firmware and configuration files, please see the [Chapter 35 on page 469](#) for firmware and configuration file maintenance details. To use this feature, your computer must have an FTP client.

To change your X6004's FTP settings, click **Maintenance > Administration > Remote Management > FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

Figure 269 Remote Management > FTP

The following table describes the labels in this screen.

Table 185 Remote Management > FTP

LABEL	DESCRIPTION
Activate FTP Remote Management White List	Select this to allow only computers which use any IP addresses listed in this screen to access your X6004 via an FTP connection.
#	This field displays the index number of records in this table.
Access Interface	This field displays the interface(s) through which a computer may access the X6004 using this service.

Table 185 Remote Management > FTP (continued)

LABEL	DESCRIPTION
Address	<p>This field displays trusted computers' IP addresses that is allowed to communicate with the X6004 using this service.</p> <p>0.0.0.0 displayed means all computers are allowed to access the X6004 using this service.</p> <p>An IP address displayed (for example, a.b.c.d) means only the computer is allowed to access the X6004 using this service.</p> <p>An IP address with a subnet mask displayed (for example, a.b.c.d/255.255.255.0) means only the computers in the subnet network are allowed to access the X6004 using this service.</p>
Add	Click Add to add a new trusted computer record.
Edit	Click Edit to modify a trusted computer record.
Delete	Click the Delete icon to delete a single record in this table. Alternatively, select one or multiple records and click the Delete button to delete record(s) at one time.

33.7 The FTP > Add/Edit Screen

Use this screen to add trusted computer(s) which is allowed to access your X6004 using FTP. Click the add or edit icon in the **Maintenance > Administration > Remote Management > FTP** screen.

Figure 270 FTP > Add/Edit

Access Interface	WAN ▼
Address Type	Subnet ▼
Network	10.1.1.0
Subnet Mask	255.255.255.0

The following table describes the labels in this screen.

Table 186 FTP > Add/Edit

LABEL	DESCRIPTION
Access Interface	Select the interface(s) through which computer(s) may access the X6004 using this service. Select ALL to allow the specified computer(s) to access the X6004 through either LAN or WAN interface.
Address Type	Select ALL to allow any computers to access the X6004 using this service. Select Host and specify the IP address of a trusted computer to allow the computer to access the X6004 using this service. Select Subnet and specify the IP addresses of a trusted subnet to allow all computers from the subnet network to access the X6004 using this service.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to begin configuring the fields again.

33.8 The ICMP Screen

If an outside user attempts to probe an unsupported port on your X6004, an ICMP response packet is automatically returned. This allows the outside user to know the X6004 exists. Your X6004 supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your X6004 when unsupported ports are probed.

To change your X6004's security settings, click **Maintenance > Administration > Remote Management > ICMP**. The screen appears as shown.

Figure 271 Remote Management > ICMP

ICMP White List

Activate ICMP Remote Management White List

Delete

+ :Add ✎ :Edit 🗑 :Delete

<input type="checkbox"/>	#	Access Interface	Address	<input type="checkbox"/>
<input type="checkbox"/>	1	LAN	0.0.0.0	<input type="checkbox"/>

Delete

The following table describes the labels in this screen.

Table 187 Remote Management > ICMP

LABEL	DESCRIPTION
Activate ICMP Remote Management White List	The X6004 will not respond to any incoming Ping requests when this is selected.
#	This field displays the index number of records in this table.
Access Interface	This field displays the interface(s) through which a computer may access the X6004 using this service.
Address	This field displays trusted computers' IP addresses that is allowed to communicate with the X6004 using this service. 0.0.0.0 displayed means all computers are allowed to access the X6004 using this service. An IP address displayed (for example, a.b.c.d) means only the computer is allowed to access the X6004 using this service. An IP address with a subnet mask displayed (for example, a.b.c.d/255.255.255.0) means only the computers in the subnet network are allowed to access the X6004 using this service.
Add	Click Add to add a new trusted computer record.
Edit	Click Edit to modify a trusted computer record.
Delete	Click the Delete icon to delete a single record in this table. Alternatively, select one or multiple records and click the Delete button to delete record(s) at one time.

33.9 The ICMP > Add/Edit Screen

Use this screen to add trusted computer(s) from which your X6004 will respond ping packets using ICMP. To open this screen, click the add or edit icon in the **Maintenance > Administration > Remote Management > ICMP** screen.

Figure 272 ICMP > Add/Edit

Access Interface	LAN ▼
Address Type	Host ▼
Secured Client IP Address	192.168.1.254

The following table describes the labels in this screen.

Table 188 ICMP > Add/Edit

LABEL	DESCRIPTION
Access Interface	Select the interface(s) through which computer(s) may ping the X6004 using this service. Select ALL to have the X6004 respond ping packets sent from the specified computer(s) X6004 through either LAN or WAN interface.
Address Type	Select ALL to have the X6004 respond ping packets from any computers. Select Host and specify the IP address of a trusted computer to have the X6004 respond ping packets from the computer. Select Subnet and specify the IP addresses of a trusted subnet to have the X6004 respond ping packets from all computers from the subnet network.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to begin configuring the fields again.

33.10 The CTI Screen

You can use a ZyXEL V200 SIP phone to access and download the X6004's phonebook information through port 5038.

To view or change your X6004's CTI settings, click **Maintenance > Administration > Remote Management > CTI**. The screen appears as shown. Use this screen to specify which interfaces allow CTI access and from which IP address the access can come.

Figure 273 Remote Management > CTI

CTI White List

Activate CTI Remote Management White List

Delete

+ :Add ✎ :Edit 🗑 :Delete

#	Access Interface	Address
1	LAN	0.0.0.0

Delete

The following table describes the labels in this screen.

Table 189 Remote Management > CTI

LABEL	DESCRIPTION
Activate CTI Remote Management White List	Select this to allow only CTI-compatible SIP phones which use any IP addresses listed in this screen to access your X6004.
#	This field displays the index number of records in this table.
Access Interface	This field displays the interface(s) through which a CTI-compatible device may access the X6004 using this service.
Address	This field displays trusted CTI-compatible device's IP addresses that is allowed to communicate with the X6004 using this service. 0.0.0.0 displayed means all devices are allowed to access the X6004 using this service. An IP address displayed (for example, a.b.c.d) means only the device is allowed to access the X6004 using this service. An IP address with a subnet mask displayed (for example, a.b.c.d/255.255.255.0) means only the devices in the subnet network are allowed to access the X6004 using this service.
Add	Click Add to add a new trusted computer record.
Edit	Click Edit to modify a trusted computer record.
Delete	Click the Delete icon to delete a single record in this table. Alternatively, select one or multiple records and click the Delete button to delete record(s) at one time.

33.10.1 The CTI Add/Edit Screen

Use this screen to add trusted ZyXEL CTI-compatible SIP phone(s) which is allowed to access your X6004. Click the add or edit icon in the **Maintenance > Administration > Remote Management > CTI** screen.

Figure 274 CTI > Add/Edit

Access Interface	LAN ▼
Address Type	Host ▼
Secured Client IP Address	192.168.1.254

The following table describes the labels in this screen.

Table 190 CTI > Add/Edit

LABEL	DESCRIPTION
Access Interface	Select the interface(s) through which ZyXEL CTI-compatible SIP phone(s) may access the X6004 using this service. Select ALL to allow the specified device(s) to access the X6004 through either LAN or WAN interface.
Address Type	<p>Select ALL to allow any CTI-compatible devices to access the X6004.</p> <p>Select Host and specify the IP address of a trusted device to allow it to access the X6004.</p> <p>Select Subnet and specify the IP addresses of a trusted subnet to allow all CTI-compatible devices from the subnet network to access the X6004.</p>
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to begin configuring the fields again.

33.11 Remote Management Technical Reference

HTTPS Example

If you haven't changed the default HTTPS port on the X6004, then in your browser enter "https://X6004 IP Address/" as the web site address where "X6004 IP Address" is the IP address or domain name of the X6004 you wish to access.

Internet Explorer Warning Messages

When you attempt to access the X6004 HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the X6004.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 275 Security Alert Dialog Box (Internet Explorer)



Netscape Navigator Warning Messages

When you attempt to access the X6004 HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the X6004.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the X6004's certificate into the SSL client.

Figure 276 Security Certificate 1 (Netscape)

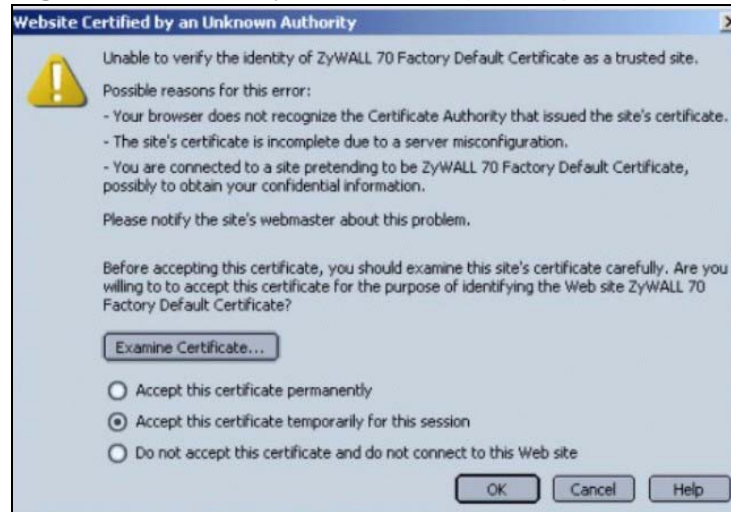


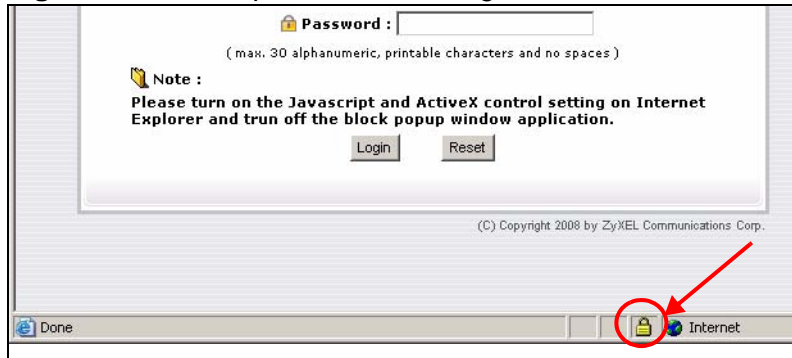
Figure 277 Security Certificate 2 (Netscape)



Login Screen

After you accept the certificate, the X6004 login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

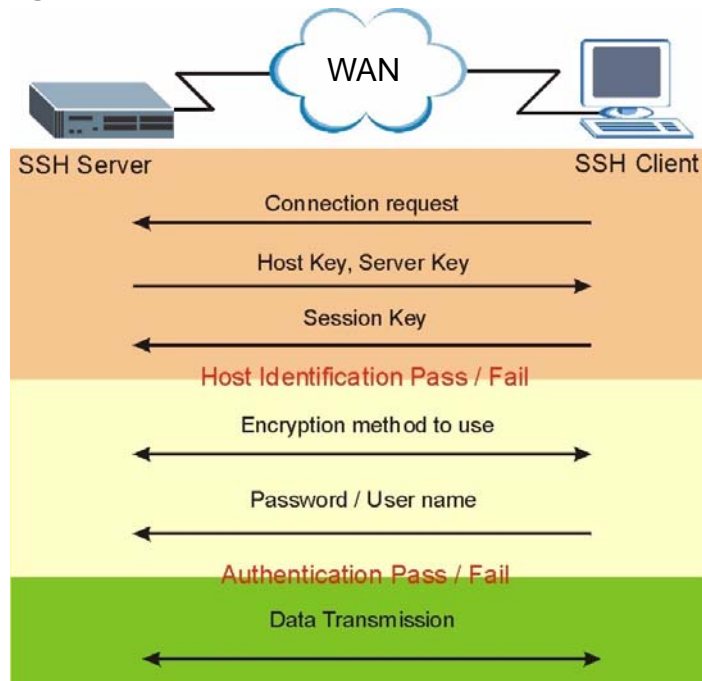
Figure 278 Example: Lock Denoting a Secure Connection



How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 279 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the X6004. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

Example 1: Microsoft Windows

This section describes how to access the X6004 using the Secure Shell Client program.

- 1 Launch the SSH client and specify the connection information (IP address, port number or device name) for the X6004.
- 2 Configure the SSH client to accept connection using SSH version 1.

- 3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 280 SSH Example 1: Store Host Key



- 4 Enter the password to log in to the X6004. The SMT main menu displays next.

Example 2: Linux

This section describes how to access the X6004 using the OpenSSH client program that comes with most Linux distributions.

- 1 Test whether the SSH service is available on the X6004.

Enter `telnet 192.168.1.1 22` at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the X6004 (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the X6004.

Figure 281 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

- 2 Enter “ssh -1 192.168.1.1”. This command forces your computer to connect to the X6004 using SSH version 1. If this is the first time you are connecting to the X6004 using SSH, a message displays prompting you to save the host information of the X6004. Type “yes” and press [ENTER].

Then enter the password to log in to the X6004.

Figure 282 SSH Example 2: Log in

```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
```

- 3 The SMT main menu displays next.

Secure FTP Using SSH Example

This section shows an example on file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. Refer to your SSH client program user’s guide.

- 1 Enter “sftp -1 192.168.1.1”. This command forces your computer to connect to the X6004 for secure file transfer using SSH version 1. If this is the first time you are connecting to the X6004 using SSH, a message displays prompting you to save the host information of the X6004. Type “yes” and press [ENTER].
- 2 Enter the password to login to the X6004.

- 3 Use the “put” command to upload a new firmware to the X6004.

Figure 283 Secure FTP: Firmware Upload Example

```
$ sftp -l 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

TFTP Management

34.1 TFTP Management

Use Trivial File Transfer Protocol (TFTP) management to load files such as phone firmware to the X6004 so TFTP client devices can check the X6004 for the latest file and download it.

To change your X6004's TFTP settings, click **Maintenance > Administration > TFTP Management**. The screen appears as shown.

Figure 284 TFTP Management

The following table describes the labels in this screen.

Table 191 TFTP Management

LABEL	DESCRIPTION
TFTP Server Setting	Select Enable to allow TFTP clients to access the X6004 TFTP server's files. Select Disable to stop TFTP clients from accessing the X6004 TFTP server's files.
Upload File	Use the Browse button to find a file to upload to the X6004's TFTP server and click Apply to upload it.
File List	These are the files stored in the X6004's TFTP server.
Delete	Click a file's Delete icon to remove it or select checkboxes for individual files (or use the heading row's checkbox to select all entries) and click Delete to remove the entries from the X6004.
File Name	This is the name of the file stored on the X6004's TFTP server.
File Size	This is the size of the file stored on the X6004's TFTP server.

System File Maintenance

35.1 Overview

This chapter shows you how to manage system files including configuration and firmware files on the X6004.

- **Configuration File** - The X6004 allows you to save a configuration file to your local computer. You should create a backup file of your configuration when you have configured all your settings and the X6004 is functioning properly. Restore the configuration if you are experiencing problems with the X6004.
- **Firmware File** - The X6004 allows you to upgrade a firmware file from your local computer.

You can perform configuration and firmware file maintenance via web configurator, FTP, or console.

35.1.1 What You Can Do in this Chapter

- Use the **Backup & Restore** screen to backup/restore your system configuration file or reset it to factory default. See [Section 35.2 on page 471](#).
- Use the **Firmware Upgrade** screen to upgrade firmware on your X6004. See [Section 35.3 on page 473](#).

35.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Configuration File Maintenance Notes

- The information related to administrator accounts and WAN/LAN network settings on the X6004 are not saved when you create a backup configuration file.
- When you restore a configuration file on the X6004, you do not change the currently configured administrator accounts and WAN/LAN network settings on the X6004.
- You must restart the X6004 manually after you restore a configuration file for the restored settings to be applied to the X6004.

Firmware File Types for Upgrade

The X6004 accepts the following four kinds of files.

- Base firmware - This type of file has a “.bin” extension, for example “100AVA2C0.bin”. This file contains basic operating instructions on how the device drivers interact with the main processing unit of the X6004. In other words, when you upload a new “.bin” file you might not see any changes in the GUI of the X6004, but you may experience improved performance.
- Main firmware - This type of file has a “.rom” extension, for example “100AVA2C0.rom”. This file contains functional instructions for the X6004. When you upload this type of file, you may see new features or changes in the GUI of the X6004.
- Factory Default Settings - This type of file has a “.romd” extension, for example “100AVA2C0.romd”. This file contains factory default settings for the X6004. When you upload this type of file, all configuration will be cleared and replaced with default settings.
- Firmware and Configuration - This type of file has a “.binromromd” extension, for example “100AVA2C0.binromromd”. This file combines all of the files listed above into a single uploadable file. It conveniently lets you upgrade the X6004 all at one time.

Note: It is highly recommended to use a “.binromromd” file for firmware upgrade.

Find firmware at www.zyxel.com. Read the firmware release notes before uploading the firmware files. The upload process uses HTTPS and may take several minutes. After a successful upload, the system reboots.

35.2 The Backup & Restore Screen

Use this screen to back up or restore a configuration on the X6004. You can also use this screen to reset the X6004 to the factory default settings and add SIP extensions by batch file. To access this screen, click **Maintenance > Backup & Restore**.

Note: Make sure you are using the correct backup “.zip” file when you restore your configuration.

Figure 285 Maintenance > Backup & Restore

The screenshot displays a web interface with four distinct sections, each with a light blue header:

- Backup Configuration:** Contains the instruction "Click Backup to save the current configuration of your system to your computer." and a "Backup" button.
- Restore Configuration:** Contains the instruction "To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload." Below this is a "File path :" label, an empty text input field, a "Browse..." button, and an "Upload file" button.
- Back to Factory Defaults:** Contains the instruction "Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the" followed by a list: "- Username will be admin", "- Password will be 1234", and "- LAN IP address will be 192.168.1.12". Below the list is a "Default" button.
- Batch Add SIP Extensions:** Contains the instruction "Click Download to get the template file and edit it for batch add SIP extensions." and a "Download" button. Below this is the same instruction as the Restore Configuration section, followed by a "File path :" label, an empty text input field, a "Browse..." button, and an "Upload file" button.

Each field is described in the following table.

Table 192 Maintenance > Backup & Restore

LABEL	DESCRIPTION
Backup Configuration	
Backup	<p>Click this to save the X6004's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings.</p> <p>Note: The administrator account and WAN/LAN network settings are not saved during the backup process.</p>
Restore Configuration	
File Path	Enter the location of the file you want to upload, or click Browse... to find it.
Browse	Click this to find the file you want to upload.
Upload	<p>Click this to restore the selected configuration file. Do not turn off the X6004 while configuration file upload is in progress. After the configuration file is uploaded successfully a message appears at the bottom of the screen "Info : Restore success. Please restart the system."</p> <p>Note: You must restart the X6004 to apply the settings from the restored configuration file.</p> <p>When you restore a configuration file on the X6004, you do not change the currently configured administrator accounts and WAN/LAN network settings on the X6004.</p>
Back to Factory Defaults	
Default	Click this to return the X6004 to its factory defaults.
Batch Add SIP Extensions	Click Download to save a template batch file for SIP extensions to your computer. After you edit the file, click Browse to locate the file and Upload to copy it to the X6004.

35.2.1 Batch Add SIP Extensions Template File

Here is the SIP extensions template file.

