

VoiceFinder

AP2120 VoIP Gateway

User's Guide

AddPac Technology, Co. Ltd.

3rd fl., Jeong-Am Building., 769-12 Yoksam-dong

Kangnam-ku Seoul, Korea 135-080

Phone (82 2)568-3848

Fax (82 2)568-3847

E-mail : info@addpac.com

<http://www.addpac.com>

[Contents]

About this document

Chapter 1	VoiceFinder AP2120 Overview.....	14
1.1.	Introduction to AP2120 VoIP Gateway	14
1.2.	Main Features.....	16
Chapter 2	Before Installation	22
2.1.	Unpacking.....	22
2.2.	Parts and descriptions.....	24
2.3.	Network interface: Fixed	28
2.4.	Voice network modules	30
2.5.	Installation Requirements.....	33
2.5.1.	Electrical Requirements	33
2.5.2.	General Requirements	34
Chapter 3	Installation and Operation Environment	35
3.1.	Installation	37
3.1.1.	Installation Procedure	37
3.1.2.	Console Connection.....	38
3.1.3.	Connect power	40
3.2.	Environment Configuration	43
3.2.1.	User and Gateway Management Environment.....	44
3.2.2.	Interface Configuration Environment	45
3.2.3.	Routing Configuration Environment	45
3.2.4.	Security and Internet Configuration Environment.....	46
3.2.5.	System Status and Debugging Environment.....	46
3.2.6.	Voice Integration Configuration Environment.....	46
Chapter 4	Gateway Configuration and Commands	48
4.1.	Gateway Booting.....	48
4.2.	Commands.....	52
4.2.1.	Commands of the User Mode	55
4.2.2.	Commands of the Manager Mode	56
4.2.3.	Commands of the Configuration Mode.....	58
4.2.3.1.	Global Configuration (config) Commands.....	58
4.2.3.2.	Commands of the Interface Configuration Mode 1	60

4.2.3.3.	Commands of the Interface Configuration Mode 2	60
4.3.	Starting Gateway Configuration.....	63
4.4.	Ethernet Configuration	65
4.4.1.	Ethernet basic configuration	65
4.4.2.	PPPoE Configuration	70
4.5.	Routing Configuration	79
4.5.1.	Static Routing Configuration	80
4.5.2.	RIP Configuration.....	84
4.5.3.	OSPF Configuration	90
4.6.	Filter (Access-List) Configuration.....	98
4.7.	NAT(Network Address Translation) Configuration.....	105
4.8.	DHCP (Dynamic Host Configuration Protocol) Configuration	115
4.9.	Transparent Bridging Configuration	123
4.10.	Traffic Management	129
4.11.	SNMP Configuration.....	135
4.12.	Gateway Management Command.....	141
4.12.1.	Command in the EXEC Mode	141
4.12.2.	Command in the Global Configuration Mode	144
4.13.	Fault Management and Debugging	148
4.13.1.	Logging Command	148
4.13.2.	Show commands.....	149
4.13.3.	Debug Commands	153
4.14.	User, Password, Software Image and Configuration File Management	156
4.14.1.	User Registration and Change	156
4.14.2.	Password Recovery	157
4.14.3.	Software Image Upgrade and Backup	160
4.14.4.	Configuration File Backup & Restore	162
Chapter 5	Voice Configuration and Command	165
5.1.	Voice Technologies and Concepts	165
5.1.1.	Voice Over IP	165
5.1.2.	Codecs and MOS(Mean Opinion Score)	165
5.1.3.	Dial Peer.....	169
5.1.4.	Voice ports	170
5.2.	VoIP Interface Configuration	173
5.3.	Numbering Plan, Number Handling and Dial Peer Configuration.....	175
5.3.1.	Numbering Plan	175
5.3.2.	Dial Peer Configuration	175
5.3.2.1.	Inbound Dial Peer & Outbound Dial Peer	175

5.3.2.2.	POTS Peer Configuration	178
5.3.2.3.	VoIP Peer Configuration	179
5.3.2.4.	Setting CODEC and VAD in the Dial Peer	180
5.3.3.	One-Stage Dialing versus Two-Stage Dialing	183
5.3.4.	Hunt Group-related Configuration	185
5.3.4.1.	Basic Concept and Configuration	185
5.3.4.2.	Rerouting to the PSTN.....	187
5.3.4.3.	Call barring	188
5.3.5.	Prefix and Forwarding Telephone Numbers	189
5.3.6.	Configuring Number Expansion	190
5.3.6.1.	Number Expansion Table.....	190
5.3.6.2.	Configuring Number Expansion	191
5.3.7.	Configuring Number Translation	191
5.3.7.1.	Creating Translation Rules	191
5.3.7.2.	Applying Translation Rules to the Inbound POTS Calls.....	193
5.3.7.3.	Applying Translation Rules to the Inbound VoIP Calls.....	194
5.3.7.4.	Applying Translation Rules to the Outbound Calls	194
5.4.	Configuration Voice Ports	196
5.4.1.	Configuration Voice Ports of AP2120 Gateway	196
5.4.2.	Voice Ports Configuration Task List and Steps.....	196
5.4.2.1.	Configuring FXS or FXO Voice Ports	196
5.4.2.2.	E&M Port configuration.....	197
5.4.2.3.	E&M Voice Port Tunning	200
5.4.2.4.	Activating/Deactivating the Voice Ports	201
5.5.	Configuring FAX Application.....	202
5.5.1.	T.38 FAX Relay using VoIP H.323	202
5.5.2.	Configuring T.38 FAX Relay for VoIP H.323.....	203
5.5.3.	FAX Relay setting by Bypass.....	203
5.6.	Other VoIP Configuration	206
5.6.1.	Setting H.323 Gateway	206
5.6.2.	Configuring H323 Call Start Mode	207
5.6.3.	Configuring User Class	207
5.7.	VoIP Configuration Command	210
5.7.1.	VoIP-Related whole Command.....	210
5.7.2.	Global Configuration Command	215
5.7.2.1.	dial-peer hunt.....	215
5.7.2.2.	dial-peer ipaddr-prefix.....	217
5.7.2.3.	dial-peer terminator	218
5.7.2.4.	dial-peer voice.....	220

5.7.2.5.	gateway.....	222
5.7.2.6.	num-exp.....	223
5.7.2.7.	translation-rule.....	226
5.7.2.8.	voice-port	227
5.7.2.9.	voice class clear-down-tone.....	228
5.7.2.10.	voice class codec	229
5.7.2.11.	voice class user	231
5.7.2.12.	voice service	233
5.7.2.13.	voip-interface.....	234
5.7.3.	Voice Port Configuration Command.....	236
5.7.3.1.	comfort-noise	236
5.7.3.2.	connection	237
5.7.3.3.	description (voice port)	238
5.7.3.4.	echo-cancel	239
5.7.3.5.	input gain.....	240
5.7.3.6.	operation (E&M Voice Port Command).....	241
5.7.3.7.	output gain.....	243
5.7.3.8.	polarity-inverse	244
5.7.3.9.	ring number	245
5.7.3.10.	shutdown (voice-port)	246
5.7.3.11.	signal (E&M Voice Port Command)	247
5.7.3.12.	timing delay-duration (E&M Voice Port Command)	249
5.7.3.13.	timing delay-start (E&M Voice Port Command).....	250
5.7.3.14.	timing dialout-delay (E&M Voice Port Command)	251
5.7.3.15.	timing wait-wink (E&M Voice Port Command)	252
5.7.3.16.	timing wink-duration (E&M Voice Port Command)	252
5.7.3.17.	timing wink-wait (E&M Voice Port Command)	253
5.7.3.18.	translate-incoming	254
5.7.3.19.	type (E&M Voice Port Command).....	255
5.7.4.	Dial Peer Commands.....	258
5.7.4.1.	answer-address.....	258
5.7.4.2.	codec.....	259
5.7.4.3.	description (dial-peer)	260
5.7.4.4.	destination-pattern	261
5.7.4.5.	dtmf-relay	264
5.7.4.6.	forward-digits	265
5.7.4.7.	huntstop	267
5.7.4.8.	port.....	268
5.7.4.9.	preference.....	269

5.7.4.10.	prefix	270
5.7.4.11.	register	271
5.7.4.12.	sid	273
5.7.4.13.	session target.....	274
5.7.4.14.	polarity-inverse	275
5.7.4.15.	shutdown (Dial-Peer).....	276
5.7.4.16.	translate-outgoing.....	277
5.7.4.17.	vad.....	278
5.7.4.18.	voice-class codec	279
5.7.5.	Gateway, Voice Service, Voice Class and Rule Configuration Command....	281
5.7.5.1.	announcement.....	281
5.7.5.2.	codec preference	282
5.7.5.3.	counter.....	283
5.7.5.4.	discovery.....	284
5.7.5.5.	fax protocol	285
5.7.5.6.	fax rate	286
5.7.5.7.	h323 call start	288
5.7.5.8.	gkip	289
5.7.5.9.	h323 call channel	290
5.7.5.10.	h323 call response	292
5.7.5.11.	h323-id	293
5.7.5.12.	lightweight-irr	294
5.7.5.13.	max-digits.....	295
5.7.5.14.	password.....	295
5.7.5.15.	public-ip	296
5.7.5.16.	register	297
5.7.5.17.	rule	298
5.7.5.18.	security password	301
5.7.5.19.	security permit-FXO	302
5.7.5.20.	timeout	303
5.7.5.21.	translate-voip-incoming	305
5.7.6.	Miscellaneous Commands	307
5.7.6.1.	clear h323 call.....	307
5.7.6.2.	clear voice port	308
5.7.6.3.	show call active.....	308
5.7.6.4.	show call history	309
5.7.6.5.	show clear-down-tone	310
5.7.6.6.	show codec class.....	311
5.7.6.7.	show dial-peer	312

5.7.6.8.	show dialplan number	313
5.7.6.9.	show dialplan port	314
5.7.6.10.	show gateway	314
5.7.6.11.	show num-exp	315
5.7.6.12.	show translation-rule	316
5.7.6.13.	show user-class	317
5.7.6.14.	show voice port	318
5.7.6.15.	show voip-interface	319
5.7.6.16.	debug voip call	320
5.7.6.17.	debug voip	321
Appendix A. AP1100 VoIP Gateway Specifications.....		324
VoIP(Voice over IP) Config. Example		328
Appendix C AP1100 Call Finishing Cause Code		350
Appendix D Cable Specifications		354

About this document

This chapter outlines the structure of VoiceFinder AP2120 VoIP Gateway User's Guide and explains the symbols and legends.

[Organization]

The VoiceFinder AP2120 user's manual is offered to assist the operation of the 2120 Gateway. This manual is composed of 5 chapters and 4 Appendixes.

Experienced users may refer directly to the related chapters. However, Less experienced users are highly recommended to thoroughly review this manual before operation of the Gateway.

- Chapter 1 『**VoiceFinder AP2120 Overview**』 provides an introduction to the H/W and S/W of VoiceFinder AP2120 and how to apply for technical supports.
- Chapter 2 『**Before Installation**』 provides an explanation on the installation environment and cable requirements along with recommendations for safe operation of the equipment.
- Chapter 3 『**Installation and Operation Environment**』 explains the basic installation information and environmental requirements on connecting with LAN, WAN and Console Port
- Chapter 4 『**Gateway Configuration and Commands**』 explains in detail about configuring user Interface and the corresponding commands along with configuration examples. This chapter provides very important information, so please make sure to have comprehensive understanding.
- Chapter 5 『**Voice Configuration and Commands**』 explains in detail about configuring the User Interface and the corresponding commands along with configuration examples for Voice Integration. This chapter provides important information about maintaining and optimizing quality of voice and also requires comprehensive understanding.

- Appendix A 『 **VoiceFinder AP1100 Specifications** 』 provides detailed specifications on VoiceFinder AP2120 Gateway
- Appendix B 『 **Example of Gateway Port Configuration** 』 provides examples of basic VoiceFinder AP2120 Gateway configurations.
- Appendix C 『 **Cable Specification** 』 describes the console cable, Ethernet cable specifications and Pin numbers for VoiceFinder AP2120 Gateway.
- Appendix E 『 **Miscellaneous Information** 』 defines VoiceFinder AP2120 Gateway guarantee of quality and related policies.

For technical supports, please contact AddPac Technology Co. Ltd.

AddPac Technology Co., Ltd
3rd Fl. Jeong-Am Bulding, 769-12
Yeoksam-Dong, Kangnam-Ku, Seoul, Korea
Phone (02) 568-3848
Fax (02) 568-3847
E-mail : info@addpac.com
<http://www.addpac.com>

The revision history of VoiceFinder AP2120 Gateway User's Guide is as follows.



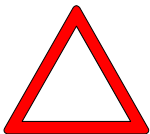

Revision No.	Date	Comments	Written by
Version 1.0	Dec. 18, 2002	Initial Released	AddPac R&D Center

[Symbols and Legends]

The symbols and legends used in this User's Manual are as follows :

- Commands and Keywords are typed in **Bold**.
- Variables that require user inputs are typed in *Italic*.
- Square brackets ([]) are optional values.
- Keywords that are required but need to be selected are grouped in braces ({}), and are separated by Slashes (/).
- Angle brackets (<>) are required parameters must be inputted.

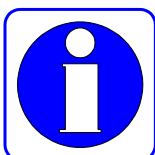
The following conventions are also used to attract the user's attention.

Danger 	Danger This symbol signals possible danger. Misuse could result in physical injuries. Please follow the instructions to avoid any electronic shocks.
Warning 	Warning It warns the users to be careful with the operation. Otherwise, it could result in hardware damage of the equipment or loss of data.
Caution 	Caution This symbol calls for the user's caution. Otherwise, it could result in hardware damage of the equipment, loss of data or system configuration.
Information 	Information This symbol indicates additional information offering detailed information for understanding this user guide.

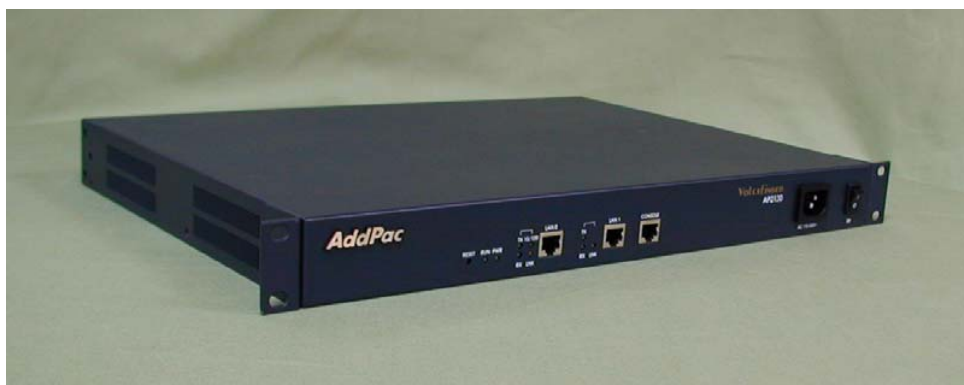
Chapter 1 VoiceFinder AP2120 Overview

1.1. Introduction to AP2120 VoIP Gateway

Information VoiceFinder AP2120 VoIP Gateway is a VoIP product offering cost efficient voice service via Internet for companies (main and branch offices), public offices and SMB (small and medium business).



AP2120 VoIP Gateway guarantees toll-quality voice service both on low and high speed Internet connection with cutting edge voice compression algorithm and AddPac's unique patent pending QoS algorithm. Also, AP2120 supports up to 16 voice channels according to user's needs along with various voice interfaces of FXS, FXO and E&M. AP2120 offers flexible configuration to meet the customers' needs which reduces additional investment on customers' side.

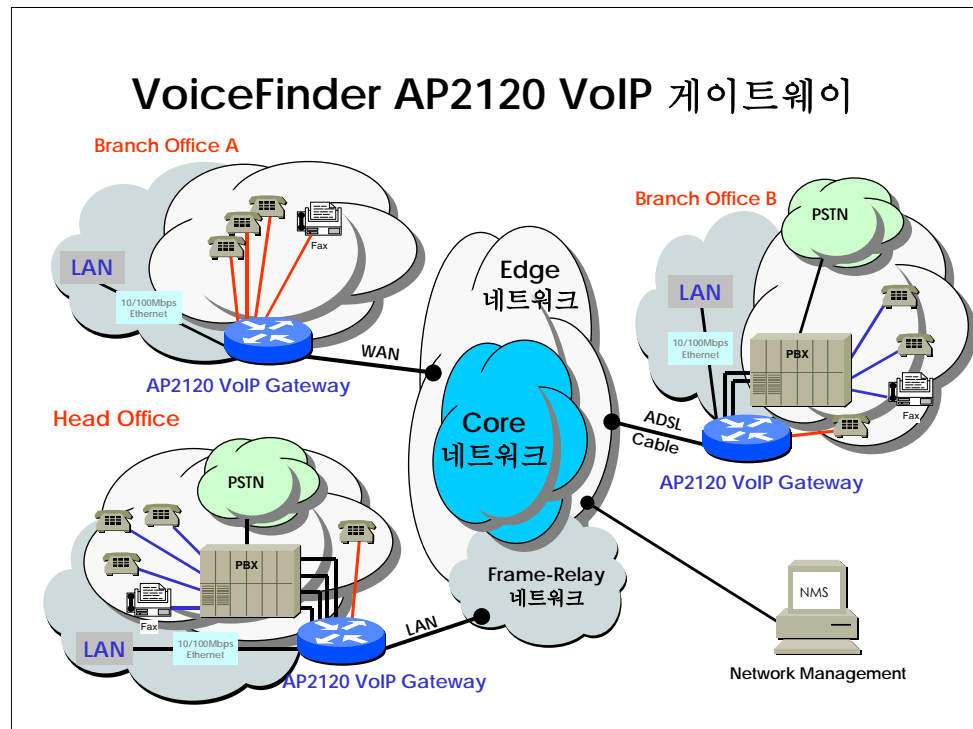


[Figure 1-1 Exterior view of AP2120 VoIP Gateway]

AP2120 supports stable network such as dedicated line/LAN, and static and dynamic IP address of ADSL and Cable network. Also, not only Voice Gateway function, it offers Static, RIP v1/2, OSPF v2 routing function useful for flexible network formation and management along with NAT/PAT Internet application functions. Especially, in dynamic IP environment, it offers VoIP and IP sharing function at one platform making possible effective and economic solution for high speed Internet environment.

AP2120 shows perfect interoperability with currently available domestic and overseas middle-large scale Gateway and Gatekeeper. Also, it offers same operation environment with existing AP voice Gateway/Router realizing easy installation and operation for even beginning users.

The following Diagram is a sample network diagram using AP2120 VoIP Gateway.



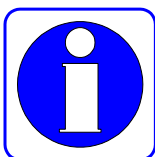
[Figure 1-2 Network Diagram using AP2120 VoIP Gateway]

Additionally, Packet Filtering and Access List type Firewall is supported, thus preventing intrusion using IP layer and packet source and destination address information of TCP/UDP layer.

The DHCP(Dynamic Host Configuration Protocol) function automatically assigns IP addresses to sub-network clients, and uses NAT(Network Address Translation) to prevent IP address depletion while hiding internal IP addresses which also strengthens network security.

1.2. Main Features

Information



VoiceFinder AP2120 VoIP Gateway is for enterprises (main & branch offices) and public offices with Ethernet interface and 4 port FXS interface of cutting-edge compression algorithm. In addition to that, it offers Voice interface slot for FXS, FXO and E&M according to users needs.

VoiceFinder AP2120 VoIP Gateway offers superior solution for SOHO and SME . Also, VoiceFinder AP2120 VoIP Gateway supports various voice modules to meet the customers' service needs. Along with easy installation and management, it supports Static, RIP v1/2, OSPF v2 Routing and can be directly connected to High-speed Internet Modem such as ADSL.

● Hardware Description

VoiceFinder AP2120 VoIP Gateway is based on cutting-edge embedded H/W technology offering various voice interface with ample system memory. The key H/W features are as shown below.

- ✓ High-performance VoIP service solution integrating voice and data
 - ✓ Modularized H/W structure realizing high extensibility
 - ✓ High-performance 32bit RISC Microprocessor structure
 - ✓ Independent, high-performance 2-Voice Network Module Slots
 - ✓ Fixed 1-Port 10/100Mbps Fast Ethernet Interface for LAN Service (RJ45)
 - ✓ Fixed 1-Port 10Mbps Ethernet Interface for WAN Interface (RJ45)
 - ✓ Fixed 1-Port Asynchronous Serial Interface for Console Port (RJ45)
 - ✓ Optional 8-Port FXS Voice Processing Network Module (8 x RJ11)
 - ✓ Optional 8-Port FXO Voice Processing Network Module (8 x RJ11)
 - ✓ Optional 8-Port E&M Voice Processing Network Module (8 x RJ48)
 - ✓ Optional 4-Port FXO and 4-Port FXS Voice Processing Network Module (8 x RJ11)
 - ✓ 1U x 19" Rack Mountable Standard Chassis
 - ✓ AC Power Supply unit (Free Voltage)
 - ✓ Variuos LEDs, system indicators.
-
- **Supports various routing/bridging protocols**
 - ✓ VoiceFinder AP2120 VoIP Gateway supports various routing/bridging protocols as shown below.

- ✓ IP Routing (Static, RIP v1/v2, OSPF v2)
- ✓ IEEE802.1Q VLAN Routing
- ✓ Transparent Bridging (IEEE Spanning Tree Protocol)

● **Supports voice & data integration service (VoIP)**

VoiceFinder AP2120 VoIP Gateway supports various voice over IP service applications as shown below.

- ✓ Supports ITU-T H.323 v2 VoIP Protocol
- ✓ Supports ITU-T H.235 Security Feature
- ✓ Supports ITU-T H.323 Gateway, Gatekeeper
- ✓ Supports Session Initiation Protocol (SIP)
- ✓ Supports G.723.1, G.729.A, G.711 Voice Compression algorithm
- ✓ Supports various Voice Processing Features
 - VAD(Voice Activity Detection)
 - T.38 G3 FAX Relay(In-band 및 Out-band)
 - DTMF(Dual Tone Multi Frequency)
 - CNG (Comfort Noise Generation)
 - G.168 Echo Cancellation
- ✓ Supports Enhanced QoS Management Features for voice traffic
- ✓ Offers scalability, reliability, stability for H.323 based VoIP services
- ✓ Supports Fast Connect Mode
- ✓ Supports H.323 call setup via normal connect mode if the peer side does not support Fast Connect Mode.
- ✓ Supports Voice Codec automatic negotiation function and Voice Codec Mode Setting by Operator.
- ✓ Supports Adjustment of Frame Number per Packet
- ✓ Supports GK Discovery and Communication.(GRQ/GCF/GRJ)
- ✓ Supports H.323 Endpoint Registration and Deregistration in GateKeeper (RRQ/RCF/RRJ, URQ/UCF/URJ).
- ✓ Supports Lightweight RRQ Function
- ✓ Supports VoIP Gateway H.323 ID Assignment, Modification and Transfer Function.
- ✓ Supports Capital and Small letter Recognition of H.323 ID.
- ✓ Supports H.323 E.164 Telephone Number Assignment, Modification and Transfer Function.
- ✓ Supports Outbound Call routing function via GateKeeper.
- ✓ Supports Inbound Call routing function using Phone number
- ✓ Supports Inbound/Outbound Call Number deletion and addition.

- ✓ Support PBX side outbound call number Insertion in Calling Party Address.
 - ✓ Supports Voice Prompt for 1 Stage and 2 Stage Dialing
 - ✓ Supports Last digit recognition
 - ✓ Call restriction about Specific Phone Number or Line
 - ✓ Tone (Dial tone, Ring back tone, Busy tone, Congestion tone)
 - ✓ Supports LLO (Line Lock Out)
 - ✓ Supports Announcement Function for incorrect dialing, busy, network failure, Non-exist Phone number
 - ✓ Configuration Management and System Management
 - ✓ Operation Data Automatic Backup and restore Function
 - ✓ Port Diagnosis and Testing Function
 - ✓ Supports Secondary Gatekeeper in case of First Gatekeeper Failure
 - ✓ H.225, RAS, H.245 Call Tracing Function
 - ✓ DTMF transmission and Recognition Function (Out of band)
 - ✓ FAX Tone automatic recognition
 - ✓ Supports Real-time FAX and Simultaneous FAX Transmission in All Channel (T.38)
 - ✓ Redundancy Support in T.38 FAX
 - ✓ Supports PLAR (Private Line Auto Ring Down)
 - ✓ Trunk Emulation for Broadcasting Equipment
 - ✓ Ring Cadence Adjustment for Broadcasting Equipment
 - ✓ BusyOut Function in case of LAN or Gatekeeper Failure (Rerouting at PBX)
 - ✓ Call Pickup and Call Transfer between FXS port
 - ✓ Polarity Inversion in FXS port
 - ✓ Hook Flash Relay for supplementary service
- **Supports standard SNMP for equipment management**
 - ✓ VoiceFinder AP2120 VoIP Gateway supports standard SNMP Agent, standard MIB II and Bridge MIB for efficient equipment management.
 - ✓ For more precise equipment management, RMON MIB is also supported.
 - **Supports remote S/W upgrade**
 - ✓ VoiceFinder AP2120 VoIP Gateway supports remote S/W upgrade with TFTP and FTP program minimizing maintenance expenses.
 - **Simplified user interface**

- ✓ VoiceFinder AP2120 VoIP Gateway supports Command Line Interface which is adopted by most of router/gateway. Also, it offers on-line help with "?" key input and command history function for easy operation and management.
- **Superiour diagnosis function**
 - ✓ VoiceFinder AP2120 VoIP Gateway offers various dignosis and status monitoring commands along with powerful packet analysis and debugging function. So the users/operators can easily monitor the status of the Gateway or the network.
- **Various management tools**
 - ✓ VoiceFinder AP2120 VoIP Gateway supports Asynchronous Console port along with Telnet and Rlogin realizing management of the gateway by remote users.
- **Enhanced security function**
 - ✓ VoiceFinder AP2120 VoIP Gateway offers network secutiry function with Packet Filtering and Access-List type Fireweall function. Also, it minimizes the possibility of accessing local network by realizing multi-level user accounts.
- **Effective IP address resource management**
 - ✓ VoiceFinder AP2120 VoIP Gateway supports DHCP server, Relay function and NAT function realizing simple and effective IP address resource management.
- **Various traffice management tools**
 - ✓ VoiceFinder AP2120 VoIP Gateway offers Traffic Queuing for each protocol and offers Flow Control for effective use of limited WAN bandwidth.
 - ✓ With enhanced QoS for voice application, the customers using 56/64Kbps delicated lines can use up to 4 voice channels without degradation of voice qulity.
- **Stable power supply**
 - ✓ VoiceFinder AP2120 VoIP Gateway support automatic detection of 110~220V power reducing malfunction of Gateway due to power supply along with default dual power supply.

- **LEDs for easy status checking**
 - ✓ VoiceFinder AP2120 VoIP Gateway's power and communication cables are placed at the back panel. Also, the LEDs are placed at the front panel so that users can check the operation status also realize clean installation environment at the same time.





Chapter 2 Before Installation

2.1. Unpacking

Before unpacking, check for external damage of the packaging box .

If there is any external damage of the packaging, please contact AddPac Technology Co. Ltd. R&D center/ Customer supports (Tel : +82-2-568-3848) for an immediate replacement of the product.

If no external damage has found, open the box and check all the items are included.

No.	ITEM	Image	Q'ty
1	VoiceFinder AP2120 Gateway		1
2	LAN cable (RJ45 to RJ45)		1
3	Console cable (RJ45 to DB9)		1
4	Power cable (220V Power Cord)		1

5	AP2120 User's Guide (English)		1
---	----------------------------------	--	---

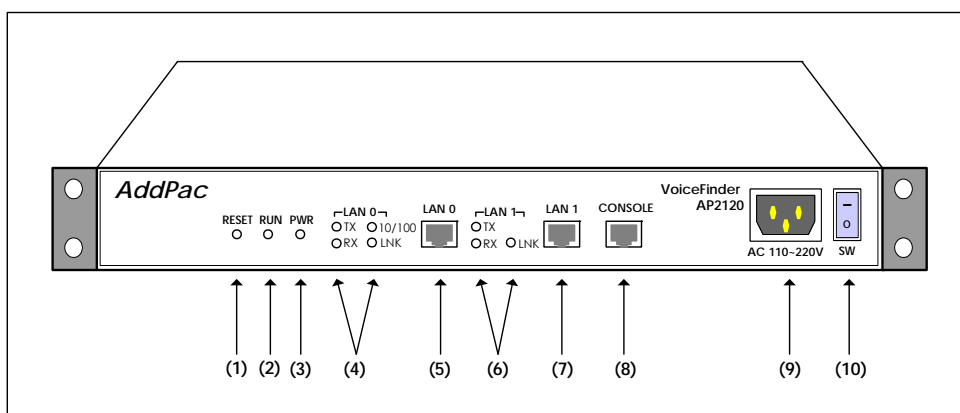
[Table 2-1 VoiceFinder AP2120 package]

If any item is missing, immediately contact AddPac Technology Co. Ltd.
customer support

2.2. Parts and descriptions

AP2120 VoIP Gateway is 1U-high, 19" rack-mountable standard Chassis. LEDs are located on the front panel for easy monitoring along with fixed network interfaces such as 10Mbps Ethernet network interface for WAN and 10/100Mbps high-speed Ethernet for LAN. Also, 2 voice network module slots are placed at the back panel.