```

; Example file (Add SIP extension(s))
; Fields: <Group Name>,<Extension Number>,<Password>,<PIN Code>,<CODEC
List>,<DTMF>,<First Name>,<Last Name>,<Department>
; Format:
; <Group Name>:= [A-Za-z0-9_]{1,20}
; <Extension Number>:= [0-9]{3,10}
; <Password>          := ^[^\;:\=" '&* \'\ \ |]{3,32} (Blank: as <Extension
Number>)
; <PIN Code>          := [0-9]{3,10} (Blank: as <Extension
Number>)
; <CODEC List>        := <CODEC>[,<CODEC>]
; <CODEC>             := g729|ulaw|alaw|g726|h263|h261|g722|g722.2|h264|mp4
; <DTMF>              := info|inband|rfc2833 (Blank: info)
; <First Name>        := [A-Za-z0-9_ -]{0,40}
; <Last Name>         := [A-Za-z0-9_ -]{0,40}
; <Department>        := [A-Za-z0-9_ -]{0,40}
; Example: Add a SIP extension
; Service,1000,password1000,1234,"ulaw,alaw",rfc2833,Chad,Russell,Service
Group Name,Extension Number,Password,PIN Code,CODEC List,DTMF,First
Name,Last Name,Department
Bob,1000,0000,1111,h261,rfc2833,Bob,Somebody,testing
Joe,1001,0000,1111,h261,rfc2833,Joe,Somebody,finance

```

35.3 The Firmware Upgrade Screen

Use this screen to view the current firmware version on the X6004 and to update the X6004 if you have newer firmware. To access this screen, click the **Maintenance > Firmware Upgrade**.

Do not turn off the device while firmware upload is in progress!

Figure 286 Maintenance > Firmware Upgrade

Information	
Boot Module:	1.00
Current Version:	1.11(AVA.0)b1
Released Date:	2009-03-27 13:59:06
Select Upload File	
To upload firmware package, browse to the location of the file and then click Upload.	
File Path:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>

Each field is described in the following table.

Table 193 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Information	This section displays information about the firmware currently installed on the X6004.
Boot Module:	This field indicates the version of the boot module installed on the X6004. The boot module is software that tells the X6004 how to install and run the firmware. Each firmware release only works when the proper boot module is installed on the X6004.
Current Version	This field indicates the firmware version number.
Released Date	This field indicates the date and time that the currently installed firmware on the X6004 was released.
Select Upload File	Use this section to upload new firmware to the X6004.
File Path	Enter the location of the .bin, .rom, .romd or .binromromd file you want to upload, or click Browse... to find it. You must decompress compressed (.zip) files before you can upload them.
Browse...	Click this to find the .bin, .rom, .romd or .binromromd file you want to upload.
Upload	Click this to begin uploading the selected file. This may take several minutes. Note: Do not turn off the device while firmware upload is in progress!

35.4 Technical Reference

This section shows some examples of uploading files to the X6004 using FTP commands. First, understand the filename conventions.

Filename Conventions

Like the firmware upgrade function in the GUI, four types of files can be FTP uploaded to the X6004 (See [Section 35.3 on page 473](#)):

Regardless of which file you want to upload to the X6004, you must first rename it to the internal firmware file name on the X6004: **ZLD-current**.

Example FTP Commands

Do the following to upload the firmware and configuration file to the X6004:

- 1 Rename the file you want to upload to ZLD-current and place it in the directory from which you launch your FTP session. In our example this is the root directory "C:\".
- 2 Launch the FTP client on your computer. For example, from the command prompt type ftp, followed by a space and the IP address of your X6004.
- 3 Type your username and press [ENTER] when prompted (the default is "admin").
- 4 Enter your password as requested (the default is "1234").
- 5 Enter bin to set transfer mode to binary.
- 6 Use put to transfer files from the computer to the X6004, for example, put ZLD-current transfers the firmware and configuration that your renamed to **ZLD-current** to the X6004.
- 7 The X6004 uploads the file and automatically reboots. The FTP session with the X6004 is automatically terminated.

This is a sample FTP session showing the transfer of the **ZLD-current** file to the X6004:

```
C:\>ftp 172.23.37.201
Connected to 172.23.37.201.
220 ProFTPD 1.2.10 Server (ProFTPD Default Installation)
[172.23.37.201]
User (172.23.37.201:(none)): admin
331 Password required for admin.
Password: ****
230 User admin logged in.
ftp> bin
200 Type set to I
ftp> put ZLD-current
200 PORT command successful
150 Opening BINARY mode data connection for ZLD-current
226-path /etc/zyxel/ftp/.tmp/ZLD-current
226-firmware verifying...
226-firmware updating...
226-Please Wait about 5 minutes!!
226-Do not poweroff or reset,
226-system will reboot automatically after finished updating.
226 Transfer complete.
226-copy_firmware:file /etc/zyxel/ftp/.tmp/ZLD-current
226-done
226-Receive firmware success!
226-System reboot automatically!
```

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 194 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Normal. The server requires a unique User ID and Password to login. The X6004 requires Normal login type. Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

License Control

36.1 Overview

This chapter shows you how to register your X6004 and subscribe to services (for example, additional number of SIP extensions and softphone extensions support) available at myZyXEL.com.

myZyXEL.com is ZyXEL's online services center where you can register your X6004 and manage subscription services available for the X6004.

You can directly create a myZyXEL.com account, register your X6004 and activate a service using the **REGISTRATION** screen. (Alternatively, go to <http://www.myZyXEL.com> with the X6004's serial number and WAN MAC address to register it.) Refer to the web site's on-line help for details.

Note: To activate a service on a X6004, you need to access myZyXEL.com via the X6004.

36.1.1 What You Can Do in this Chapter

- Use the **Registration** screen to fill out your personal details and register your X6004. See [Section 36.2 on page 479](#).
- Use the **Service** screen to view your licensed service(s) and upgrade your service licenses. If you reset your X6004 to the factory default, you can also use this screen to get your licensed service information. See [Section 36.3 on page 480](#).
- Use the **License Status** screen to view your service license status. See [Section 36.4 on page 481](#).

36.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Subscription Services Available on the X6004

At the time of writing, the following services are available on the X6004:

- **SIP extension registration** - The number of SIP extensions you can create on the X6004 is limited by your service subscription. In order to add more SIP extensions to the X6004, you need to buy an iCard and register for additional extensions via myZyXEL.com.
- **ZyXEL softphone** - ZyXEL offers a software-based SIP IP phone that you can install on the following operating system: Microsoft Windows 2000 and Microsoft Windows XP.

After installation you can connect to the X6004 and use a computer to make calls via the X6004. Refer to the documentation that came with your ZyXEL softphone.
- **Attendent Console** - ZyXEL offers a software-based SIP Attendent Console that you can install on the following operating systems: Microsoft Windows 2000 and Microsoft Windows XP.
- **Click To Talk** - The number of click to talk extensions that can create on the X6004 is limited by your service subscription. In order to add more CTT extensions to the X6004, you need to buy an iCard and register for additional extensions via myZyXEL.com.

Note: At the time of writing ZyXEL offers the V100 and V120 SoftPhones. Contact your vendor for more information about what softphone ZyXEL offers.

Note: See the [Chapter 40 on page 521](#) for more information about the subscriber services the X6004 supports.

36.1.3 Before You Begin

Before you register your X6004 and activate the services at myZyXEL.com, you need to do the following.

- Create a user account using the X6004's web configurator or myZyXEL.com website.
- Buy a license key for the services you want.

36.2 The Registration Screen

Use this screen to register your X6004 with myZyXEL.com and activate a service, such as a softphone extension license. Click **Maintenance > License Control > Registration** in the navigation panel to open the screen shown next.

Figure 287 License Control > Registration

Each field is described in the following table.

Table 195 License Control > Registration

LABEL	DESCRIPTION
Device Registration	If you select Existing myZyXEL.com account , only the User Name and Password fields need to be filled in.
New myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your X6004.
Existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your X6004.
User Name	Enter a user name for your myZyXEL.com account. The name should be between 6 ~ 20 alphanumeric characters. Underscores are allowed but spaces are not.
Check	Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used.
Password	Enter a password of between 6 ~ 20 alphanumeric characters. Underscores are allowed but spaces are not.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.

Table 195 License Control > Registration (continued)

LABEL	DESCRIPTION
Country	Select your country from the drop-down box list.
Apply	Click this to save your changes.

36.3 The Service Screen

Use the **Service** screen to register and enter your license key information (provided in the box with your X6004). You can also view the services to which you currently subscribe. Click **Maintenance > License Control > Service** to open the screen as shown next.

Note: If you restore the X6004 to the default configuration file or upload a different configuration file after you register, click the **Service License Refresh** button to update license information.

Figure 288 License Control > Service

The screenshot shows the 'Service Management' screen. It features a table with two columns: 'Service' and 'Quantity'. The table lists four services: Extension Number (32), Soft Phone Number (8), Click To Talk Number (0), and Attendant Console Number (0). Below the table is a 'License Upgrade' section with a 'License Key' input field and an 'Update' button. At the bottom, there is a 'Service License Refresh' button with a tooltip that says '(Sync with myZyXEL.com to download license Info.)'.

Service	Quantity
Extension Number	32
Soft Phone Number	8
Click To Talk Number	0
Attendant Console Number	0

License Upgrade

License Key

(Sync with myZyXEL.com to download license Info.)

Each field is described in the following table.

Table 196 License Control > Service

LABEL	DESCRIPTION
Service Management	Use this section to view details about the services you are subscribing to.
Service	This field displays the name of the service available on the X6004.
Quantity	This field displays the number of licenses you have registered for a each service.
License Upgrade	Use this section to update your license information.
License Key	Enter your license key (provided in the box with your X6004) and click Update to activate or extend a standard service subscription.
Service License Refresh	Click this button to renew service license information (such as the license key and registration status).

36.4 The License Status Screen

Use this screen to view the registration status of your subscription services. Click **Maintenance > License Control > License Status** to open the screen as shown next.

Figure 289 License Control > License Status

License Status	
Machine ID: IPPBX_001 (Unregistered)	
Service	Quantity
Extension Number	32
Soft Phone Number	8
Click To Talk Number	0
Attendant Console Number	0

Each field is described in the following table.

Table 197 License Control > License Status

LABEL	DESCRIPTION
Machine ID	This field displays the name (automatically assigned to the X6004) as well as the registration status (Unregistered or Registered) of the X6004.
Service	This field displays the name of the service available on the X6004.
Quantity	This field displays the number of licenses you have registered for a each service.

Web Portal

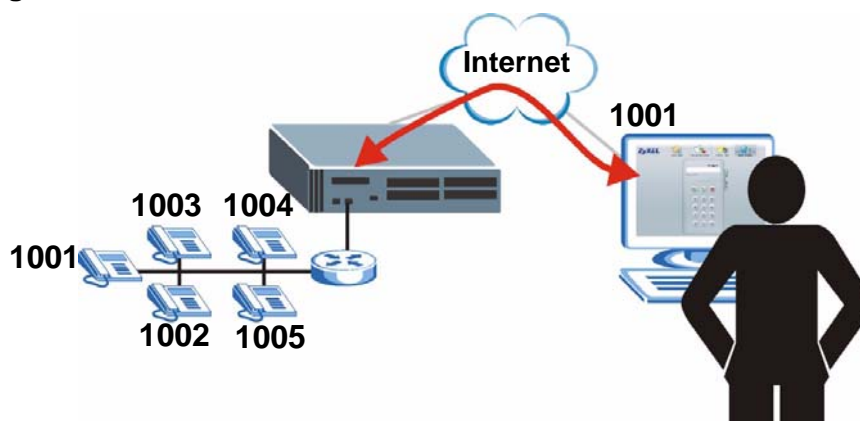
37.1 Overview

This chapter shows you how to use the web portal to make calls via the web phone and manage settings for individual users.

The web portal is a HTML-based phone as well as a management tool that allows users to manage some of the settings related to their telephone extension. Each extension created on the X6004 has an associated account which allows it to log into the web portal. When you login to the web portal you can pick up and make calls using your browser.

The web portal can be used by members of your organization who are working away from the office. As long as they have a reliable Internet connection, they can login to the web portal and answer and make calls from the same extension as they have in the office. For example, a user working from home, can log into the web portal with their desk phone extension (1001) and use the HTML-based phone to call extension 1002. He can also receive calls directed to extension 1001.

Figure 290 Web Portal Overview



37.1.1 What You Can Do in this Chapter

- Use the **Account Settings** screen to configure SIP authentication information for your extension. See [Section 37.2 on page 485](#).
- Use the **Call Forwarding and Blocking** screen to configure call forwarding and call blocking rules for your extension. See [Section 37.3 on page 487](#).
- Use the **Voice Mail Settings** screen to set up the voice mail settings for your extension. See [Section 37.4 on page 493](#).
- Use the **Web Phone** screen to make a call from the web phone. See [Section 37.5 on page 494](#).
- Use the **Utility Download** screen to download utilities. See [Section 37.6 on page 495](#).

37.1.2 What You Need to Know

The following terms and concepts may help you as you read through the chapter.

Web Portal Login

- 1 Start your web browser.
- 2 Type "https://" and the IP address of the X6004 (for example, the default LAN IP address is 192.168.1.12) in the **Location** or **Address** field. Press [ENTER].
- 3 The login screen appears. Enter your extension number and the associated web password in the upper part of the login screen and click **Login**.

Note: The web password is set up by the administrator when the extension is initially created. See [Chapter 13 on page 197](#).

Figure 291 Web Portal: Login

ZyXEL

IPPBX X6004

Language : English

Enter Extension number and PIN Code then click Login.

☺ Extension :

🔒 PIN Code :

Enter Administrator Username and Password then click Login.

☺ Username :

🔒 Password :

(max. 32 alphanumeric, printable characters and no spaces)

Note :
Please turn on the Javascript and ActiveX control setting on Internet Explorer and trun off the block popup window application.

Login Reset

37.2 Account Settings

Use this screen to manage the passwords associated with your extension. To access this screen, click **Peer info.** in the web portal. This is also the first screen you see when you login to the web portal.

Note: Some of the fields are not applicable for FXS and BRI extensions and do not display when analog or ISDN phone users log into the personal web portal.

Figure 292 Peer Info

The screenshot shows the ZyXEL web portal interface. At the top, there is a navigation bar with the ZyXEL logo and five icons: Peer Info, Forward/Block, Voice Mail, Web Phone, and Utility Download. Below this is a window titled "SIP Peer 2000 Setting". Inside the window, the following fields are visible:

- Group: CustomerSupport
- SIP Auth. User Name: 2000
- SIP Auth. Password: [masked] (Confirm: [masked])
- Web/IVR/VM PIN Code: [masked] (Confirm: [masked])

At the bottom of the window, there are two buttons: "Apply" and "Reset".

Each field is described in the following table.

Table 198 Peer Info

LABEL	DESCRIPTION
Group	This is a read-only field showing the authority group this extension belongs to.
SIP Auth. User Name	This is a read-only field showing the SIP user name associated with this extension. This field is not available for FXS and BRI extensions on the X6004.
SIP Auth. Password	Use these fields to change the SIP password associated with this extension. Type and retype the new password for this extension. This is the password you will need to enter when registering a SIP phone with the X6004. This field is not available for FXS and BRI extensions on the X6004.
Web/IVR/VM PIN Code	Use these fields to change the PIN (Personal Identification Number) you need to enter when accessing the web portal, Interactive Voice Response system or Voice Mail. Type and retype the new PIN.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to begin configuring the fields again.

37.3 Call Forwarding and Blocking

Use this screen to set up call forwarding and call blocking rules for your extension. To access this screen, click **Forward/Block** in the web portal.

Figure 293 Forward/Block

Each field is described in the following table.

Table 199 Forward/Block

LABEL	DESCRIPTION
Call Forward Setting	Use this section to configure call forwarding settings for your extension.
Office Hours	The X6004 has separate rules for call forwarding during office hours than after office hours. The time you configure specifies the office hours for this extension and affects call forwarding during those office hours.
Office Hours	Click this button to open the configuration screen for office hours. For information, see Chapter 12 on page 193 .

Table 199 Forward/Block (continued)

LABEL	DESCRIPTION
DND (Do Not Disturb)	<p>Select Enable and the X6004 will not forward calls to your extension. Click on White List to configure telephone numbers which ignore whether you have DND turned on or off. See Section 37.3.2 on page 491.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p> <p>Select Disable to turn this feature off for this extension.</p>
Blind Forward	<p>Select Enable and specify an extension. The X6004 will forward all incoming calls to that extension.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p> <p>Select Disable to turn this feature off for this extension.</p>
Busy Forward	<p>Select Enable and specify an extension. The X6004 will forward all incoming calls to that extension when your phone is in use.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p> <p>Select Disable to turn this feature off for this extension.</p>
No Answer Forward	<p>Select Enable and the X6004 will forward all incoming calls to the extensions you specify when you do not answer the phone within the default ring time. Click Find Me List to specify a list of extensions that the X6004 will forward incoming calls to. See Section 37.3.3 on page 491.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p> <p>Select Disable to turn this feature off for this extension.</p>
After Office Hours	<p>These fields specify how to treat calls to your extension that occur after office hours.</p> <p>Select Enable and specify an extension. The X6004 will forward all incoming calls to that extension.</p> <p>Select Voice Mail and the X6004 will forward calls directly to voice mail.</p> <p>Select Disable to turn this feature off for this extension.</p>
Call Blocking Setting	Use this section to configure call blocking settings for your extension.
Black List	<p>Select Enable and the X6004 will block all incoming calls from extensions that you specify as blacklisted. Click the Black List button to configure phone numbers that you want to block from calling you. See Section 37.3.4 on page 492.</p> <p>Select Disable to turn this feature off for this extension.</p>
Block the calls without Caller ID	Select Enable and the X6004 will block all incoming calls from phone that do not send caller ID.

Table 199 Forward/Block (continued)

LABEL	DESCRIPTION
Mobile Extension Setting	This section displays information about your mobile extension, if one has been configured for you. For more information on this, see Chapter 13 on page 197 .
Mobile Extension	This displays the phone number to which all calls sent to your extension will be forwarded.
Status	This indicates your mobile extension feature is on, off, or not enabled.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to begin configuring the fields again.

37.3.1 Office Hours

Use this screen to specify office hours for the X6004. To access this screen, click the **Office Hours** button in the **Forward/Block** screen.

Figure 294 Office Hour Setting

Office Hour Setting

Office Hours

Days of Week	<input type="checkbox"/> Sun	<input checked="" type="checkbox"/> Mon	<input checked="" type="checkbox"/> Tue	<input checked="" type="checkbox"/> Wed	<input checked="" type="checkbox"/> Thu	<input checked="" type="checkbox"/> Fri	<input type="checkbox"/> Sat
Time	<input type="text"/>	08:00-12:00	08:00-12:00	08:00-12:00	08:00-12:00	08:00-12:00	<input type="text"/>
	<input type="text"/>	13:00-17:30	13:00-17:30	13:00-17:30	13:00-17:30	13:00-17:30	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Holiday

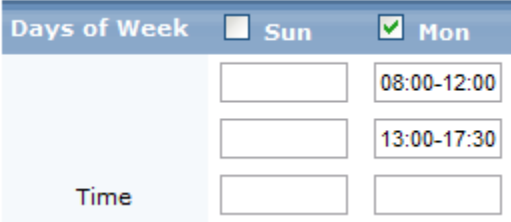

Date	Description	
02/14	Lunar New Year	
01/01	New Years Day	
02/14	Lunar New Year	
07/04	July 4th	
10/10	Double 10 Day	
12/24	Christmas Eve	
12/25	Christmas Day	

Each field is described in the following table.

Table 200 Office Hour Setting

LABEL	DESCRIPTION
Office Hour Setting	Use this section to specify office hours on the X6004.
Days of Week	Check the days of the week which you want the X6004 to treat as working days.

Table 200 Office Hour Setting (continued)

LABEL	DESCRIPTION
Time	<p>Specify the time range during the working days that you want the X6004 to treat as working hours.</p> <p>When entering a time range, the following conditions apply:</p> <ul style="list-style-type: none"> You can enter up to six time ranges, with each range consisting of a start time and an end time. The time entered in each field must be in 24 hr format (such as "08:00" for 8 AM or "24:00" for midnight). The start and end times must be separated by a hyphen. <p>For example, a standard work day may look like this:</p>  <p>In this example, the first time block is from 8 AM until 12 noon. The second time block is from 1 PM until 5:30 PM.</p>
Holiday	<p>This section allows you to set a specific day of the year as a holiday, which the X6004 will then treat as "after office hours".</p>
Date	<p>Enter a date in mm/yy format (double digit month / year; for example, 02/09 for February, 2009.)</p> <p>You can also click the "... " icon to open the interactive calendar:</p>  <p>Click a day to select it.</p> <p>Use the < and > buttons to cycle through the year and months.</p> <p>Click the X button to close the calendar.</p>
Description	<p>Enter a description of the holiday using up to 63 alphanumeric characters (a-z, A-Z, 0-9, spaces, underscores and hyphens allowed).</p>
Add	<p>Click this to add the newly configured holiday to the list.</p> <p>You must fill out the Date and Description fields first.</p>
Delete	<p>Click this to remove a holiday from the list.</p>
Apply	<p>Click Apply to save your changes.</p>
Default	<p>Click this button to set every field in this screen to factory default configuration.</p>

37.3.2 DND White List

Use this screen to edit the **DND White List** for your extension. The X6004 will forward calls to these extensions even if you have DND enabled. To access this screen, click the **DND White List** button in the **Forward/Block** screen.

Figure 295 Forward/Block > DND White List

Each field is described in the following table.

Table 201 Forward/Block > DND White List

LABEL	DESCRIPTION
Number	Enter the telephone number you want to allow to call you even if you DND turned on. Click Add and the number you entered displays in the field below.
Delete	Highlight an existing DND White List number and click the Delete icon to remove it from the list.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to return to Forward/Block screen.

37.3.3 Find Me List

Use this screen to edit the **Find Me List** for your extension. This is a list of extensions that the X6004 tries to call if you do not pick up a call. To access this screen, click the **Find Me List** button in the **Forward/Block** screen.

Figure 296 Forward/Block > Find Me List

Each field is described in the following table.

Table 202 Forward/Block > Find Me List

LABEL	DESCRIPTION
Number	Enter the telephone extension you want the X6004 to forward calls to when you do not pick up a call. Click Add and the number you entered displays in the field below.
Priority	Highlight an existing Find Me List extension and use the up arrow to move it up in the list or use the down arrow to move it down in the list. The X6004 will try to forward the call to the extensions in the list in the order they appear from top to bottom. If the topmost extension in the list does not pick up it tries the one below and so on.
Delete	Highlight an existing Find Me List extension and click the Delete icon to remove it from the list.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to return to Forward/Block screen.

37.3.4 Blacklist

Use this screen to edit the **Black List** for your extension. This is a list of phone numbers from which the X6004 will block calls to your extension. To access this screen, click the **Black List** button in the **Forward/Block** screen.

Figure 297 Forward/Block > Black List

Each field is described in the following table.

Table 203 Forward/Block > Black List

LABEL	DESCRIPTION
Number	Enter the telephone number you want to block from calling you when you enable call blocking. Click Add and the number you entered displays in the field below.
Delete	Highlight an existing Black List number and click the Delete icon to remove it from the list.
Apply	Click this to save your changes and to apply them to the X6004.
Cancel	Click this to return to Forward/Block screen.

37.4 Voice Mail Settings

Use this screen to set up the voice mail settings for your extension. To access this screen, click the **Voice Mail** tab in the web portal.

Figure 298 Voice Mail Setting

Each field is described in the following table.

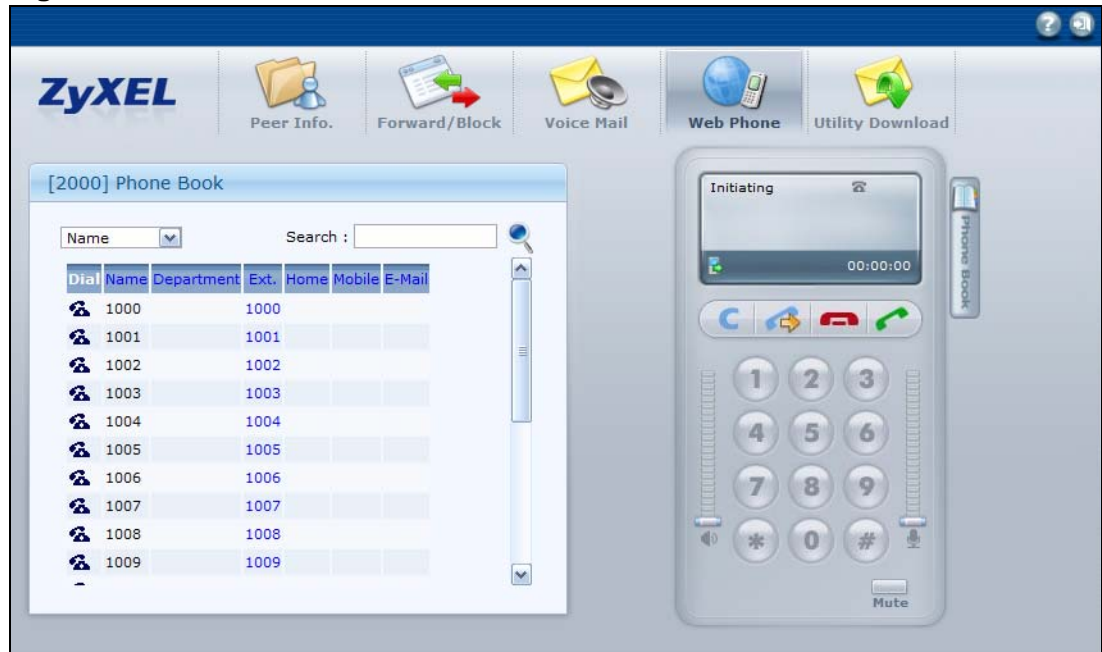
Table 204 Voice Mail Setting

LABEL	DESCRIPTION
Received E-mail Address	Specify the e-mail address you want to forward your voice message notifications to. If you select the Attached Voice File option, then complete voice messages are sent to this e-mail address.
Attached Voice File	Select this feature if you want complete voice messages to be sent to the e-mail address you specified in the Received E-mail Address field.
Delete Voice Mail After Mailed	Check this box to delete voicemail messages stored on the X6004 after they have been e-mailed.
Apply	Click this to save your changes and to apply them to the X6004.
Reset	Click this to begin configuring the fields again.

37.5 Web Phone

Use this screen to make calls from the web phone. To access this screen, click the **Web Phone** tab in the web portal.

Figure 299 Web Phone







Each field is described in the following table.

Table 205 Web Phone

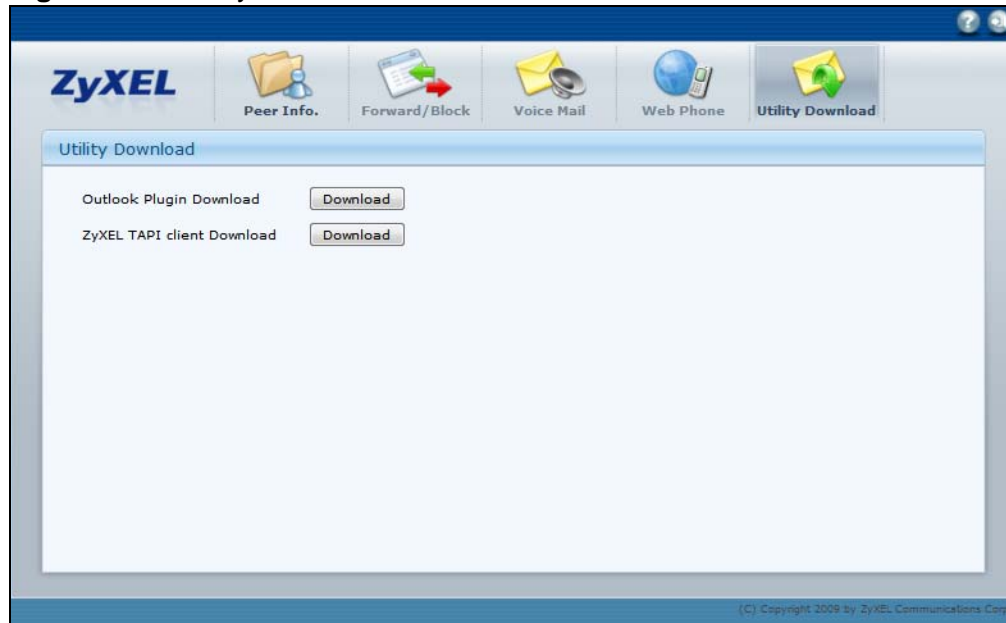
LABEL	DESCRIPTION
Phone Book	Click the Phone Book tab on the right side of the Web Phone screen to display or hide the phone book feature. The phone book feature allows you to search all entries configured in your personal phone book or system phone book configured on the X6004.
Search	In the left drop down list box select the search criteria. The search criteria consist of the fields you fill in when creating phone book entries. In the right text box type in your search criteria. Click Search to display any phone book entries that match your query.
Call Duration	This total time of your conversation is displayed above the input field in the web phone GUI.
Input Text	Type or use your keypad to enter the phone number you want to dial. The web phone follows the same dialing rules that you have to follow when you are making calls from any other phone connected to the X6004.

Table 205 Web Phone (continued)

LABEL	DESCRIPTION
Status	The status of your phone call is displayed below the text input field. The web phone GUI displays the current status of a phone call, that is "Ringing", "Talking" or "Bye". It also displays the phone number you dialed from the web phone.
Phone Keypad	<p>You can use your mouse to click on the numbers that make up the telephone number you want to dial.</p> <p>Use the Clear icon () to delete digits from the screen.</p> <p>Use the Dial/Pick up icon () to dial the number.</p> <p>Use the Hang up icon () to end a call or to delete a number in the input field.</p> <p>Use the Transfer icon () to forward a call to another extension.</p>

37.6 Utility Download

Use this screen to download any X6004 utilities. To access this screen, click the **Utility Download** tab in the web portal.

Figure 300 Utility Download

Each field is described in the following table.

Table 206 Utility Download

LABEL	DESCRIPTION
Download	Click this button to download any available utilities to your computer.

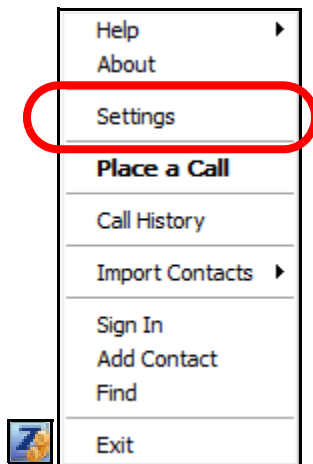
37.6.1 The Outlook Plugin

The Web Portal is the Microsoft Outlook plugin is a small utility that allows you to issue an invite to any person in your address book. When the invite is sent out, both your extension and the extension of the invited person ring.

Note: The Outlook plugin can only be installed on computers using both Microsoft Windows 2000 and higher and Microsoft Office 2003 and higher.

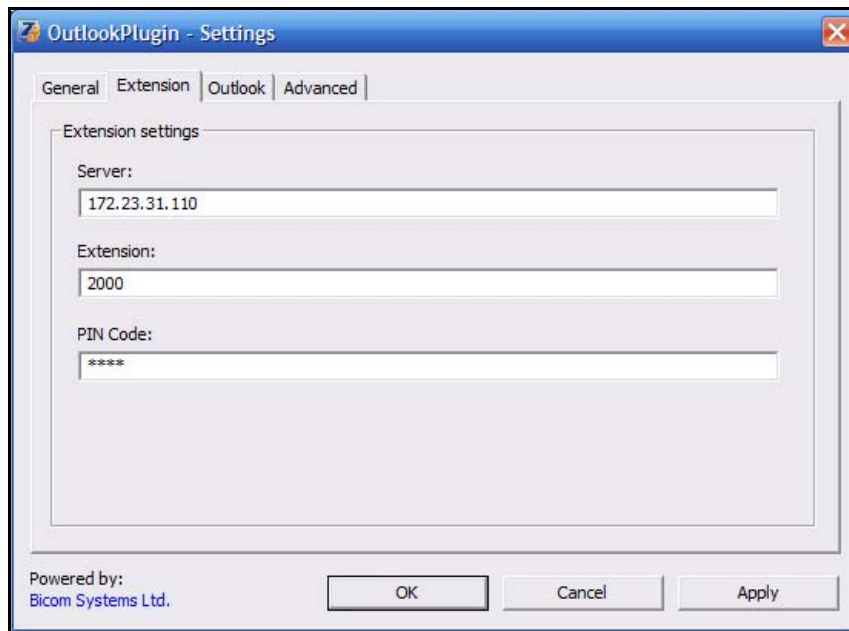
To use the Outlook plugin:

- 1 In the **Web Portal > Utilities Downloads** screen, click the **Download** button for the Outlook Plugin.
- 2 After the file finishes downloading it, unzip it and then double-click the plugin.exe file to start the Installation Wizard. Follow the on-screen instructions.
- 3 When installation is complete, click **Start > Programs > ZyXEL > OutlookPlugin > OutlookPlugin** to run the Setup Wizard. Follow the on-screen instructions.
- 4 After installation, right-click on the Outlook plugin Taskbar menu icon and then click **Settings**.

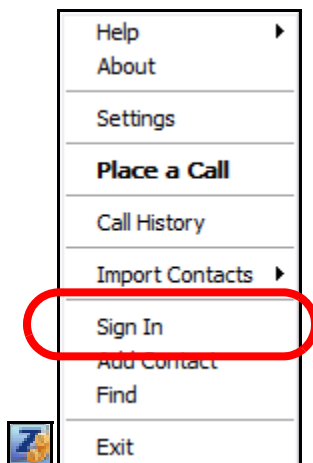


The Outlook Plugin - Settings dialog opens

- 5 In the Outlook Plugin - Settings dialog, configure the X6004's **Server** IP address, your **Extension** number and your extension **PIN Code** on the **Extension** screen..

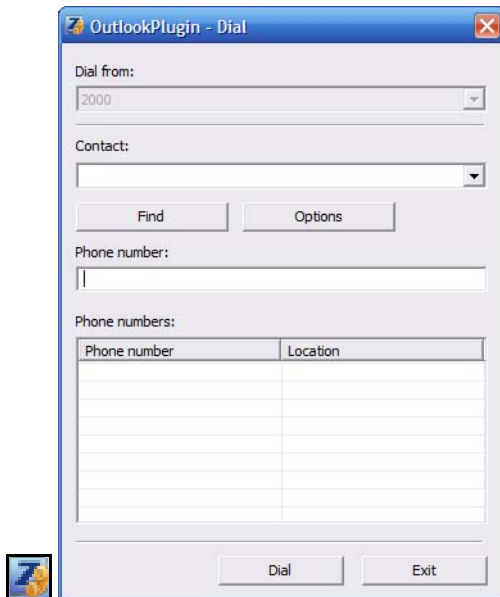


- 6 Click **OK** to save your settings and close the dialog.
- 7 Next, right-click on the Outlook plugin Taskbar menu icon and click **Sign In**.



The icon flashes while the plugin signs in with the X6004. It turns green upon success. If it cannot sign in, an error message pops up.

- 8 Once you are signed in, double-click the Outlook plugin's Taskbar icon to open the Outlook Plugin - Dial dialog..l



- 9 Select a **Contact**. This list is populated with entries from your Microsoft Outlook address book. The first time you run it, there may not be any address book entries. If so, click the **Options** button and select **Import Contacts > From Outlook**. You can also import contacts from a comma-delimited CSV.
- 10 Select a **Phone Number**. The phone numbers that appear in this list are match the phone numbers associated with the contact in your Outlook address book.
- 11 Click the **Dial** button. The X6004 rings both your phone and the phone number of the person you selected

Note: If you cannot sign in, open the X6004 web configurator **Maintenance > Administration > Remote Management > CTI** screen and disable the CTI white list. Or, alternatively, you can add your WAN to the CTI white list.

37.6.2 TAPI Client Driver

The ZyXEL client TAPI driver allows you to use Microsoft Outlook from a Windows 2000 or later computer to issue an invite to any person in your address book. When the invite is sent out, both your extension and the extension of the invited person ring. For a snom phone, you can also click to answer a call.

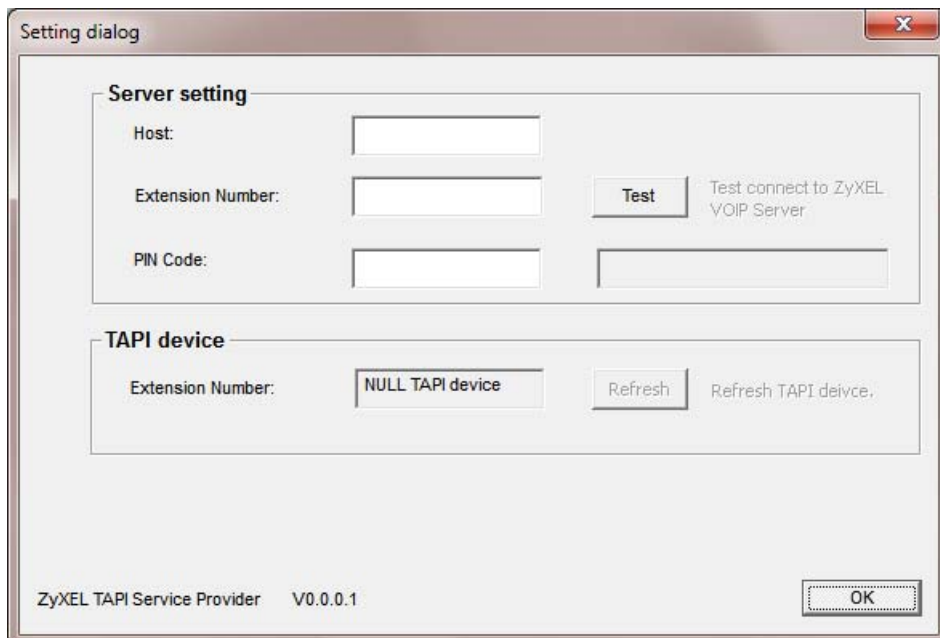
37.6.2.1 Setting Up the TAPI Client Driver

ZyXEL's TAPI driver is called the ZyXEL TSP (Telephony Service Provider). Your computer needs to be on the X6004's LAN. To download and install the driver:

- 1 In the **Web Portal > Utilities Downloads** screen, click the **Download** button for the ZyXEL TAPI client.
- 2 Unzip the file and run it, following the on-screen instructions to install it.



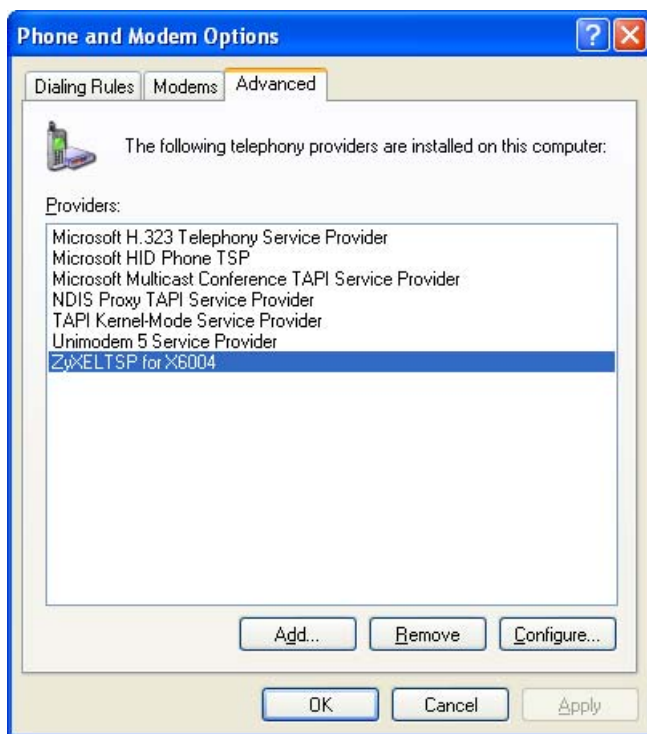
- 3 In the **Setting dialog** window:



- 3a **Host** - enter the X6004's host name or IP address.
 - 3b **Extension Number** - enter your extension number

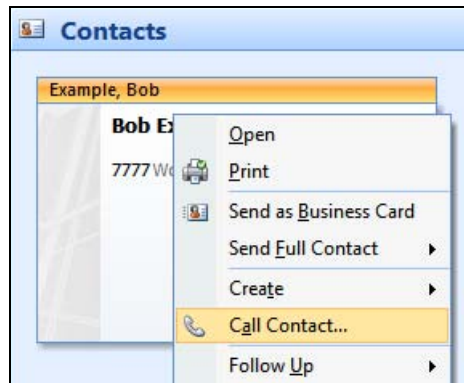
- 3c **PIN Code** - enter your PIN code
- 3d Click **Test** to make sure you can connect to the X6004.
- 3e After "Connect Success" displays, click **Refresh** to update your extension in the **Extension Number** field.
- 3f Click **OK**.

To confirm that the driver is installed, click **start > Control Panel > Phone and Modem Options**. If you haven't configured your modem settings, you'll need to do so. Then click the **Advanced** tab and make sure a ZyXEL TSP entry appears in the list of providers.



37.6.3 Sending Call Invites from Microsoft Outlook

In Outlook, right-click a contact and click **Call Contact**. Your extension and the called party's extension both ring.



IVR System

38.1 Overview

This chapter shows you how to use the personal Interactive Voice Response (IVR) system on the X6004.

IVR is a phone technology that allows a computer to detect voice and touch tones using a normal phone. An IVR system can respond with pre-recorded audio prompts to further direct callers on how to proceed. IVR systems can be used to control most functions where the interface can be broken down into a series of simple menu choices.

The X6004 has a personal IVR system which allows users to edit some of their personal (unique to each extension) settings. The IVR system on the X6004 allows users to:

- Change their voicemail, IVR, and web phone PIN.
- Configure their call forwarding and blacklist settings.
- Configure their voicemail settings.

38.1.1 What You Need to Know About IVR

The following terms and concepts may help as you read through the chapter.

Accessing IVR

Users can access their personal IVR system by dialing the feature code for IVR followed by their extension number. The feature code for IVR is configured in the **Configuration > PBX > Server Configuration > Server > Feature Code** screen (see [Section 6.8 on page 141](#)). For example, if the feature code for IVR is an asterisk (*), then a caller with extension **1001** must dial ***1001** to access their personal IVR system.

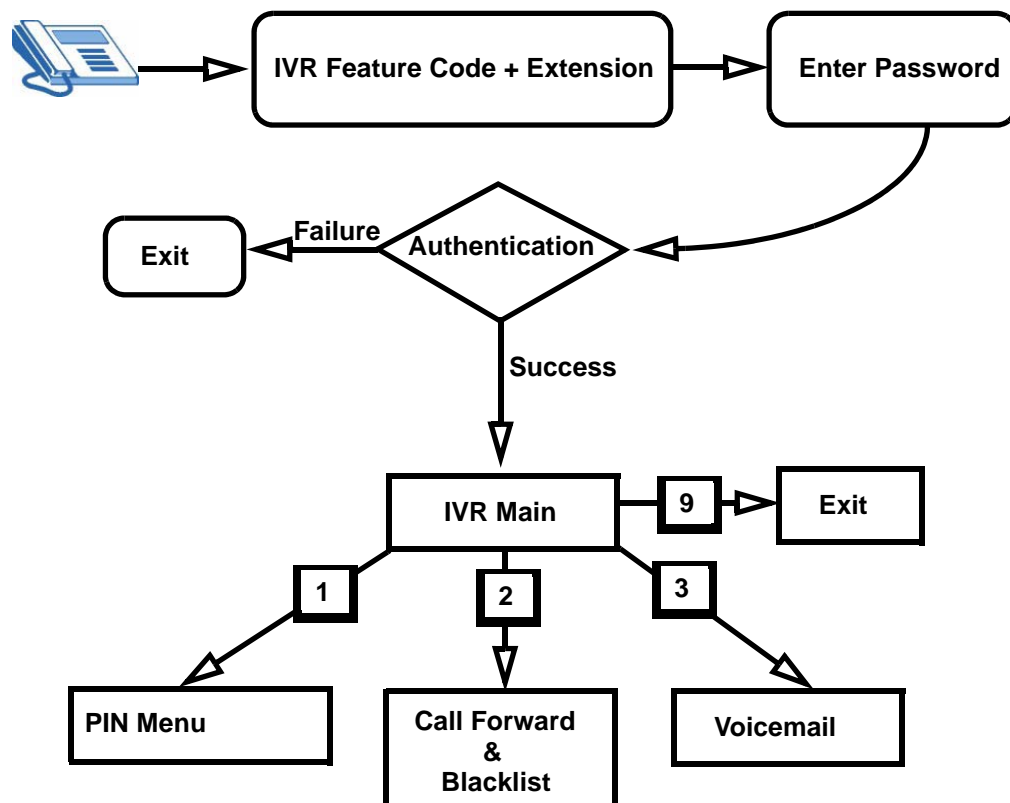
Personal IVR can be accessed as an internal call or users can call from an outside line and dial the feature code for IVR followed by their extension when an auto-attendant prompts them to dial the extension they wish to reach.

Users must authenticate before they can edit their configuration settings via IVR. When users dial into their personal IVR they are prompted to enter their PIN. The IVR PIN is assigned to each extension when the extension is created. See [Section 13.3.3 on page 208](#) for information on how to configure the IVR PIN for SIP extensions and [Section 13.3.12 on page 221](#) for analog phone extensions. If a user authenticates successfully, then he or she is guided through the personal IVR menus via pre-recorded audio prompts. If a user fails to authenticate, the X6004 plays a message indicating that an incorrect password was entered and the call is dropped.

Personal IVR Main Flow

The following figure describes the main flow in the personal IVR system.

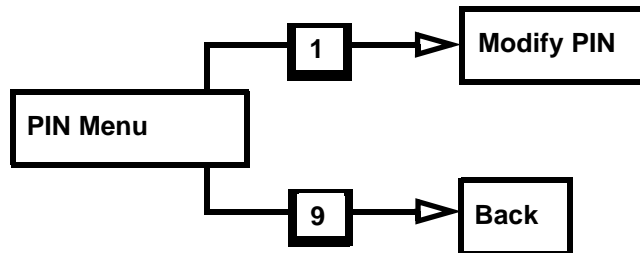
Figure 301 Personal IVR Flow



Personal IVR PIN Menu

The following figure describes the **PIN Menu**. From **IVR Main**, press number **1** on your phone keypad to enter the **PIN Menu**. This menu allows you to change the PIN used to authenticate with your voicemail system, web phone, and personal IVR system.

Figure 302 IVR: PIN Menu

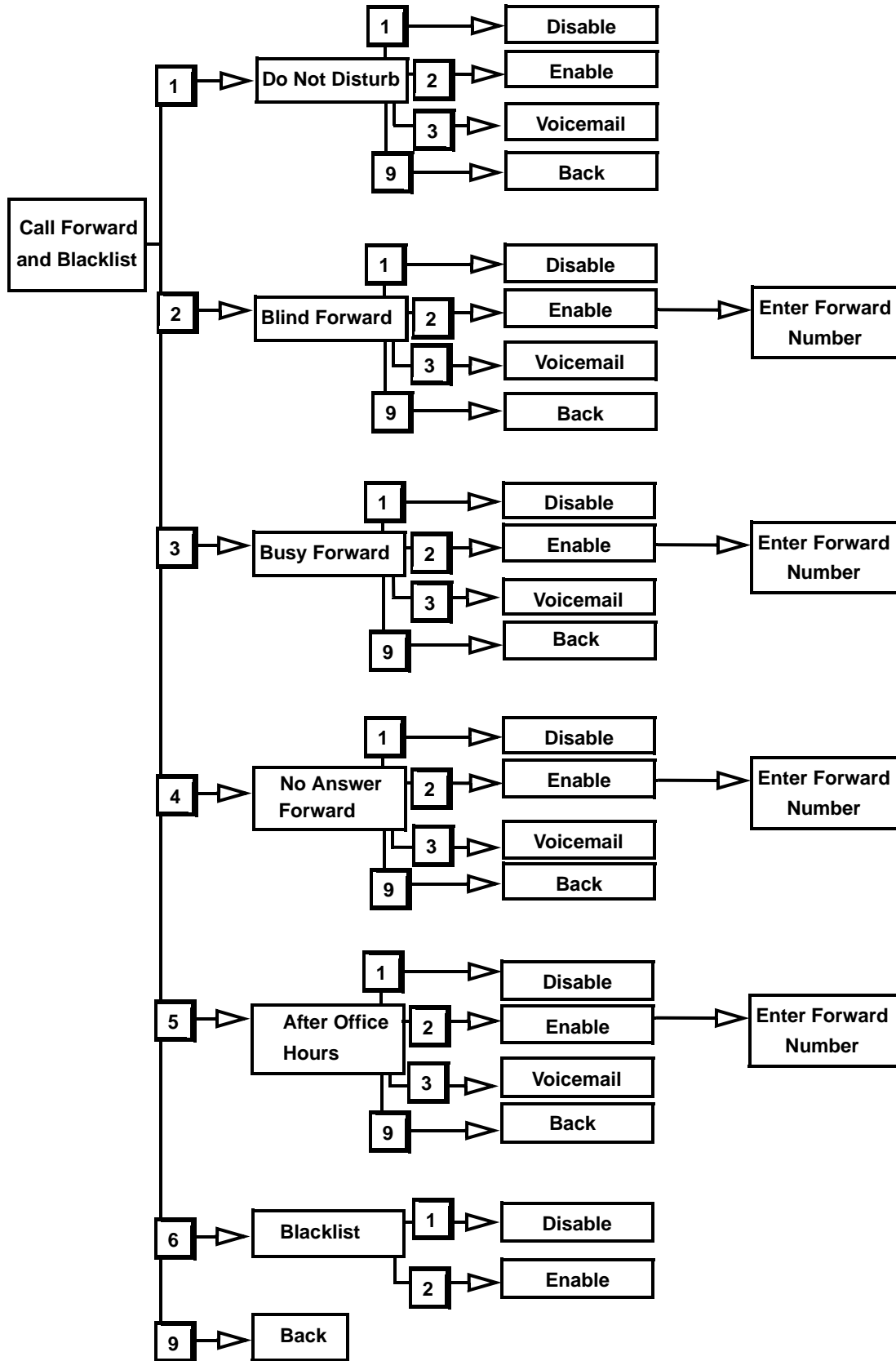


Personal IVR Call Forward & Blacklist

The following figure describes the **Call Forward & Blacklist Menu**. From **IVR Main**, press number **2** on your phone keypad to enter the **Call Forward & Blacklist Menu**. This menu allows you to enable the **Do Not Disturb**, **Blind Forward**, **Busy Forward**, **No Answer Forward**, **After Office Hours** (forward) and **Blacklist** functions. You can also specify the telephone extension you want your calls forwarded to or alternatively you can choose to forward calls to your voicemail.

See [Section 13.3.13 on page 222](#) for more information on call forwarding features and how to configure office hours settings for individual extensions.

Figure 303 IVR: Call Forward & Blacklist



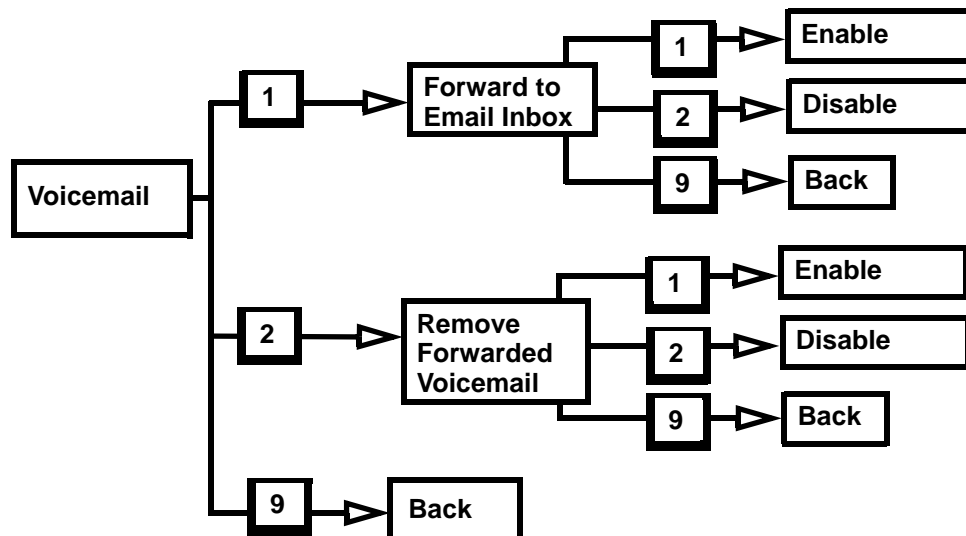
Personal IVR Voicemail

The following figure describes the **Voicemail Menu**. From the **IVR Main** menu, press number **3** on your phone keypad to enter the **Voicemail Menu**. This menu allows you to have the system send voicemail as an audio file attachment to your email inbox.

You can also have the system erase your voicemail from the X6004 once it has been forwarded to your email inbox. Enable this option if you do not want to use the built-in flash memory on the X6004 to store your voicemail messages.

See [Chapter 9 on page 173](#) for more information on the voicemail feature and [Section 6.8 on page 141](#) for information on how to configure the feature code for voicemail (this is the number you have to dial to listen to your voicemail messages via your handset).

Figure 304 IVR: Voicemail



Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [X6004 Access and Login](#)
- [Internet Access](#)
- [Advanced Features](#)
- [Reset the X6004 to Its Factory Defaults](#)
- [The Console Port](#)

39.1 Power, Hardware Connections, and LEDs

The X6004 does not turn on. None of the LEDs turn on.

- 1 Make sure the X6004 is turned on.
- 2 Make sure you are using the power adaptor or cord included with the X6004.
- 3 Make sure the power adaptor or cord is connected to the X6004 and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the X6004 off and on.
- 5 Disconnect and re-connect the power adaptor or cord to the X6004.
- 6 If the problem continues, contact the vendor.

The ALM LED is on.

- 1 Turn the X6004 off and on.
- 2 Disconnect and re-connect the power adaptor to the X6004.
- 3 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.4 on page 32](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the power adaptor to the X6004.
- 5 Turn the X6004 off and on.
- 6 If the problem continues, contact the vendor.

39.2 X6004 Access and Login

I forgot the IP address for the X6004

- 1 The default LAN IP address is 192.168.1.12.
- 2 Use the console port to log into the X6004 (see [Section 39.6 on page 516](#)).
- 3 Use the command `network interface show ip all` to check the WAN and LAN IP addresses of the X6004.
- 4 Enter the `initrd` screens and change the X6004's IP address to the WAN/LAN default (see [Section 39.6.3 on page 517](#)).

- 5 If this does not work, you have to reset the X6004 to its factory defaults. See [Section 35.2 on page 471](#).

I forgot the password

- 1 The default password is **1234**.
- 2 Enter the `initrd` screens and reset the admin password to its default (see [Section 39.6.3 on page 517](#)).
- 3 If this does not work, you have to reset the X6004 to its factory defaults. See [Section 35.2 on page 471](#).

I cannot see or access the **Login** screen in the web configurator

- 1 Make sure you are using the correct IP address.
 - The default LAN IP address is 192.168.1.12 and WAN IP address is 172.16.1.1.
 - If you changed the IP address ([Section 5.2 on page 114](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the X6004](#)
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.4 on page 32](#).
- 3 Make sure your computer is in the same subnet as the X6004's LAN or WAN. (If you know that there are routers between your computer and the X6004, skip this step.)
- 4 Make sure you access the X6004 web configurator via HTTPS (`https://the X6004's IP address`), not HTTP.
- 5 Make sure your computer is with an IP address which is in the white list of the X6004's WWW access.
- 6 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Section 4.1 on page 101](#).

- 7 Press the **RESET** button on the front panel of the X6004 to reset to its factory defaults. Then try to access the X6004 with the default IP address. See [Section 35.2 on page 471](#).
- 8 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the X6004 using another service, such as SSH. If you can access the X6004, check the remote management settings to find out why the X6004 does not respond to HTTPS.

I can see the **Login** screen, but I cannot log in to the X6004

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone who has logged into the X6004 using an administrator account with the same privilege rank as yours ([Section 30.3 on page 433](#)). Log out of the X6004 in the other session, or ask the person who is logged in to log out.

Alternatively, you can check the status of the account you used and failed to login using CLI commands. Log in to the X6004's console using a "Debug admin" administrator account and type the following commands.

2a system admin show webuser loggedin

2b system admin logout webuser username <admin-username>

In this example, the account "admin" has been used to log into the X6004's web configurator from an address 172.16.17.109. But the user has logged out.