Front View of AP2120



[Figure 2-1 Front view of VoiceFinder AP2120 VoIP Gateway]

The below chart describes the parts of AP2120 VoIP Gateway

No.	Part		Description
(1)	RESET		RESET switch for system H/W reset. (Push button in red)
(2)	RUN		RUN LED indicating normal operation of the equipment (Green)
(3)	PWR		Power LED. It indicates the power is being supplied normally. (Green)
(4)	LAN 0	TX,RX	LAN LED for local LAN connetion. Indicating TX and RX status of Ethernet ports. (Green)
		10/100	10/100 LED for 100BaseTx showing Fast Ethernet condition. (Green)
		LNK	LINK LED for LAN connection. (Yellow)
(5)	LAN 0 Port		LAN Interface port. UTP Type. 10/100Mbps high-speed Ethernet port.
(6)	LAN 1	TX,RX	LAN LED for WAN connection. Indicating TX/RX stuatus of Ethernet port. (Green)
		LNK	LINK LED for LAN connection. (Yellow)
(7)	LAN 1 Port		WAN Interface port. UTP Type. Connecting10Mbps Ethernet.
(8)	Console Port		To connected PC and the Gateway. For initial setting, Console should be used.
(9)	Power Plug		To connect power cable. AP2120 VoIP Gateway can use 110/220VAC.
(10)	Power switch		A switch to supply or terminate power.

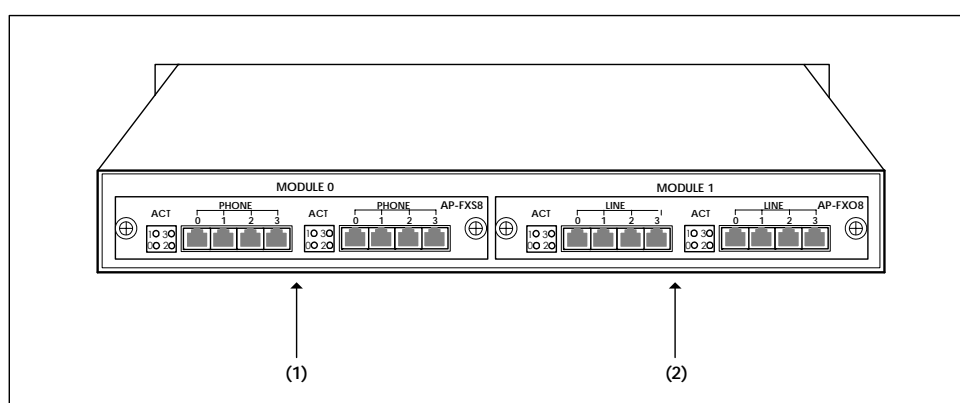
[Table 2-2 Parts and description of the front panel of VoiceFinder AP2120 VoIP Gateway]

Rear View of AP2120

The rear panel of AP2120 VoIP Gateway consists of 2 voice interface slots for voice service.

Standard Configuration Model

The below shows the rear view of standard AP2120 VoIP Gateway.



[Figure 2-2 The rear view of VoiceFinder AP2120 VoIP Gateway]

The below shows the parts and description of standard AP2120 VoIP Gateway rear panel. Also, it is only an example and users can install modules according to their network environment.

No.	Parts	Description
(1)	Voice Module 0 Slot	RJ11 Connector Type. Supporting 8 Voice Ports. ◆ Supports Status LEDs 8Port FXS, 8Port FXO, 8Port E&M, 4Port FXS & 4Port FXO modules are available.
(2)	Voice Module 1 Slot	RJ11 Connector Type. Supporting 8 Voice Ports. ◆ Supports Status LEDs 8Port FXS, 8Port FXO, 8Port E&M, 4Port FXS & 4Port FXO modules are available.

[Table 2-3 The parts and description of VoiceFinder AP2120 VoIP Gateway rear panel]

The blow is the rear view of AP2120 VoIP Gateway.



[Figure 2-3 The picture of VoiceFinder AP2120 VoIP Gateway rear panel]

2.3. Network interface: Fixed

AP2120 VoIP Gateway supports network interface (fixed) as follows.

- 1 port 10/100Mbps high-speed Ethernet interface/ LAN 0 (RJ45)
- 1 port 10Mbps high-speed interface/ LAN 1 (RJ45)
- 1 port async. serial interface for Console (RJ45)

The above interfaces are for various WAN such as LAN, behind the dedicated Router, ADSL(PPPoE), and Cable Modem(DHCP). Also, high-speed Ethernet interface is used to form sub-network with VoIP Gateway for voice/data integration.

Descriptions on AP2120 VoIP Gateway network interfaces are as follows.

1-Port 10/100Mbps Fast Ethernet Interface (RJ45)

AP2120 VoIP Gateway supports one (1) 10/100Mbps Fast Ethernet interface for Local Area Network (LAN). This interface offers 10/100Mbps auto-sensing with RJ-45 standard interface.

1-Port 10Mbps Ethernet Interface (RJ45)

AP2120 VoIP Gateway supports one (1) 10Mbps Ethernet Interface to form Wide Area Network (WAN). This interface can be connected to the LAN port of the dedicated line Router. Also, it supports PPPoE and DHCP/ Dynamic route for ADSL and Cable network. It is RJ45 standard LAN interface.

1-Port Async. Ethernet Interface for Console Port (RJ45)

AP2120 VoIP Gateway offers 1 RS-232C Async. Ethernet interface for Console.
The interface is RJ45 type.

2.4. Voice network modules

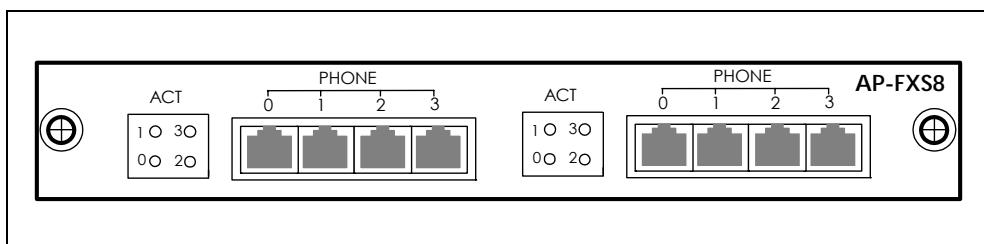
The multi-service network modules of AP2120 VoIP Gateway are optional and can be selected according to users' network. Multi-service network modules for high quality multimedia solution can be divided as follows.

- **FXS Interface voice module**
- **FXO Interface voice module**
- **E&M interface voice module**

AP2120 VoIP Gateway supports not only data service but also multimedia service of voice and image in one device with above modules. Multiservice Network Modules can be selected to form ideal solution for users' network environment.

AP-FXS8 : 8-Port FXS Voice Interface Module

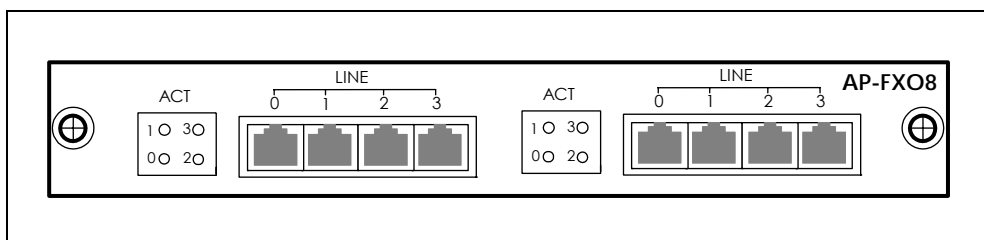
AP2120 VoIP Gateway offers 8 channel Foreign Exchange Station (FXS) to connect ordinary telephones and PBX directly.



[Figure 2-4 AP2120 AP-FXS8 module images]

AP-FXO8 : 8-Port FXO Voice Interface Module

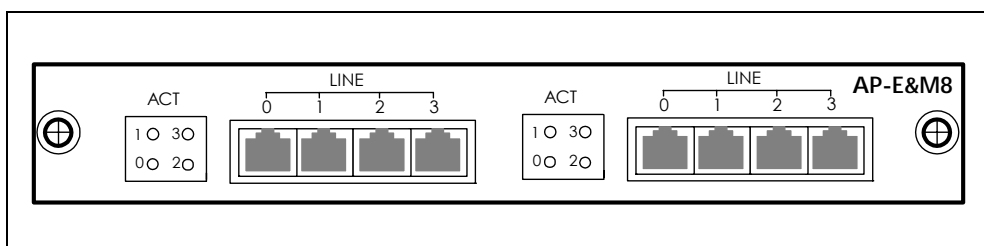
AP2120 VoIP Gateway offers 8 channel Foreign Exchange Office (FXO) to connect the switching office of Public Switched Telephone Network (PSTN) or ordinary telephones



[Figure 2-5 AP2120 AP-FXO8 module image]

AP-E&M8 : 8-Port E&M Voice Interface Module

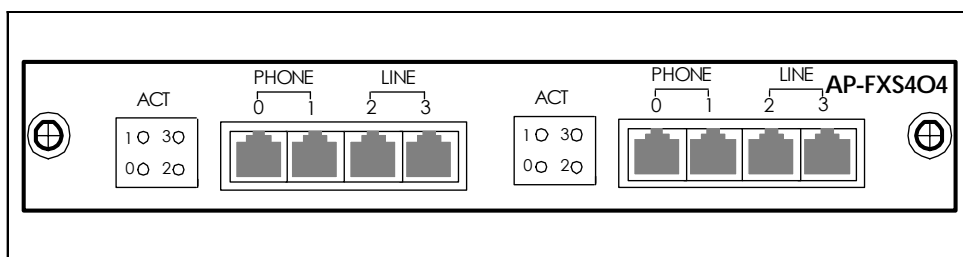
AP2120 VoIP Gateway supports 8 channel voice service module of receive and transmit (E&M). This analog E&M Interface is used to connected Trunk line of PBX.



[Figure 2-6 AP2120 AP-E&M8 module]

AP-FXS4O4 : 4-Port FXO and 4-Port FXS Voice Interface Module

AP-FXS4O4 offers various voice service with 4- channel FXS voice interface and 4- channel FXO interface in one module.



[Figure 2-7 AP2120 AP-FXS4O4 Module]

2.5. Installation Requirements

Warning

The below is the recommendation for safe operation of the equipment.



- Make sure AP21200 VoIP Gateway is in a dust-free environment before and after installation.
- Make sure to open AP2120 Gateway cover on a flat and safe surface.
- To prevent accidents, be careful with ties, scarf, sleeves, and any other loose clothing from entangling with the Chassis.
- Avoid any actions that may effect the equipment or the operator.

2.5.1. Electrical Requirements

There are two main sources of electrical problems with the AP1100 Gateway :
Danger the power supply and static electricity..



This section describes safety recommendations for each case.

- **Electrical Safety**

- ✓ Operate at a position where immediate shut-off of power supply is possible.
- ✓ Turn off the power while installing or taking the cover off the equipment.
- ✓ Avoid operating the equipment alone at potentially dangerous environment.
- ✓ Do not assume the power is switched off, but always confirm the power status.
- ✓ Be extremely cautious when operating in a humid environment or with an ungrounded power extension cable.

- **Prevention of Static Electricity**

- ✓ The main chip-set of the Gateway are very delicate and misuse may result in static electrical damage.
- ✓ If a static prevention waist strap is available, strap it around the wrist

and earth the cord before operating the equipment.

- ✓ If no waist tap is available, earthing by holding a metal part of the chassis will help to prevent static electricity.

2.5.2. General Requirements

Warning



VoiceFinder 2120 Gateway is ready for use where other electronic products can be used. However, the following conditions are recommended for maximum performance.

- A flat and well ventilated location
- Secure the equipment safely at the desired place to install.
- Do not place any objects on top of the equipment.
- A location without direct sunlight.
- Keep away from flammable, chemical, or magnetic objects

Chapter 3 Installation and Operation Environment

This chapter provides information about the basic installation procedure of VoiceFinder AP2120 and related commands.

[Necessaries] Unless ordered in advance, the tools and certain cables are not provided in the package. Prepare the following equipments and tools before the installation.

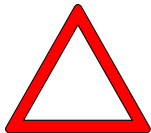
- Standard screwdriver set
- Cable for LAN and WAN(Serial) port connection
 - ✓ RJ-45 to RJ-45 cable for LAN port
 - ✓ Telephone line with RJ-11 connector to connect PBX or telephones
 - ✓ RS-232c console cable with RJ-45 connector (included in the package)
- PC with Console Terminal or Communication Emulator application (The Hyper Terminal Program in Windows will suffice. Configure it as : 9,600 Baud, No Parity, 8Bit Data 1Stop Bit)
- DSU/CSU or other DCE device to connect Synchronous WAN(Ethernet) port.

3.1. Installation

3.1.1. Installation Procedure

- Connect the console cable and configure the console terminal. (Refer to 3.1.2 for details.)
- Connect the network to the desired port. Connect LAN port with HUB/Switch using RJ-45 cable.
- Log in to the Gateway after the booting message with root account. (Configuration is only possible when logged in with the root account.)
- Switch to Configuration Mode.
- Assign an Internet address to the desired port. (Refer to Interface Configuration.)
- For WAN(Ethernet) port, select the mode (ex, PPPoE). (Refer to Interface Configuration)
- Configure the routing and VoIP related parameters. (Refer to Chapter 4 and 5.)
- Confirm the configuration. (Refer to the Gateway administrative commands.)

Caution

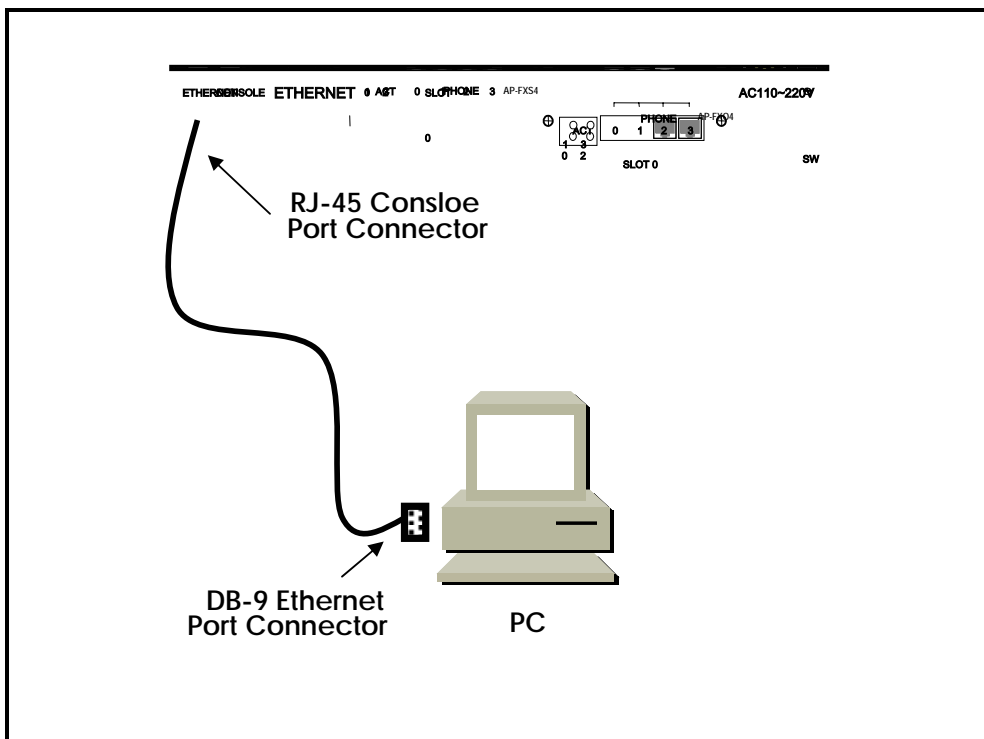


- Save the settings at the Flash Memory. **(New settings are applied immediately, but under certain network environments rebooting is required. Refer to the following instructions for this part.)**
- With the commands such as Ping, Telnet, rlogin etc., check the status of other Gateways or the PC connected to the Gateway.

- Check the routing table to confirm if the Gateway is receiving the network information correctly.
- Use Ping command to check the connectin of other Gateways or PC.
- The basic configuration procedure is completed. For optional functions, refer to the related chapter.

3.1.2. Console Connection

- Connect the console port in the rear side of the Gateway with the serial port of the prepared console terminal. **(Refer to [Diagram 3.1 Console Cable Connection])**
 - ✓ Use the console cable provided with the package.
 - ✓ If using a PC as the console terminal, connect to the Ethernet port of the PC.
- In order to use a PC as a console terminal, a communication emulator application is required. Under normal circumstances, the Hyper Terminal Program in Windows is suffice.
- The console terminal should be configured as : 9,600 Baud, No Parity, 8Bits Data, One(1) Stop Bit. VoiceFinder 2120 Gateway is set to operate with the configurations above. Therefore, these settings are required for communication between the Gateway and the console terminal. **(Refer to [Table 3-1 Hyper Terminal Configuration])**
- To configure Hyper Terminal, select from the Hyper Terminal menu: File → Configuration → Connection Target → Format and set each item.
- The console port is used to configure VoiceFinder 2120 Gateway and check its operating status.



[Figure 3-1 Console Cable Connection]

Port Configuration	Settings
Modem to Connect	Direct connection(Null Modem) to Com port
Bit per Second	9,600
Data Bit	8
Parity	None
Stop Bit	1
Flow Control	None

[Table 3-1Hyper Terminal configuration]

3.1.3. Connect power

Warning



- VoiceFinder AP2120 Gateway can detect and use both 110V and 220V.
- The package includes a power cable with 220V plug. If the power supply is 110V, please use a 110V adapter.
- Turn on the power switch. Then the Power LED on the front panel is turned on.
- The booting message is displayed on the console terminal. Also, the green RUN LED is turned on.
- When the Gateway is being booted, the following messages are displayed.(Refer to Diagram 3.3)
 - ✓ The booting title message is displayed. (This message contains information about the routing software version, Gateway status monitoring results, memory size and status)
 - ✓ With the log-in message, input the username "root" and the password "Gateway".
 - ✓ After the log-in process, the prompt "1router#" is displayed on the Gateway console terminal.
 - ✓ There are two types of prompts used for the VoiceFinder AP1100 : "1router>" and "1router#". The ">" prompt indicates that the user is not an administrator. With this prompt, the user is unable to use certain commands : particularly the configuration commands. The "#" prompt indicates that the user is an administrator (or root), and the user is authorized to use all the functions and commands.
 - ✓ Log-in as "Admin" allows to change Gateway settings. Therefore, it is advised to change the default Gateway password for security

purposes. Refer to the Administrative contents for password change.

The below is the message for initial booting of VoiceFinder 2120 Gateway.

```
System Boot Loader, Version 1.3.1/0
Copyright (c) by AddPac Technology Co., Ltd. Since 1999.

System Flash Memory is 4 Mbytes.
1 Ethernet/IEEE 802.3 Interface (100BaseTX).
1 Ethernet networks interface.
1 RS232 Ethernet console interface.

VoiceFinder Router Series (AP2120)
Ethernet Number: AP2120-ffff55
MPC855T 50MHz With 33554432 Bytes System Memory
524288 Bytes System Flash Memory
4194304 Bytes 2nd System Flash Memory
DS1742 Timekeeping RAM

1 RS232 Ethernet Console Interface
1 Ethernet/IEEE 802.3 Interface
1 Ethernet Networks Interface

AP2120 System software Revision 5.44
Released at Jun 5 14:25:32 2001
Program is 3012088 bytes, checksum is 0xd976800

Local Time   : Mon Jul  9 11:07:14 2001

Copyright (c) by AddPac Technology Co., Ltd. Since 1999.

The System is ready. Please login to system.
login:
```

[Figure 3-2 Initial message of VoiceFinder AP2120 Gateway]

3.2. Environment Configuration

Information



The Gateway requires various environment parameters according to the applications. This section provides important information for using the Gateway, so the users are highly advised to check the following procedures before configuring the Gateway.

- Clarify the network address according to the IP protocol with the network diagram.
- Select a proper routing protocol. (e.g. Static, Default etc.) Consulting with the administrator of the connecting network is recommended.
- Determine the protocol to use with each LAN 1(WAN) port. (e.g. PPPoE, Ethernet etc.)
- When the conditions above are determined, thoroughly understand the related commands.

Environment configuration is required only once at initial installation. But when the network components have changed, it should be reconfigured. After configuration change, always save the settings to prevent loss of data when switching the power on/off.

In order to log in an unconfigured Gateway, the user must use the default username and password. The user access authority for VoiceFinder 2120 is divided into 4 levels : admin, high, normal, low. All users, other than Admin have "1router>" prompt at log-in stage.

The user must log-in at admin level for Gateway configuration. **The default username and password for admin level log-in is "root" and "router". After logging-in as admin level, the prompt is changed into "1Gateway#" and is allowed to change the configuration.**

VoiceFinder 2120 environment configuration is divided into two parts : Global Configuration, which effects the whole Gateway, and Interface Configuration, which effects only the certain interface. By function, configuration is divided into: "User and Gateway Management", "Interface Configuration", "Routing and Bridging Configuration", and "System Status and Debugging Configuration".

This manual describes configuration according to its functions.

3.2.1. User and Gateway Management Environment

The Gateway may be accessed through console connection or telnet. VoiceFinder AP2120 Gateway allows 1 connection through console session, and 512 connections through application sessions such as telnet, FTP, SNMP, etc. The sessions may effect the Gateway's performance, therefore the user is advised not to connect more than 10 sessionsn at the same time.

At User and Gateway Management Environment, the user password can be configured. The default username for VoiceFinder AP2120 Gateway is "root" and its password is "router". (This default setting is for "admin" level access.) When the Gateway configuration is completed, pleaes change the password. This is to prevent unauthorized users from reconfiguring the Gateway. VoiceFinder AP2120 Gateway saves the password and the configuration in a safety area.

Also, the commands related to Gateway software upgrade and system administration such as configuration saving and backup can be used.

It also provides commands for monitoring the system status. These include commands for displaying CPU resource availability, Debugging commands to show packets received and dispatched by the Gateway, and Show commands to show the configuration status.

3.2.2. Interface Configuration Environment

In order to communicate in Ethernet and WAN(LAN or HomePNA Port) environment, an IP address must be assigned for each port. For commands related to IP address configuration, refer to interface related commands. For WAN(Ethernet) port, configuration for lower level protocols is required as well as IP address.

All the WAN (Ethernet) ports of VoiceFinder AP2120 are used as LAN port and Ethernet/PPPoE are used as Layer 2 protocol. In order to connect to the network, the WAN protocol must be matched with the one used at the other equipment, including configuration variables. Referring to the administrator of the other equipment is recommended.

The Interface configuration mode allows traffic management of particular packets per interface. For security related Access-List and DHCP information, refer to the "Configurations for Security and Internet" section.

For packet management information, refer to the "Routing Configuration" section.

3.2.3. Routing Configuration Environment

VoiceFinder 12120 Gateway supports Static, RIP v1/v2, OSPF v2 routing protocols. The routing protocol is responsible for assignment of packet route, and VoiceFinder AP2120 supports multi-protocols simultaneously. Therefore it is required to configure which protocol to use for each interface. Refer to "Routing Configuration Environment" and "Interface Configuration Environment".

Refer to "route static" for Static routing, "route rip" for RIP routing and "route ospf" for OSPF routing.

3.2.4. Security and Internet Configuration Environment

VoiceFinder AP2120 Gateway supports additional functions for security and internet environment.

It includes Packet Filtering, Access-List, NAT(Network Address Translation), PAT(Port Address Translation) and Multi-Level account for security and DHCP server, client and relay for internet connection. Refer to Chapter 4 for more details

3.2.5. System Status and Debugging Environment

VoiceFinder AP2120 Gateway supports "Show" command for checking the system operation status and "Debug" command for locating system errors. "Show" commands provides information about not only the status of interface, but also the status for NAT configuration, Access-list, DHCP, registered user, buffers and all other configurations for the Gateway.

"debug" command provides information regarding proper operation of the Gateway by displaying operating TCP/IP terminal screen.

or Layer 2 on the

For more details, refer to Chapter 4.

3.2.6. Voice Integration Configuration Environment

VoiceFinder AP2120 Gateway supports integration of voice applications and data. VoiceFinder AP2120 Gateway provides configuration and monitoring of voice and fax connection, voice gateway, quality of voice control, PABX connection, and other related parameters.

For detailed information, refer to Chapter 5 "Voice Configuration and Related Commands".

Chapter 4 Gateway Configuration and Commands

This chapter describes how to configure VoiceFinder AP2120 Gateway and related commands.

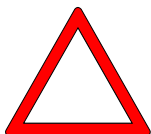
4.1. Gateway Booting

The user can use all commands of AP2120 through the consol or Telnet connection.

When power is supplied, the Gateway is booted as described below. :

- The Gateway performs a self-test and checks basic operations of the CPU, the memory and interfaces.
- The boot loader is executed, and the boot loader seeks for proper Gateway software image files. The boot loader loads Gateway software from the flash memory.
- If the boot loader can not find proper Gateway software image file from the flash memory, the boot loader stands by in the boot mode until it receives proper Gateway software from the system. (At this time, the boot loader can download Gateway software through TFTP or FTP protocol.)
- When Gateway software is loaded, Gateway starts to operate according to configuration information. However, if there is no configuration information, the Gateway operates according to the default values, and in this case, the operator shall set up related items for normal operation of the network.

Caution



When booting the system, set Gateway environment and save configuration information with "copy running-config" command.

If the system is normally booted, the following message will appear.

```
System Boot Loader, Version 1.3.1/0
Copyright (c) by AddPac Technology Co., Ltd. Since 1999.

System Flash Memory is 4 Mbytes.
1 Ethernet/IEEE 802.3 Interface (100BaseTX).
1 Ethernet networks interface.
1 RS232 Ethernet console interface.

VoiceFinder Router Series (AP2120)
Ethernet Number: AP2120-ffff55
MPC855T 50MHz With 33554432 Bytes System Memory
524288 Bytes System Flash Memory
4194304 Bytes 2nd System Flash Memory
DS1742 Timekeeping RAM

1 RS232 Ethernet Console Interface
1 Ethernet/IEEE 802.3 Interface
1 Ethernet Networks Interface

AP2120 System software Revision 5.44
Released at Jun 5 14:25:32 2001
Program is 3012088 bytes, checksum is 0xd976800

Local Time   : Mon Jul  9 11:48:44 2001

Copyright (c) by AddPac Technology Co., Ltd. Since 1999.

The System is ready. Please login to system.
login: root
```

```
password:  
AP2120 - Login : root at Console on Mon Jul  9 11:48:54 2001  
  
1 router#
```

[Figure 4-1 System Boot Loader]

4.2. Commands

The operator can use all commands of VoiceFinder AP2120 Gateway through the consol or Telnet terminal (VTY100 terminal.)

There are three kinds of commands – commands of the user mode, commands of the manager mode and commands of the configuration mode. Commands of the user mode enable the operator to check limited information of the system and provide a connection function for data communication. Commands of the manager enable the operator to check configuration status of the Gateway and perform debugging. Also commands of the configuration mode enable the operator to change configuration environment and set new environment.

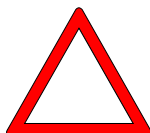
VoiceFinder AP2120 Gateway has following features regarding entering commands.

- Although the operator enters only a part of the command, AP2120 automatically recognizes the whole command. For example, if the operator enters only "sh" or "sho" instead of "show", AP2120 automatically recognizes "sh" or "sho" as "show."
- VoiceFinder AP2120 Gateway provides an online help function so the user can check related information of the command and command syntax.
- VoiceFinder AP2120 Gateway provides "More" function that divides a long message into several messages.
- VoiceFinder AP2120 Gateway provides Help and "?" functions to display available commands for the mode and descriptions of the commands.
- VoiceFinder AP2120 Gateway provides "History" function. With the history function, the operator does not need to enter the command that used before. Instead, the operator only needs to use the numbers on the

Gateway prompt.

- There are three modes for the Gateway commands, and in each mode, different commands are used. The following describes commands in each mode.

Caution

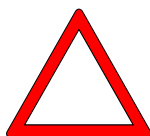


The commands indicated with "*" among the optional commands are not currently supported. They are to be supported in the higher version Gateways.

Ex.) router# clear ?

counters	Clear counters on one or all interfaces
*interface	Clear the hardware logic on an interface
logging	Clear logging buffer
utilization	Clear system usage information

Caution



To cancel commands, use "no" command. If the operator uses "no" command for the commands that have default values, the optional values will be returned to the default values.

Ex.) router(config)# no ?

access-list	: Add an access list entry
arp	: Remove a static ARP entry
bridge	: Set bridge Parameter to default value
dhcp-list	: Configure list entry
ethernet	: Configure ethernet
hostname	: Set system's network name
interface	: Select an interface to configure
ip	: Set Ip routing mode
logging	: Modify message logging facilities
nat-list	: List NAT(Network Address Translation) lists
queue-list	: Build a custom queue list
route	: Establish static routes
router	: Enable a routing process
service	: Modify use of network based services

snmp	: Set SNMP community/configuration information
user	: Remove router user
utilization	: System resource using information

4.2.1. Commands of the User Mode

Any person who logged in the Gateway can use commands of the user mode.

The prompts is indicated as "1router >" in the user mode.

Command	Description
?	Displays commands and their description currently available.
clock	Diaplys system time.
exit	Logs out the operator from the Gateway.
help	Explains how to use the command in an interactive way.
history	Shows history of the previously used commands.
ping	Sends an echo message to another network device and tests if the echo message reaches the destination.
rlogin	Establishes rlogin connection that is similar to the Telnet by an original login.
show	Shows configuration status and operating status of the Gateway. However, in the user mode, "show" command shows only limited information.
telnet	Establishes a protocol connection to log in a neighboring network device through a virtual terminal.
traceroute	Traces the path of the packet to the destination.
user	Adds a Gateway user or shows user information of the Gateway. With this command, the current user cannot check information of the user who has higher authority than him/herself.

[Table 4-1 Commands of the user mode]

4.2.2. Commands of the Manager Mode

The device manager who logged in the Gateway can use commands of the manager mode. To use commands of the manager mode, the user shall log in the Gateway with the root account or manager's ID. Only the manager can return to the configuration mode of the Gateway. In the manager mode, commands usually show more information than in the user mode according to the options. For example, "show" command shows more information in the manager mode than in the user mode.

In the manager mode, the manager can use commands that are used in the user mode.

The prompt is indicated as "1router#" in the manager mode.

Commands	Description
?	Displays commands and their description currently available.
clear	Clears statistical data saved in the Gateway.
clock	Displays system time.
configure	Enters into the system configuration mode.
copy	Saves configuration data that is currently used in the non-volatile memory of the system.
debug	Displays packets and other information of the system for system debugging. Be careful with this command since it can increase system load. (See "un-debug" command.)
exit	Logs out the operator from the Gateway.
help	Explains how to use the command in an interactive way.
history	Shows history of the previously used command.
load	VoIP related command. Loads the VoIP configuration script file to the VoIP Configuration of the Gateway.
no	Cancels previously executed commands or returns into default values.

ping	Sends an echo message to another network device and tests if the echo message reaches the destination.
reboot	Reboots the system.
rlogin	Establishes remote login 'rlogin' connection that is similar to Telnet
save	VoIP Command. Makes VoIP Configuration Script File uses Gateway VoIP Running Configuration.
show	Shows configuration status and operating status of the Gateway.
telnet	Logs in a neighboring network device through a virtual terminal.
test	Tests sub-systems of the Gateway – the memory, interfaces and so on.
traceroute	Traces the path of the packet to a certain destination.
who	Checks users who are currently online in the Gateway, login method and login time.
write	Saves the Gateway configuration file.
undebug	Stops execution of "debug" command.
user	Adds a Gateway user or shows user information of the Gateway. With this command, the current user cannot check information of the user who has higher authority than him/herself.

[Table 4-2 Commands of the manager mode]

4.2.3. Commands of the Configuration Mode

Only the user with the root account or equivalent authorities can access to the configuration mode. In the configuration mode, the user can change the existing configuration of the Gateway and make a new configuration of the Gateway. The configuration mode can be divided into two modes – the interface Configuration mode and the Global Configuration mode.

The prompt is indicated as "router(config)#" in the global configuration mode. In the global configuration mode, the user can make any configuration related to the Gateway except the interface configuration. And in the interface configuration mode, the user can make any configuration relating to the interface – IP address configuration, WAN protocol configuration and so on.

The prompt is indicates as "router(config-Ethernet0)" in the interface configuration mode.

4.2.3.1. Global Configuration (config) Commands

Command	Description
access-list	Creates the access-list. From #0 to #29 are covered by the standard access-list, and from #30 to #59 are covered by the extended access-list.
account-list	A configuration command to use the IP account.
arp	Adds or deletes a certain Ethernet address in the ARP table.
bridge	Sets bridge related items.
clock	Sets system time of the Gateway.
debug-port	Displays debug message into remote telnet terminal.
dhcp-list	Enables the Gateway to function as a DHCP server or send a DHCP packet broadcasting to other Gateways.
dial-peer	Sets dial-peer with "VoIP" command.

exit	Goes to the previous mode.
gateway	Makes voice gateway related configuration with "VoIP" command.
help	Explains command-using method in an interactive way.
history	Shows history of the used command lines.
hostname	Changes the Gateway name of the network.
Interface	Enters into the interface configuration mode or creates a logical interface.
ip	Enables IP routing.
kill	Disconnects a certain Telnet session in the Telnet process.
logging	Changes or sets the message logging function.
nat-list	Creates Network Address Translation (NAT.)
no	Cancels commands entered in the command line or returns commands into default values.
num-exp	Sets a phone number extension in the VoIP.
queue-list	Creates a queue-list to set the custom queue.
route	Adds or deletes static routes.
router	Enables a routing processor to use routing protocol.
service	Sets network-based service configuration – SNMP, Telnet, FTP and TFTP.
snmp	Sets "SNMP" command related items.
traceroute	Execute traceroute
translation-rule	Set translation rules in VoIP Service.
ttl	Changes Time-To-Live (TTL) value.
user	Registers or changes Gateway users.
utilization	An optional command to set time intervals to check availabilities of the CPU, the Ethernet and the serial.
voice	Sets VoIP Service or Available Codecs.
voice-port	Sets the VoIP port.
voip-interface	Sets the VoIP Interface.

[Table 4-3 Global Configuration commands]

4.2.3.2. Commands of the Interface Configuration Mode 1

In the interface configuration mode, the user needs to define a certain interface before starting configuration.

* For voice related interface commands, see Chapter 5.

Command	Description
arp	Adds or deletes an Ethernet address from ARP table. (for Ethernet interface)
bridge	Sets the bridge parameters.
clock	To use gateway interface as DCE mode, set the colock speed of DCE. (For Ethernet interface)
encapsulation	Sets and changes the encapsulation method of the interface.
exit	Returns to the previous (configuration) menu.
end	Returns to the initial (Exec) mode.
frame-relay	Sets Frame-Relay for WAN(ETHERNET) port.
help	Explains how to use the commands in an interactive way.
history	Shows history of the previously used commands.
Interface	Selects an interface to set additional interface.
ip	Sets IP protocol and IP service related items.
no	Cancels commands executed or returns to default values.
mtu	Sets the size of the IP Maximum Transmission Unit (MTU.)
ppp	Sets PPP protocol related parameters.
shutdown	Shuts down the selected interfaces.

[Table 4-4 Commands of the Interface Configuration Mode 1]

4.2.3.3. Commands of the Interface Configuration Mode 2

The user can use IP related commands in the selected interface. The prompt is indicated as "router(config-Ethernet0-ip)#".

Command	Description
access-group	applies the access-list that has been set in the global configuration environment to the interface.
address	Sets or changes the IP address of the Interface.
dhcp-group	applies the DHCP-list that has been set in the global configuration environment to the interface.
exit	Returns to the previous (configuration) menu.
end	Returns to the initial (Exec) mode.
help	Explains who to user commands in an interactive way.
history	Shows history of the previously used commands.
nat-group	applies the NAT-list that has been set in the global configuration environment to the interface.
no	Cancels the environment parameters that have been set in the configuration mode or returns them to the default values.
ospf	Sets environment parameters of OSPF routing.
proxy-arp	Enables IP proxy ARP for the corresponding interface
queue-group	Applies the queue-list that has been set in the global configuration environment to the interface.
rip	Set environment parameters of RIP routing.
secondary	Sets or changes the secondary IP address of the interface.

[Table 4-5 Commands of the Interface Configuration Mode 2]

4.3. Starting Gateway Configuration

To set up the Gateway, log in as the configuration mode. To log in as the configuration mode, the user shall know the manager password. If the user does not know proper commands, use "Help" command.

[Procedures]

Order	Operation and Related Commands
1	Boot the Gateway and log in with the manager's account.
2	Move to the configuration mode. 1 router# <i>configure</i> 2 router(config)#

[Example] Starting Gateway Configuration Mode

```
The System is ready. Please login to system.
login: root  ➤ Enter the manager's ID. (The manager's ID is set as
"root" in the factory.)
password:*****  ➤ Enter the password. (The password is set as
"router" in the factory.)
AP2120 Login : root at Console on Thu Jan 11 11:28:34 2001
1 router#configure  ➤ Enter the command to move to the configuration
mode.
1 router(config)#  ➤ Configuration is possible in this mode.
```


4.4. Ethernet Configuration

4.4.1. Ethernet basic configuration

The Ethernet port of VoiceFinderAP2120 Gateway basically supports RJ-45. However, if the connection device of the other side supports only the AUI port, 10 Base-T Medial Attach Unit (MAU) shall be used in the other side. The Ethernet of VoiceFinderAP2120 Gateway uses the standard ARPA encapsulation method as default. However, if necessary, the network manager can use SNAP or IEEE 802.3 encapsulation method.

The Ethernet of VoiceFinderAP2120 Gateway can be separated logically. If the user wishes to use only one Ethernet port, the user must designate the logical port.

Follow as shown below to use Ethernet.

[Procedure]

Order	Operation
1	Enter into the interface configuration mode.
2	Enter into the IP configuration mode.
3	Assign IP address to the interface.
4	Designate the encapsulation method to use (if necessary.)
5	Make the interface up.
6	Set other necessary optional parameters.

[Related Commands and Syntax]

- **Ethernet full-duplex**
 - 1.Sets the operation mode of the Ethernet interface.
 - 2.The default is half-duplex.

- **interface { ethernet / Ethernet } { 0 / 1 },[logical I/F #]**
 1. Selects the interface to set up and enters into the interface configuration mode.
 2. {0/1} represents the main interface while [logical I/F #] represents the sub-interface.
 3. The Ethernet shall be set as a sub-interface, and if the manager needs to use the frame-relay encapsulation, the serial interface can use a sub-interface.

- **ip**

Select the interface and move to IP configuration mode.

- **address <ip_address> <net_mask>**
 1. Sets the IP address for the selected interface.
 2. One of sub-commands of "ip" command

- **secondary <ip_address>**
 1. Sets Secondary IP Address
 2. *This command is different from the secondary IP address of other gateways. The secondary IP address of AP2120 can only use the same Subnet address of that of Primary IP address.*
 3. *To set Secondary IP, configure Logical Interface and set the secondary IP to the interface.*

[Example] Ethernet Configuration (Start)

When operating with "Primary IP: 192.20.1.1/24bits, Secondary IP: 210.10.2.1/24Bits"

```
1router(config)# interface ethernet 0 0
2router(config-ether0.0)# ip
3router(config-ether0.0-ip)# address 192.20.1.1 255.255.255.0
4router(config-ether0.0-ip)# exit
5router(config-ether0.0)# interface ethernet 0 1
6router(config-ether0.1)# ip
7router(config-ether0.1-ip)# address 210.10.2.1 255.255.255.0
```

- **encapsulation {ethernet/ieee/vlan}**
 - 1.An optional command to change the encapsulation method for the current Ethernet interface
 - 2.The default is "Ethernet".
 - 3.VLAN supports 802.1Q VLAN.
- **mtu <mtu-size>**
 - 1.Sets the MTU size for the current interface.
 - 2.The default is 1,500 Bytes.
- **arp request <ip-address>**

Forces the Gateway to send the ARP (MAC) request for the corresponding address. (Usually used for the test.)
- **arp static <ip-address> <hardware(MAC)-address>**

Forcefully registers information about the IP address and the its hardware address in the ARP table.
- **arp table-size <table-size>**
 - 1.Defines the size of the ARP table for the corresponding interface.
 - 2.The default is 50. The size of the ARP table can be changed between 10

and 256. Adjust the size of the ARP table according to the number of PCs or terminals connected to the network.

- **shutdown / no shutdown**

1. Up/Down current Interface.
2. For Ethernet interface, main Interface cannot be shutdown. To Up/Down certain Ethernet Interface, configure its sub-interface.

- **no interface <if-name>**

Removes Logical interface. "If-name" is "logical Interface Name".

- **show interface <if-name>**

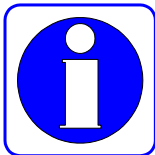
Shows the interface status of "if-name."

[Example] Ethernet Configuration

```
router(config)#interface ethernet 0.0  ⚡  ⚡  Creat Logical
interface "Ethernet 0.0" under Main interface " Ethernet 0" and
move to the Logical interface.
router(config-ethernet0.0)#  ⚡  ⚡  The configuration for e0.0 is
possible.
router(config-ethernet0.0)# ip  ⚡  ⚡  Move to IP configuration
mode.
router(config-ethernet0.0-ip)#address          131.12.1.1
255.255.0.0  ⚡  ⚡  Set the IP address as" 131.12.1.1/16bit mask".
router(config-ethernet0.0-ip)#secondary 131.13.1.1  ⚡  ⚡  Set
the Secondary IP address as "131.13.1.1".
router(config-ethernet0.0-ip)#exit  ⚡  ⚡  Move to Inerface
configuration mode.
router(config-ethernet0.0)#no shutdown  ⚡  ⚡  Up the inetface. *
If the Main is "Up", the sub-intefaces becomes "Up" automatically.
router(config-ethernet0.0)# mtu 2000  ⚡  ⚡  Set MTU Size as
"2000Byte".
router(config-ethernet0.0)#end  ⚡  ⚡  Exit from the configuration
mode.
router#show interface ethernet 0 0
      Interface Configuration Information for ethernet
      (131.12.1.1)
      Network = 130.100.0.0  NetMask      = 255.255.0.0
      SubNetwork = 130.100.0.0  SubNetMask = 255.255.0.0
      Administrator Status = UP  Operation Status = UP
      Ethernet CSMA-CD  Speed - 10 Mbps
      MTU = 1500  Hareware Address = 00 00 00 00 00 42
      Secondary addresses : NONE
router#
```

4.4.2. PPPoE Configuration

Information



Point to Point Protocol (PPP) is one of standard protocol to send data through the WAN link. RFC1661 describes PPP specifications. Not only in the synchronous WAN (serial) line but also in the asynchronous WAN (dial up line,) PPP can be used. Since PPP is a standard rules, it guarantees interoperability among different manufacturers' devices.

Nowadays PPP extended to not only Serial Line but also Ethernet and ATM Lines. PPPoE(PPP over Ethernet) means PPP Protocol in the Ethernet Line.

VoiceFinder AP21200 Gateway can be installed under ADSL modem. In this case, AP2120 supports PPP and the Ethernet Interface Encapsulation is "PPPoE".

PPP consists of two kinds of protocol as follows:

- Link Control Protocol (LCP): LCP decides the encapsulation format, limits the packet size, performs authentication in the link, decides normal operation time and breakdown time, detects loop-back link faults and other faults, and automatically terminates the link.
- Network Control Protocol (NCP): NCP communicates with various higher layer (network layer) protocols.

If a PPP encapsulation option is given to VoiceFinder AP2120 Gateway, PPPoE is activated. Current software installed in the Gateway supports Challenge Handshake Authentication Protocol (CHAP), the authentication option that uses Password Authentication Protocol (PAP,) and the magic number configuration option. The software always sends the magic number configuration option, but sends the authentication option only when the authentication option is set.

[Procedures]

Order	Operation
1	Enter into the interface configuration mode.
2	Give PPP encapsulation protocol to the interface.
3	Give an IP address to the interface.
4	Enable CHAP or PAP authentication. (Optional)
5	Set CHAP or PAP parameters. (Optional)
6	Set PPP default peer IP. (Optional)
7	(If necessary) use "debug" command to check if the Gateway is normally operating.
8	Make the interface up.
9	With "show interface" command, check if the interface is normally operating.
10	(For abnormal operation) find faults and recover faults with "debug" command.

[Related Commands and Syntax]

- **interface { ethernet / loopback / null } { 0 / 1 }**

Select the interface to set up and enters into the interface configuration mode.

- **encapsulation { Ethernet / ieee / vlan / pppoe }**

Set the serial encapsulation mode for the interface

- **ip address <ip_address> <net_mask>**

Assign IP address for the selected interface. To assign IP dynamically with PPPoE, the IP address is not required to assign.

- **user add <username> <password> {admin/high/normal/low}**

1. Set the login name and the password to authenticate a Gateway that is trying to access to another Gateway that function as a PPP PAP/CHAP server.

2. This command functions same as the command that the Gateway manager uses to register a login user. This is because the Gateway shares the PPP registered user database and the Gateway user database. The operator registers users as using the same command.
3. The difference from the registration of Gateway users is that "user add" command does not use the registered user level for PPP connection in the user registration.

- **ppp authentication {chap/pap} [callin/{pap/chap}]**

1. Set the PPP authentication method as CHAP or PAP in the interface configuration mode.
2. The "callin" option is to connect only incoming calls with CHAP authentication.
3. {pap/CHAP} option is to respond to the calls which request both of CHAP and PAP authentication..

- **ppp chap hostname *name***

1. This command is for PPP client devices. This command registers a user name to request connection to the PPP server device when using PPP CHAP authentication. (An optional command for CHAP authentication))
2. If this command is not used, the Gateway name (displayed in the Gateway prompt) will be considered as the user name.

- **ppp chap password *password***

This command is for PPP client devices. This command registers a password to request connection to the PPP server device when using PPP CHAP authentication. (An optional command for CHAP authentication)

- **ppp pap sent-username *username* password *password***

Sets PAP authentication in the PPP client device. When the client device makes a PPP call, the client device sends the user name and the password to the server for authentication. At this time, the user name and the password shall be the same with those set in the server. (An optional command for PAP authentication)

- **ppp peer default-ip-address <ip-address>**
 1. Sets the Gateway as a PPP server and the IP address to allocate to the serial interface of the other side. (An optional command)
 2. When the Gateway receives the IP address, the Gateway decides the subnet mask of the IP address that it received based on the IP subnet of its local interface.

- **ppp timeout <second>**
 1. Sets PPP negotiation timeout for PPP negotiation between two Gateways.
(An optional command)
 2. The default is 5 seconds.

- **shutdown / no shutdown**

An optional command to make the current interface up/down.

- **show interface <if-name>**

Shows the interface status of "if-name."

- **debug ppp { chap/error/negotiation/packet }**
 1. Decodes PPP low level packets.
 2. "CHAP" option decodes challenge authentication related information.
 3. "Error" option decodes PPP protocol level errors and error statistics.
 4. "Negotiation" option decodes LCP and NCP protocol to set the PPP link.
 5. "Packet" option decodes PPP low level packets.

[Example] Normal PPP Configuration and Usage

```
Router# configuration  ⚡ Enters into the configuration mode
Router(config)#interface ethernet 0.  ⚡ Enters into the interface
configuration mode.
Router(config-ether0.0)#  ⚡ Configuration is possible in this
mode.
Router(config-ether0.0)# encapsulation ppp  ⚡ Sets the PPP mode
Router(config-ether0.0)# ip address 131.12.1.1 255.255.0.0
⚡ Sets the IP address as "131.12.1.1/ 16 bit mask".
Router(config-ether0.0)# no shutdown  ⚡ Makes the interface up.
Router(config-ether0.0)# end  ⚡ Exits from the configuration
menu.

Router # show interface ethernet 0  ⚡ Checks the status of the
serial interface 0.

router# sh int e 0 0
Interface : ether0.0

IP Address:211.238.72.221  Physical Inteface : Ethernet0
Network : 211.238.72.0      Subnet Mask : 255.255.255.0
Administrator Status : UP   Operation Status : UP
Network Type : Ethernet    MTU : 1500
Hardware Address : 00 02 a4 01 01 02

Ethernet0 is UP, Line protocol is UP
bandwidth : 10000 Kbit
operating mode : HALF-DUPLEX
operating speed : 10 Mbps
last 1 minute data rate : tx 0 bps, rx 728 bps
input : 95305 packets, 8979269 bytes, 0 no buffers
error : 0 (0 length, 0 align, 0 short,
        0 crc, 0 overrun, 0 collision)
output: 3 packets, 288 bytes, 0 drop
error : 0 (0 underrun 0 deferred 0 collision)
```

[Example] Additional Commands for PAP Configuration (Server)

If the Gateway functions as a server, it means AP2120 Gateway functions as the PPP authentication server.

```
Router(config)# user ADDPAC password ADDPACRouter1 normal
Registers the user name (addpac) and the password (Router1) with the
normal priority in the server.

Router (config)#interface ethernet 0.0
Enters into the
interface configuration mode.

Router(config-ether0.0)# encapsulation ppp
Sets the PPP mode.

Router(config-ether0.0)# ppp authentication pap
Sets the PPP
authentication mode as PAP for the ethernet0.0 interface.

Router(config-ether0.0)# ip address 132.12.1.1 255.255.255.0
Sets the IP address as "130.1.1.1" and the subnet mask as "24Bit."

Router(config-ether0.0)# ppp peer default-ip address
132.12.1.2
When the other Router receives the serial interface
IP from this Gateway, this command enables the Gateway to provide
default address (130.1.1.2) to the other Router. (* If an IP address
has been set already in the other Router, the operator does not need
to use this command.)

Router(config-ether0.0)# ppp timeout 100
Sets PPP connection
negotiation timeout value as 100 seconds.

Router(config-ether0.0)# end
Exists from the configuration
menu.

Router # debug ppp packet
Decodes PPP Packet.

Router #
    Ether0.0 LCP: TIMEOUT
    Ether0.0 LCP: O CONFREQ id=1
    Ether0.0 BCP: TIMEOUT
    Ether0.0 BCP: O CONFREQ id=1
    Ether0.0 LCP: TIMEOUT
    Ether0.0 LCP: O CONFREQ id=1
    Ether0.0 BCP: TIMEOUT
    Ether0.0 BCP: O CONFREQ id=1

Router # debug ppp packet
Stops PPP packet debugging.
```

[Example] Additional Commands During PAP Configuration (Client)

This is when AP2120 Gateway is used as a PPP Client on the client side.

```
Router (config)#interface serial 1  ⚡ Enters into the interface
configuration mode.

Router(config-ether0.0)# encapsulation ppp  ⚡ Sets the PPP
mode.

Router(config-ether0.0)# ppp authentication pap  ⚡ Sets the
PPP authentication mode as PAP for the ethernet0.0 interface.

Router(config-ether0.0)# ppp pap sent-username ADDPAC
password ADDPACRouter1  ⚡ Sends the user name and the password
that were are in the server during PPP connection.

Router(config-ether0.0)# ppp timeout 100  ⚡ Sets PPP
connection negotiation timeout value as 100 seconds.

Router(config-ether0.0)# end  ⚡ Exits from the configuration
menu.

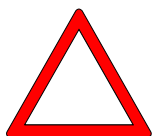
Router # debug ppp packet  ⚡ Decodes PPP Packet.

Router #

      Ether0.0 LCP: TIMEOUT
      Ether0.0 LCP: O CONFREQ id=1
      Ether0.0 BCP: TIMEOUT
      Ether0.0 BCP: O CONFREQ id=1
      Ether0.0 LCP: TIMEOUT
      Ether0.0 LCP: O CONFREQ id=1
      Ether0.0 BCP: TIMEOUT
      Ether0.0 BCP: O CONFREQ id=1

Router # debug ppp packet  ⚡ Stops PPP packet debugging.
```

Caution



If the interface of the Gateway is not configured as DHCP, the IP address must be set in the corresponding interface.

[Example]Additional Commands of CHAP Configuration (Server)

This is when the AP1100 Gateway functions as a PPP authentication server in the server side.

```
Gateway(config)# user ADDPAC password ADDPACGateway1 normal
```

☞ Registers the user name (addpac) and the password (router1) as the normal priority in the server.

```
Gateway (config)#interface ethernet 0.0 ☞ Enters into the interface configuration mode.
```

```
Gateway(config-ether0.0)# encapsulation ppp ☞ Sets the PPP mode.
```

```
Gateway(config-ether0.0)# ppp authentication chap ☞ Sets the PPP authentication mode as CHAP for the ethernet0.0 interface.
```

```
Gateway(config-ether0.0)# ip address 132.12.1.1 255.255.255.0 ☞ Sets the IP address as "130.1.1.1" and the subnet mask as "24Bit."
```

```
Gateway(config-ether0.0)# ppp peer default-ip address 132.12.1.2 ☞ When the other Gateway receives the ethernet interface ID from this Gateway, this command sets the IP address as the default address "130.1.1.2."
```

```
Gateway(config-ether0.0)# ppp timeout 100 ☞ Sets PPP connection negotiation timeout value as 100 seconds.
```

```
Gateway(config-ether0.0)# end ☞ Exits from the configuration menu.
```

```
Gateway # debug ppp packet ☞ Decodes PPP Packet.
```

```
Gateway #
```

```
    Ether0.0 LCP: TIMEOUT
```

```
    Ether0.0 LCP: O CONFREQ id=1
```

```
    Ether0.0 BCP: TIMEOUT
```

```
    Ether0.0 BCP: O CONFREQ id=1
```

```
    Ether0.0 LCP: TIMEOUT
```

```
    Ether0.0 LCP: O CONFREQ id=1
```

```
    Ether0.0 BCP: TIMEOUT
```

```
    Ether0.0 BCP: O CONFREQ id=1
```

```
Gateway # debug ppp packet ☞ Stops PPP packet debugging.
```

[Example] Additional Commands of CHAP Configuration (Client)

This is when AP2120 Gateway functions as a PPP CallIn client in the client side.

```
Gateway (config)#interface Ethernet 0.0 ⚡ Enters into the
interface configuration mode.

Gateway(config-ether0.0)# encapsulation ppp ⚡ Sets the PPP
mode.

Gateway(config-ether0.0)# ppp authentication chap ⚡ Sets the
PPP authentication mode as CHAP for the ethernet0.0 interface.

Gateway(config-ether0.0)# ppp chap hostname ADDPAC ⚡ If the
user name that is saved in the server during PPP CHAP connection is
different from the user name of the client Gateway, this command sends
the user name of the server side.

Gateway(config-ether0.0)# ppp chap password ADDPACGateway ⚡
Sets the user name of the server side to check the password that the
server sends during PPP CHAP connection.

Gateway(config-ether0.0)# ppp timeout 100 ⚡ Sets PPP connection
negotiation timeout value as 100 seconds.

Gateway(config-ether0.0)# end ⚡ Exits from the configuration
menu.

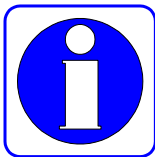
Gateway # debug ppp packet ⚡ Decodes PPP packets.

Gateway #
    Ether0.0 LCP: TIMEOUT
    Ether0.0 LCP: O CONFREQ id=1
    Ether0.0 BCP: TIMEOUT
    Ether0.0 BCP: O CONFREQ id=1

Gateway # debug ppp packet ⚡ Stops PPP packet debugging.
```

4.5. Routing Configuration

Information



VoiceFinder AP2120 Gateway supports static routing protocol and dynamic routing protocol. There are two kinds of dynamic routing protocol – Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP.) IGP is used for routing among the networks in the same manager's domain while EGP is for routing among the networks in different manager's domains. IGP includes RIP, OSPF and IS-IS, and EGP includes BGP. VoiceFinderAP2120 Gateway supports only IGP – RIP and OSPF.

To use routing protocol of VoiceFinderAP2120 Gateway, upload the routing process to the Gateway and designate the network that is going to use the routing process.

It is not easy to select routing protocol for each Gateway. Please note the followings when selecting the routing protocol.

- Network Size and Complexity – Normally, static routing is enough for edge network. However, to perform dynamic routing in a small scale network, use RIP. If the network is large or complex, use OSPF.
- Whether Variable Length Subnet Mask (VLSM) Is Supported or Not – If there are several subnet classes within the network, use routing protocol that support VLSM such as static route, RIP v2 and OSPF.

Besides, the user needs to consider convergence time, reliability needs and Internetwork delay characteristics.

The user can perform several kinds of routing protocol in VoiceFinder AP2120 Gateway at the same time. If several kinds of routing protocol is used in one Gateway, each protocol may have its own path for the same destination. In this case, routing protocol has priority to be displayed in the routing table in the order of static route, OSPF route, RIP route and default route.

4.5.1. Static Routing Configuration

The static route means a route that the manager designates to send the packet from a certain source to a certain destination. The static route is used for the following three cases:

- If routing software cannot create a proper route to send packets to a certain destination.
- If the network is small or is not complex, so it is easy to configure a static route and if the user does not want to have packets such as route update packet resulting load to the network
- If the user wants to send all packets of which destinations do not appear in the routing table to a certain next-hop address using the default route (or gateway of last resort)

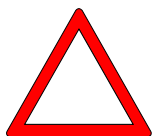
Once a static route is set in the Gateway, the Gateway keeps the static route until the manager forcefully removes that static route. To remove the static route, use "no" command and remove the static route from the route configuration.

The default route is one of static routes and designates the next-hop address of the packet of which destination is not displayed in the routing table. The default route has the least priority in VoiceFinderAP2120 Gateway. Therefore, only when the Gateway does not find any path, the Gateway uses the default route.

[Procedures]

Order	Operation
1	Go to the configuration mode.
2	Enable the static Gateway process.
3	Set the source address and the static route for the destination network.
4	Use "show" command and check if the route is correctly set in the routing table.
5	With "Ping" command, check if the route can reach the network.

Caution



1. The next-hop address of the static route should be the address directly connected with the desired Gateway.
2. The default route is one of static routes, and the setting is same as that of the static route. However, the destination address shall be zero subnet (0.0.0.0 address and 0.0.0.0 mask) in the zero network, and the next-hop address shall be same with that of the static route.