```
> system admin show webuser loggedin
Username "admin" ClientIPAddr = 172.16.17.109
> system admin logout webuser username admin
admin logouted
```

- 3 Turn the X6004 off and on.
- 4 Disconnect and re-connect the power adaptor or cord to the X6004.
- 5 If this does not work, you have to press the **RESET** button on the front panel of the X6004 to reset to its factory defaults. See [Section 35.2 on page 471](#).

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

I cannot SSH to the X6004

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

39.3 Internet Access

I cannot access the Internet

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.4 on page 32](#).
- 2 Make sure you entered your network settings correctly in the wizard or in the **Configuration > Network**.
- 3 Connect a computer in the same network as the X6004's WAN. Check if you can access the X6004, the X6004's gateway, and Internet from the computer. See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#) if you cannot access the X6004. Contact your network administrator or your ISP if you can access the gateway but cannot access the Internet.

I cannot access the Internet anymore. I had access to the Internet (with the X6004), but my Internet connection is not available anymore

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.4 on page 32](#).

- 2 Reboot the X6004.
- 3 Disconnect and re-connect the power adaptor to the X6004.
- 4 Turn the X6004 off and on.
- 5 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.4 on page 32](#). If the X6004 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Reboot the X6004.
- 3 Disconnect and re-connect the power adaptor to the X6004.
- 4 Turn the X6004 off and on.
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.
- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

39.4 Advanced Features

Fail to add a device in a ZyStack.

- 1 The X6004 only supports up to five X6004s in a ZyStack. It would be failed If you try to add the sixth ZyStack X6004.

- 2 Make sure the ZyStack X6004 is up and connected to the network. You can make a ping from the X6004 to it through the CLI command mode.
- 3 Makes sure that the IP address of the ZyStack interface on the slave server is in the same subnet as the one on the master server.
- 4 Make sure that the serial number, WAN and LAN IP addresses you configured in the **Configuration > ZyStack > Setting > Add** or **Edit** screen are correct.

Fail to initiate packet capturing in **Maintenance > Administration > Diagnostics > Packet Capture**.

The diagnostics are only available for a “debug administrator”. You have to use an account with “debug admin” privilege rank to log into the X6004 first. See [Section 3.8 on page 86](#).

39.5 Reset the X6004 to Its Factory Defaults

If you reset the X6004, you lose all of the changes you have made. The X6004 reloads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the X6004,

- 1 Make sure the **PWR** LED is on and not blinking.
- 2 Press and hold the **RESET** button for five to ten seconds. Release the **RESET** button when the **PWR** LED begins to blink. The default settings have been restored.

If the X6004 restarts automatically, wait for the X6004 to finish restarting, and log in to the web configurator. The password is “1234”.

If the X6004 does not restart automatically, disconnect and reconnect the X6004’s power. Then, follow the directions above again.

39.6 The Console Port

In some special circumstances, such as when you forget your admin password or the X6004's LAN IP address, you may need to log in directly to the command line and make changes to the configuration there. The following sections show you how to do this.

Note: For details on the X6004 command line features, see the Command Line Reference Guide included on your installation disc.

39.6.1 Use the Console Port to Access the CLI

- 1 Connect your computer to the console port on the X6004 using the appropriate cable.
- 2 Use terminal emulation software with the following settings:

Table 207 Default Settings for the Console Port

SETTING	DEFAULT VALUE
Terminal Emulation	VT100
Baud Rate	115200 bps
Parity	None
Number of Data Bits	8
Number of Stop Bits	1
Flow Control	None

- 3 Press [ENTER] to open the login screen.

39.6.2 The Login Screen

After you have successfully established a connection to the X6004 using a direct console connection or SSH, a login screen displays as shown below. For your first login, enter the default administrator login username "admin" and password "1234".