[Related Commands and Syntax]

- **router { static/rip/ospf }**
Enables or disables a certain routing process.
- **route <destination-IP-network> <address-mask> { <next-hop-address> / ethernet / Ethernet / null } [(0/1)/<null_int_#>] [sub_int_#]**
 1. Designates the route to send the packet to the destination address
 2. When using Candidate Default (default route,) both of the destination address and the mask filed shall be zero.
 3. The Gateway should be able to recognize the "next-hop-address"

(directly connected port or where the Gateway can reach through dynamic protocol.)

4. The user can designate an interface port of the Gateway instead of the "next-hop-address."
5. To drop a packet that is headed for a certain destination, use the static route with a null interface.

- **show route**

Check the routes in the routing table.

- **show static**

Check the configured static route.

[Example] Static Routing Configuration and Usage

```
router# config
router(config)# Configuration is possible in this mode.

router(config)# ip routing Enable IP Routing.

router(config)# router static Enable static Routing Process

router(config)# route 130.2.0.0 255.255.0.0 131.20.1.1 Set
the packet, whose destination address is "130.2.0.0/24bit", to go
to address "131.20.1.1".

router(config)# route 0.0.0.0 0.0.0.0 132.20.1.1 Set all
packets, whose address is not listed in routing table, go to the address
"132.20.1.1". (Candidate Default; Setting of Default route)

router(config)# exit Exit from setting mode.

router(config)# show route Show routing table.
```

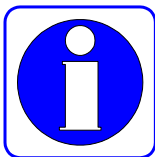
Destination	Network-Mask	Gateway	Cost	Interface	TTL	Protocol
130.1.1.0	255.255.255.0	130.1.1.1	1	Ethernet0	0	DIRECT
130.2.0.0	255.255.0.0	131.20.1.1	1	Ethernet0	0	STATIC
0.0.0.0	0.0.0.0	131.20.1.1	1	Ethernet0	0	STATIC

```
router(config)# show static  Show routing table setted as static
```

Destination	Network-Mask	Gateway	Cost	Interface	TTL	Protocol
130.2.0.0	255.255.0.0	131.20.1.1	1	Ethernet0	0	STATIC
0.0.0.0	0.0.0.0	131.20.1.1	1	Ethernet0	0	STATIC

4.5.2. RIP Configuration

Information



RIP(Routing Information Protocol) is a well-known IGP(Interior Gateway Protocol), which is relatively old but, still generally used. RIP is used for a small-scale and Homogeneous (with single Subnet Mask) network. RIP uses Distance-Vector and is described at RFC 1058.

RIP uses UDP (User Datagram Protocol) Broadcast to exchange routing information and VoiceFinder AP2120 Gateway sends routing information at every 30 sec. If a Gateway cannot receive update packet in 180 sec. from the other Gateway, it recognizes the Gateway is not operable and deletes from the routing table in 240 sec.

RIP uses Hop-Count as Metric (values to indicate the difference of paths to the certain destination). Hop-Count marks as number of Gateways to pass over the route. The Metric of directly connected Gateway is "0" and the max. Metric is "15". (If Metric is "16", it is recognized as "Unreachable" network). Due to this characteristic, RIP is not suitable for a large-scale network.

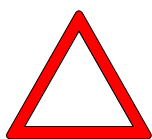
RIP sends Update to the interface designated by the operator. If RIP is not configured at the certain interface, RIP update is not sent to the interface. So to use RIP, configure RIP to the interface.

There is difference between RIP Version 2 and RIP Version 1. RIP v2 supports VLSM (Variable Length Subnet Mask) and can support Heterogeneous network. Also, RIP v2 uses Multicast for routing Update.

[Procedures]

Order	Description
1	Go to the configuration mode.
2	Enable RIP Process.
3	Move to Interface Configuratio mode.
4	Move to IP Configuration mode.
5	Enable RIP protocol for the interface to use RIP (If necessary) Set the RIP Version to use.)
6	(If necessary) Change the RIP configuration.
7	Set other necessary parameters. (EX. authentication).
8	Make the Main Interface 'Up'.
9	Use "show" command and check if the route is correctly set in the routing table.
10	With "Ping" command, check if the route can reach the network.
11	(For abnormal operation) Find and recover faults with "debug" command.

Caution



1. VoiceFinder AP2120 Gateway supports Authentication among RIP Neighbor. (Supports Simple Text type and MD5 Encryption.)
2. VoiceFinder AP2120 Gateway can Enable/Disable the Split-Horizon, Holddown-time, Poison-Reverse of each interface as RIP Option.
3. The RIP version should be defined (Version Define) for each interface. If the version is not defined, it operates as RIP v1.

[Related Commands and Syntax]

- **router { static/rip/ospf }**
Enable/Disable a specific Routing Process.
- **rip send {1/2/12}**
Decide the routing information of a certain interface sent as RIP v1, v2 or v1/v2.
- **rip receive {1/2/12}**
Decide the routing information sent via a certain interface includes only RIP v1, v2 or both v1/v2.
- **rip metric <metric_value>**
 1. Decide RIP Metric (Hop-Counts) regarding routing information sent via a certain interface.
 2. If the RIP Routing Metric is bigger than "16", it is regarded as unreachable network and is dropped from the routing tabl.
- **rip {default-information/static-information}**
 1. When the Gateway sends RIP Routing information, static Route information or Default Route information is Re-Distributed to RIP Process.
 2. With this function, without setting Default/Static Gateway information to all the network devices, all the devices can have the same Route Table by enabling RIP Routing.
- **rip auth-type {simple/md5}**
An option to chooes to use Authentication when sharing Routing informatioin with neighbor Gateways. The administrator needs to choose whether to use simple text type or MD5 Encryption type for the authentication.
- **rip auth-key <key-string>**
When using authentication for sharing Routing information with neighboring

Gateways, the key for authentication should be set. (To use Authentication, the Key must be set. It should be the same value of that of neighbor route.)

- **rip convergence** {split-horizon/hold-down/poison reverse}

Enable options to prevent routing loop such as split-horizon, hold-down timer, poison reverse and etc. Usually, it is recommended to enable all these options. But for HUB of NBMA (Non-broadcast Multi-access) network such as Frame Relay, the split-horizon should be disabled.

- **show route**

Show the route of the routing table.

- **show router**

Show the enabled Routing Process.

- **show rip**

Show the RIP condition of each interface.

- **debug rip**

Decode and show the RIP Packet of the Gateway.

[Example] RIP configuration and usage

```
router# config
router(config)# ip routing  ⓘ Enable IP routing.

Router(config)# router rip  ⓘ Enble RIP Process.

Router(config)# interface ethernet 0.0  ⓘ Enter into the
configuration environment of sub interface 0 of Ethernet interface
0.

Router(config-ether0.0)# ip  ⓘ Enter into IP configuration mode.

Router(config-ether0.0-ip)# rip send 12  ⓘ Sends advertise packet
with RIP v1/v2 protocol.

Router(config-ether0.0-ip)# rip receive 1  ⓘ Receive only PRI
V1 packet among advertise packets.

Router(config-ether0.0-ip)# rip auth-type simple  ⓘ Set simple
authentication for sharing RIP information.

Router(config-ether0.0-ip)# rip convergence split-horizon  ⓘ
From RIP Process, enable Split-Horizon for Convergence Mechanism.

Router(config-ether0.0-ip)# rip convergence poison-revers  ⓘ
From RIP Process, enable poison-reverse for Convergence Mechanism.

Router(config-ether0.0-ip)# end  ⓘ Exit from the configuration
mode.

Router # show router  ⓘ Show enabled Routing Process.

      Current Routing Information :
      OSPF(Open Shortest Path First) : DISABLE
      RIP(Routing Information Protocol) : ENABLE
      Static Routing : ENABLE

Router # show rip  ⓘ Show the configured RIP Process.

      RIP Configuration : Ethernet0

      IP address : 121.1.1.1   Subnet-Mask : 255.255.255.0
      Metric : 0       Send : v1/v2  Recv : v1/v2
      Auth Type : NONE       Ayth Key :
      Convergence Type : split-horizon
```


Default/Static Information : DISABLE / DISABLE

RIP Configuration : ether0.0

IP address : 135.14.1.2 Subnet-Mask : 255.255.255.0

Metric : 0 Send : NONE Recv : NONE

Auth Type : SIMPLE Ayth Key : router

Convergence Type : split-horizon poison-reverse

Default/Static Information : DISABLE / DISABLE

RIP Configuration : ether0.1

IP address : 0.0.0.0 Subnet-Mask : 255.255.255.255

Metric : 0 Send : NONE Recv : NONE

Auth Type : NONE Ayth Key :

Convergence Type : split-horizon

Default/Static Information : DISABLE / DISABLE

RIP Debug Configuration : DISABLE

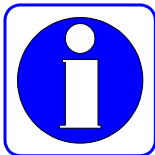
Router # show route  Show the Routing Table.

Destination	Network-Mask	Gateway	Interface	Protocol
121.1.1.0	255.255.255.0	121.1.1.1	Ethernet0	DIRECT
140.1.1.0	255.255.255.0	0.0.0.0	ether0.1	STATIC
131.12.1.0	255.255.255.0	131.12.1.1	Ethernet0.1	DIRECT
135.14.1.0	255.255.255.0	135.14.1.2	ether0.0	DIRECT

Router # debug rip  Decode and show RIP Packet.

4.5.3. OSPF Configuration

Information



OSPF(Open Shortest Path First) is IGP (Interior Gateway Protocol) using Link State Algorithm developed by OSPF Working Group of IETF(Internet Engineering Task Force). OSPF is designed to support IP network with tagging of routing information of sub-network. Also, it offers Packet Authentication with neighbor gateways and utilizes IP multicase when sharing Routing information packet.

VoiceFinder AP2120 Gateway support OSOPF Version 2 described at Internet RFC 1583. The below describes OSPF functions of VoiceFinder AP2120 Gateway

- Stub Area : Supports definition of Stub Area.
- Route Redistribution : Redistribute Routing information of IP routing protocol to other routing protocols.
- Authentication : Supports Plain Text and MD5 Authentication among Neighboring Gateways in an area.
- Routing Interface Parameter : The administrator can configure interface parameters such as Interface output cost, retransmission interval, interface transmit delay, router priority authentication key.
- ABR (Area Boarder Router) : It supports Area Border Routers function when a Gateway exists on two different OSPF areas.

Network with OSPF has several Area include Back-bone area in one routing domain.

- Routing domain: An area where routing is processed with one routing protocol. If a network with different routing protocol is connected, it is regarded as outside network by OSPF. One (1) OSPF routing doman consists of one back-bone Area and several Areas.
- Area : a combination of several networks, and each Area has network diagram called condition database. All the gateways at the same area has the same condition database. These Areas can communicate with

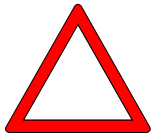
Back-bone Area via ABR(Area Boarder Router). Typically, the Gateway in the Area has Area internal route, other Area route and external routing route. To reduce these routes, it defines Stub Area and keeps only internal Area route.

- Back-bone Area : Area between Areas (Area 0). One OSPF routing domain should have one Back-bone Area, and each Area should be connected to Back-bone Area. If an Area cannot connected to the Back-bone area, it should be connected to the Back-bone area via Virtual Link (OSPF Tunnel).

[Procedure]

Order	Description
1	Move to configuration mode
2	Move to interface configuration mode.
3	Move to IP configuration mode.
4	Enable OSPF protocol for the interface to use OSPF.
5	Set the Area-ID for the interface.
6	Set other necessary parameters (Authentication).
7	Up the Main Interface.
8	Enable OSPF Process.
9	Check the routing table with "Show" command.
10	Check it can be connected to the certain network with "Ping" command.
11	(abnormal operation) With "debug" command, Find out the problem.

Caution



After OSPF configuration, make sure to enable OSPF Process. If not, OSPF might not work properly.

[Related Commands and Syntax]

- **router { static/rip/ospf }**
Enable/ Disable a Routing Process.
- **ospf enable**
Enable OSPF for the interface.
- **ospf area-id <ospf-area-value>**
Set area-id of the interface.
- **ospf cost <cost-value>**
Option to set OSPF cost statically.
- **ospf auth-type { simple/md5 }**
Option to use authentication when sharing routing information among the interface and the gateways in the same Area. The administrator can use Simple Text and MD5 Encryption for the authentication.
- **ospf auth-key <key-string>**
To use authentication when sharing routing information among the interface and the gateways in the same Area, set the Key. (It should be configured to use Authentication and the value should be same with those of gateways at the same area.)
- **ospf auth-id <key-id>**
To use authentication when sharing routing information among the interface and the gateways in the same Area, set the Key identifier. (It should be configured to use Authentication and the value should be same with those of gateways at the same area.)

- **ospf priority** <priority-value>
 1. Set Priority of becoming DR when choosing DR/BDR/Router among the interface and neighboring gateway. The acceptable values are "1~255". The higher the number is, the higher the priority is.
 2. Default value is "1".

- **ospf hello-interval** <interval-time>
 1. To set Hello Interval when establishing Adjacency among the Interface and neighboring gateways. the value should be same with those of gateways at the same area.
 2. Default value is 10 sec. (for Frame-Relay network, the default value is 30 sec.)

- **ospf dead-interval** <interval-time>
 1. To set dead-interval when the neighboring gateway declare 'DEAD'.
 2. Default value is 4 times of "Hello-Interval".

- **ospf poll-interval** <interval-time>
 1. To set Polling packet interval.
 2. Default value is same as Hello-Interval.

- **ospf retransmit-interval** <interval-time>
 1. To set retransmit interval when the gateway lost Link State Advertisement value.
 2. Default value is same as Hello-Interval.

- **ospf default-router**
 1. To notify itself as Default Router to OSPF Network.
 2. It is the same command with Default-information Originate.
 3. It works only when Router is ABR.

- **ospf neighbor** <neighbor_ip_address>
 1. To set Neighbor Statically..
 2. Used for HUB interface at NBMA(Non Broadcasting Multiple Access)

Network such as Frame-Relay Network.

- **ospf network { broadcast / non-broadcast / point-to-multipoint }**

1. To forcefully set Interface character at OSPF
2. Only available for Ethernet Interface.
3. To set Neighbor statically.

- **show route**

Show route on the routing table.

- **show router**

Show Enabled Routing Process.

- **show ospf**

{area/config/debug/interface/lsdb/nbma-nbr/neighbor/nexthop}

1. Check the OSPF condition according to each option.
2. The below describes each option.
 - 1) area : Show information on the area.
 - 2) Config : Show the configuration information.
 - 3) Debug : show the enabled Debugging function.
 - 4) interface : Show the OSPF enabled interface.
 - 5) lsdb : show LSA(Link State Advertisement) Database.
 - 6) nbma-nbr : Show neighboring relations established for NBMA Network such as Frame-Relay.
 - 7) neighbor : Show the relationship among Neighboring gateways.
 - 8) nexthop : Show Next-Hop information made by OSPF Process.

- **debug ospf { all/error/event/packet/spf }**

1. Decodes OSPF Packet and show operation information of OSPF.
2. The below describes each Option.
 - 1) all : Enable all debugging information related to OSPF.
 - 2) error : Decode error packet in OSPF Processing.
 - 3) event : Decode Event packet in OSPF Processing.
 - 4) packet : Decode all packet related to OSPF
 - 5) spf : Show SPF(Shortest Path First) related OSPF Events.

[Example] OSPF Configuration and usage

```
router# config
router(config)# ip routing  ➤ Enable IP routing.
router(config)# interface ethernet 0 0  ➤ Move to the
configuration interface of sub-interface 0 of Ethernet Interface
0.
router(config-ether0.0)# ip  ➤ Move to IP configuration mode.
router(config-ether0.0-ip)# address 130.1.1.1
255.255.255.0  ➤ Set the IP address as "130.1.1.1/24bit".
router(config-ether0.0-ip)# ospf enable  ➤ Enable OSPF for
the Interface.
router(config-ether0.0-ip)# ospf area-id 10  ➤ Make
Ethernet Interface belong to OSPF Area 10. With this process,
the network address of the Ethernet Interfaec is included at OSPF
Process area 10.
router(config-ether0.0-ip)# ospf priority 10  ➤ Set the
gateway does negotiation with Priority 10 while selecting DR.
router(config-ether0.0-ip)# ospf cost 5  ➤ Set to advertise
with Cost(metric) of "5".
router(config-ether0.0-ip)# int Ethernet 0  ➤ Move to Ethernet
1 Inerface configuration.
router(config-Ethernet0)# ip  ➤ Move to IP configuration mode.
router(config-Ethernet0-ip)# address 135.1.1.1
255.255.255.0  ➤ Set the IP address as "135.1.1.1/24bit".
router(config-Ethernet0-ip)# ospf enable  ➤ Enable OSPF for
the Interface.
router(config-Ethernet0-ip)# ospf area-id 0  ➤ Make Ethernet
Interface 0 belong to OSPF Area 0. With this process, the network
address of the Ethernet Interfaec is included at OSPF Process area
0.
router(config-Ethernet0-ip)# ospf priority 1  ➤ Set the
gateway does negotiation with Priority 10 while selecting DR.
router(config-Ethernet0-ip)# ospf cost 10  ➤ Set to advertise
```

with Cost(metric) of "10".

router(config-Ethernet0-ip)# ospf network broadcast ➤ Set the interface to work as Broadcast.

router(config-Ethernet0-ip)# exit ➤ Move to the previous configuration mode.

router(config-Ethernet0)# exit ➤ Move to the previous configuration mode.

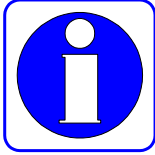
router(config)# router ospf ➤ Enable OSPF for the Interface. OSPF Process is working. Use this command, after finishing OSPF configuration. If there is configuration change while OSPF is processed, disable OSPF with "no router ospf". Then enable OSPF process with "router ospf".

router(config)# exit ➤ Move to Exec mode.

router# copy running-config ➤ Save configuration File.

4.6. Filter (Access-List) Configuration

Information



Packet filtering enables the manager to control packet movement on the network. With the packet filtering function, the manager can prevent unauthorized user's access to the inside network from outside and disclosure of information to outside.

VoiceFinder AP2120 Gateway uses the access-list to control traffic from a certain user (or an equipment or a network) to a certain network (or an equipment.) In this way, the Gateway can permit or deny packets passing through certain interfaces.

There are two kinds of access-list – the standard access-list and the extended access-list. The standard access-list uses IP addresses of the source and the destination in controlling traffic. And the extended access-list uses application port numbers and protocol IDs as well as IP addresses of the source and the destination in controlling traffic. The access-list is a continuous set of permit/deny conditions that are applied to the IP address. Software of VoiceFinderAP2120 Gateway checks theses conditions with each address field of the packet.

With the first condition that matches with the address field, the Gateway decides to accept or reject the packet. After first matching, software stops testing the address. Therefore, orders of conditions are very important for the normal operation the access-list. If there is no matching condition, software rejects the corresponding packet. (Default)

The VoiceFinderAP2120 Gateway supports 30 standard access-lists (List # 0~29) and 30 extended access-list(List # 30 ~ 59.)

[Procedure]

Order	Operation
1	Go to the configuration mode.
2	Create an access-list defining the access-list number and access conditions.
3	Go to the interface configuration mode.
4	Enter into the IP configuration mode.
5	Apply the access-list that has been set to the corresponding interface. Decide where to apply the access conditions – inbound packets or outbound packets.
6	Use "Show access-list" command to check if the access-list has been correctly set.

[Related Commands and Syntax]

Standard IP Access-List: The standard IP address-lists uses only the source IP address in checking the access conditions.

- **access-list** *<access-list-number>* {deny/permit} *<source-address>* *<source wildcard>*
 1. Creates an access-list.
 2. access-list-number: Any number within 0 to 29, source: Source Network Address, Source-wildcard: Inverse mask of the source address
 3. Instead a pair of "source" and "source-wildcard," the user can use a pair of "any (any address)" and "host (a certain address.)"
 4. Wildcard is the inverse mask. For example, if the user writes 132.1.20.1 255.255.255.0 network in a wildcard form, the network will be 132.1.20.1 0.0.0.255.
 5. Since the default is the deny value, it is recommended to use "Permit Any Option" at the last line to permit all packets that do not satisfy conditions.

- **access-group** *<access-list-number>* [in/out]

An interface command. Applies the access-list to the incoming packet or the outgoing packet of the corresponding interface.

Extended IP Access-List: To check access conditions, the extend IP access-list uses source IP address, destination IP address, protocol ID, application port number and establishment status.

- **access-list** *<access-list-number>* {deny/permit}<protocol> *<source>*
<source wildcard> *<destination>* *<destination-wildcard>* [operator]
[port-number][established]

1. Creates Access-list.

2. Option explanation

- 1) access-list-number : Extended Access-List (Number in range of 30~59)
- 2) protocol : protocol ID Number or protocol name (Ex: TCP, ICMP, UDP IP and so on)
- 3) source : Source Network Address,
- 4) Source-wildcard : Inverse Mask of Source Address
- 5) Destination : Destination Network Address
- 6) destination-wildcard : Inverse Mask of Destination Address
- 7) operator : operator for Port #
 - ✓ eq : equal
 - ✓ gt : greater then
 - ✓ lt : less then
 - ✓ neq : not equal
- 8) port-number: As application port number, well known port # is as follows:
 - ✓ chargen : Character generator (19)
 - ✓ daytime :Daytime (13)
 - ✓ discard : Discard (9)
 - ✓ domain : Domain Name Service (53)
 - ✓ echo : Echo (7)
 - ✓ finger : Finger (79)

- ✓ ftp : File Transfer Protocol (21)
- ✓ ftp-data: FTP data connections (used infrequently, 20)
- ✓ hostname: NIC hostname server (101)
- ✓ nntp: Network News Transport Protocol (119)
- ✓ pop2: Post Office Protocol v2 (109)
- ✓ pop3: Post Office Protocol v3 (110)
- ✓ smtp : Simple Mail Transport Protocol (25)
- ✓ sunrpc : Sun Remote Procedure Call (111)
- ✓ talk : Talk (517)
- ✓ time : Time (37)
- ✓ telnet : Telnet (23)
- ✓ uucp : Unix-to-Unix Copy Program (540)
- ✓ whois : Nicname (43)
- ✓ www : World Wide Web (HTTP, 80)


9) established : Established session


3. source/destination, Instead of source-wildcard/destination-wildcard pair, any(all Addresses), host(specified Host) can be used.


- **access-group** <access-list-number> {in/out}


Applies the access-list that has been set by an interface command to the incoming packet or the outgoing packet of the corresponding interface.

[Example] Standard Access-List Configuration and Usage

```
router(config)#  In this mode, Access-list Config is possible.

router(config)# access-1 1 deny 132.1.2.1 0.0.0.255 
Denies all packets whose source addresses are "132.1.2.0/24bit."

router(config)# access-1 1 deny 150.1.3.2 0.0.0.223 
Denies all packets whose source addresses are "150.1.3.0/21 bit."

router(config)# access-1 1 deny host 132.1.3.15  Denies all packets incoming from the host whose source address is
```

"132.1.3.15."

router(config)# access-list 1 permit any ⚡ Permits all packets that do not satisfy conditions of the Access-List 1 above. * If this command line does not exist, all default packets will be denied.

router(config)# interface ethernet 0 0 ⚡ Enters into the configuration mode of the interface Ethernet 0.0.

router(config-ether0.0)# ip ⚡ Enters into the IP configuration mode.

router(config-ether0.0-ip)# access-group 1 in ⚡ applies the Access-List 1 that has been set to all IP packets incoming through the Ethernet 0.0 interface.

router # show access-list ⚡ Shows Access-List.

Standard Access List (Index = 1)

```
1 : deny    132.1.2.1 0.0.0.255
2 : deny    150.1.3.2 0.0.0.224
3 : deny    host 132.1.3.15
4 : permit  any
```

[Example] Extended Access-List Configuration and Usage

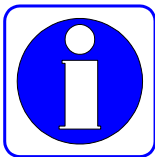
```
router (config)# ☞ In this mode, Access-list Config is possible.
router (config)# access-list 31 deny tcp 140.1.1.0 0.0.0.255
145.1.1.0 0.0.0.255 eq ftp ☞ Denies all TCP packets accessing
to the host whose destination address is "145.1.1.0/24Bit" from
"140.1.1.0/24bit" of the source address through the ftp port.
router (config)# access-list 31 deny tcp 140.1.1.0 0.0.0.255
145.1.1.0 0.0.0.255 eq ftp-data ☞ Denies all TCP packets
accessing to the host whose destination is "145.1.1.0/24Bit" from
"140.1.1.0/24bit" of the source address through the ftp-data port.
router (config)# access-list 31 permit tcp 140.1.1.0
0.0.0.255 145.1.1.0 0.0.0.255 eq ftp establish ☞ Permits only
packets whose sessions are set already among the TCP packets
accessing to the host whose destination is "145.1.1.0/24Bit" from
"140.1.1.0/24bit" of the source address through the ftp port.
router (config)# access-list 31 permit ip any any ☞ Permits
all IP packets except those matching conditions above.
router (config)# interface Ethernet 0 0 ☞ Enters into the
configuration mode of the interface Ethernet 0.0
router(config-ether0.0)# ip ☞ Enters into ip configuration
mode.
router (config-ether0.0)# ip access-group 31 in ☞ Applies
the Access-List 31 that has been set for all IP packets incoming
through the Ethernet 0.0 interface.
router (config-ether0.0)# end
router # show access-list 31 ☞ Shows the Access-List 31 that
has been set.

Extended Access List (Index = 31)
1 : deny tcp 140.1.1.0 0.0.0.255 145.1.1.0 0.0.0.255
2 : deny tcp 140.1.1.0 0.0.0.255 145.1.1.0 0.0.0.255 eq
ftp-data
3 : deny tcp 140.1.1.0 0.0.0.255 145.1.1.0 0.0.0.255 eq ftp
established
```

4 : permit ip any any

4.7. NAT(Network Address Translation) Configuration

Information



One of problems of the Internet is that number of available IP addresses is decreasing. The Network Address Translation (NAT) changes uncertified address that is used in the inside network into another IP address (usually, registered address) when the address goes outside. Also, when a registered IP address comes to the inside network from outside, NAT changes it into an internal IP address.

NAT can be useful for the following cases:

- When the user wants to use Internet but the user cannot have a unique, public address. In this case, NAT connects the private IP network that uses an unregistered IP address with the global Internet.

NAT shall be set in the Gateway that is located in the boarder between the public network (usually called an outside network) such as the Internet and the stub domain (usually called an inside network.) Before sending packets to outside networks, NAT converts internal private IP address into unique IP address.

- When the manager needs to change inside network address for the security reason or other reasons. In this case, without changing IP address that is a lot of work, the manager can translate addresses with NAT.
- When the manager needs to distribute TCP traffic for load-sharing. In this case, the manager can map several local IP addresses into one global IP address with the TCP load distribution function. When users access to the network from outside, they need to use the global IP address to access to the network and pass through the Gateway. Through the TCP session, load distribution is possible.

[NAT Glossaries]

- Inside local address: The address set in the host of the inside network
- Inside global address: An IP given by the Network Information Center (NIC) or the service provider. There are more than one IP address representing internal local IP addresses in the outside network.
- Outside local address: The IP address of the host in the outside network. The outside local address appears in the inside network.
- Outside global address: The address that the host owner gave to the host in the outside network. The outside global address is allocated to the globally routable addresses or networks.

NAT supports static address translation and dynamic address translation.

- Static Address Translation: When there is any access request from the outside network, NAT regularly maps an unregistered IP address of the internal host to a certified IP address, and converts the registered IP addresses to an unregistered IP address. Also, if an internal host accesses to the outside network, NAT performs the opposite and converts addresses.
- Dynamic address Translation: NAT keeps registered IP addresses, and when an inside network requests to access to the outside network, NAT allocates one of IP addresses that it keeps. However, if all registered IP address that NAT keeps are in use, NAT cannot allocate any registered IP address to the inside network.

VoiceFinder AP2120 Gateway usually supports both of NAT function and Port Address Translation (PAT) function.

NAT function converts several internal, unregistered IP addresses into several external, registered IP addresses. And PAT function converts several internal,

unregistered IP addresses into a protocol port number of an external, registered IP address.

1. VoiceFinder AP2120 Gateway currently supports only dynamic address translation.
2. VoiceFinder AP2120 Gateway supports 256 NAT addresses.
3. VoiceFinder AP2120 Gateway offers only static routing and RIP for NAT.

[Procedure]

Order	Operation
1	Move to the configuration mode.
2	Create the NAT/PAT-list defining the official address to use. ✓ At this time, decide where to use the global address – inside or outside. ✓ Define and set the entry to statically match address translation between the inside address and the outside address. ✓ The user needs to set timeout value of the session and recovery of the allocated address for the idle status when no data is transmitted through NAT.
3	Go to the interface configuration mode.
4	Enter into the IP configuration mode.
5	Apply the NAT/PAT-List that has been set to the corresponding interface.
6	Use "Show nat-list" command to check if correct access-list has been set.

[Related Commands and Syntax]

- **nat** *<nat-list-number>* **nat outside-global** *<start-address>* *<end-address>* *<mask>*
 1. Creates NAT pool for the outside global address in the global

configuration location.

2. NAT-list-number : Define any number between 0 and 7.
3. Start-address/End Address/Mask : Define the start address and the end address of NAT and the subnet masks for these addresses.

- **nat** *<nat-list-number>* **nat inside-global** *<start-address>* *<end-address>*
<local-ip address >

1. Creates a NAT pool for the outside global address in the global configuration location.
2. NAT-list-number: Define any number between 0 and 7.
3. Start-address/End Address: Designate the start address and the end address to use in the NAT.
4. Local -IP-Address: When there is a subnet that uses a registered IP in the local network, the user can register this subnet in the outside interface to route and advertise the subnet to the outside network.