```
localhost login: admin
Password:
```

39.6.3 The Initrd Screens

Initrd is a shell that contains special commands not available in the regular command line interface. It allows you to reset the X6004 to the default WAN/LAN settings, check the file system integrity, and reset the admin password.

To access the initrd screens:

- 1 Connect your managing computer directly to the X6004's console port using the terminal settings described in [Section 39.6.1 on page 516](#).
- 2 Reboot or startup the X6004. You cannot access the debugging menu from the regular command line interface; you can only access it during the boot sequence.
- 3 During the initialization phase of the boot sequence, wait until the message "Press Enter to run initrd !!!!!" appears, then press [ENTER].

Figure 305 The X6004 Boot Sequence

```

Tera Term Web 3.1 - COM1 VT
File Edit Setup Web Control Window Help
PCI Autoconfig: BAR 2, Mem. size=0x1000, address=0x4bfff000
PCI Autoconfig: BAR 3, Mem. size=0x20000, address=0x4bfc0000
PCI: bus0: Fast back to back transfers disabled
irq = -1, slot = 0, pin = 1
irq = 22, slot = 6, pin = 1
%6)Linux NET4.0 for Linux 2.4
Based upon Swansea University Computer Society NET3.039
Initializing RT netlink socket
ISP Revision 92
Starting ksvapd
Disabling the Out Of Memory Killer
Journalled Block Device driver loaded
pty: 256 Unix98 pty's configured
Serial driver version 5.05c (2001-07-08) with MANY_PORTS SHARE_IRQ SERIAL_PCI enabled
ttyS00 at 0x1f000000 (irq = 15) is a XSCALE UART
ttyS01 at 0x1f001000 (irq = 13) is a XSCALE UART
RAMDISK driver initialized: 16 RAM disks of 36864K size 1024 blocksize
loop: loaded (max 8 devices)
PPP generic driver version 2.4.2
PPP Deflate Compression module registered
PPP BSD Compression module registered
SCSI subsystem driver
NET4: Linux TCP/IP
IP Protocols: ICMP
IP: routing cache
TCP: Hash tables
IP-Config: No settings
ip_contrack version
ip_tables: (C) 2001
NET4: Unix domain
802.1Q VLAN Support
All bugs added by
NetVinder Floating Point Emulator v0.9b (C) 1998-1999 Redhat.com
RAMDISK: Compressed image found at block 0
Freeing initrd memory: 3545K
WFS: Mounted root (ext2 filesystem).
Freeing init memory: 236K
tfts: TrueFFS driver 632.68
tfts: Socket 0: type 13 0x9877 chips 2 floors 2 size 256M in addr 0x50000000 ebs 0x40000
tfts: Device 0x0: size 0x78000000 HV sector 0x200 (recommended 0x1000)
tfts: Device 0x1: size 0x64c00000 HV sector 0x200 (recommended 0x1000)
tfts: Registered module at major 100
Partition check:
  tftfsa: unknown partition table
  tftfsb: unknown partition table
ixp425_eth: Initializing IXP425 NPE Ethernet driver software v. 1.2
ixp425_eth: CPU clock speed (approx) = 627 MHz
DB: NFE failed to respond within 100ms
DB: (FeatureScan) warning, could not send message to the NFE
ixp425_eth: ethu is using NPEB and the PHY at address 20
ixp425_eth: Use default MAC address 00:02:b3:01:01:01 for port 0
88e6063 setting vlan
<6>EXT3-fs: recovery complete.
Press Enter to run initrd !!!!!

```

- 4 The initrd main menu appears.

39.6.3.1 The Initrd Menus

The `initrd` menus emulate a simple text-based user interface.

Figure 306 The Main Menu

```

+-----Main Menu-----+
| IP Address              |
| Check File System      |
| Admin Default          |
| Command Mode           |
|                         |
| Reboot                 |
+-----+

```

You should be familiar with the following operations before you try to use the `initrd` menus to modify the X6004's configuration.

Table 208 Navigation

OPERATION	KEYSTROKE	DESCRIPTION
Select a menu item	[UP/DOWN]	To select a menu item, use either the UP or DOWN arrow keys on your keyboard. To enter the selected menu item's corresponding submenu, press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Enter information	[ENTER]	After selecting a menu item that requires information input, press [Enter]. A dialogue line appears, allowing you to type the information into it. Press [ENTER] again to save your changes or press [ESC] to return to the menu.

The following table describes the labels in the `initrd` main menu screen.

Table 209 Initrd

LABEL	DESCRIPTION
IP Address	Select this to open the IP Address sub-menu. See Section 39.6.3.2 on page 520 for details.
Check File System	Select this to run the check file system command. This ensures the integrity of the data blocks stored in the X6004's internal memory. If a problem is discovered, it automatically attempts to correct it.
Admin Default	Select this to restore the admin to password to its default, "1234".

Table 209 Initrd

LABEL	DESCRIPTION
Command Mode	Select this to enter the command line interface, where you can configure the <code>initrd</code> options. Type <code>help</code> to view a list of all available commands. Type <code>exit</code> to return to the main menu.
Reboot	Select this to restart the X6004. This is the only way to exit the <code>initrd</code> screens and return to the normal command line. Note: Once you select this option, the device immediately shuts down and restarts without confirmation.

39.6.3.2 The IP Address Screen

This screen allows you to configure the X6004's WAN and LAN IP settings.

Figure 307 The IP Address Screen