- **nat** *<nat-list-number>* **nat static-entry** *<inside-local-address>*
<outside-global-address>

1. When it is necessary to access servers in the local network from outside, the user can define static entry for address translation with this command.
2. NAT-list-number: Define any number between 0 and 7.
3. Start-address/End Address: Define the start address and the end address that NAT uses.

- **nat** *<nat-list-number>* **nat time-out** *<timer-value>*

1. Defines time value for the NAT list to recover the address into free status when communication is idle.
2. The default is 300 seconds.

- **nat-group** *<nat-list-number>* {**nat/pat**}

An interface command. Applies the NAT-list that has been set in the global mode to the corresponding interface.

- **nat** *<nat-list-number>* **pat** *< pat-address >*

1. Sets the PAT list to use PAT in the global configuration location and PAT address.
2. NAT-list-number: Define any number between 0 and 7.

- **nat** *<nat-list-number>* **pat static-entry { tcp*/udp } <udp-port-number>**
<IP-address for PAT> <IP-address for PAT>.....<IP-address for PAT>

1. For certain application such as Dial Pad, this command statically sets PAT translation between a certain port number and the IP address.
2. NAT-list-number: Define any number between 0 and 7.
3. Static-entry for TCP is to be implemented.
4. IP-Address for PAT: The address of a terminal whose port shall be statically set. IP-Address for PAT is one of local network addresses. With this command, the user can set several IPs at the same time.

- **nat** *<nat-list-number>* **pat { fin-timeout / icmp-timeout / syn-timeout / tcp-timeout / udp-timeout } <timeout-value>**

1. Select timeout value when the session is in idle status while using PAT conversion.
2. Details of each option are as follows:
 - 1) Fin-timeout: Set timeout after TCP Fin. The default value is 10 sec.
 - 2) icmp-timeout: Set timeout after ICMP Session Idle. The default is 60 sec.
 - 3) sys-timeout: Set timeout after TCP sync Idle. The default is 60 seconds.
 - 4) tcp-timeout: Set timeout after TCP Session Idle. The default is 3,600 sec.
 - 5) udp-timeout: Set timeout after UDP Session Idle. The default is 60 seconds.

- **show nat-list** [nat-list-number]

1. Show NAT-list that has been set..
2. If no NAT-List-Number is designated, the status of all NATs is displayed.

- **show nat-list** [ethernet/Ethernet] *<main-interface-number>*.
<sub-interface-number>

Show NAT-list that has been set for a certain interface.

- **show running-config**

Show configuration contents including the NAT-list that has been set.

[Example] NAT Configuration and Usage

```
router# config
router(config)#  In this mode, NAT-list Config is possible.
router(config)# nat-list 0 nat outside-global 2.2.2.1
2.2.2.252 255.255.255.0  Set NAT pool so that the internal
packet can take "2.2.2.X/24bit" address as the source address when
it goes outside.
router(config)# nat-list 0 nat static-entry 1.1.1.253
2.2.2.254  Set NAT pool so that the internal packet can take
"2.2.2.254" address when it goes outside from the host whose source
is "1.1.1.253."
router(config)# nat-list 0 nat static-entry 1.1.1.254
2.2.2.253  Set NAT pool so that the packet can take "2.2.2.253"
address when it goes outside from the host whose source is
"1.1.1.254."
router(config)# nat-list 0 nat timeout 250  Set the time
value to turn into Address Free state when session is in Idle
status for 250 seconds.
router(config)# interface ethernet 0 0  Enter into the
configuration mode of the interface Ethernet 0.0
router(config-ether0.0)# ip  Enter into the IP configuration
mode.
router(config-ether0.0-ip)# address 1.1.1.3 255.255.255.0
 Assign an IP address to the Ethernet 0.0 interface. One of Indise
local addresses should be selected.
router(config-ether0.0-ip)# nat-group 0 nat  Apply NAT pool
of NAT-list 0 to the Ethernet 0.0 interface. NAT should be
configured for the inside network always.
```

```
router(config-ether0.0-ip)# end  Exit frm the configuraton.
router# sh nat-list 0  Show the ocnfiguration of NAT List 0.
```

```
NAT/PAT table Id: 0   Type : NAT TYPE

PAT Outside Public Address : 0.0.0.0

NAT Outside Public : 2.2.2.1 - 2.2.2.252 Netmask: 255.255.255.0

NAT Timer(secs) : 250

PAT Timer(secs) : ICMP(60) TCP(3600) UDP(60) TCPSYN(60) TCPFIN(10)

NAT static entry :

Local IP address : 1.1.1.254  Outside Global address : 2.2.2.253

Local IP address : 1.1.1.253  Outside Global address : 2.2.2.254
```

```
router# sh nat-list ethernet 0.0  Show the NAT configuratin
and NAT table configured for Ethernet Interface 0.0.
```

```
NAT/PAT table Id: 0   Type : NAT TYPE

PAT Outside Public Address : 0.0.0.0

NAT Outside Public : 2.2.2.1 - 2.2.2.252 Netmask: 255.255.255.0

NAT Timer(secs) : 250

PAT Timer(secs) : ICMP(60) TCP(3600) UDP(60) TCPSYN(60) TCPFIN(10)

NAT static entry :

Local IP address : 1.1.1.254  Outside Global address : 2.2.2.253

Local IP address : 1.1.1.253  Outside Global address : 2.2.2.254
```

Local IP	Global IP	Timer
1.1.1.2	2.2.2.3	120
1.1.1.1	2.2.2.2	15

```
router# sh running-config  Show present Configuration File.
```

```
!

interface ether0.0

ip address 1.1.1.3 255.255.255.0

Operation is UP







NAT/PAT table Id: 0   Type : NAT TYPE

NAT Outside Public : 2.2.2.1 - 2.2.2.252 Netmask: 255.255.255.0

NAT Timer(secs) : 250
```

```
NAT static entry :  
  
Local IP address : 1.1.1.254  Outside Global address : 2.2.2.253  
  
Local IP address : 1.1.1.253  Outside Global address : 2.2.2.254  
  
!  
  
!  
  
interface Ethernet0  
  
    ip address 132.1.1.1 255.255.255.0  
  
    Encapsulation HDLC  
  
    Operation is UP  
  
!  
  
interface Ethernet1  
  
    no encapsulation  
  
!
```

[Example] PAT Configuration and Usage

```
router# config  
  
router(config)#  In this mode, NAT-list Config is possible.  
  
router(config)# nat-list 0 pat 2.2.2.2  Set PAT so that the  
internal packet can take IP address 2.2.2.2 as the source address  
when it goes outside.  
  
router(config)# nat 0 nat static-entry udp 1000 1.1.1.4  
1.1.1.5  Statically set that packets should be sent to "1.1.1.4"  
and "1.1.1.5" of internal host for applications (Dial Pad, Wow  
Call or UDP No. 1000 port) trying to access to the network from  
outside. If there are several internal hosts configured, the load  
is distributed in order.  
  
router(config)# interface ethernet 0 0  Enter into the  
configuration mode of the interface Ethernet 0.0  
  
router(config-ether0.0)# ip  Enter into the IP configuration  
mode.  
  
router(config-ether0.0-ip)# address 1.1.1.3 255.255.255.0  
  
 Assign an address to Ethernet 0.0 interface. The address shall  
be one of Indise local addresses.
```


router(config-ether0.0-ip)# nat-group 5 pat ➤ Apply PAT pool of NAT-list 5 to Ethernet 0.0 interface. NAT/PAT shall be set in the inside network always.

router(config-ether0.0-ip)# end ➤ Exit from the configuration mode.

router# sh nat-list 5 ➤ Show the configuration of NAT/PAT List #5.

NAT/PAT table Id: 5 Type : PAT TYPE

PAT Outside Public Address : 2.2.2.2

NAT Outside Public : 0.0.0.0 - 0.0.0.0 Netmask: 0.0.0.0

NAT Timer(secs) : 300

PAT Timer(secs) : ICMP(60) TCP(3600) UDP(60) TCPSYN(60) TCPFIN(10)

PAT static entry :

UDP port(1000) :

1.1.1.4

1.1.1.5

router# sh nat-list ethernet 0.0 ➤ Show NAT/PAT configuration of ethernet interface 0.0 and Address Translation Table.

NAT/PAT table Id: 5 Type : PAT TYPE

PAT Outside Public Address : 2.2.2.2

NAT Outside Public : 0.0.0.0 - 0.0.0.0 Netmask: 0.0.0.0

NAT Timer(secs) : 300

PAT Timer(secs) : ICMP(60) TCP(3600) UDP(60) TCPSYN(60) TCPFIN(10)

PAT static entry :

UDP port(1000) :

1.1.1.4

1.1.1.5

STATE	PROTOCOL	TIMER	LOCAL-IP/Port	GLOBAL_IP/Port
Dynamic	TCP	120	1.1.1.2:1723	2.2.2.2:1723
Dynamic	TCP	150	1.1.1.1:1024	2.2.2.2:1024
Dynamic	TCP	120	1.1.1.2:1723	2.2.2.2:1723

```
Dynamic TCP      150      1.1.1.1:1024      2.2.2.2:1024

router# sh running-config  Show the Configuration File.

!

!

interface ether0.0

  ip address 1.1.1.3 255.255.255.0

  Operation is UP

  NAT/PAT table Id: 5   Type : PAT TYPE

  PAT Outside Public Address : 2.2.2.2

  PAT Timer(secs) : ICMP(60) TCP(3600) UDP(60) TCPSYN(60) TCPFIN(10)

  PAT static entry :

    UDP port(1000) :

      1.1.1.4

      1.1.1.5

!

interface Ethernet0

  ip address 132.1.1.2 255.255.255.0

  Encapsulation HDLC

  Operation is UP

!

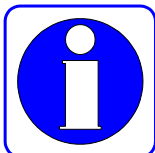
interface Ethernet1

  no encapsulation

!
```

4.8. DHCP (Dynamic Host Configuration Protocol) Configuration

Information

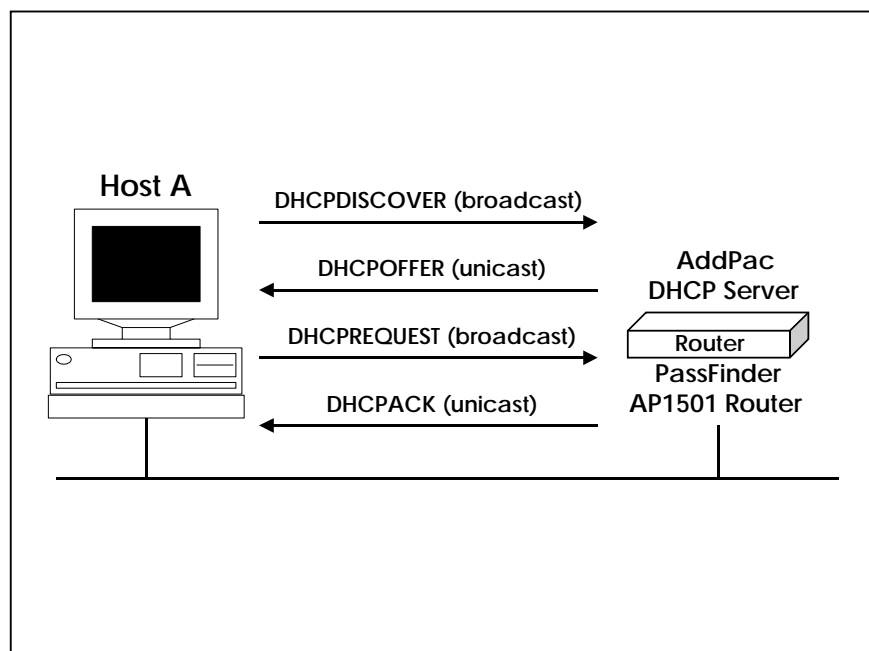


Dynamic Host Configuration Protocol (DHCP) automatically allocates IP addresses to DHCP clients.

The DHCP function of VoiceFinder AP2120 Gateway uses the address pool configured for the Gateway to allocate IP addresses to DHCP clients and manage IP addresses.

If software of VoiceFinder AP2120 Gateway cannot respond to the request of DHCP through the database that is set in the Gateway, the Gateway will send the request to another DHCP server configured by the network manager.

The following figure shows the basic procedure that the DHCP client requests an IP address to the DHCP server.



Host A (a client) sends a broadcast message "DHCPDISCOVER" to the DHCP server of the Gateway. Then, the DHCP server sends the DHCPOFFER Unicast message that contains configuration information – IP address to be allocated,

domain name and allocation status of the IP address – to the client. The DHCP client sends official IP address request to the server through the DHCPREQUEST broadcast messages. The DHCP server sends back the DHCPACK Unicast message to the client, and confirms the IP address that has been allocated to the client.

The DHCP function of VoiceFinder AP2120 Gateway complies with DHCP of RFC 2131, BOOTP of RFC 951 and Bootstrap Specifications of RFC 1542. The DHCP function provides following benefits.

- It is easy to configure DHCP so the user can save time and cost in configuring clients.
- The network manager can easily manage addresses and other related items of the sub-network by managing only the central server.

To implement the DHCP server function, the following conditions shall be satisfied.

- When the DHCP server function is enabled, IP addresses to be allocated to the server shall be separated from the addresses that will not be used the DHCP function. (For example, servers and printers whose addresses shall be fixed.)
- If necessary, the user shall define DHCP options for the Gateway – the default Gateway and the DNS server.

[Procedure-DHCP Server]

Order	Operation
1	Move to the configuration mode.
2	Define the DHCP-list type to use in the Gateway.
3	Create a DHCP-list defining DHCP-list number, DHCP mode to use in the Gateway, or DHCP address pool. ✓ If the server type is DHCP, set a DHCP pool that defines the DHCP start-address and the DHCP end-address. ✓ If the server type is DHCP, set a DHCP pool that defines the DHCP start-address and the DHCP end-address.
4	Set other necessary options.
5	Go to the interface configuration mode.
6	Enter into the IP configuration mode.
7	Apply the DHCP-list that has been set to the corresponding interface.
8	Use "Show dhcp-list" to check if desired DHCP has been correctly set.

[Related Commands and Syntax]

Mandatory Commands

- **dhcp-list <dhcp-list-number> type {server/relay}**

Creates the DHCP list of the Gateway (dhcp-list-number: any number between 0 and 4) and sets DHCP in the list should function as a server or protocol relay.

- **dhcp-list <dhcp-list-number> address relay <relay-IP-address>**

1. Set that the Gateway should send broadcast DHCP protocol to an equipment of the relay-ip-address through Unicast.
2. relay-IP-address: IP address of the equipment that is going to transfer DHCP broadcast through Unicast

- **dhcp-list** *<dhcp-list-number>* **address** **server** *<start-IP-address>*
<end-ip-address>

1. Set DHCP pool that the Gateway can function as a DHCP server.
2. *<start-IP-address>*,*<end-IP-address>* : Defines IP address range of the DHCP pool.

- **dhcp-group** *<dhcp-list-number>*

Bind DHCP-list with the interface to use.

- **show dhcp-list** [*dhcp-list-number*]

Show a certain DHCP list or whole DHCP configuration.

- **show running-config**

Show configuration contents include DHCP.

Optional Commands






- **dhcp-list** *<dhcp-list-number>* **option** [*option command*]

1. Set options used in the DHCP-list configured in the Gateway..
2. Optional Commands
 - 1) **arp-cache-timeout** *<time(second)>* : Set time value that the ARP cache table can keep the Mac address.
 - 2) **default-ip-ttl** *<time(second)>* : Set IP TTL value of the packet.
 - 3) **dhcp-lease-time** *<time(second)>* : Set valid time of assigned IP address by the DHCP server. The default is one hour.
 - 4) **dns** *<dns-address>* : Set the IP addresses of the DNS server that DHCP clients can use.
 - 5) **domain-name** *<domain-name>* : Designate the domain name to be used by DHCP clients. The domain name and the IP address are given together to DHCP clients.
 - 6) **ethernet-encapsulation** {*ethernet/ieee*} : Set that the DHCP clients should inform the Ethernet encapsulation method that the Gateway is going to use. VoiceFinderAP2120 Gateway supports Ethernet

Version 2 and IEEE802.2 address. *The default is Ethernet Version 2.*

- 7) **interface-mtu** <mtu-value> : Set MTU value for the interface.
- 8) **name-server** <name-server-address> : Set the name server address.
- 9) **ntp-server** <ntp-server-address> : Set the NTP server address.
- 10) **max-lease-time** <time(second)> : Set time value to check how long each IP address allocated by the DHCP server. After time passes, all addresses are recovered to be free regardless of the connection status.
- 11) **smtp-server** <smtp-server-address> : Set the SMTP server address.
- 12) **pop3-server** <pop3-server-address> : Set POP3 mail server address.
- 13) **router-option** < default-router-address > : After the DHCP client is booted, the DHCP client sends packets to its default Gateway. Therefore, the address and the default Gateway of the DHCP client shall be set. With this command, the user can set the address and the default Gateway.
- 14) **static-route** <destination-address> <router-address> : Routes an initial DHCP packet to a certain address.
- 15) **time-server** < time-server-address > : Set the time server address.
- 16) **www-server** < www-server-address > : Set the web server address.

[Example] DHCP Server Mode Configuration and Usage

```
router# config
router(config)#  In this mode, DHCP-list Config is possible.
router(config)# dhcp-list 0 type server  Set the Gateway
should operate as a DHCP server.
router(config)# dhcp-list 1 address server 211.1.1.1
211.1.1.125  Set the DHCP address pool. The DHCP address pool
configured here is from "211.1.1.1" to "211.1.1.125.".
router(config)# dhcp-list 1 option domain-name AddPac  Set
that the Gateway should give AddPac as a domain name to the client
when the Gateway functions as a DHCP server.
router(config)# dhcp-list 1 option router-option
211.1.1.126  Set that the Gateway should give "211.1.1.126" of default
```

Gateway address to the client when the Gateway functions as a DHCP server.

router(config)# interface ethernet 0 0 ⚡ Enter into enter 1.1 configuration mode which DHCP client is connected.

router(config-ether0.0)# ip ⚡ Enter into IP address configuration mode.

router(config-ether0.0-ip)# address 211.1.1.126 255.255.255.127 ⚡ Set Ethernet 0.0 interface address as "211.1.1.126/25 Bit." At this time, the address shall have the same network address of DHCP address, and does not exist in the DHCP pool to prevent overlapping.

router(config-ether0.0-ip)# dhcp-group 0 ⚡ Set that all DHCP packets coming through Ethernet 0.0 interface should be allocated with addresses according to rules of DHCP-0.

router(config-ether0.0-ip)# end ⚡ Exist from the configuration mode.

router# show dhcp-list 0 ⚡ Show the configuratioin of DHCP List 0.

DHCP Type = SERVER

ADDRESS POOL Start = 211.1.1.1 End = 211.1.1.127

DOMAIN NAME = addpac

Lease Time = 3600, Max lease time = 268435455

ARP Timeout = 180, Enthnet Enc = 0

Interface MTU = 1500 default-TTL = 255

Routers Option : 211.1.1.126

[Example] DHCP Relay Mode Configuration and Usage

router# config

router(config)# ⚡ In this mode, DHCP-list Config is possible.

router(config)# dhcp-list 1 type relay ⚡ Set that the Gateway should pass DHCP broadcast packets.

router(config)# dhcp-list 1 address relay 151.1.12.1 ⚡ Change the DHCP request packet into a Unicast packet and sends it to a host whose IP address is "151.1.12.1."


```
router(config)# interface ethernet 0 0  Enter into the
configuration mode of the Ethernet 0.0 to which DHCP clients are
going to be connected.
```

```
router(config-ether0.0)# ip  Enter into IP configuration
mode.
```

```
router(config-ether0.0-ip)#      address      211.1.1.126
255.255.255.127  Set the address of the Ethernet 0.0 interface
as "211.1.1.126/25 Bit."
```

```
router(config-ether0.0-ip)# dhcp-group 1  Relay all DHCP
packets coming through Ethernet 0.0 interface according to rules
of DHCP-List 1.
```

```
router(config-ether0.0-ip)# end  Exist from the
configuration mode.
```

```
router# show dhcp-list 1  Show the configuration of DHCP List
0.
```

```
DHCP Type = RELAY
```

```
Next Server = 151.1.12.1
```

```
router# show running-config  Show the configuration.
```

```
interface ether0.0
```

```
ip address 211.1.1.126 255.255.255.0
```

```
Operation is UP
```

```
DHCP Type = RELAY
```

```
Next Server = 151.1.12.1
```

```
!
```

```
interface Ethernet0
```

```
ip address 132.1.1.2 255.255.255.0
```

```
Encapsulation HDLC
```

```
Operation is UP
```

```
!
```

```
interface Ethernet1
```

```
no encapsulation
```

```
!
```


4.9. Transparent Bridging Configuration

VoiceFinder AP2120 Gateway supports transparent bridging for Ethernet and serial ports. Also, to manage networks, VoiceFinder AP2120 Gateway supports Bridge MIB that is defined in RFC 1286.

The bridge functions supported by VoiceFinder AP2120 Gateway are as follows:

- Complying with IEEE 802.1D standard
- Segmenting transparent bridged network to the logical VLAN
- The bridge function is supported not only through the Ethernet but also through the serial network and the frame-relay network.
- Supporting the spanning-tree algorithm of IEEE-based Bridged Protocol Data Unit (BPUD)

VoiceFinder AP2120 Gateway series only support one bridge-group. Therefore, the concept of the bridge-group is not used.

[Procedure]

Order	Operation
1	Move to the configuration mode.
2	Set option values to use in the bridge.
3	Go to the interface configuration mode.
4	Apply the bridge-group that has been set to the corresponding interface.
5	For multi-access interfaces including frame-relay, make a map.
6	Apply other bridging option parameters to use.
7	Use "show bridge" or "show span" commands to check if the bridge has been correctly set and the spanning tree algorithm normally operates.

[Related Commands and Syntax]

- **bridge**

An interface command. Set the corresponding interface should function as a bridge group.

- **frame-relay map bridge <dlci-number>**

1. An interface command. If the interface using the bridge is frame-relay, this command sets the map for sending bridge packets.
2. DLCI values is any number between 16 and 1007.
3. *If a bridge is used in the frame-relay interface, the user must use "MAP" command to enable the bridge.*

- **bridge priority <priority-number>**

1. This command defines the priority of the interface to be blocked or forwarded while participating in the spanning tree procedure.
2. The range is between 0 and 255. The lower the number is, the higher the priority is. The default is 0.

- **bridge path-cost <path-cost-value>**

1. An option of the interface command. This command defines the priority of the interface to be blocked or forwarded while participating in the spanning tree procedure.
2. The range is between 0 and 65535. The lower the number is, the higher the priority is. The default is 100 for Ethernet or 128 for Serial.

- **bridge hello-time <hello-interval>**

1. An optional command of "Global" command. This command defines Hello Interval between BPDUs.
2. The range is between 1 ~ 10 seconds. The default value is 2 seconds.

- **bridge forward-time <forward-interval>**

1. An option of the global command. This command decides the forward delay interval.

2. The range is between 10 and 200 seconds. The default value is 30 seconds.
- **bridge max-age** *<max-age-time>*
 1. An option of the global command. This command decides standby time to wait until receiving BPDU from the root bridge.
 2. The range is between 100 to 200 seconds. The default value is 15 seconds.
 - **no ip routing**
 1. An option of the global command. Use this command to operate the Gateway as a pure bridge without operating routing functions.
 2. For rerouting, the user must use "**ip routing**" command.
 - **show bridge**

Show bridge forwarding database entry.
 - **show bridge**

Show spanning-tree topology that the bridge is aware of.
 - **show running-config**

Show configuration including bridging.

[Example] Transparent Bridging Configuration and Usage

```
router# config
router(config)# interface ethernet 0.0  ➤ Create Ethernet
interface 0.0 and start configuration.
router(config-ether0.0)# bridge  ➤ Apply bridge to Ethernet
interface 0.0.
router(config-ether0.0)# bridge priority 2  ➤ Set the spanning
tree priority of the interface as 2.
router(config-ether0.0)# interface Ethernet 0  ➤ Enter into
the configuration mode of the interface serial 0.
```

```
router(config-Ethernet0)# encapsulation frame-relay ➤
```

Encapsulate with the frame-relay.

```
router(config-Ethernet0)# frame-relay map bridge 100 ➤
```

Enable the bridge in the frame-relay interface. This command also encapsulates the bridge packet.

```
router(config-Ethernet0)# exit ➤ Go back to the global configuration mode.
```

```
router(config)# bridge forward-time 150 ➤ Set the bridge forward delay interval as 150 seconds.
```

```
router(config)# bridge hello-time 5 ➤ Set the bridge hello BPDU interval as five seconds.
```

```
router(config)# bridge max-age 150 ➤ Set the standby time to wait until receiving BPDU from the root bridge as 150 seconds.
```

```
router(config)# exit ➤ Exist from the configuration mode.
```

```
router # show running-config ➤ Show the configuration.
```

```
interface ether0.0
```

```
no ip address
```

```
Operation is UP
```

```
bridge
```

```
!
```

```
interface Ethernet0
```

```
no ip address
```

```
Encapsulation FRAME-RELAY
```


```
Operation is UP
```

```
bridge
```


```
!
```

```
interface Ethernet1
```

```
no encapsulation
```

router # show bridge  Show the Bridge Forwarding Database.

Address	type	status	Age	Port
1111.1111.1111	static	bppu0	0	--
FFFF.FFFF.FFFF	static	our mac	0	--
AA11.0000.1111	dynamic	single-port	3	e0
0000.0C06.1122	dynamic	single-port	10	e0
0000.0C06.1123	dynamic	single-port	144	s0
0000.0C12.125A	dynamic	single-port	11	e0

router # show spanning-tree  Show the Spanning Tree Topology of Bridge(Router).

Bridge is executing the IEEE compatible Spanning Tree protocol

Bridge has priority 32768, address 0000.0000.0000.0000

Configured hellot time 2, max age 15, forward delay 30

Current root has priority 128, address 0000.30c3.098a.f789

[We are the root of the spanning tree]

Topology change flag not set, detected flag not set

Times: hold 1, topology change 30, notification 30

Hello 2, max age 15, forwarded delay 30, ageing 300

Timers: hello 1, topology change 0, notification 0

Port 1(ETH0), forward status

Port path cost 0, prot priority 128

Designated root has priority 128, address 0000. 304c.f686

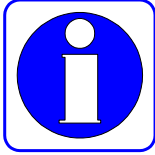
Designated bridge has priority 128, address 0000. 304c.f686

Designated port is 1, path cost 0

Timers : message age 0, forward delay 0, hold 0

4.10. Traffic Management

Information There are four Queuing methods - First-Come-First-Serve(FCFS), Weighted Fair Queuing(WFQ), Priority Queuing and Custom Queuing.



VoiceFinder AP2120 Gateway supports Traffic Queuing for effective delivery of traffic and effective use of bandwidth. Queuing is offered for Out-going Traffic with Priority OutPut Queuing of 4 level priority- High, Medium, Normal and Low, along with custom queuing to maximize the performance.

The algorithm of Priory Queuing is as follows.

Each port of the Gateway has 4 type of Queue with different Priority(High, Medium, Normal and Low). To send a packet, it analyzes the packet according several guidelines (for example, Protocol Number, the interface it comes from, the source and destination address of the packet) and put it into the right Queue. When the Gatway send out packets it follows the priority level. At first, it processes all High Priority Queue and then the next priority Queue. Because it first processes High Queue, the essential packets such as Hello Packet can always be process.

Typically, the Queue size is fixed but for more effective process, VoiceFinder AP2120 Gateway supports Custom Queuing, so that the administrator can modify the Queue size.

AP2120 Gateway Queuing is supported at Ethernet Interface of Low Speed Line.

[Procedure]

Order	Description
1	Move to configuration mode
2	Set Queue- List defining Queue-List Number and Queue Condition.
3	Set Default Queue for packets do not meet Queue-List condition.
4	Move to Interface configuration mode.
5	Move to IP configuration mode.
6	Apply Queue-Group to the Ethernet Interface.
7	With "show queue-list" or "show running-config / show interface" commands, confirm the Queue setting and whether the Queue is properly applied to the interface.

[Related Commands and Syntax]

- **queue-list <queue-list-number> interface {Ethernet0/Ethernet1/ether0} {high/medium/normal/low}**
 1. Set up Queuing rule at queue-list. Assign priority to packets sent from a certain interface.
 2. queue-list-number : A number between " 0~39"
- **queue-list <queue-list-number> protocol {<0-255>/udp/tcp/icmp} {high/medium/normal/low}**
 1. Set up Queuing rule at queue-list. Assign priority to a certain IP protocol packet.
 2. queue-list-number : A number between "0~39"
 3. 0~255 : IP Protocol Number.
- **queue-list <queue-list-number> port {udp/tcp} {scr/dsr} <por-Number> {high/medium/normal/low}**
 1. Creat queue-list. Set priority to packets with a certain protocol and with a certain Source/Destination Port.

2. queue-list-number : A number between "0~39"
- **queue-list** <queue-list-number> **ip** {scr/dsr} <ip-address>
{high/medium/normal/low}
 1. Set up Queuing rule at queue-list. Set priority to packets having certain IP address as Source/Destination.
 2. queue-list-number : A number between "0~39"
 - **queue-list** <queue-list-number> **size** <small-packet-size> <max-packet-size>
{high/medium/normal/low}
 1. Set up Queuing rule at queue-list. Set priority for packets of certain size limit (Small Packet Size, Max Packet Size).
 2. queue-list-number : A number between "0~39"
 - **queue-list** <queue-list-number> **default** {high /medium /normal /low}
 1. Set priority for packets do not meet any conditions.
 2. queue-list-number : A number between "0~39"
 - **queue-list** <queue-list-number> **qcount** <high-queue-size>
<medium-queue-size> <normal-queue-size> <low-queue-size>
 1. Customize the size of each Queue.
 2. Default Queue Size is 20.
 3. The Default Queue should be set. If not, the packets do not meet the condition are discarded.
 - **queue-group** <queue-list-number>
 1. Apply the Queue-List to certain interface.
 2. *Queue-List can be applied to Ethernet Interface.*
 - **show queue-list** [<queue-list-number>]
Show Queue-List.
 - **show running-config / show interface Ethernet** <interface-number>
Show Queue-List applied to the interface.

[Example] Queuing Configuration and Usage

```

router# config
router(config)# Queue-list Config is possible.
router(config)# queue-list 1 ip src 140.1.1.1 high Assign
all the packets with the source Address of "140.1.1.1" as high-queue.
router(config)# queue-list 1 protocol udp normal Assign
all UDP Packets as normal-queue.
router(config)# queue-list 1 size 64 128 medium Assign
packets of 64~128byte size as medium-queue.
router(config)# queue-list 1 default low Assign all the
packet do not meet above condition as low-queue.
router(config)# queue-list 1 qcount 20 30 50 30 Assign the
Queue size of Queue-List 1 as "High:20, Medium:30, Normal:50,
Low:30".
router(config)# interface Ethernet 0 Move to Ethernet0
configuration mode.
router(config-Ethernet0)# encapsulation hdlc.
router(config-Ethernet0)# ip Move to IP configuration mode.
router(config-Ethernet0-ip)# queue-group 1 Apply
Queue-List 1 to all the packets going out from Ethernet 0 interface.
router(config-Ethernet0-ip)# end
router # show interface Ethernet 0 Show the interface
condition.

Interface : Ethernet0

      IP Address : 134.12.1.1      Physical Interface : Ethernet0
      Network : 134.12.1.0        Subnet Mask : 255.255.255.0
      Administrator Status = UP   Operation Status = UP
      Network Type : HDLC         MTU : 1500
      Traffic Queueing is attached, (Id = 1)

Ethernet0 is UP, Line protocol is UP
last 1 minute data rate : tx 0 bps, rx 0 bps
input : 0 packets, 0 bytes, 0 no buffers
error : 0 (0 length, 0 align, 0 abort,

```

```


0 CRC, 0 overrun, 0 carrier)

output: 0 packets, 0 bytes, 0 under runs

error : 0 (0 busy)

DCD(up) DSR(up) DTR(up) RTS(up) CTS(up)

```

router # show running-config  Show the operation condition.

```

!
interface ether0.0
 ip address 132.1.3.1 255.255.255.0
 Operation is UP
!
interface Ethernet0
 ip address 134.12.1.1 255.255.255.0
 Encapsulation HDLC
 Operation is UP
!
Traffic Queue Id : 1
    Queue Size - Hign (20) Medium (30) Normal (50) Low (30)
    Source IP Address IP Address 140.1.1.1 - High level Queue
IP Protocol -      UDP : Normal level Queue
    IP Pakcet Size From 64 To 128 - Medium level Queue
    Default Queue - Low level Queue
!
!
interface Ethernet1
 no encapsulation
!

```

router # show queue-list 1  Show the configuration of Queue-List

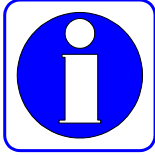
```

1.
Traffic Queueing Table Information (Index = 1)
Queue Size - Hign (20) Medium (30) Normal (50) Low (30)
Source IP Address IP Address 140.1.1.1 - High level Queue
IP Protocol - UDP : Normal level Queue
IP Pakcet Size From 64 To 128 - Medium level Queue
Default Queue - Low level Queue

```


4.11. SNMP Configuration

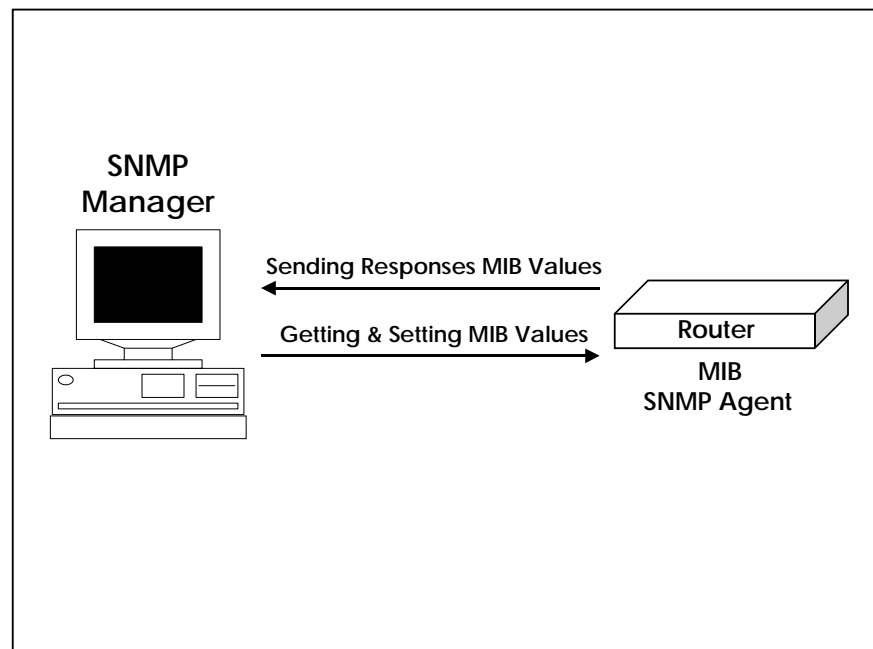
Information



SNMP is Application layer protocol providing a message format for the communication between the SNMP Manager and the SNMP Agent. Elements configuring an SNMP system to manage the network include the SNMP Manager, the SNMP Agent and the Management Information Base (MIB.)

The SNMP Manager composes a part of a commercialized Network Management System (NMS) such as the HP Openview. The SNMO Agent and the MIB are located in the Gateway. To configure SNMP in the Gateway, the user shall know the relations between the SNMP Manager and the SNMP Agent.

The SNMP Agent has MIB parameters that the SNMP Manager requests and changes. The SNMP Manager receives management information from the SNMP Agent or gives certain information to the SNMP agent for setting.



[Figure 4-2 Communication between SNMP Manager and SNMP Agent]

The SNMP Agent collects data from the MIB that manages data or equipment

parameters for the routing function. According to the request of the SNMP Manager, the SNMP Agent gives or sets these data. However, if the SNMP Agent sends information without receiving any request from the SNMP Manager, it is called "Trap." Usually, trap is a warning message. A warning message is created upon fault occurrence in the network, configuration change or important event occurrence.

[Figure 4-2 Communication between SNMP Manager and SNMP Agent] shows the relations between the SNMP Agent and the SNMP Manager. The SNMP Manager sends requests to get or set MIB values to the SNMP Agent, and the SNMP Agent sends responses. Also, the SNMP Agent sends trap for important network events that the manager should know.

SNMP standards are as follows:

- SNMPv1 : Full standard protocol defined in RFC1157
- SNMPv2C : Consisting of followings.
 - ✓ SNMPv2 : SNMP v2 protocol defined in RFC 1902~1907. An Internet draft standard
 - ✓ SNMPv2C : Standard defined in RFC 1901. Community-based management structure of SNMPv2

VoiceFinder AP2120 Gateway supports SNMPv1 and SNMPv2C.

[Procedure]

Order	Operation
1	Move to the configuration mode.
2	Set a SNMP community.
3	Set the host to receive SNMP trap.
4	Set SNMP related parameters.
5	Moves to the IP configuration mode.
6	Apply the queue-group that has been set to the corresponding serial

	interface.
7	Use "show snmp" command to check if configuration has been correctly made.

[Related Commands and Syntax]

- **snmp community** *<snmp-manager-ip/0.0.0.0>* *<community-string>* {ro/rw}
 1. Register the Gateway in a certain SNMP community.
 2. *<snmp-manager-ip/0.0.0.0>* : IP address of the SNMP Manager. "0.0.0.0" is an option that enables all NMSs that have same community-string values to function as the manager of the SNMP.
 3. Community-String : String used for authentication during SNMP communication
 4. {ro/rw} : Sets whether to only read Gateway information or read and write setting values of the Gateway

- **snmp host** *<trap-host-ip>* *<community-string>* {v1/v2c}
 1. Register the host to which the Gateway sends trap and the SNMP version when trap occurs.
 2. *<trap-host-ip>* : IP address of the trap host (SNMP manager)
 3. Community-String : String to be used for authentication during SNMP communication
 4. {v1/v2c} : SNMP Version

- **snmp contact** *<string>*

Indicate the contact point (equipment manager) to solve trap problem in case of trap.

- **snmp location** *<string>*

Indicate installation location of the faulty equipment when the Gateway sends trap.

- **snmp name** *<string>*

Indicates the faulty equipment when the Gateway sends trap.

- **snmp system-shutdown**

1. Decide to shutdown (reboot) the Gateway or not by SNMP from a remote place
2. This command can greatly affect equipment operation in insecure network. So be careful with this command. (This command is to be implemented during the latter half of 2000.)

- **snmp trap-authentication**

When another SNMP Manager accesses to the SNMP Agent with incorrect community-string value, this command sends authentication violation information.

- **show snmp**

Show SNMP setting status.

[Example] SNMP Configuration and Usage

```
router# config
router(config)#  In this mode, SNMP Config is possible.
router(config)# snmp community 0.0.0.0 ADDPAC-Domain1 rw
 Exchange information with all SNMP Managers whose
community-string is AddPac-Domain1.
router(config)# snmp host 131.23.1.1 ADDPAC-Domain v2c 
Send trap to the SNMP manager in "131.23.1.1" through SNMP v2c
protocol. At this time, the string is AddPac-Domain.
router(config)# snmp contact HongKilDong  Send a message
indicating that the contact point is "HongKilDong" when trap occurs
router(config)# snmp location 9FlofBuilding4  Send a message
indicating that the installation location of the faulty equipment
is 9FlofBuilding4 when trap occurs
router(config)# snmp name Tac_router1  Send a message indicating
that the equipment name is Tac_Gateway1 when trap occurs
```

```
router(config)# snmp trap-authentication  If an SNMP Manager  
accesses to an equipment with incorrect string, this commands  
informs this to all SNMP Managers that are set in the Gateway.
```

```
router(config)# exit
```

```
router # show snmp  Show SNMP configuration status.
```

```
TRAP version
```

TYPE	Community-Name	IP-Address	Access Mode
community	public	0.0.0.0	read-only
community	private	0.0.0.0	read-write
community	proxy	0.0.0.0	read-write
community	ADDPAC-Domain1	0.0.0.0	read-write
host	ADDPAC-Domain	131.23.1.1	SNMPv2c
contact	: HongKilDong		
location	: 9FlofBuilding4		
name	: Tac_router1		
system-shutdown	: Not Implemented		
trap-authentication	: ENABLE		

4.12. Gateway Management Command

This chapter describes commands used in the EXEC mode or the global configuration mode, which are necessary for management and operation of the Gateway in an alphabetical order. For commands regarding special configuration of the Gateway, refer to the previous chapters.

4.12.1. Command in the EXEC Mode

[Command Formats and Optional Commands]

- **clear { counters/interface/logging/utilization }**
 1. Reset certain functions or certain parts of the Gateway.
 2. Command Options
 - 1) counters : Clear the counters of all interfaces.
 - 2) interface : Reset the hardware logic of a certain interface and functions as if rebooting certain interfaces.
 - 3) logging : Clear logging buffer. To be implemented.
 - 4) utilization : Clear system utilization information of the Gateway.
- **clock [current/running/start]**
 1. Show the system clock of the Gateway.
 2. Command Options
 - 1) current : Show current time of the Gateway.
 - 2) running : Show total running time.
 - 3) start: Show the time that the Gateway started operation.
 3. If there is no option, all values of the three options will be displayed.
- **configuration**

Enter into the configuration mode.
- **copy {startup-clear/running-config}**
 1. Save or delete configuration data.

2. Command Options.

- 1) startup-clear : Delete configuration data that is saved in the flash memory of the present Gateway.
- 2) running-config : Save current configuration information in the Gateway.

● **Debug** <Option>

1. Decode packets passing the Gateway and check if the Gateway is operating normally.
2. For more information and options, refer to "4.13 Fault Handling and Debugging."
3. To disable Debug, use "no debug" or "Un-debug" commands.

● **exit**

1. Exist from the current mode, and enter into the sub-mode.
2. If the user uses "exit" command in the Exec mode, the user needs to log in again.

● **help**

Describe the interactive help system.

● **history**

1. Shows the commands history.
2. AP2120 Gateway keeps maximum 25 histories for each mode..
3. To use a command from History, enter "! History#."

● **no {option}**

An important command to negate commands used or set.

● **ping** [-flt] [-s *source-ip-address*] *Target-host-IP* [*datasize(max:1500)*]
[*npakcets*]

1. Send echo messages.
2. Command Options.
 - 1) [-f : fast send mode]
 - 2) [-l : loopback mode for HDLC]

- 3) [-t : send one datagram per seconds]
- 4) [-s : specify the sending interface IP address]

- **reboot**

Reboot the Gateway system.

- **rlogin [-l username] target-host**

Open the Rlogin connection.

- **show {option}**

1. Show information that has been set in the Gateway or collected by the Gateway. With this function, the user can check operation status of the Gateway.
2. For more information and options, refer to "4.13 Fault Handling and Debugging."

- **telnet { target-host-ip }**

Open a Telnet connection in the remote host.

- **test { memory/interface } [ethernet/hdlc] [main-interface.sub-interface]**

1. Test the Gateway itself.
2. Command options are as follows:
 - 1) memory: Tests the Gateway memory.
 - 2) interface: Performs the loopback test for the designated interface.

- **traceroute [-w waittime] [-m max_ttl] [-s src_addr] host [packetlen]**

Check the path that can access a remote host.

- **undebug <Option>**

1. Negates debugging configuration.
2. For more information and options, refer to " 4.13 Fault Handling and Debugging."

4.12.2. Command in the Global Configuration Mode

[Command Formats and Optional Commands]

- **access-list { option }**
 1. Set the access-list for the packet.
 2. For more information, refer to Access-List in the previous chapter.

- **arp {option}**
 1. Statically or dynamically registers ARP entries.
 2. Option
 - 1) **request** [*ip-address-number*]: Forcefully sends ARP requests for the host of a certain IP and registers it in the ARP table
 - 2) **static** <*ip-address-number*> <*mac-address-number*>: Statically registers Mac address in the ARP table for the IP host.
 - 3) **table-size** <*table-size-number*>: Sets the size of the ARP table. The AP2120 Gateways supports 10 ~ 256 size.

- **bridge { option }**
 1. Set the bridge.
 2. For more information, refer to Bridge Configuration in the previous chapter.

- **clock** [*yy mm dd hh mm ss*]

Set the system clock of the present Gateway.

- **dhcp-list { option }**
 1. Set DHCP.
 2. Refer to DHCP Configuration in the previous chapter.

- **ethernet [full-duplex]**
 1. To set Ethernet interface as "Full-Duplex".
 2. Default is "Half-Duplex".

- **exit**

1. Exit from the current mode, and enters into the sub- mode.
2. If the user uses "exit" command in the global configuration mode, the user will be able to go back to the Exec mode.

- **help**

Describe the interactive help system..

- **history**

1. Show history of used commands.
2. AP2120 Gateway keeps maximum 25 histories in each mode.
3. To use a certain command again, enter "! History#."

- **hostname { host-name }**

Set host name of the gateway on the network.

- **interface { ethnet/Ethernet } < main-interface.sub-interface >**

Set the name of the Gateway in the network.

- **logging { option }**

1. Set logging of the equipment.
2. For more information, refer to "4.13 Fault Handling and Debugging."

- **nat-list { option }**

1. Set Network Address Translation (NAT.)
2. For more information, refer to NAT Configuration in the previous chapter.

- **no {option}**

An important command to negates commands that the user used or have been set.

- **queue-list { option }**

1. Set the traffic queuing.
2. For more information, refer to Traffic Queuing Configuration in the previous chapter.

- **route {option}**
 1. Set the static route.
 2. For more information, see Routing Configuration in the previous chapter.

- **router {static/rip/ospf}**
 1. Enable or disable static routing process.
 2. For more information, see Routing Configuration in the previous chapter.

- **service {ftpd/snmpd/telnetd/tftpd}**
 1. Enable Application demon for a certain service.
 2. To disable the service, use "**no service**" command.

- **snmp { option }**
 1. Set SNMP protocol for management.
 2. For more information, refer to SNMP Configuration.

- **user { Option }**
 1. The command to manage Gateway users.
 2. For more information, refer to "4.14 User, Password, Software Image and Configuration File Management."

- **utilization { cpu/ethernet/Ethernet } [interface] [interface-number]
[measuring-period]**
 1. Check the availability of the CPU or a certain interface. With this command, the user can check the availability at a certain interval.
 2. The default is 5 minutes.

4.13. Fault Management and Debugging

This chapter describes how to handle and process faults while operating VoiceFinder AP2120 Gateway. The AP2120 Gateway provides "show", "Debug" and "logging" commands for fault handling.

4.13.1. Logging Command

Logging command logs equipment operation status to manage equipments, and decide the level of log information. Logging commands also can send log information to a certain host outside. Logging configuration can be made in the global configuration mode.

Logging configuration related commands are as follows:

- **logging on**

Enable logging for all available destinations.

- **logging condition {option}**

1. Set logging targets.
2. Option
 - 1) **command** : Log commands used.
 - 2) **event interface {ethernet/Ethernet} [interface-number]** : Log changes of a certain interface.
 - 3) **event protocol {all/critical/icmp}** : Log events of certain protocol.
 - 4) **alarm {all/critical/information/major/minor/warning}** : Set logging targets for alarms of certain level.
 - 5) **debugging** : Log debugging information.

- **logging destination {option}**

1. Set conditions of the destination host to send logging information.
2. Option
 - 1) **ip <destnation-ip-address>** : Set IP address of the remote host to send

logging information.

- 2) **port** [*port-number*] : Define the port number of the remote host to send logging information.
- 3) **on** : Enable logging in the remote host.

4.13.2. Show commands

With “show” command, the user can check configuration that the device manager has set and system status.

“Show” command can be used in the Exec mode and the syntaxes are as follows:

- **Show {option}** : Display option contents.

The below is Option commands related to “show”.

- **access-list** [*access-list-number*]
 1. Show the access-list that has been set.
 2. For more information, refer to Access-List Configuration in the previous chapter.
- **arp** [*ip-address for ARP entry*]

Show the contents of the ARP table.
- **bridge**
 1. Show forwarding/blocking database of the bridge.
 2. For more information, refer to Bridge Configuration in the previous chapter.
- **clock** [*current/running/start*]

Show the system clock of the current Gateway.
- **dhcp-list** [*dhcp-list-number*]

1. Show the DHCP that has been set.
2. For more information, refer to DHCP Configuration in the previous chapter.

- **ethernet**

Show the mode and operation speed of the Ethernet interface.

- **frame-relay {lmi/map/pvc}**

1. Show information on Frame-Relay.
2. Lmi Option shows "LMI Statistic".
3. Map Option shows "Frame-Relay Map Table".
4. PVC Option shows "Frame-Relay PVC Statistic".

- **interface [ethernet/Ethernet] [<main-interface>.<sub-interface>]**

Describe the status and the configuration of the interface.

- **logging [history]**

1. Show contents of the logging buffer.
2. History option shows the contents of the system log history table.

- **nat-list [nat-list-number]**

1. Show NAT that has been set.
2. For more information, refer to NAT Configuration in the previous chapter.

- **ospf {area/config/debug/interface/lsdb/nbma-nbr/neighbor/next-hop}**

1. Show OSPF configuration and operation status.
2. Options are as shows below;
 - 1) area : Show OSPF Area.
 - 2) config : Show the current configuration.
 - 3) debug : Show whether the Debug of OSPF is on.
 - 4) interface : Show OSPF information of the Interface.
 - 5) lsdb : Show Link State Database.
 - 6) nbma-nbr : Show the Neighbor relations of NBMA network such as Frame-Relay.

- 7) neighbor : Show the Neighbor relations of OSPF
- 8) next-hop : Show the Next-Hop information of OSPF.

- **proxy-arp**

Show whether the proxy ARP is enabled.

- **. queue-list** *[queue-list-number]*

1. Show configured Traffic-Queue.
2. For more information, refer to Traffic Queuing Configuration.

- **rip**

1. Show configured RIP information and Parameter.
2. For more information, refer to Routing configuration.

- **route {ospf/rip/static}**

1. Show decided route information table.
2. OSPF/RIP/Static option shows tables of each algorithm.
3. For more information, refer to Routing Configuration in the previous chapter.

- **router**

1. Display enabled routing processes.
2. For more information, refer to Routing Configuration in the previous chapter.

- **running-config**

Show currently running configuration file.

- **session**

Display information of the Telnet session that is currently connected to the Gateway.

- **service**

Display enabled service processes in the current Gateway.

- **snmp**

Display SNMP protocol state of the Gateway and options.

- **Spanning-Tree**

If the bridge is currently enabled in the Gateway, this command displays spanning-tree topology.

- **static**

Display static routes that are set in the Gateway.

- **system task**

Show information and the state of the task that is currently running in the Gateway.

- **tcp**

Display information and the state of the external system that is connected to the TCP among information of the current Gateway.

- **udp**

Display information and the state of the external system that is connected to the UDP among information of the current Gateway.

- **user**

Display profiles of the users registered in the Gateway.

- **utilization { cpu/ethernet/Ethernet } [interface] [interface-number]
[measuring-period]**

Show utilization state and values currently set.

- **version**

Show hardware information of the Gateway and software version that is currently running in the Gateway.

- **ppp {chap/error/negotiation/packet }**

1.Decode and show configuration and operation status of PPP.

2.Details of each option are as follows:

1) chap: Decode and show information exchanged when CHAP is being set.

2) error: Decode and show error information in the PPP process.

3) negotiation: Decode and show PPP link negotiation information.

4) packet: Decode PPP packets.

- **Ethernet interface [interface-number]**

Decode and show packets passing certain Ethernet Interface.

- **rip**

Decode RIP Protocol configuration and operation status.

- **tcpip {arp/icmp/tcp/udp }**

1.Decode and show TCP/IP packets passing through the Gateway.

2.Details of each option is as follows:

1) arp: Decode and show ARP packets.

2) icmp: Decode and show ICMP packets.

3) tcp: Decode and show TCP/IP packets.

4) udp: Decode and show UDP/IP packets.

4.14. User, Password, Software Image and Configuration File Management

This chapter describes how to register and change users, recover passwords, download and back up software image, and back up and restore configuration file, which are very useful in using VoiceFinder AP2120 Gateway.

4.14.1. User Registration and Change

This chapter describes how to register Gateway users, change passwords and change user's authorities.

Commands relating to managing Gateway users are as follows:

- **user {option}**: Register or change users.

User's command related optional commands are as follows:

- **add** <login-name> <password> [**admin/high/normal/low**]
 1. Register Gateway users.
 2. Set the user's authority level as admin, high, normal or low.
- **change** <login-name> <old-password> <new-password>
Change the password of the Gateway user.
- **level** <login-name> <password> [**admin/high/normal/low**]
 1. Change the authority level of the Gateway user.
 2. Change the user authority level into admin, high, normal and low.
- **timeout** <login-name> <timeout-period>
 1. For the security reason, this command defines timeout value according to the Gateway user when the console of the Telnet session is idle.
 2. If timeout is 0, it means "forever."

4.14.2. Password Recovery

The Gateway manager shall know the password to change Gateway configuration and check the Gateway status. Therefore, the Gateway manager shall remember the password and keep it confidentially. This chapter describes how to recover the password when the Gateway manager forgets the password.

The following describes how to recover the password.

[Procedure]

Order	Operation
1	Connect the console and prepare to recover the password. Password recovery shall be made in the console only.
2	Initialize the system. (Turn on/off the system.)
3	After the initial messages are displayed, enter Ctrl+x and Ctrl+c once or twice.
4	Wait for a while until entering into the boot mode.
5	Use "Show password" command to check the root password.
6	Reboot the system.
7	Log in the system with verified password.

Initialize the system in the booter mode, not in the Gateway program state. *To enter into the booter mode, enter Control-X and Control-C keys once or twice when the booter mode message Appears.*

In the booter mode, "BOOT#" prompt Appears on the screen as in the following figure. See the following figure.

System Boot Loader, Version 1.10a

```
Copyright (c) by AddPac Technology Co., Ltd. Since 1999.

System Flash Memory is 4 Mbytes.
1 Ethernet/IEEE 802.3 Interface (10BaseTX).
1 RS232 Ethernet console port, 2 Ethernet networks interface.

The "BOOT LOADER" is ready

1 BOOT# ?
configure : Enter configuration mode
copy : Copy configuration data
exit : Exit from the EXEC
history : Show command line history
ping : Send echo messages
reboot : reboot system
show : Show running system information
telnet : Open a telnet connection
2 BOOT#
```

[Figure 4-3 Boot Mode Login Screen]

Available commands in the booter mode: Enter "?" as in the normal Gateway mode.

```
1 BOOT# ?
configure : Enter configuration mode
copy : Copy configuration data
exit : Exit from the EXEC
history : Show command line history
ping : Send echo messages
reboot : reboot system
show : Show running system information
telnet : Open a telnet connection
```

Verify "root" command that is currently set. The following is when "root"

password is "Router.

3 BOOT# sh password

password = "router"

To change current password in the booter, enter into the configuration mode and change the password as using "passwd" command.

The following is when changing "root" command into "Route1"

[Example] Password Change Configuration and Usage

```
1 BOOT# conf
1 BOOT(config)# ?
    address :      Set the IP address of an interface
    clock :        Manage the system clock
    exit :         Exit from the EXEC
    history :      Show command line history
    passwd :       Change password
2 BOOT(config)# passwd ?
    <new password> New Passowrd
3 BOOT(config)# passwd router ?
    <repeat new password> New Passowrd for confirm
4 BOOT(config)# passwd router router ?
    < cr >
5 BOOT(config)# passwd router router1
    password changed
6 BOOT(config)#
```

4.14.3. Software Image Upgrade and Backup

Software of AP2120 Gateway will be upgraded regularly in case of functional upgrade or debugging. It is recommended for the existing users to upgrade software in this method. This chapter describes how to upgrade or back up Gateway software.

The following describes how to upgrade or back up Gateway software and related commands.

If the user uses FTP, the user must enter correct user ID and password when logg-in to the system. If the user upgrades new Gateway software from the user consol of the PC or a workstation through FTP, the user shall use "put" command. Or, to download Gateway software that is currently in use to a PC or a workstation, the user shall use "get" command.

The following is when downloading Gateway software that is currently in use to a PC. Use "put" command to copy software to be upgraded to the current directory. Use "put" command instead of "get" command.

[Example] Software Backup through FTP

```
155 sun10:#> ftp 211.170.87.221
Connected to 211.170.87.221.
220 router FTP server (Version 1.12) ready.
Name (211.170.87.221:noname): root
331 Password required for root.
Password:
230 User root logged in ok.
ftp> bi
200 Type set to I.
ftp> get router.bin
200 PORT command successful.
150 BINARY data connection for router.bin (211.170.87.99,44100).
```



```
226 BINARY Transfer complete.  
local: router.bin remote: router.bin  
201622 bytes received in 0.52 seconds (375.13 Kbytes/s)  
ftp> quit  
221 Goodbye.  
156 sun10:/#>
```

Software backup method through TFTP is same as FTP. However, login procedure is not necessary. The following is when using "put" command for software. When software upgrade is completed, "Router Software is updated" is displayed in the screen.

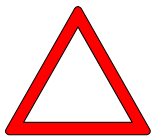
[Example] Software Upgrade through TFTP

```
156 sun10: #> tftp 211.170.87.221  
tftp> bi  
tftp> put addpac.bin  
Sent 201622 bytes in 0.4 seconds  
tftp> quit  
157 sun10: #>
```

The following message is displayed in the user's console.

```
" Router Software " is updated
```

Caution



To upgrade or backup software image, use a same procedure in the Gateway program that is currently in use or in the booter mode. If any fault occurs in the currently running Gateway program, upgrade software image by the procedure explained above.

4.14.4. Configuration File Backup & Restore

AP2120 Gateway saves the configuration file in the flash memory of the Gateway. However, sometimes it is necessary to back up the configuration file or restore the backed up configuration file.

This chapter describes how to back up or restore the configuration file and related commands.

Backup and restoring procedures of the configuration file are same as upgrade and backup procedures of software image. However, the configuration file name is router.cfg. The configuration file is backed up or restored through FTP/TFTP. When restoring is completed, "Config Database is updated" message is displayed on the screen.

When backing up the configuration file, use "get" command, and when restoring the configuration file, use "put" command. The following is an example of backup and restore of configuration information through TFTP.