```

+-----IP Address-----+
| Wan_ip_realtime Host Netmask |
| Wan_gw_realtime Host         |
| Lan_ip_realtime Host Netmask |
| WAN default                  |
| LAN default                  |
|                               |
| Main Menu                    |
+-----+

```

The following table describes the labels in this screen.

Table 210 Initrd

LABEL	DESCRIPTION
Wan_ip_realtime Host Netmask	Select this option and press [Enter]. When the command line dialogue appears, type in the required information and then press [Enter] again.
Wan_gw_realtime Host	Select this option and press [Enter]. When the command line dialogue appears, type in the required information and then press [Enter] again.
Lan_ip_realtime Host Netmask	Select this option and press [Enter]. When the command line dialogue appears, type in the required information and then press [Enter] again.
WAN default	Select this to reset the X6004's WAN IP address to its factory default of "172.16.1.1".
LAN default	Select this to reset the X6004's LAN IP address to its factory default of "192.168.1.12".
Main Menu	Select this to return to the <code>initrd</code> main screen.

Product Specifications

The following tables summarize the X6004's hardware and firmware features.

Table 211 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	Standard 19" rack mountable 438 mm (W) x 309 mm (D) x 66 mm (H)
Weight	5.6 Kg
Power Specification	One Backup Power Supply (BPS) connector: 120W 12 V DC AC: 100 - 240 VAC 50/60Hz 1.5A max internal universal power supply
Interfaces	LAN: 10/100 Base-Tx ports WAN: 10/100 Base-Tx ports Auto-negotiation Auto-MDIX One console port
Expansion Slots	4 expansion slots with support for the following interface cards: <ul style="list-style-type: none"> • 4-port FXO interface card • 4-port FXS interface card • Combination 2-port FXS 2-port FXO interface card with lifeline support (calls can be made to the PSTN in case of a power failure on the X6004) • 1-port ISDN PRI interface card (T1/E1 configurable) • 4-port ISDN BRI/ST interface card (NT/TE configurable)
Hard Drive Support	One hard drive slot for an 80 GB hard drive installation
DSP Module Support	The system comes with a built-in 32 channel DSP channel and has 2 slots for additional DSP modules. Contact your vendor for DSP modules suitable for the X6004.

Table 211 Hardware Specifications

LEDs	BPS, PWR, SYS, ALM, HDD Per LAN/WAN port: 10, 100 Per FXO or FXS interface card: Sys, Port 1-4 Per FXO/FXS interface card: Sys, Port S1-S2, Port O1-O2 Per ISDN BRI interface card: Sys, Port 1-4 Per ISDN PRI interface card: LOS, RAI, AIS, and L2
Operating Environment	Temperature: 0° C ~ 40° C (32° F ~ 104° F) Humidity: 10 ~ 90% (non-condensing)
Storage Environment	Temperature: -30° C ~ 60° C (13° F ~ 158° F) Humidity: 20 ~ 90% (non-condensing)
Power Wire Gauge	18AWGX3C
Fuse Specification	250 VAC, T4A

Table 212 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	LAN: 192.168.1.12 WAN: 172.16.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234
Administrator Accounts	Max. number of Administrator Account: 5
Device Management	Use the web configurator or commands to easily configure the rich range of features on the X6004.
Remote Management Sessions	Max. concurrent HTTPS sessions: 3 (with different administrator ranks) Max. concurrent SSH sessions: No limited Max. concurrent FTP sessions: No limited
SIP Server	The X6004 performs SIP proxy, registrar and redirect server functions.
Auto Provisioning	The X6004 can send auto configuration files to ZyXEL IP phones (for example, V100, V300 and V500).
QoS	The X6004 can mark outgoing VoIP frames with DiffServ code point values, ToS priority values or user specified values for the ToS field in the IP header.

Table 212 Firmware Specifications

FEATURE	DESCRIPTION
Voicemail	The X6004 can store voicemail messages on the flash memory, hard drive (if installed) or it can forward voicemail messages to individual end user email accounts. Default maximum voicemail length per message: 90 seconds Default maximum total voicemail length per user: 300 seconds
Static Route	Static routes tell the X6004 how to forward VoIP traffic to remote networks.
Extension Management	Manage extensions by placing them in authority groups. You can then assign calling privileges to the authority groups. The X6004 supports SIP client devices as well as traditional analog phones if an FXS interface card has been installed.
Auto-attendant	The X6004 supports up to 3 sets of auto-attendant profiles to handle incoming calls. Auto-attendant helps guide incoming calls to their destination. Audio Format for Auto-Attendant: G.711 format audio file (*.wav), μ -law 8-bit mono mode. Maximum size of a single message: 1 MB. Maximum size of all messages 10 Mb.
Outbound Line Groups	The X6004 supports outbound lines via SIP/Skype connections to an ITSP, trusted peer connections. PSTN/ISDN connections are also supported, if an FXO/BRI/PRI interface card is installed.
LCR	Least Cost Routing allows administrators to set up dialing rules and configure priorities for outbound lines used when users make phone calls.
Hunt Group	Configure a group of user extensions which can be reached by dialing a single phone number. This can be used for a call center application.
Page Group	Configure sets of extensions that can all be called at the same time by dialing a single number (page group number). When a page group number is dialed, all of the extensions automatically pick up via speakerphone.
Emergency Call	Configure emergency telephone numbers which are given the highest priority for outbound lines on the X6004.
Conference Calling	Configure conference rooms which can be accessed by callers from within your organization as well as from outside your organization.
Music on Hold	Specify an audio file to play for callers who are placed on hold. G.711 format audio file (*.wav), μ -law
Distinctive Ring	Specify different rings for calls based on the source of the call.
Auto Callback	The X6004 can automatically call back a busy extension once it frees up.
Call Parking	The X6004 allows you to put a call on hold and pick up the call again from another location within your organization.

Table 212 Firmware Specifications

FEATURE	DESCRIPTION
Call Recording	The X6004 can record up to four channels at the same time. The maximum length for a single recorded call is 24 hours.
ZyStack	Configure up to 5 X6004 to work together under a single management IP address.
Call Detail Record	The X6004 can generate call detail records and send them to a MySQL database and the aged file (compressed file containing CDRs) can be sent to the administrator via email. Max. number of call records: 20000
Syslog	The X6004 can generate syslog messages and send it to a syslog server.
IVR	Interactive Voice Response system allows users to edit some of their personal (unique to their extension) settings via their handsets. For example, users can change their voicemail and forwarding settings using IVR.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator or an FTP tool to put it on the X6004. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the X6004's configuration and put it back on the X6004 later if you decide you want to revert back to an earlier configuration.
Subscribing Services	The default number of SIP extensions: 32 iCard for additional number of SIP extension support: 32 The max. number of SIP extensions: 128 The default number of softphone extensions: 8 iCard for additional number of softphone extension support: 8 The max. number of softphone extensions: 128
Softphone Support	ZyXEL V100

The following list, which is not exhaustive, illustrates the standards supported in the X6004.

Table 213 Standards Supported

STANDARD	DESCRIPTION
RFC 791	IP
RFC 793	TCP
RFC 826	Address Resolution Protocol (ARP)
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 894	Ethernet II Encapsulation
RFC 1305	Network Time Protocol (NTP version 3)

Table 213 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 1889	RTP
RFC 1890	RTCP
RFC 2131, RFC 2132	Dynamic Host Configuration Protocol (DHCP)
RFC 2136	DDNS
RFC 2327	Session Description Protocol (SDP)
RFC 2833	DTMF
RFC 3164	Syslog
RFC 3261	SIP
RFC 3842	Message Waiting Indicator
Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

ISDN PRI Cable (E1/T1) Pin Assignments

Use RJ-48 cables to connect the **ISDN PRI** ports to the PBX (Private Branch Exchange). The following diagram and chart show the pin assignments of the ISDN PRI cable.

Figure 308 ISDN PRI Cable Pin Assignments

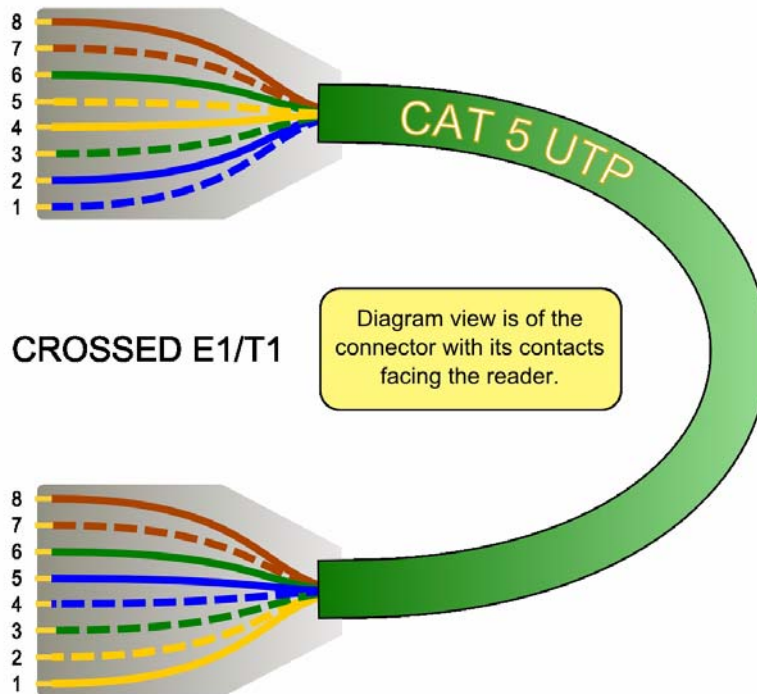


Table 214 ISDN PRI Cable Pin Assignments

RJ-48 PIN	RJ-48 PIN	SIGNAL
1	4	RX/Ring/- <-->TX/Ring/-
2	5	RX/Tip/+ <-->TX/Tip/+
4	1	TX/Ring/- <-->RX/Ring/-
5	2	TX/Tip/+ <-->RX/Tip/+
3	3	Shield/Return/Ground
6	6	Shield/Return/Ground
7	7	No connect
8	8	No connect

ISDN BRI Cable Pin Assignments

Use RJ-45 cables to connect the **ISDN BRI** ports to ISDN phones or PBXs. The following diagram and chart show the pin assignments of the ISDN BRI cable.

Figure 309 ISDN BRI Cable Pin Assignments

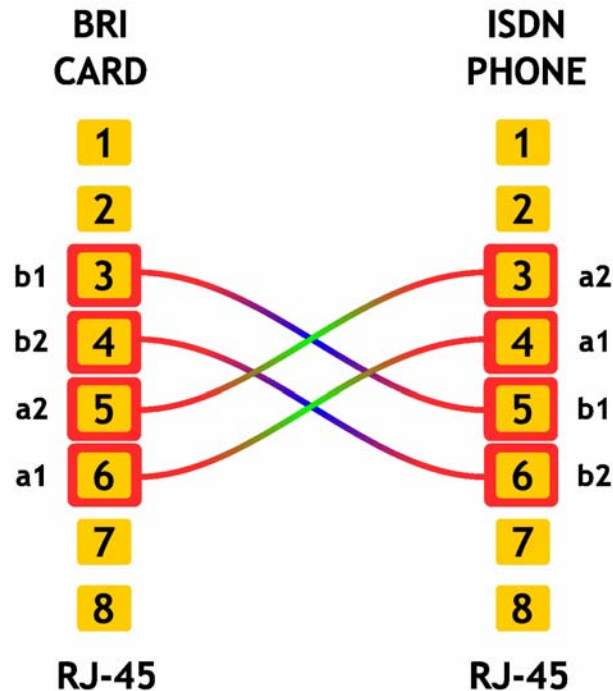


Table 215 ISDN BRI Cable Pin Assignments

RJ-45 PIN	RJ-45 PIN	SIGNAL
1	8	No connect
2	7	No connect
3	6	Transmit Data + <--> Transmit Data -
4	5	Receive Data + <--> Receive Data -
5	4	Receive Data - <--> Receive Data +
6	3	Transmit Data - <--> Transmit Data +
7	2	No connect
8	1	No connect

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

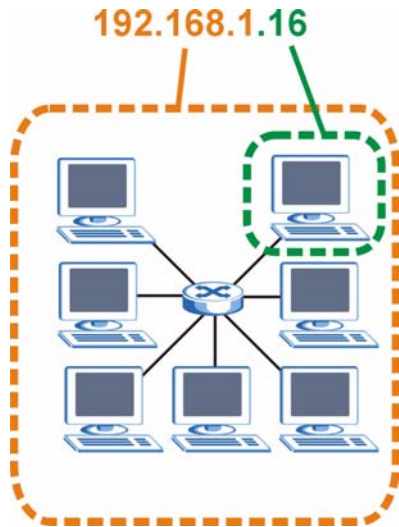
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 310 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 216 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	11111111	11111111	11111111	00000000
Network Number	11000000	10101000	00000001	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 217 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 218 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 219 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

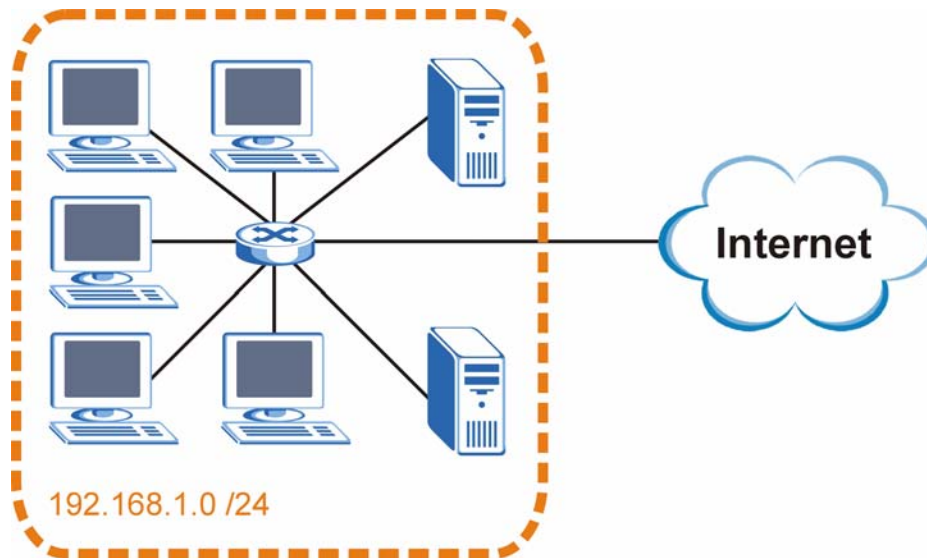
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 311 Subnetting Example: Before Subnetting

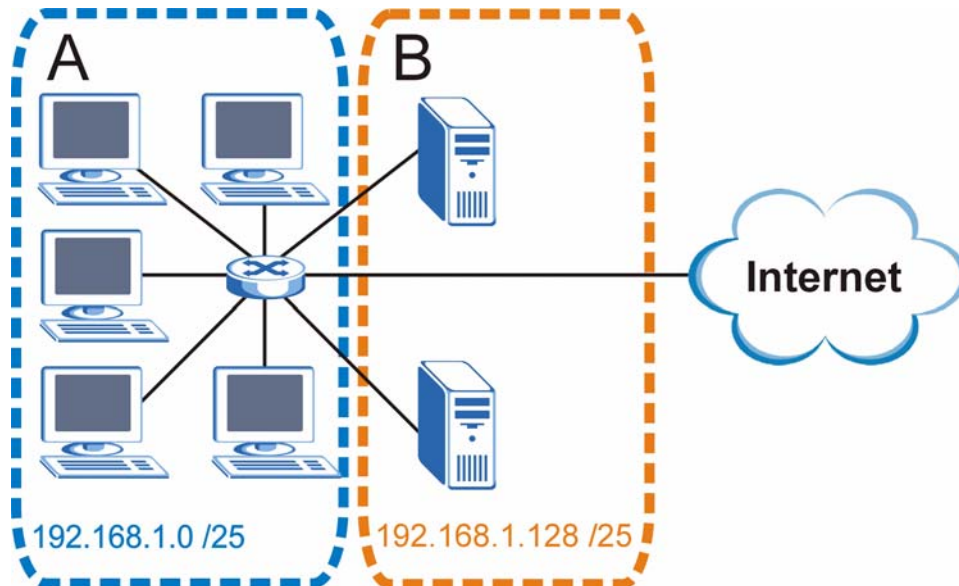


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 312 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 220 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 221 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 222 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 223 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001. .	11000000
Subnet Mask (Binary)	11111111.11111111.11111111 .	11000000

Table 223 Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 224 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 225 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 226 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the X6004.

Once you have decided on the network number, pick an IP address for your X6004 that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your X6004 will compute the subnet mask automatically based on the IP address that

you entered. You don't need to change the subnet mask computed by the X6004 unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

IP Address Conflicts

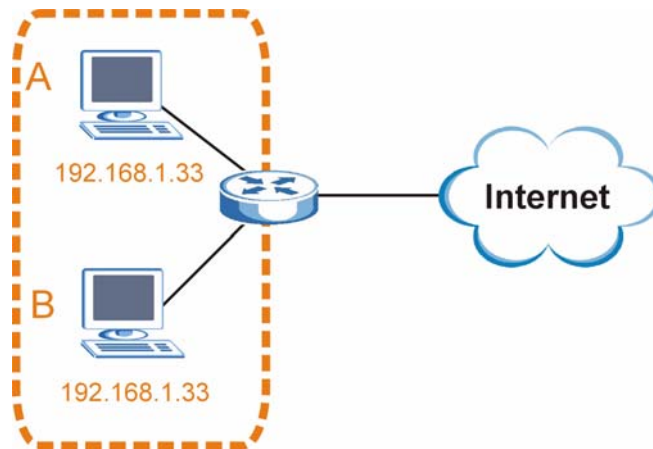
Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device cannot use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP

address to computer **A** or setting computer **A** to obtain an IP address automatically.

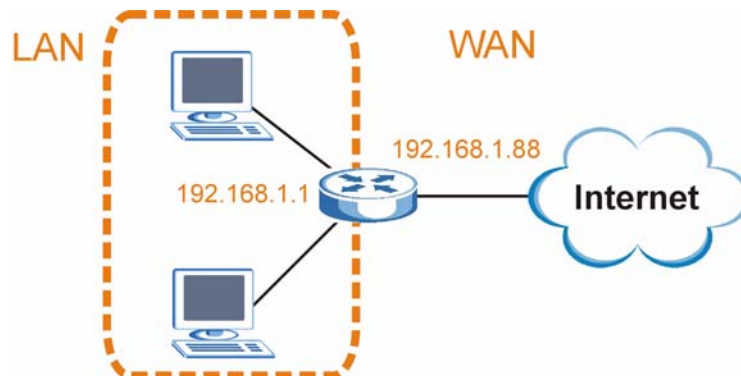
Figure 313 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

Figure 314 Conflicting Computer IP Addresses Example

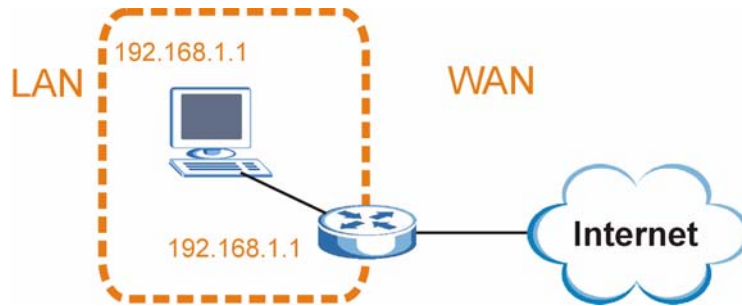


Conflicting Computer and Router IP Addresses Example

More than one device cannot use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address.

The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 315 Conflicting Computer and Router IP Addresses Example



Open Software Announcements

End-User License Agreement for “X6004”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER CERTAIN COMPONENTS OF THE SOFTWARE, AND THIRD PARTY OPEN SOURCE PROGRAMS INCLUDED WITH THE SOFTWARE, HAVE BEEN OR MAY BE MADE AVAILABLE BY ZyXEL LISTED IN THE BELOW NOTICE (COLLECTIVELY THE “OPEN-SOURCED COMPONENTS”). FOR THESE OPEN-SOURCED COMPONENTS YOU SHOULD COMPLY WITH THE TERMS OF THIS LICENSE AND ANY APPLICABLE LICENSING TERMS GOVERNING USE OF THE OPEN-SOURCED COMPONENTS, WHICH HAVE BEEN PROVIDED ON THE LICENSE NOTICE AS BELOW FOR THE SOFTWARE.

1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3. Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Notice (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the License Notice as below for the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the Software, and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6. No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7. Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8. Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9. Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10. Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11. General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate source code covered under the open source code licenses. Further, for at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes dhcp software under the ISC License

ISC license

Copyright (c) 4-digit year, Company or Person's Name

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

This Product includes busybox, msmtplib, proftpd, syslog-ng, iptables, Linux kernel, asterisk, monit, hc-cron, ez-ipupdate, and mysql software under GPL license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we

have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program

itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same

place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN

IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes tcpdump, outCall, net-snmp, openssh, and libupnp software under BSD license

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes activa software under the MPL License

Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use"

means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor"

means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version"

means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code"

means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism"

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable"

means Covered Code in any form other than Source Code.

1.6. "Initial Developer"

means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work"

means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License"

means this document.

1.8.1. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications"

means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

a. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

b. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code"

means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims"

means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code"

means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your")

means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

a. under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

b. under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

c. the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

d. Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

a. under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

b. under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

c. the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

d. Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party

modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor

under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously

included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also

choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

a. such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/ or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree

in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

b.any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48

C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License

Version 1.1 (the "License"); you may not use this file except in

compliance with the License. You may obtain a copy of the License at

<http://www.mozilla.org/MPL/>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____
_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[_____] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [_____] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [_____] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit

A rather than the text found in the Original Code Source Code for Your Modifications.

This Product includes php software under PHP license.

The PHP License, version 3.01

Copyright (c) 1999 - 2010 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a

distinguishing version number.

Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP software, freely available from
<<http://www.php.net/software/>>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see [<http://www.php.net>](http://www.php.net).

PHP includes the Zend Engine, freely available at [<http://www.zend.com>](http://www.zend.com).

Legal Information

Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

Symbols

μ-law [206](#), [227](#)

A

AA [259](#), [269](#), [274](#)

AbS [228](#)

account ranking [433](#)

account types [431](#)

adapter, telephone
see ATA

Adaptive Differential Pulse Code Modulation
see ADPCM

address book [179](#)

administrator account [431](#)

add [434](#)

change password [432](#)

edit [435](#)

list [433](#)

rank [433](#)

ADPCM [227](#), [228](#)

after hours [211](#)

aged file [413](#)

aggregating multiple devices [355](#)

AIS [33](#)

a-law [206](#)

alias [112](#)

AMR-WB [206](#), [227](#)

analog

audio [187](#), [227](#)

extension settings [133](#)

FXO line settings [132](#)

telephones [35](#), [386](#)

status [388](#)

Analog Telephone Adapter
see ATA

Analysis-by-Synthesis

see AbS

anti-probing [455](#)

applications, critical [169](#)

associating groups [326](#)

assured forwarding [170](#)

ATA [28](#), [158](#), [220](#)

audio

channels [187](#)

files [327](#), [329](#)

for auto-attendant [299](#)

recording [305](#)

on hold [333](#)

sampling [227](#)

audio files

format [299](#)

authority groups [35](#)

add [202](#)

and call access code [253](#)

and call routing [37](#)

and extensions [35](#)

BRI peer [203](#)

configuration [203](#)

creation guidelines [199](#)

creation tutorial [43](#)

descriptions [200](#)

edit [202](#)

extensions [199](#)

features

call blocking [204](#)

call forwarding [204](#)

voice mail

forwarding [204](#)

FXS [203](#)

group names [200](#)

grouping [199](#)

LCRs [55](#), [64](#), [71](#), [318](#)

limitations [199](#)

management [318](#)

overview [197](#)

query [201](#)

ring groups [319](#)

SIP peer [203](#)

Auto Attendant

- see AA
- auto callback [327, 338](#)
- auto configuration [48](#)
- auto provisioning [48, 219](#)
 - client configuration [49](#)
 - MAC address [49](#)
 - overview [153](#)
 - serial number [49](#)
 - settings [157, 161](#)
 - SIP extensions [219](#)
- auto-attendant [36, 52, 60, 69, 193, 291](#)
 - adding, deleting [296](#)
 - advanced example [292](#)
 - and fax [36, 291](#)
 - audio
 - files [299](#)
 - BRI trunk [276](#)
 - call routing [291](#)
 - diagram [292](#)
 - FXO trunks [265](#)
 - management [295](#)
 - menus [293, 297](#)
 - night service [301](#)
 - PRI trunk [270](#)
 - recording instructions [305](#)
 - SIP trunks [282](#)
 - structure [292](#)
 - trusted peer [289](#)
- automatic pickup [229](#)
- automatic switchboard operator [291](#)

B

- backup configuration [471](#)
- bandwidth [169](#)
- Basic Rate Interface
 - see BRI
- basic setup tutorial [41](#)
- batch file format [156](#)
- black list [141, 212, 215, 487, 492](#)
- blind forward [211](#)
- blocking calls [141, 204, 209, 487](#)
- BRI [127, 150](#)
 - connections [385](#)
 - extensions [225](#)
 - adding [223](#)

- status [389](#)
- interface [386](#)
- PBX [258](#)
- peer status [389](#)
- settings [134](#)
- switch types [128](#)
- trunk [258](#)
 - adding and editing [271](#)
 - auto-attendant [276](#)
 - settings [272](#)
- busy detect [132](#)
- busy forward [211](#)

C

- call access code [253](#)
 - adding and editing [255](#)
 - configuration [255](#)
- call black list settings [140](#)
- call blocking [204, 209, 212](#)
 - settings [139](#)
- Call Detail Record
 - see CDR
- call features [76, 327](#)
- call forwarding [141, 204, 209, 215, 487](#)
- call handling [193](#)
- call length, maximum [173](#)
- call parking [327, 339](#)
 - configuration [340](#)
 - overview [339, 341](#)
- call recording [327, 345](#)
- call records query [418](#)
- call restrictions [199](#)
- call routing
 - ZyStack [356](#)
- call routing terms [35](#)
- call services [327](#)
 - auto callback [338](#)
 - call parking [339](#)
 - call transfer [345](#)
 - call waiting [341](#)
 - conference calls [331](#)
 - distinctive ring [337](#)
 - emergency call [329](#)
 - MOH [333](#)

- call transfer [141](#), [327](#), [345](#)
 - configuration [345](#)
 - call waiting [327](#), [341](#)
 - configuration [343](#)
 - example [344](#)
 - callback, auto [327](#), [338](#)
 - caller ID [212](#)
 - calling emergency numbers [329](#)
 - calls
 - between extensions [37](#)
 - conference [331](#)
 - emergency [328](#)
 - to ITSP [36](#)
 - to PSTN [36](#)
 - calls, emergency [327](#), [328](#)
 - Canonical Format Indicator
 - see CFI
 - CAS [258](#), [267](#)
 - CDR [413](#), [423](#)
 - aged file [414](#)
 - backup results [417](#)
 - executing SQL script [414](#), [423](#)
 - external server [414](#), [423](#)
 - local database [413](#)
 - management [414](#)
 - MySQL [414](#)
 - overview [413](#), [423](#)
 - query [418](#)
 - remote server configuring procedure [416](#), [425](#)
 - report [420](#), [428](#)