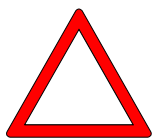
[Example] Software Backup through FTP

```
56 sun10#> tftp 211.170.87.221
tftp> bi
tftp> get router.cfg
Received 201622 bytes in 0.4 seconds
tftp> quit
157 sun10:#>
158 sun10:#> tftp 211.170.87.221
tftp> bi
tftp> put router.cfg
Sent 201622 bytes in 0.5 seconds
tftp> quit
```

The following message is displayed in the user's console.

"Config Database" is updated

Caution



To back up or restore the configuration file, use a same procedure in the Gateway program that is currently in use or in the booter mode. If any fault occurs in the currently running Gateway program, restore the configuration file in the booter mode by the procedure explained above.

Chapter 5 Voice Configuration and Command

This chapter explains voice configuration and commands to operate voice integration function of VoiceFinder AP2120.

5.1. Voice Technologies and Concepts

5.1.1. Voice Over IP

Voice over IP enables a VoIP Gateway to carry voice traffic (for example, telephone calls and faxes) over an IP network. In Voice over IP, the DSP segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets.

These voice packets are transported using IP in compliance with ITU-T specification H.323.

Because it is a delay-sensitive Application, you need to have a well-engineered network end-to-end to successfully use Voice over IP.

Fine-tuning your network to adequately support Voice over IP involves a series of protocols and features geared toward quality of service (QoS). Traffic shaping considerations must be taken into account to ensure the reliability of the voice connection.

All the commands used AP2120 can be used either by Console or Telnet.

Voice over IP is primarily a software feature; however, to use this feature on a VoIP Gateway, you must install a voice interface cards (AP-FXS, AP-FXO, AP-E&M), each of which is specific to a particular signaling type associated with a voice port.

5.1.2. Codecs and MOS(Mean Opinion Score)

Codec(Coder-Decoder) codes analog voice signal to digital bit stream and

decodes bit stream to analog voice signal. In special cases, it also indicated the compression type (For example, G.723a CODEC).

Typically, telephone network uses PCM Codec. PCM does sampling of analog sound 8,000 times/ 1 sec. (Sampling gap: 125micro sec.) and converts each sample to number code. On the telephone network, PCM code uses 8 bits, so the standard transmission speed of digital telephone is 64Kbps.

The other commonly used compression algorithm is ADPCM(Adaptive Differential Pluse Code Modulation). The typical ADPCM is ITU-T G.726 using 4 bits sample encoding with the transmission speed of 32Kbps. It encodes the difference of amplitude and its rate.

PCM and ADPCM is Waveform Codec compression method. In addition to waveform CODECs, there are source CODECs that compress speech by sending only simplified parametric information about voice transmission; these CODECs require less bandwidth. Source CODECs include linear predicative coding (LPC), code-excited linear prediction (CELP), and multi-pulse, multi-level quantization (MP-MLQ). Coding techniques are standardized by the ITU-T in its G-series recommendations. The most popular coding standards for telephony and voice packet are:

- G.711 : Describes the 64-kbps PCM voice coding technique. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs.
- G.726 : Describes 40, 32, 24, 16Kbps ADPCM voice coding technique. Used for Packet Voice, ordinary telephone network and PBX. In that case, public telephone network or PBX needs to support ADPCM.
- G.729 : Describes CELP compression where voice is coded into 8-kbps streams. There are two variations of this standard (G.729 and G.729 Annex A) that differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM.
- G.723.1 : Describes a compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This CODEC has two bit rates associated with it: 5.3 and 6.3 kbps. The higher bit rate is based on ML-MLQ technology and provides a somewhat higher quality of sound. The lower bit rate is based on CELP and provides system designers with additional

flexibility.

Each CODEC provides a certain quality of speech. The quality of transmitted speech is a subjective response of the listener. A common benchmark used to determine the quality of sound produced by specific CODECs is the mean opinion score (MOS). With MOS, a wide range of listeners judge the quality of a voice sample (corresponding to a particular CODEC) on a scale of 1 (bad) to 5 (excellent). The scores are averaged to provide the mean opinion score for that sample. Table 5-1 shows the relationship between CODECs and MOS scores

Compression Method	Bit Rate (kbps)	Processing (MIPS)	Framing Size	MOS Score
G.711 PCM	64	0.34	0.125	4.1
G.729 CS-ACELP	8	20	10	3.92
G.729a CS-ACELP	8	10.5	10	3.7
G.723.1 MP-MLQ	6.3	16	30	3.9
G.723.1 ACELP	5.3	16	30	3.65

[Table 5-1 Compression Methods and MOS Scores]

Although it might seem logical from a financial standpoint to convert all calls to low-bit rate CODECs to save on infrastructure costs, you should exercise additional care when designing voice networks with low-bit rate compression. There are drawbacks to compressing voice. One of the main drawbacks is signal distortion due to multiple encoding (called tandem encoding). For example, when a G.729 voice signal is tandem encoded three times, the MOS score drops from 3.92 (very good) to 2.68 (unacceptable).

Another drawback is CODEC-induced delay with low bit-rate CODECs. There are two kinds of delay inherent in today's telephony networks: propagation delay and handling delay. Propagation delay is caused by the characteristics of the speed of light traveling via a fiber-optic-based or copper-based media. Handling delay (sometimes called serialization delay) is caused by the devices that handle voice information. Handling delays have a significant impact on voice quality in a packetized network.

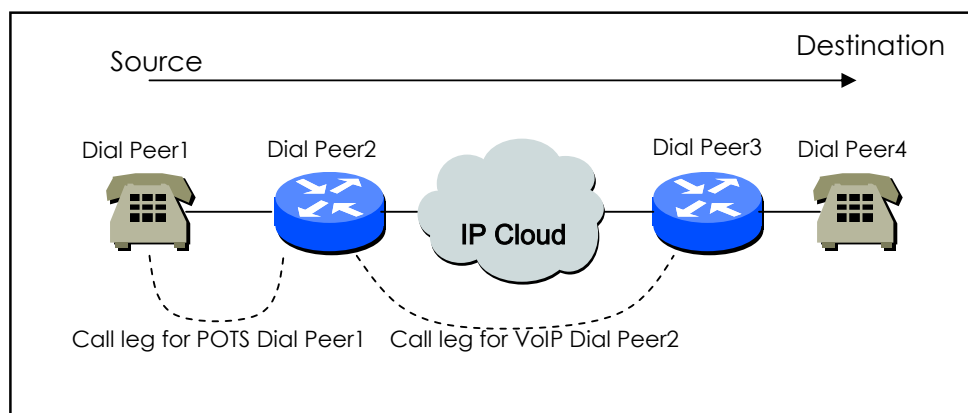
CODEC-induced delays are considered a handling delay. [Table 5-2](#) shows the delay introduced by different CODECs.

Compression Method	Bit rate (Kbps)	Compression delay (ms)	MOS Score
G.711PCM	64	0.75	4.1
G.729 CS-ACELP	8	10	3.92
G.729a CS-ACELP	8	10	3.7
G.723.1 MP-MLQ	6.3	30	3.9
G.723.1 ACELP	5.3	30	3.65

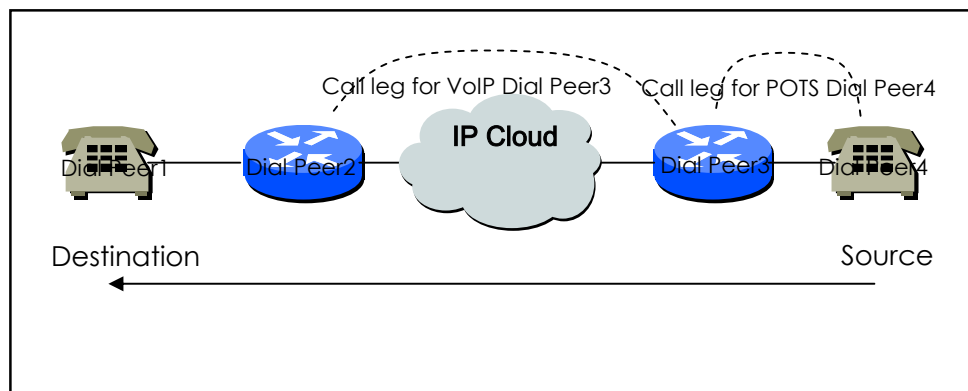
[Table 5-2 Compression Method and delay]

5.1.3. Dial Peer

The key to understand our voice implementation is to understand the use of dial peers. Dial peers describe the entities to and/or from which a call is established. All of the voice technologies use dial peers to define the characteristics associated with a call leg. A call leg is a discrete segment of a call connection that lies between two points in the connection, as shown in [Figure 5-1](#) and [Figure 5-2](#). Four call legs comprise an end-to-end call, two from the perspective of the source Gateway as shown in [Figure 5-1](#), and two from the perspective of the destination Gateway, as shown in [Figure 5-2](#). You use dial peers to Apply specific attributes to call legs and to identify call origin and destination. Attributes Applied to a call leg include Quality of Service (QoS), compression/decompression (CODEC), Voice Activation Detection (VAD), and fax rate.



[Figure 5-1 Dial Peer Call Legs from the Perspective of the Source Gateway]



[Figure 5-2 Dial Peer Call Legs from the Perspective of the Destination Gateway]

There are basically two different kinds of dial peers with each voice implementation:

- POTS Dial peer : POTS Dial peer describes the characteristics of a traditional telephony network connection. POTS peers point to a particular voice port on a voice network device. When configuring POTS dial peers, the key commands that must be configured are the **port** and **destination-pattern** commands. The **destination-pattern** command defines the telephone number associated with the POTS dial peer. The **port** command associates the POTS dial peer with a specific logical dial interface, normally the voice port connecting the AP2120 VoIP Gateway to the local POTS network.
- Voice Network Dial peer : Voice Network Dial peer describes the characteristics of a packet network connection; for example, in the case of Voice over IP, this is an IP network. Voice-network peers point to specific voice-network devices. When configuring voice-network dial peers, the key commands that must be configured are the **destination-pattern** and **session-target** commands. The **destination-pattern** command defines the telephone number associated with the voice-network dial peer. The **session-target** command specifies a destination address for the voice-network peer. If configuring a Voice over IP network peer, the session target is a destination IP address.

5.1.4. Voice ports

Voice port commands for AP2120 VoIP Gateway define the characteristics associated with a particular voice-port signaling type. Voice ports of the AP2120VoIP Gateway provides support for three basic voice signaling formats:

- FXS (Foreign Exchange Station) Interface : The Foreign Exchange Station interface. The FXS interface is an RJ-11 connector that allows connection for basic telephone equipment, keysets, and PBXes; FXS connections supply ring, voltage, and dial tone.
- FXO (Foreign Exchange Office) Interface : The FXO interface is an RJ-11 connector that allows a connection to be directed at the public switched

telephone network's (PSTN's) central office.

- E&M (Ear and Mouse or RecEive and TransMit) : E&M Interface is an RJ-48 connector that allows a connection to be directed at PBX Trunk Line (Tie Lines). E&M is signaling technology for 2-wire and 4-wire telephone/Trunk Interface

Currently, AP2120 offers only analog voice ports for VoIP service. The voice port signaling type depends on the hardware platform. On AP2120 series, the voice-port syntax is **voice-port** *slot-number/port-number*

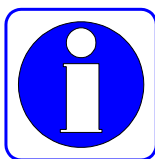
5.2. VoIP Interface Configuration

AP 2520G Gateway has various interfaces. It is the Ethernet which is defined to provide VoIP service among those interfaces.

As Default, Ethernet 0.0 Interface is defined to provide VoIP service, and can be determined to use for another purpose by the following procedure.

In case VoIP Interface is changed during VoIP service, the signal connection is terminated and reregistering process with gatekeeper is executed. Therefore, it is advised that VoIP Interface should not be changed after the initiate Setup of system is completed.

Information



If the defined VoIP interface doesn't have IP address, you cannot configure and search those related to VoIP. Therefore, defining VoIP Interface and setting up IP Address is prior to make configuration related to VoIP.

In case IO Address of VoIP Interface is changed during VoIP service, the signal connection is terminated and reregistering process with gatekeeper is executed

Step	Commands	Description
1	Router# configure	Go to Configuration Mode.
2	Router(config)# voice-interface <i>interface-name</i>	Define Interface on Router. The names of Interfaces are, for instance, Ethernet 0.0, Ethernet 1.0, serial 0, and so on.

5.3. **Numbering Plan, Number Handling and Dial Peer Configuration**

5.3.1. **Numbering Plan**

The first step in configuring VoIP router is planning the number which is efficient, and proper between routers.

Public telephone network has hierarchical structure, (Country Code) + (Area Code) + (Dialing Code) + (Directory Number) so that this hierarchical number planning is advantageous. As each router on Voip network is corresponding to switcher on telephone network, has a number plan in accordance the size of VoIP network.

It is important whether the Gateway is interworking with a gatekeeper in number planning. If the Gateway interworks with the existing gatekeeper, you should follow the number planning defined on the gatekeeper.

The simplest number configuration is assigning the Gateway with the public telephone number already used in the installatin place of the Gateway. This means a call trial to the public telephone number is advantageous by the number when co-operating with other VoIP routers or failing in VoIP call.

When configuring VoIP network with strong private features, configure network by having a private number planning.

5.3.2. **Dial Peer Configuration**

5.3.2.1. **Inbound Dial Peer & Outbound Dial Peer**

Dial peers are used for both inbound and outbound call legs. It is important to remember that these terms are defined from the *Gateway's* perspective. An inbound call leg originates *outside* the Gateway. An outbound call leg originates *from* the Gateway.

For inbound call legs, a dial peer might be associated with the calling number or the port destination. Outbound call legs always have a dial peer associated with them. The destination pattern is used to identify the outbound dial peer.

POTS peers associate a telephone number with a particular voice port so that incoming calls for that telephone number can be received and outgoing calls

can be placed. VoIP peers point to specific devices (by associating destination telephone numbers with a specific IP address) so that incoming calls can be received and outgoing calls can be placed. Both POTS and VoIP peers are needed to establish Voice over IP connections.

Establishing communications using Voice over IP is similar to configuring an IP static route: you are establishing a specific voice connection between two defined endpoints. As shown in Figure 5.3, for outgoing calls (from the perspective of the POTS dial peer 1), the POTS dial peer establishes the source (via the originating telephone number or voice port) of the call.

The VoIP dial peer establishes the destination by associating the destination phone number with a specific IP address.

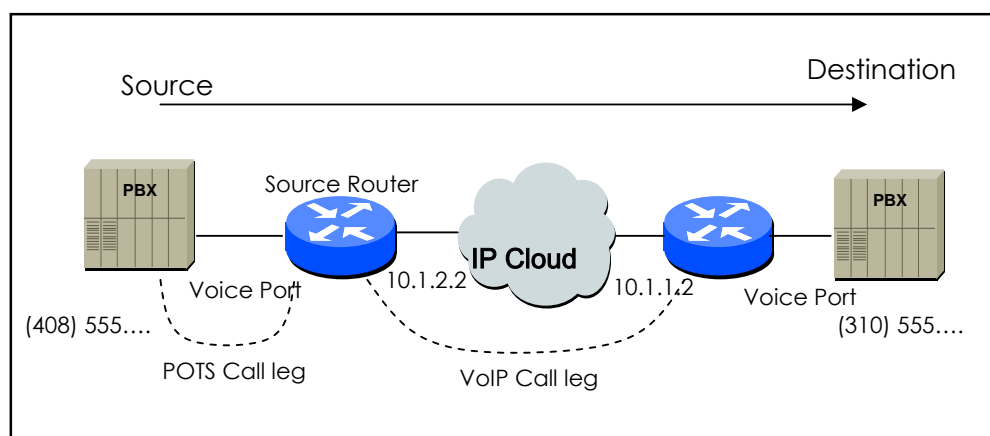


Figure 5.1 Outgoing Call in POTS Dial Peer 1's view

To configure call connectivity between the source and destination as illustrated in Figure 5.3, enter the following commands on router 10.1.2.2:

```
dial-peer voice 1 pots
  destination-pattern 1408555 . . . .
  port 1/0
```

```
dial-peer voice 2 voip
  destination-pattern 1310555 . . . .
  Session target 10.1.1.2
```

In the previous configuration example, the last four digits in the VoIP dial peer's

destination pattern were replaced with wildcards. This means that from access server 10.1.2.2, calling any number string that begins with the digits "1310555" will result in a connection to access server 10.1.1.2. This implies that access server 10.1.1.2 services all numbers beginning with those digits.

Figure 5.2 shows how to setup a End-to-End call between Dial Peer 1 and Dial Peer 4.

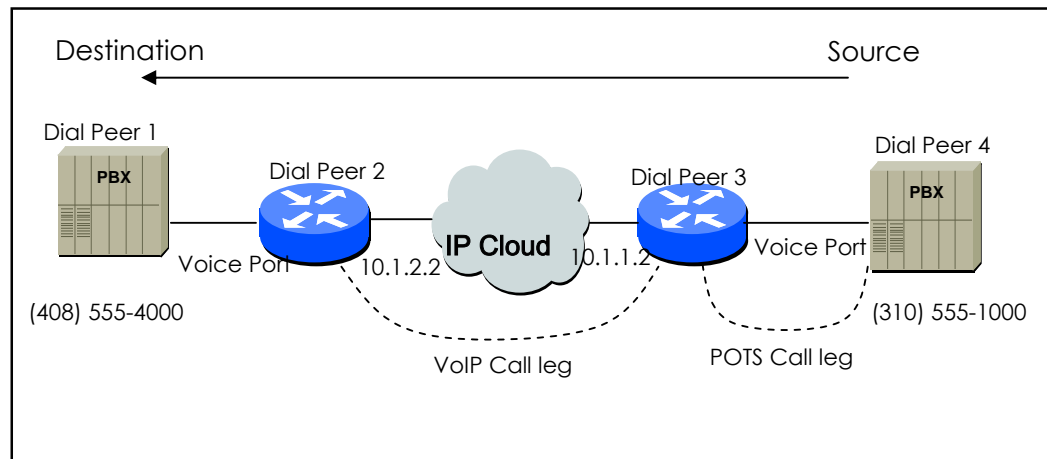


Figure 5.2 Outgoing Call in POTS Dial Peer 2's view

To complete the end-to-end call between dial peer 1 and dial peer 4 as illustrated in Figure 5.4 enter the following commands on router 10.1.1.2:

```
dial-peer voice 4 pots
  destination-pattern 1310555 . . . .
  port 1/0

dial-peer voice 3 voip
  destination-pattern 1408555 . . . .
  Session target 10.1.2.2
```

As explained above, call inside router is completed by selecting inbound dial and outbound.

While the selection of Outbound Dial peer is basically decided by matching POTS Peer and VoIP Peer with destination pattern of Dial Peer, Inbound Dial Peer is decided by other ways.

First of all, the procedure of Inbound POTS Peer is as follows;

- Select POT peer assigned by voice port receiving Call.
- In case more than one POTS peer are assigned by voice port, the POT made at first gets selected.

The procedure of selecting Inbound VoIP Peer.

- Select VoIP peer having the same IP address with receiving Router among VoIP peers.
- When the above selection fails, Select VoIP peer having answer-address which is matched with calling party number of Inbound call.
- When the above selection fails, Select VoIP peer having destination-pattern which is matched with calling party number of Inbound call.

The selection of Inbound Dial Peer is a proper measurement for receiving side. That is, parameters assigned by POTS or VoIP peer applies to the elected dial Peer. Ultimately, because the failure of the selection for VoIP means POTS peer related to choice port doesn't exist, Call doesn't advance. Meanwhile Inbound VoIP peer will proceed regardless of the selection of Inbound VoIP peer.

5.3.2.2. POTS Peer Configuration

Set the POTS peer as follows:

- Decide the dial peer tag value.
- Decide the destination pattern.
- Decide the port.

In most of the cases, other values than these shall be default values.

Step	Command	Description
1	Router# configure	Enters into the configuration mode.
2	Router(config)# dial-peer voice tag pots	Enters into the POTS configuration mode of the dial-peer configuration.

		The tag is the only identifier of the dial-peer of this system, and tag values range from 0 to 65535. The POTS means communication service configuration of the FXS and the FXO ports.
3	Router(config-dial-peer)# destination-pattern <i>string</i> [T]	Enters the telephone number of the corresponding dial peer. The string means the telephone number, and string values include 0 ~ 9, (#), (*) and the wildcard (.). The period (.) means the wildcard. Users can selectively enter (T) after the telephone number, and if a user enters (T) the system will collect dial digits till the end-of-dialing key (default #) or till the interdigit timer finishes.
4	Router(config-dial-peer)# port <i>location</i>	Maps the corresponding POTS with the port that the location indicates. The location is indicated by the slot-number or the port-number.
5	Router(config-dial-peer)# prefix <i>string</i>	(Selectively used.) When the corresponding POTS is selected as the termination side, the string is automatically dialed-out. String values include 0 ~ 9, (#), (*) and (.). When there is (,) the corresponding digit stops dialing-out for one second.
6	Router(config-dial-peer)# exit	Terminates the dial peer configuration mode.

5.3.2.3. VoIP Peer Configuration

Set the VoIP peer as follows:

- Decide the dial peer tag value.
- Decide the destination pattern.
- Decide the session target.

In most of the cases, other values than these shall be default values.

Step	Command	Description
1	Router# configure	Enters into the configuration mode.
2	Router(config)# dial-peer voice <i>tag</i> VoIP	Enters into the VoIP configuration mode of the dial-peer configuration. The tag is the only identifier of the dial-peer of this system, and tag values range from 0 to 65535. The VoIP means communication service configuration of the VoIP

		peer.
3	Router(config-dial-peer)# destination-pattern <i>string</i> [T]	Enters the telephone number of the corresponding dial peer. The <i>string</i> means the telephone number, and string values include 0 ~ 9, (#), (*) and wildcard (.). The period (.) means the wildcard. Users can selectively enter (T) after the telephone number, and if a user enters (T) the system will collect dial digits till the end-of-dialing key (default #) or till the inter-digit timer finishes.
4	Router(config-dial-peer)# session target <i>destination-ip-address</i>	Enters the IP address of the corresponding VoIP peer. The <i>destination-ip-address</i> shall be entered as a dotted decimal IP address. (Example: 123.321.1.2) If the <i>destination-ip-address</i> is "ras" the IP address of the corresponding VoIP peer will be found through the gatekeeper.
5	Router(config-dial-peer)# dtmf-relay [h245-alphanumeric]	(Selectively used.) Decides the DTMF tone transmission method for the corresponding VoIP-peer. The default value is h245-alphanumeric .

5.3.2.4. Setting CODEC and VAD in the Dial Peer

To set the COder-DECoder(CODEC) and the Voice Activity Detection (VAD) in the dial peer, how much bandwidth the voice session can have shall be defined. Normally, the CODEC converts analog signals into digital bit streams and vice versa. During this procedure, the CODEC defines the voice coder rate for the dial peer. The VAD prohibits silent packets (created while the caller/callee does not talk) from being sent.

5.3.2.4.1. Setting CODEC in the VoIP Dial Peer

To set the coder rate for the selected VoIP peer, use the following commands in the global setup mode (start.)

Step	Command	Description
1	dial-peer voice <i>tag</i> VoIP	Enters into the dial-peer setup mode to set the VoIP peer.

2	codec [g711alaw / g711ulaw /g729 / g7231r63 /g7231r53]	Selects the CODEC for the voice considering the coder rate.
----------	---	---

Codec The default of "Codec" command is **g7231r63**. In normal cases, the default value is the most suitable. However, to connect to a network that has high bandwidth or to get the highest voice quality, select **g711alaw** or **g711ulaw** from "Codec" command. These values allow better voice quality but require more bandwidth for the voice session.

For example, to use a CODEC with G.711a-law Rate for the VoIP dial peer 108, set the CODEC as follows:

```
dial-peer voice 108 voip
  destination-pattern 14085551234
  codec g711alaw
  session target 10.0.0.8
```

Besides doing the above, users can create CODEC classes and store them in the VoIP peer. While the above method sets only one CODEC, creating a CODEC class makes several CODEC lists and enables flexible negotiation with the VoIP router.

Create CODEC classes as follows:

Step	Command	Description
1	Router# configure	Enters into the configuration mode.
2	Router(config)# voice class codec tag	Enters into the CODEC class configuration mode. The tag is an identifier of the CODEC class.
3	Router(config-class)# codec preference value <i>codec-type</i>	Enters into the configuration mode.
4	Router(config-class)# codec preference value <i>codec-type</i>	Enters into the configuration mode.
5	Router(config-class)# exit	Terminates the CODEC class configuration mode. (After configuration is completed, configuration becomes valid.)

Then, save CODEC classes created above in a certain VoIP peer by the following method.

Step	Command	Description
1	dial-peer voice <i>tag</i> VoIP	Enters into the dial-peer setup mode to set the VoIP peer.
2	voice-class <i>codec</i> <i>codec-class-tag</i>	Selects a CODEC for the voice considering the voice coder rate.

The following example shows how to create CODEC class 99 and store it in the VoIP peer 108.

```
voice class codec 99
  codec preference 1 g7231r63
  codec preference 2 g729
dial-peer voice 108 voip
  voice-class codec 99
```

5.3.2.4.2. Setting VAD in the VoIP Dial Peer

To disable transmission of silent packets for the selected VoIP, use the following commands in the global setup mode (start.)

Step	Command	Description
1	dial-peer voice <i>number</i> VoIP	Enters into the dial-peer setup mode to set the VoIP peer.
2	vad	Disables transmission of silent packets. In other words, enables the VAD.

In the default status, the **VAD** is enabled. Normally, the default is the most suitable. However, to connect to a network with high bandwidth or to get the best voice quality, disable the **VAD**. By disabling the VAD, users can get better voice quality but more bandwidth is required for the voice session.

To enable the VAD for the VoIP dial peer 108, set the VAD as follows:

```
dial-peer voice 108 voip
  destination-pattern 14085551234
```

```
vad
session target 10.0.0.8
```

5.3.3. One-Stage Dialing versus Two-Stage Dialing

The VoIP network configuration inter-works with the normal telephone network or PABX of the office in most of cases, so multi-staged dialing is made. To decrease dialing stages, users shall add the telephone number of the termination side and the telephone number of the next stage to the called party number when setting a call in the termination side.

Consider that a subscriber connected to the voice port of the Gateway A attempts to make a call to the subscriber who is using PABX line #100 that is connected to the other VoIP Gateway B.

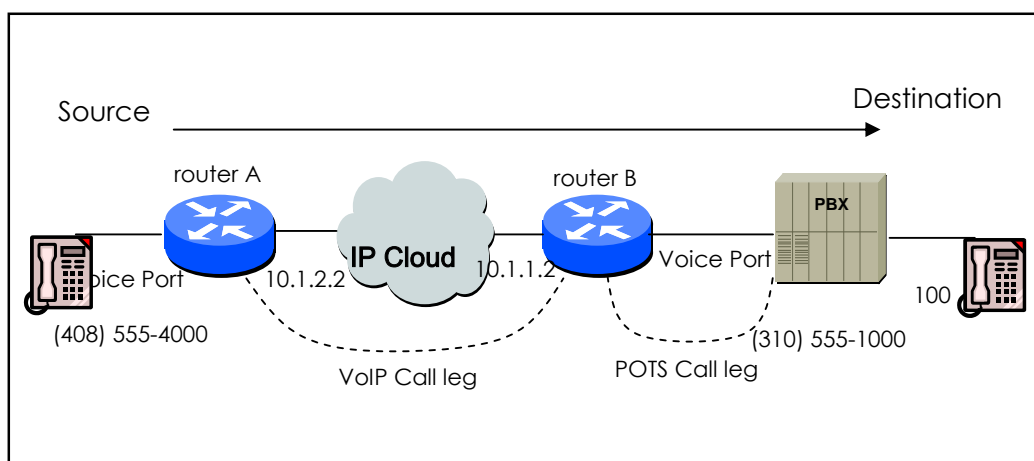


Figure 5.3 Two-Stage Dialing

Consider that the VoIP peer setup of the Gateway A is as follows:

```
dial-peer voice 555 VoIP
destination-pattern 310555....
```

In the above, as soon as the subscriber of Gateway A enters 3105551000, the outbound VoIP peer 555 will be decided and a call will be connected to Gateway B.

Consider that the POTS peer setup of Gateway B is as follows:

```
dial-peer voice 1000 pots
  destination-pattern 3105551000
```

At this time, the originating subscriber hears the dial tone that the PABX sends and will enter 100.

To change two-stage dialing into one-stage dialing, users shall set the VoIP peer of Gateway A as follows:

```
dial-peer voice 555 VoIP
  destination-pattern 310555.....
```

In this kind of setup, the subscriber of Gateway A shall enter 3105551000100 to establish a call, and Gateway B sends called party number and other digits than fixed digit information except the wildcard of the destination pattern to the voice port when the outbound POTS peer is selected as 1000. In this case 100 is sent.

If the length of the inter-working number is not fixed, it is better to use "T" as the destination pattern.

Set the VoIP peer of Gateway A as follows:

```
dial-peer voice 555 VoIP
  destination-pattern 310555T
```

In this case, if the subscriber of Gateway A enters the termination digit (#) after entering 31055510001234567 or if the inter-digit is timed-out, a call will be connected to Gateway B and Gateway B will send 1234567 to the selected voice port.