 - types of files [414](#)
 - central office [386](#)
 - certifications [565](#)
 - notices [566](#)
 - viewing [566](#)
 - CFI [123](#)
 - Channel Associated Signaling, see CAS
 - channel detection [188](#)
 - channels [187](#), [190](#)
 - CIDR [361](#)
 - circuit-switched [150](#)
 - Class of Service
 - see CoS
 - class selector [171](#)
 - Classless Inter-Domain Routing
 - see CIDR
 - codecs [217](#), [218](#), [227](#)
 - and trusted peers [288](#)
 - G.723.1 [131](#)
 - SIP trunk [281](#)
 - coder/decoders [206](#), [227](#)
 - commands
 - logging in [516](#)
 - compression
 - audio [227](#)
 - variable compression ratio [227](#)
 - video [228](#)
 - conference calls [327](#), [331](#)
 - add [332](#)
 - and DSP usage [331](#)
 - edit [332](#)
 - maximum number of members [333](#)
 - overview [331](#)
 - conference room [331](#), [333](#)
 - conference, meet-me [327](#)
 - configuration
 - backup [471](#)
 - backup and restore notes [469](#)
 - configuration file [469](#)
 - saving [108](#)
 - text file [48](#)
 - congestion [170](#)
 - connecting IP telephones [46](#)
 - connecting to ITSP [57](#)
 - connecting to PSTN [50](#)
 - Console Cable Pin Assignments [526](#), [527](#)
 - console port (accessing the CLI) [516](#)
 - copyright [565](#)
 - CoS [123](#), [170](#)
 - cost, minimizing [170](#)
 - country code [133](#)
 - critical applications [169](#)
- ## D
- Database Management System
 - see DBMS
 - date and time [119](#)
 - daylight saving [119](#)
 - daytime call handling [193](#)

- DBMS [414](#)
 - DDI [269, 274](#)
 - DDNS [112, 113, 117](#)
 - debug admin [431, 437](#)
 - decoders [206, 217, 218](#)
 - default gateway [113, 116](#)
 - default IP addresses [522](#)
 - delay [169, 170](#)
 - Delta PCM [228](#)
 - de-militarized zone [111](#)
 - deployment
 - and auto provisioning [48](#)
 - diagnostics [437](#)
 - information collection [437](#)
 - network traffic information [438](#)
 - packet capturing [440](#)
 - privilege used [437](#)
 - status check [438](#)
 - dial condition [36](#)
 - examples [54, 62, 70](#)
 - dialing rules [61](#)
 - DID [269, 274](#)
 - Differential PCM [228](#)
 - DiffServ [169, 170](#)
 - DiffServ Code Point
 - see DSCP
 - digit handling [135, 139](#)
 - digital audio [187](#)
 - digital sampling [227](#)
 - Digital Signal Processing
 - see DSP
 - digital telephones [386](#)
 - dimensions [521](#)
 - direct pickup [141](#)
 - disclaimer [565](#)
 - distinctive ring [327, 337](#)
 - setup [337](#)
 - DMZ [111](#)
 - DND [141, 204, 211, 488](#)
 - white list [491](#)
 - DNS [112, 116, 117](#)
 - domain name [112, 117](#)
 - Domain Name System
 - see DNS
 - drop precedence [170](#)
 - DSCP [169, 170](#)
 - DSP [30, 187](#)
 - and conference calls [331](#)
 - channel assignation [188](#)
 - channel detection [188](#)
 - channel sharing [188](#)
 - channels [190](#)
 - management [190](#)
 - module [188](#)
 - hatch [188](#)
 - installation [188](#)
 - removal [189](#)
 - modules supported [521](#)
 - resources [331](#)
 - DTMF [206, 217, 218, 278, 286](#)
 - Dynamic DNS
 - see DNS
 - dynamic IP address [112, 113](#)
- ## E
- E1 [127](#)
 - E911 [328](#)
 - echo [169](#)
 - email, attaching voice file [493](#)
 - emergency calls [327, 328](#)
 - configuration [329](#)
 - overview [328](#)
 - en-bloc [135, 139](#)
 - Enhanced 911
 - see E911
 - expansion slots supported [521](#)
 - expedited forwarding [171](#)
 - export phonebook [181](#)
 - extensions [27, 35, 37, 43](#)
 - and pickup groups [239](#)
 - busy [327](#)
 - call transfer [327](#)
 - for analog phones [35](#)
 - FXS [35](#)
 - grouping [199](#)
 - ISDN BRI [35](#)
 - query number [200](#)
 - ring groups [229](#)
 - SIP [35](#)
 - user login [483](#)

- voice mail [216](#)
- VoIP [386](#)
- web portal [483](#)

external lines

- see outbound line groups

external time server [112](#)

F

fax [36, 291](#)

FCC interference statement [565](#)

feature codes [76](#)

- example [76](#)
- settings [141](#)
- tutorial [77](#)
- voice mail [77](#)

file transfer using FTP

- command example [474](#)

find me list [214, 487](#)

- web portal [491](#)

firewall [113](#)

firmware

- file [469](#)
- file types for upgrade [470](#)
- filename convention for FTP upload [474](#)
- FTP upgrading example [474](#)
- specifications [522](#)
- upgrading [473](#)
- viewing current firmware version [473](#)
- where to download [470](#)

follow me [141](#)

Foreign Exchange Office

- see FXO

Foreign Exchange Subscriber

- see FXS

forwarding calls [209](#)

FTP

- firmware upgrade example [474](#)
- GUI-based clients [476](#)

full admin [431](#)

functional overview [35](#)

FXO [126](#)

- and FXS relationship [36](#)
- connections [385](#)
- interface cards [36, 50](#)

- interfaces [386](#)
- ports [36, 50](#)
- settings [132](#)
- trunk [36, 51, 68, 258](#)
 - adding and editing [263, 266](#)
 - status [391, 393, 394](#)

FXO trunk

- auto-attendant [265](#)

FXS [126](#)

- and FXO relationship [36](#)
- extensions [35, 385](#)
 - adding [220](#)
 - configuration [221](#)
 - group pickup [223](#)
 - status [388](#)
- interface cards [35](#)
- interfaces [386](#)
- peer status [388](#)
- ports [35](#)

FXS settings [133](#)

G

G.279 [228](#)

G.711 [206, 227](#)

G.722 [206, 227](#)

G.722.2 [227](#)

G.723.1 [131, 227](#)

G.726 [206, 228](#)

G.729 [206](#)

G.729A [206](#)

gateway [113](#)

getting help [110](#)

group management [317](#)

- associate to authority and outbound line groups [322](#)
- granting calling rights [318](#)

group pickup [141, 217, 219, 239](#)

- adding and editing [242](#)
- example [240](#)

groups, ring [229](#)

H

- H.261 [206, 228](#)
 - H.263 [206, 228](#)
 - H.264 [228](#)
 - MP4 [206](#)
 - hard drive [30, 521](#)
 - hardware information [379](#)
 - help, web configurator [110](#)
 - hold [327, 329](#)
 - hop [170](#)
 - hostname [112](#)
 - hours [193](#)
 - HTML-based phone [483, 494, 495](#)
 - HTTP [154](#)
 - HTTPS [448, 470](#)
 - example [459](#)
 - humidity [522](#)
 - hunt group [229](#)
 - add [237](#)
 - creating [235](#)
 - edit [237](#)
 - fewest calls [238](#)
 - least recent [238](#)
 - night service [238](#)
 - office hours [238](#)
 - random [238](#)
 - ring algorithm [238](#)
 - ring all [238](#)
 - round robin [238](#)
 - hunt groups [321](#)
 - Hyper Text Transfer Protocol over Secure Socket Layer
 - see [HTTPS](#)
- I**
- IANA [538](#)
 - iCard [478](#)
 - ICMP (Internet Control Message Protocol) [449](#)
 - idle timeout [445](#)
 - IEEE 802.1p [123](#)
 - IEEE 802.1Q [113, 123](#)
 - import phonebook [181, 182](#)
 - inactivity timeout [445](#)
 - inbound calls, and auto-attendant [291, 293](#)
 - incoming calls
 - distinctive ring [327](#)
 - handling [193](#)
 - second call [327](#)
 - transferring [327](#)
 - information [379](#)
 - Integrated Services Digital Network
 - see [ISDN](#)
 - Interactive Voice Response
 - see [IVR](#)
 - interconnected VoIP [328](#)
 - interface
 - for ZyStack [358](#)
 - interface status [386](#)
 - interfaces [521](#)
 - internal calls [37](#)
 - routing [43](#)
 - internal operator [141](#)
 - internal telephone network [29](#)
 - Internet Assigned Numbers Authority
 - See [IANA](#) [538](#)
 - Internet Service Provider
 - see [ISP](#)
 - Internet Telephony Service Provider
 - see [ITSP](#)
 - introduction [27](#)
 - IP address [112, 117](#)
 - defaults [522](#)
 - dynamic [113](#)
 - LAN [114](#)
 - IP network [29](#)
 - IP PBX [27](#)
 - IP PBX global setting
 - overview [125](#)
 - IP telephone
 - extensions [205](#)
 - IP telephones [28, 43, 113](#)
 - and auto provisioning [48](#)
 - deployment [46](#)
 - registration [47](#)
 - ISDN [127, 150](#)
 - B-channels [150](#)
 - BRI [127, 150](#)
 - switch types [135](#)

- BRI extensions [35](#)
 - calls tutorial [65](#)
 - connections [385](#)
 - D-channels [150](#)
 - E1 [127](#)
 - extensions [385](#)
 - MSNs [224](#)
 - network configuration, tutorial [73](#)
 - NT mode [127](#)
 - phone status [389](#)
 - PRI [127, 150](#)
 - T1 [127](#)
 - TE mode [127](#)
 - ISP [112, 116](#)
 - ITSP [27, 36, 258](#)
 - ITSP calls, tutorial [56](#)
 - IVR [221, 223, 225, 503](#)
 - accessing [175, 503](#)
 - authentication [504](#)
 - call forward and black list [505](#)
 - introduction of functions [503](#)
 - main flow [504](#)
 - overview of functions [176](#)
 - PIN menu [505](#)
 - voice mail [508](#)
- J**
- jitter buffer [169](#)
- L**
- L2 [33](#)
 - LAN [111, 112](#)
 - LAN IP address [114](#)
 - latency [169, 170](#)
 - LCR [36, 38, 309](#)
 - adding or deleting a dial condition [314](#)
 - advanced setup [38](#)
 - and authority group [64, 71](#)
 - and authority groups [55](#)
 - and dialing conditions [36](#)
 - and outbound line groups [36](#)
 - associations [310](#)
 - associations example [309](#)
 - authority groups [318](#)
 - basic setup [38](#)
 - components [310](#)
 - components example [309](#)
 - configuration [312](#)
 - dial conditions [310](#)
 - example [38, 61, 62](#)
 - list [311](#)
 - outbound line groups [258, 310, 321](#)
 - tutorial [53, 69](#)
 - LDAP [29, 179, 183](#)
 - Least Cost Routing
 - see LCR
 - LED [32, 33, 522](#)
 - legacy PBX [28](#)
 - license
 - key [480](#)
 - refresh [480](#)
 - status viewing [481](#)
 - license key [480](#)
 - Lightweight Directory Access Protocol
 - see LDAP
 - linking groups [326](#)
 - listening volume [132](#)
 - Local Area Network
 - see LAN
 - local calls [36](#)
 - local phonebook [179, 180, 184, 185](#)
 - log [401](#)
 - consolidation [410](#)
 - email server [409](#)
 - filtering results [404](#)
 - IPPBX [401](#)
 - merge [410](#)
 - myZyXEL.com [401](#)
 - remote syslog server [411](#)
 - schedule [410](#)
 - settings [405, 408](#)
 - settings overview [406](#)
 - severity levels [402](#)
 - summary [406](#)
 - user [401](#)
 - viewing [402](#)
 - logical network [113](#)
 - login [101](#)
 - to web portal [484](#)
 - loss of signal [32](#)

M

MAC address [219](#)
maintenance [469](#)
 configuration backup and restore [471](#)
making internal calls, tutorial [43](#)
Management Information Base (MIB) [382](#)
Management Information Base, see MIB
managing administrator accounts [433](#)
managing authority groups [317](#), [318](#)
managing auto-attendant [295](#)
managing outbound line groups [262](#), [317](#), [320](#)
managing subscription services [477](#)
managing the device [31](#)
 good habits [31](#)
 using the command interface [31](#)
marking [170](#)
master [356](#), [358](#)
maximizing reliability [170](#)
maximizing throughput [170](#)
meet-me conference [327](#)
Message Waiting Indicator
 see MWI
MIB [383](#)
minimizing cost [170](#)
minimizing delay [170](#)
module [187](#), [188](#)
MOH [327](#), [329](#)
 file format [333](#)
 overview [333](#)
monitoring
 extension status [388](#), [389](#)
 FXO links [391](#), [393](#), [394](#)
 SIP links [392](#)
Motion Picture Experts Group
 see MPEG
MPEG [228](#)
MSN [224](#), [274](#)
mu-law [206](#)
multiple SIP extensions, tutorial [45](#)
Multiple Subscriber Numbers
 see MSN
Music On Hold
 see MOH
MWI [217](#), [219](#)

MySQL [414](#), [416](#), [425](#)
myZyXEL.com [477](#)

N

NAT [113](#), [537](#)
navigation panel [104](#)
Network Address Translation
 see NAT
network congestion [169](#)
network deployment
 overview [111](#)
Network Terminal
 see NT mode
Network Time Protocol
 see NTP
network traffic information [438](#)
night service hunt group [238](#)
nighttime call handling [193](#)
no answer forward [211](#)
Nortel SIP server [279](#), [286](#)
NT mode [127](#)
NTP [112](#), [119](#)

O

office hours [193](#), [194](#), [210](#)
 after hours [211](#)
 hunt group [238](#)
operator, internal [141](#)
outbound call routing [38](#)
outbound line groups [36](#), [51](#), [58](#), [68](#), [257](#)
 and LCRs [258](#)
 BRI trunk [257](#)
 codecs [281](#)
 FXO trunk [257](#)
 LCRs [321](#)
 management [262](#), [320](#)
 PRI trunk [257](#)
 SIP trunk [257](#)
 trusted peer [257](#), [258](#)
 types of [257](#)
outgoing call restrictions [199](#)

outside connections, types of [257](#)
 outside lines
 see outbound line groups
 overlap [135, 139](#)

P

packet capturing [438, 440](#)
 packet capturing, tutorial [86](#)
 packet forwarding [170](#)
 packet loss [169](#)
 page groups [229, 321](#)
 adding [236](#)
 creating [235](#)
 editing [236](#)
 example [230](#)
 parking lot extension [339](#)
 parking, call [327](#)
 PBX [27](#)
 PCM [227, 228](#)
 peer IP PBX [28](#)
 per-hop behavior [170](#)
 personal IVR [141](#)
 PHB [170](#)
 phonebook [179, 180, 181, 184, 185, 494, 495](#)
 picking up parked calls [327](#)
 pickup group [239, 242](#)
 pickup, automatic [229](#)
 PIN code [221, 223, 225](#)
 pipeline [171](#)
 power specification [521](#)
 PPPoE [118](#)
 precedence [170](#)
 PRI [127, 150](#)
 connections [385](#)
 framing [138](#)
 interface [386](#)
 PBX [258](#)
 settings [136](#)
 trunk [258](#)
 auto-attendant [270](#)
 settings [267](#)
 Tx / Rx levels and cable length [138](#)
 Primary Rate Interface

 see PRI
 priority [123, 169](#)
 private WAN IP address [117](#)
 privilege level (in administrator account) [433](#)
 privileges [197](#)
 product registration [567](#)
 PSAP [328](#)
 PSTN [27, 36, 258](#)
 connections to [50, 385](#)
 PSTN calls, tutorial [50](#)
 Public Safety Answering Point
 see PSAP
 Public Switched Telephone Network
 see PSTN
 Pulse Code Modulation
 see PCM

Q

Q signaling
 see Q.SIG
 Q.SIG
 master [128](#)
 side A/B [128](#)
 slave [128](#)
 QoS [169, 171](#)
 Quality of Service
 see QoS
 quantization [227](#)

R

RAI LED [33](#)
 random ringing [229](#)
 ranking accounts [433](#)
 read-only admin [431](#)
 Real Time Transport Protocol
 see RTP
 realm [130](#)
 reboot [109](#)
 record of calls [418](#)
 recording audio

- files [305](#)
 - recording calls [327, 345](#)
 - registration [479](#)
 - adding additional SIP extensions [478](#)
 - adding additional softphones [478](#)
 - iCard [478](#)
 - IP telephones [47](#)
 - license key entering [480](#)
 - myZyXEL.com [477](#)
 - product [567](#)
 - reget license information [480](#)
 - service license refresh [480](#)
 - viewing license status [481](#)
 - X6004 [479](#)
 - related documentation [3](#)
 - reliability [170](#)
 - remote alarm indication [33](#)
 - remote management
 - access interface [448](#)
 - FTP white list [453](#)
 - HTTPS [448](#)
 - HTTPS example [459](#)
 - ICMP white list [455](#)
 - limitations [448](#)
 - overview [447](#)
 - requirements for using SSH [449](#)
 - secure FTP using SSH [465](#)
 - secure telnet using SSH [463](#)
 - SSH [449](#)
 - SSH implementation [449](#)
 - SSH white list [451](#)
 - SSH, how it works [462](#)
 - WWW white list [449](#)
 - ZyXEL V200 access white list [457](#)
 - report
 - CDR [420, 428](#)
 - representative number
 - SIP
 - trunk [278](#)
 - resetting [109](#)
 - resources [187](#)
 - restarting [109](#)
 - restoring configuration [109, 471](#)
 - restricting outgoing calls [199](#)
 - resuming parked calls [327](#)
 - RFC 1889 [129](#)
 - RFC 2833 [206, 218](#)
 - ring
 - random [229](#)
 - ring differentiation [337](#)
 - ring groups
 - authority groups [319](#)
 - configuration [233](#)
 - creating [233](#)
 - editing [234](#)
 - hunt group [321](#)
 - hunting [229](#)
 - overview [229](#)
 - page groups [321](#)
 - paging [229](#)
 - ring, distinctive [327](#)
 - route [120](#)
 - routing, by SIP To header [282, 289](#)
 - RTP [129, 169](#)
 - DTMF [206](#)
 - RTP and DTMF [218](#)
- ## S
- safety certifications [525](#)
 - safety warnings [7](#)
 - sampling [227](#)
 - saving the configuration [108](#)
 - second call [327](#)
 - secure FTP using SSH [465](#)
 - Secure SHell
 - see SSH
 - Secure Socket Layer
 - see SSL
 - secure Telnet using SSH [463](#)
 - serial number
 - softphone [49](#)
 - ZyStack [359](#)
 - Session Initiation Protocol
 - see SIP
 - signal loss [32](#)
 - signal processing
 - see DSP
 - Simple Network Management Protocol, see SNMP
 - simultaneous ringing [229](#)
 - SIP [28](#)

- authentication [44, 47](#)
 - connections [385](#)
 - DTMF [206, 218](#)
 - extensions [35, 43, 44, 385](#)
 - adding [207](#)
 - adding by batch [471](#)
 - configuration [208](#)
 - configuring [43](#)
 - registration [478](#)
 - status [386](#)
 - peer status [385](#)
 - peers [205](#)
 - phone configuration [47](#)
 - realm [130](#)
 - registration [47](#)
 - server [29, 117](#)
 - settings [130](#)
 - To header [282, 289](#)
 - trunk [58, 258, 386](#)
 - adding and editing [276](#)
 - auto-attendant [282](#)
 - caller ID [280](#)
 - channel limit [279](#)
 - codecs [281](#)
 - representative number [278](#)
 - settings [277](#)
 - status [392](#)
 - slave [356, 358](#)
 - SNMP [382, 383](#)
 - agents [382](#)
 - Get [383](#)
 - GetNext [383](#)
 - Manager [382](#)
 - managers [382](#)
 - MIB [382, 383](#)
 - network components [382](#)
 - Set [383](#)
 - Trap [383](#)
 - traps [383](#)
 - versions [382](#)
 - snom [159](#)
 - softphone
 - registration [478](#)
 - softphones [28](#)
 - sound [187](#)
 - quality [169, 171, 227](#)
 - SPTGEN file [154](#)
 - content [158, 162](#)
 - SQL (Structured Query Language) [414](#)
 - SSH
 - how SSH works [462](#)
 - implementation [449](#)
 - secure FTP example [465](#)
 - secure telnet example [463](#)
 - SSL [448](#)
 - stacking [355](#)
 - standards supported [524](#)
 - static IP address [112](#)
 - static route [113, 120, 121](#)
 - static VLAN [123](#)
 - status [103](#)
 - status observation [385](#)
 - status, current [438](#)
 - streaming video [228](#)
 - subnet [113, 114, 120, 529](#)
 - mask [530](#)
 - mask notation, alternative [532](#)
 - subnetting [532](#)
 - subscription
 - number of ZyXEL softphones [478](#)
 - subscription services [477](#)
 - SIP extensions [478](#)
 - switch reset [109](#)
 - synchronization [112](#)
 - syntax conventions [5](#)
 - system information [379](#)
 - system log [401, 411](#)
 - types of logs [401](#)
- ## T
- T1 [127](#)
 - Tag Control Information
 - see TCI
 - Tag Protocol Identifier
 - see TPID
 - TAPI [349, 498](#)
 - client [349, 498](#)
 - server [349](#)
 - TE mode [127](#)
 - TEI [135](#)
 - telco office [386](#)

- telephone adapter, analog
 - see ATA
 - telephone exchange device [27](#)
 - telephones
 - analog [386](#)
 - digital [386](#)
 - Telephony Application Programming Interface,
 - see TAPI
 - temperature [522](#)
 - Terminal Endpoint Identifier
 - see TEI
 - Terminal Equipment
 - see ISDN TE mode
 - terms explained [35](#)
 - text file [180](#)
 - TFTP [467](#)
 - throughput [170](#)
 - time and date [119](#)
 - time protocol [112, 119](#)
 - time zone [119](#)
 - time-based auto-attendant configuration [193](#)
 - time-critical applications [169](#)
 - To header, routing by [282, 289](#)
 - tones [206](#)
 - ToS [169, 170](#)
 - TPID [123](#)
 - trademarks [565](#)
 - traditional PBX [258](#)
 - traffic
 - forwarding [170](#)
 - marking [170](#)
 - routing [120](#)
 - type [123](#)
 - transferring call settings [345](#)
 - Trivial File Transfer Protocol, see TFTP
 - troubleshooting
 - diagnostics [437](#)
 - packet capturing [438](#)
 - system information collecting [438](#)
 - trunk [257](#)
 - trunks [257](#)
 - trusted peer [36, 258](#)
 - adding and editing [284](#)
 - and codecs [288](#)
 - auto-attendant [289](#)
 - caller ID [287](#)
 - representative number [287](#)
 - settings [285](#)
 - tutorials [41](#)
 - authority group [43](#)
 - auto provisioning [48](#)
 - configure SIP extensions [43](#)
 - dial conditions [54, 70](#)
 - feature codes [77](#)
 - internal calls [43](#)
 - IP telephones [46](#)
 - ISDN calls [65](#)
 - ISDN network configuration [73](#)
 - ITSP calls [56](#)
 - ITSP connection [57](#)
 - LCRs [53, 61, 69](#)
 - multiple SIP extensions [45](#)
 - overview [41](#)
 - packet capturing [86](#)
 - PSTN calls [50](#)
- ## U
- u-law [206](#)
 - upgrading firmware [473](#)
- ## V
- VID [123](#)
 - video codecs [206, 218, 227, 228](#)
 - Virtual Local Area Network
 - see VLAN
 - VLAN [113, 122](#)
 - ID [123](#)
 - number of possible VIDs [123](#)
 - priority frame [123](#)
 - static [123](#)
 - tag [123](#)
 - VLAN identifier
 - see VID
 - vocal synthesizer [228](#)
 - voice codecs [206, 217, 227](#)
 - voice coder/decoder [218](#)
 - voice mail [29, 141, 173, 174, 216, 221, 223, 225](#)
 - authentication [175](#)

- change folder [177](#)
 - email notifications [29](#)
 - feature code [77](#)
 - forwarding [173](#)
 - listening voice messages [177](#)
 - mail box options [178](#)
 - message stored capability [178](#)
 - settings [493](#)
 - voice mail forwarding [204](#)
 - Voice over Internet Protocol
 - see VoIP [28](#)
 - VoIP [28](#), [113](#)
 - account example [58](#)
 - and emergency calls [328](#)
 - extensions [386](#)
 - gateways [28](#)
 - interconnected [328](#)
 - trunks [385](#)
- ## W
- WAN [111](#), [112](#), [116](#)
 - and PPPoE [118](#)
 - IP address [117](#)
 - warranty [567](#)
 - note [567](#)
 - web configurator [31](#), [101](#)
 - getting help [110](#)
 - home [103](#)
 - inactivity timeout [445](#)
 - login [101](#)
 - logout [110](#)
 - navigation [103](#)
 - navigation panel [104](#)
 - web phone [483](#)
 - phonebook [494](#), [495](#)
 - web portal [221](#), [223](#), [225](#), [483](#)
 - account settings [485](#)
 - black list [492](#)
 - call forward and blocking [487](#)
 - find me list [491](#)
 - login [484](#)
 - restrictions [486](#)
 - voice mail [493](#)
 - web phone dial [494](#), [495](#)
 - white list [491](#)
 - weight [521](#)
 - white list [204](#), [487](#)
 - Do Not Disturb [491](#)
 - remote management
 - FTP [453](#)
 - ICMP [455](#)
 - SSH [451](#)
 - WWW [449](#)
 - ZyXEL V200 [457](#)
 - Wide Area Network
 - see WAN
 - wildcard [117](#)
- ## Z
- Z_Interface [358](#)
 - ZyStack [355](#)
 - advantages [355](#)
 - call routing [356](#)
 - fail reason [363](#)
 - fail-to-delete reason [363](#)
 - intranet setup [360](#)
 - master [356](#), [358](#)
 - role [358](#)
 - serial number [359](#)
 - settings [357](#)
 - slave [356](#), [358](#)
 - status [362](#)