5.3.4. Hunt Group-related Configuration

5.3.4.1. Basic Concept and Configuration

To select the outbound POTS that is going out of the Gateway or to select the VoIP dial peer, the user shall compare the called party number of the inbound call and the destination pattern of the dial peer. At this time, more than one dial peers corresponding to the called party number belong to a hunt group, and dial peers of the hunt group attempts a call according to the given priorities.

In other words, the VoIP peer attempts a call to a dial peer of the hunt group when the call is failed due to network connection failure, gatekeeper failure, or gatekeeper rejection. And the POTS peer attempts a call to another dial peer of the hunt group when the call is failed due to corresponding voice port's being busy. Factors deciding priorities to attempt calls in the hunt group include the longest match, the explicit preference, the sequential, and the random.

The longest match decides priorities by the maximum digits matched between the origination number and the destination number of the dial peer. For example, consider that the origination number is 5683848, the destination number of dial peer 1 is 568T, the destination number of dial peer 2 is 568...., the destination number of dial peer 3 is 56838..., and the destination number of dial peer 4 is 5683848. Then, priorities of the dial peer by the longest match will be in order of dial peer 4 → dial peer 3 → dial peer 2 → dial peer 1.

In the explicit preference, the order set in the **preference** of the dial peer decides priorities. For example, consider that the preference of dial peer 1 is 3, the preference of dial peer 2 is 2, the preference of dial peer 3 is 1, and preference of dial peer 4 is 0. Then, priorities of the dial peer is in order of dial peer 4 → dial peer 3 → dial peer 2 → dial peer 1.

The random decides the dial peer within the hunt group randomly.

The sequential decides priorities according to the selection count. The less selected, the higher priority is given.

This priority algorithm operates using all these factors. For example, operation

of dial-peer hunt 0 decides the first priority according to the longest matching, checks the preference order within the same longest match priority, and then randomly selects the dial peer in the same preference order.

The first setup relating to the hunt group is to select the hunt algorithm.

Step	Command	Description
1	Router# configure	Enters into the global configuration mode.
2	Router(config)# dial-peer hunt [0-7]	Algorithm 0 ~ 7 are applied as follows: 0 – (default) longest match, explicit preference, random 1 - longest match, explicit preference, sequential 2 - explicit preference, longest match, random 3 - explicit preference, longest match, sequential 4 – sequential, longest match, explicit preference 5 - sequential, explicit preference, longest match 6 – random 7 - sequential

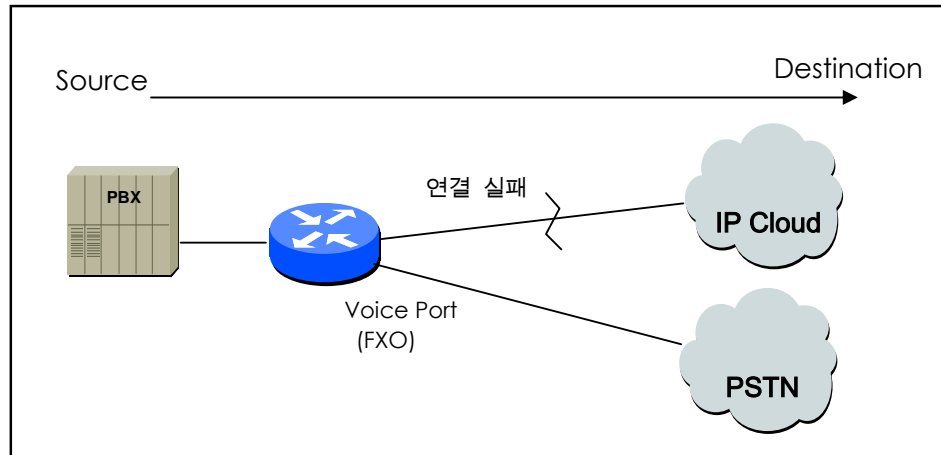
Users can also set priorities according to the **preference** or a huntstop in the corresponding peer according to the **huntstop**.

If a huntstop has been set in a certain dial peer and if an outbound call going to the dial peer is failed, the call will be terminated without hunting another dial peer.

Step	Command	Description
1	Router# configure	Enters into the configuration mode.
2	Router(config)# dial-peer voice tag { pots VoIP }	Enters into the dial-peer configuration mode. The tag is the only identifier of the dial-peer of this system, and tag values range from 0 to 65535.
3	Router(config-dial-peer)# preference number	The value ranges from 0 to 9, and the lower the value is, the higher the priority is.
4	Router(config-dial-peer)# huntstop	Sets the huntstop in the corresponding dial peer.

5.3.4.2. Rerouting to the PSTN

With the hunt group explained before, PSTN rerouting through the FXO voice port can be made when connection with the VoIP network fails. The following figure shows PSTN rerouting.



[Figure 5-3 PSTN Rerouting]

To make PSTN rerouting as shown in the above figure, set the dial peer as follows:

```

dial-peer voice 101 voip
  destination-pattern 472....
  session target 192.168.100.1
  preference 0
!
dial-peer voice 102 pots
  destination-pattern 472....
  prefix 472
  port 1/0
  preference 1
  
```

In the above example, VoIP peer 101 and POTS peer 102 exist in the same hunt group. Since the preference of the VoIP peer is low, the VoIP peer is selected first and used to attempt a call. However, if the VoIP peer fails, a call is attempted through the POTS peer 102.

5.3.4.3. Call barring

Using the **huntstop** and the **shutdown** of the dial peer explained before, users can bar the outbound/inbound calls with certain patterns.

To bar calls of the outbound peer, define the pattern to bar in the destination pattern and set the shutdown and the huntstop. If necessary, set the preference and select all dial peers to bar first.

In the following example, VoIP peer 100 has been selected for all outbound calls. However, if the called party number starts with 526 or the called party number is 5441234, the call will not processed any more.

```
dial-peer voice 100 voip
```

```
destination-pattern T
```

```
session-target ras
```

```
dial-peer voice 101 voip
```

```
destination-pattern 526T
```

```
session-target ras
```

```
huntstop
```

```
shutdown
```

```
dial-peer voice 102 voip
```

```
destination-pattern 5441234
```

```
session-target ras
```

```
huntstop
```

```
shutdown
```

To bar calls for the inbound VoIP peer, define the pattern to bar in the destination pattern and set the shutdown and the huntstop. If necessary, set the preference and select the dial peer to bar first.

In the above example, if the calling party number of the inbound call starts with 526 or is 5441234, the call will not processed any more.

To bar the inbound VoIP call and allow the outbound call of the number starting with 538, use "**answer-address**" command as follows:

```
dial-peer voice 103 voip
```

```
answer-address 538....  
shutdown
```

5.3.5. Prefix and Forwarding Telephone Numbers

Forwarding numbers for the POTS peer has been explained already. When the number for the outbound POTS peer is forwarded, only digits except fixed digits of the destination-pattern of the outbound POTS peer are forwarded.

For example, if the destination-pattern is 444...., the fixed digit is 444. At this time, if the called party number of the inbound call is 444123456, only digits "123456" are forwarded to the voice port corresponding to the outbound POTS peer. (In case of an analog voice port, DTMF tones are outputted.)

If **prefix 99,,** is set in this outbound POTS peer, 99 is output first and 123456 is output in two seconds.

The above explains number forwarding operation for the default setup. For more precise operation of number forwarding, perform **forward-digit** setting in the POTS peer setup. The dial peer for which the **forward-digit** has been set does not check fixed digits of the destination-pattern and forwards the number according to the value set in the forward-digit.

The forward-digit setting can be made by **forward-digit from** and **forward-digit last**.

Forward-digit from "*" forwards numbers from the "*"th digit, and forward-digit last "*" forward only last "*" digits.

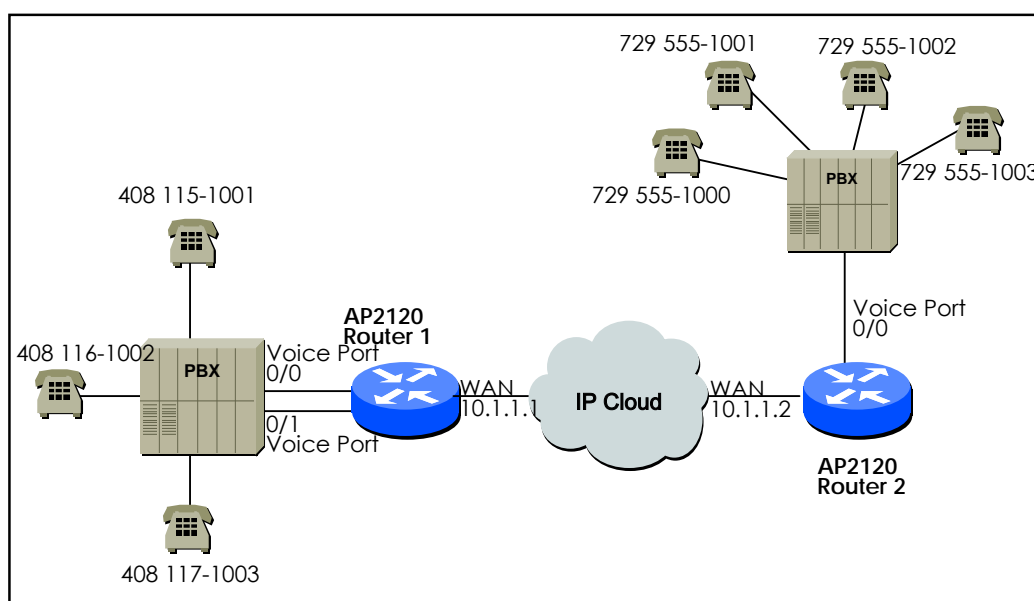
For example, if the called party number of the inbound call is 444123456 and "forward-digit from 4" is given, "123456" will be forwarded, and if the called party number is 444123456 and "forward-digit last 4" is given, "3456" will be forwarded.

5.3.6. Configuring Number Expansion

In most corporate environments, the telephone network is configured so that you can reach a destination by dialing only a portion (an extension number) of the full E.164 telephone number. Voice over IP can be configured to recognize extension numbers and expand them into their full E.164 dialed number by using two commands in tandem: **destination-pattern** and **num-exp**. Before you configure these two commands, it is helpful to map individual telephone extensions with their full E.164 dialed numbers. This task can be done easily by creating a number expansion table.

5.3.6.1. Number Expansion Table

In Figure 5.4, a small company wants to use Voice over IP to integrate its telephony network with its existing IP network. The destination pattern (or expanded telephone number) associated with Gateway 1 (located to the left of the IP cloud) are (408) 115-xxxx, (408) 116-xxxx, and (408) 117-xxxx, where xxxx identifies the individual dial peers by extension. The destination pattern (or expanded telephone number) associated with Gateway 2 (located to the right of the IP cloud) is (729) 555-xxxx.



[Figure 5-4 Sample VoIP Network]

Sample Number Expansion Table for this senario.

Extension	Destination Pattern	Num-exp Command Entry
5....	408115.....	num-exp 5 408115
6....	408116.....	num-exp 6 408116
7....	408117.....	num-exp 7 408117
1...	729555....	num-exp 2 729555

This information is used in configuration Gateway 1 and Gateway 2.

5.3.6.2. Configuring Number Expansion

To define how to expand an extension number into a particular destination pattern, use the following command in global configuration mode:

Step	Command	Description
1	num-exp <i>extension-number</i> <i>extension-string</i>	Configure Number expansion.

You can verify the number expansion information by using the **show num-exp** and **show dialplan number** command to verify that you have mapped the telephone numbers correctly.

5.3.7. Configuring Number Translation

5.3.7.1. Creating Translation Rules

Users can translate called/calling party number of the inbound/outbound calls in AP2120 Gateway. When translating called/calling party number of the inbound call, received called/calling party numbers are translated by the translation rule and used to select the outbound dial peer. When translating called/calling party numbers of the outbound call, called/calling party numbers that are used for originating a call are translated by the translation rule and calls are processed.

When changing private numbers into public numbers or vice versa or when extending numbers, number translation is used. Number translation provides more various conversions than number expansion. To translate numbers, a translation rule set shall be created first. Use "**translation-rule**" command on the global configuration mode to create a translation rule set.

Users can define more than one rules for the translation rule set using "**rule**" command on the translation-rule configuration mode. The following table shows how to define rules for the translation rule set.

Step	Command	Description
1	Router# configure	Enters into the configuration mode.
2	Router(config)# translation-rule tag	Enters into the translation rule configuration mode. The <i>tag</i> is an identifier of the translation rule set.
3	Router(translation-rule)# rule rule-tag <i>input-matched-pattern</i> <i>substituted-pattern</i>	The <i>rule-tag</i> is an identifier of the rule within the rule set. The rule-tag values range from 0 to 65535. The <i>input-matched-pattern</i> means the digit to be inputted for pattern-matching. 0 ~ 9, "#", "*", "[]", "." and T can be entered. The <i>substituted-pattern</i> is a pattern to be converted upon successful pattern matching. 0 ~ 9, "#", "*", "%", "." and T can be entered.

When one or more rules of a rule set match with the called/calling party number, the rule that most matches with the input-matched-pattern is selected.

The input-matched-pattern can perform range expression. (eg. [1-9]) Also, the wildcard (.) can be used to apply number of digits of the called/calling party number. If the input-matched-pattern is made of only (.) or (T) all called/calling-party-numbers will be translated.

The *substituted-pattern* converts the fixed digits (excluding the wildcard) of the *input-matched-pattern* into the string of the *substituted-pattern*. There are

two forms of the substituted-pattern.

For example, if the substituted-pattern is composed only of IA5 characters (0 ~9, #, and *) the substituted-pattern will convert the fixed digits of the input-matched-pattern into the string of the substituted-pattern and add other digits than fixed digits of the called/calling party number at the end.

Or, if the substituted-pattern uses "%" form, each digit of the called/calling party number is replaced by "%xx" to make a number. At the time, % values range from %01 to %99 (from the 1st digit to the 99th digit of the called/calling party number.)

If the *substituted-pattern* is composed only of (.) or (T) the called/calling-party-number will be made of other digits than fixed digits of the input-matched-pattern.

In the following example, if 00181463701234 is entered into the translation rule set 100, the number will be translated into 81463701234. In this way 0313961234 is translated into 82313961234, and 5261234 is translated into 8225261234.

translation-rule 100

rule 1 001..... .

rule 2 0..... 82

rule 3 [1-9]..... 822%01%02%03%04%05%06%07%08

Created translation rules can be verified by "**show translation-rule**" command.

For example, "show translation-rule 100" command will show rules of the translation rule set 100. To view the translation result, enter the number to test. To check the translation result of "1234" in the translation rule set 100, enter "show translation-rule 100 1234." At this time, the result will be 1234.

5.3.7.2. Applying Translation Rules to the Inbound POTS Calls

To apply the translation rule set to all calls received in the voice port, make

following setting.

Step	Command	Description
1	Router# configure	Enters into the global configuration mode.
2	Router(config)# voice-port <i>location</i>	Enters into the designated voice port configuration mode. The <i>location</i> is indicated by the slot-number/port-number.
3	Router(voice-port)# translate-incoming {called-number calling-number} <i>tag</i>	called-number: Applies the translation rule to the inbound called party number. calling-number: Applies the translation rule to the inbound calling party number. The <i>tag</i> refers to the rule set and tag values range from 0 to 65535.

If the translation rule is applied to the called party and if numbers are entered into the voice port in order, check if translation is made for each number entered. At this time, translation shall be made only once.

5.3.7.3. Applying Translation Rules to the Inbound VoIP Calls

To apply the translation rule set to all calls received from the network, make following setting.

Step	Command	Description
1	Router# configure	Enters into the global configuration mode.
2	Router(config)# voice service VoIP	Enters into the voice service VoIP setup mode.
3	Router(vservice-VoIP)# translate-VoIP-incoming {called-number calling-number} <i>tag</i>	called-number: Applies the translation rule to the inbound called party. calling-number: Applies the translation rule to the inbound calling party number. The <i>tag</i> refers to the rule set and tag values range from 0 to 65535.

5.3.7.4. Applying Translation Rules to the Outbound Calls

To apply the translation rule set to the outbound calls going to a certain dial

peer (POTS peer or VoIP peer) make following setting.

Step	Command	Description
1	Router# configure	Enters into the global configuration mode.
2	Router(config)# dial-peer voice tag { pots VoIP }	Enters into the dial-peer configuration mode. The tag is the only identifier of the dial-peer of this system, and tag values include 0 ~ 65535.
3	Router(dial-peer-config)# translate-outgoing {called-number calling-number} tag	called-number: Applies the translation rule to the outbound called party number. calling-number: Applies the translation rule to the outbound calling party number. The <i>tag</i> refers to the rule set and tag values range from 0 to 65535.

5.4. Configuration Voice Ports

5.4.1. Configuration Voice Ports of AP2120 Gateway

In general, voice port commands define the characteristics associated with a particular voice port signaling type. Under most circumstances, the default voice port command values are adequate to configure FXO and FXS ports to transport voice data over your existing IP network. For E&M port, due to the complexity of existing PBX network, it needs to have a specific voice port value to meet the existing telephone network device (PBX).

5.4.2. Voice Ports Configuration Task List and Steps

5.4.2.1. Configuring FXS or FXO Voice Ports

Under most circumstances the default voice port values are adequate for both FXO and FXS voice ports. If you need to change the default configuration for these voice ports, perform the following tasks. The first two tasks are required; the third task is optional.

- 1) Identify the voice port and enter the voice-port configuration mode.
- 2) Configure the following mandatory voice-port parameters.
- 3) Configure one or more of the following optional voice-port parameters.
 - PLAR(Private Line Auto Ringdown)
 - Description
 - Ring Number
 - Input Gain
 - Output Gain

Step	Command	Description
1	configure	Enter global configuration mode.
2	voice-port <i>location</i>	Identify the voice port you want to configure and enter voice-port configuration mode.
3	ring number <i>number</i>	(For FXO ports only) Specify the maximum number of rings to be detected before

		answering a call.
4	connection plar <i>string</i>	(Optional) Specify the private line auto ringdown (PLAR) connection, if this voice port is used for a PLAR connection. The string value specifies the destination telephone number.
5	description <i>string</i>	(Optional) Attach descriptive text about this voice port connection.
6	input gain <i>value</i>	Specify (in decibels) the amount of gain to be inserted at the receiver side of the interface. Acceptable values are from -31 to 31.
7	output gain <i>value</i>	Specify (in decibels) the amount of gain at the transmit side of the interface.

5.4.2.2. E&M Port configuration

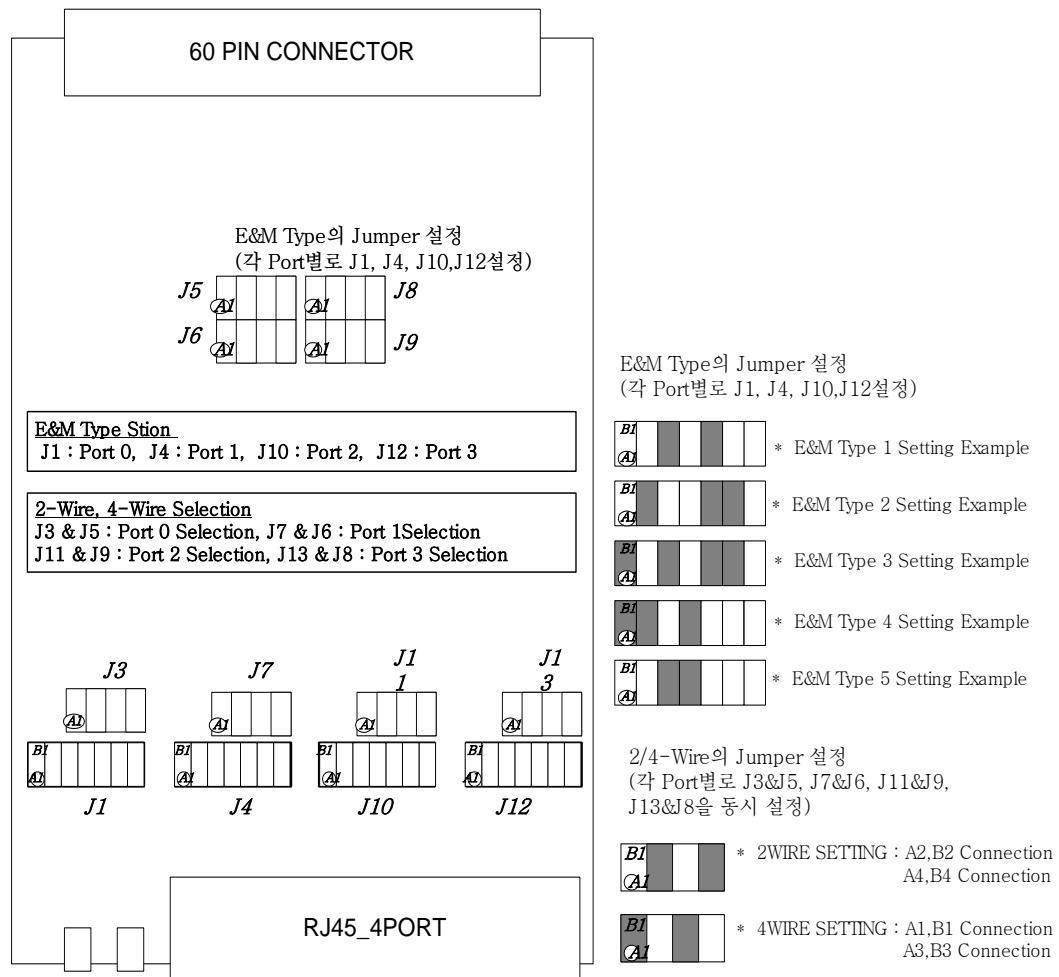
Unlike FXO and FXS Voice port, Default E&M Voice port Parameters are not sufficient to deliver voice data over IP network. So E&M Voice parameters should be set according to connected PBX.

To use E&M port, find out the proper E&M port configuration values of the PBX. Before configure E&M Voice port, follow the below steps. The first and second steps are mandatory and the third one is optional.

- 1) Select the voice port and move to voice port configuration mode.
- 2) Find out proper parameters and configure below parameters.
 - Signal Type
 - Operation
 - Type (Jumper Setting.)
- 3) Configure below optional parameters.
 - Connection Mode
 - Description

Order	Command	Description
1	Configure	Enter global configuration mode.
2	voice-port <i>location</i>	Identify the voice port you want to configure and enter voice-port configuration mode.. Location is marked as "slot-number/port-number"
3	signal { wink-start immediate delay-dial }	Select signal type for the interface.

4	Select Cabling Scheme for the port. Also, select it is 4-Wire or 2-Wire. AP2120 Gateway configures this part as Jumper setting. The default setting is 2-Wire. Refer to [Figure 5.5 E&M Module Jumper Setting].	
5	Select E&M Type of the port. Select from Type 1,2,3,5. AP2120 configures this part as Jumper setting. The default setting is Type-1. Refer to [Figure 5.5 E&M Module Jumper Setting]. The below describes signal of each E&M Type. Type 1 <ul style="list-style-type: none"> - E : output, relay to ground - M : input, referenced to ground Type 2 <ul style="list-style-type: none"> - E : output, relay to SG(Signal Ground) - M : input, referenced to ground - SB(Signal Battery) : feed for M, connected to -48V - SG(Signal Ground) : return for E, galvanically isolated from ground Type 3 <ul style="list-style-type: none"> - E : output, relay to ground - M : input, referenced to ground - SB(Signal Battery) : connected to -48V - SG(Signal Ground) : connected to ground Type 5 <ul style="list-style-type: none"> - E : output, relay to ground - M : input, referenced to -48V 	
6	operation {2-wire 4-wire} no operation	<u>This command is for Informational Description and do not applied. The real operation is conducted according to the jumper setting. This command only shows the type of wiring without checking jumper.</u>
7	type {1 2 3 5} no type	<u>This command is for Informational Description and do not applied. The real operation is conducted according to the jumper setting. . This command only shows the type of E&M without checking jumper.</u>
8	connection plar <i>string</i>	(Optional) If the port uses PLAR (Private Line Auto Ringdown), configure PLAR. String is Destination Phone Number.
9	description <i>string</i>	(Optional) To add Text description of the voice port connection.



[Figure 5-5 E&M module Jumper Setting]

5.4.2.3. E&M Voice Port Tunning

Normally, E&M Voice Port Tunning is sufficient with Default values. However, according to the existing telephone network, modify the parameters of E&M Voice port such as timing, Input Gain/ Output Gain and etc.

- 1) Enter Voice port configuration mode.
- 2) Set the optional voice port parameters.
 - Input Gain
 - Output Gain
 - Timing other then Timeout

To do E&M port Tunning, use the below commands.

After configuring voice port, activate/deactive the port with "**shutdown / no shutdown**" commands.

Order	Command	Description
1	Configure	Enter global configuration mode.
2	voice-port <i>location</i>	Identify the voice port you want to configure and enter voice-port configuration mode.. Location is market as "slot-number/ port-number"
3	input gain <i>value</i>	Set the input gain as Decibel. The acceptable values are "-6 ~ 14"
4	output gain <i>value</i>	Set the output gain as decibel. The acceptable values are "0 ~ 14".
5	timing delay-duration <i>milliseconds</i>	Set delay signal duration for delayed dial signal. The acceptable values are "100~5000msec".
6	timing delay-start <i>milliseconds</i>	The min. delay time between "Incomming seizure" and "Outgoing signal." The acceptable values are "20~2000msec".
7	timing wink-duration <i>milliseconds</i>	Set the max. Wink signal duration. The acceptable values are "100~400msec".
8	timing wink-wait <i>milliseconds</i>	Set the max. wink-wait duration of Wink start signal. The acceptable values are "100~5000msec".
9	timing dialout-delay <i>milliseconds</i>	Set Dial-out Delay to send number to E&M Trunk or to Cut-Thought. The acceptable values are "100~5000msec".
10	timing wait-wink <i>milliseconds</i>	Set the max. wait value of Wink signal. The acceptable values are "100~5000msec".

5.4.2.4. Activating/Deactivating the Voice Ports

To activate a voice port, use the following commands in voice-port configuration mode:

Step	Command	Description
1	no shutdown	Activate the voice port

To deactivate a voice port, use the following command in voice-port configuration mode

Step	Command	Description
1	voice-port <i>location</i>	Identify the voice port you want to activate and enter the voice-port configuration mode.
2	no shutdown	Activate the voice port.

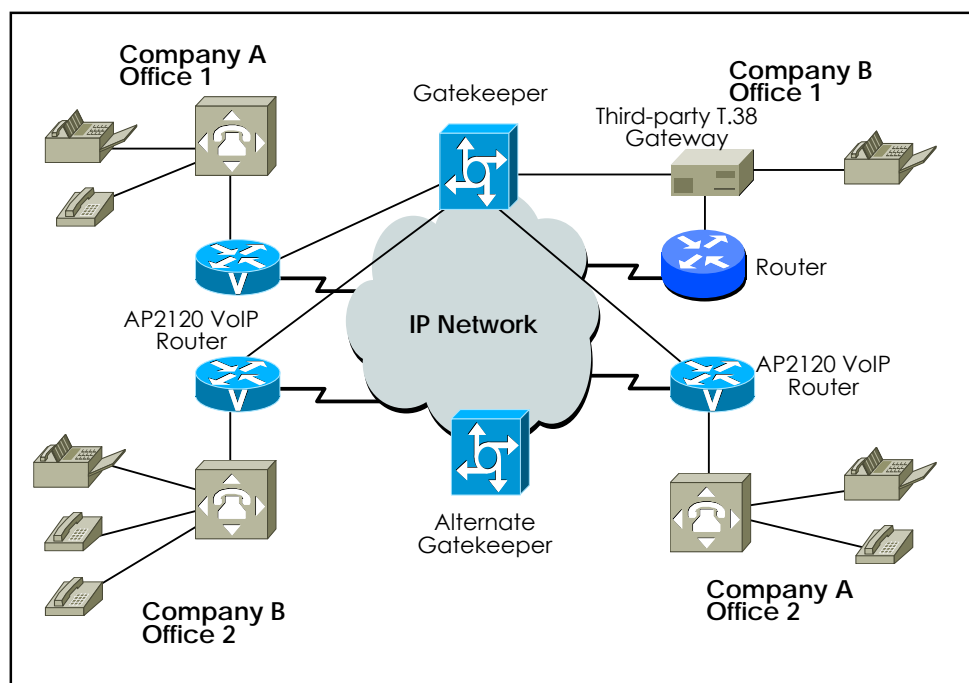
5.5. Configuring FAX Application

5.5.1. T.38 FAX Relay using VoIP H.323

The T.38 Fax Relay for VoIP H.323 feature provides standards-based fax relay protocol support on the most of VoIP router or Gateway including AP2120.

For effective use of FAX Relay, change the configuration of other company's gateway to T.38, standard protocol.

The below figure shows IP H.323 network with T.38 FAX Relay using AP2120 gateway and gateway/gatekeepers from other companies. With T.38 FAX Relay, gateways/gatekeepers of this network can send FAX to companies on the other offices.



[Figure 5-6 IP Network for T.38 Fax Relay]

For example, when a fax is sent from the originating gateway, a voice call is established. The terminating gateway detects the fax tone generated by the answering fax machine. The VoIP H.323 call stack then starts a T.38 mode request using H.245 procedures. If the opposite end of the call acknowledges the T.38 mode request, the initial audio channel is closed and a T.38 fax relay

channel is opened. When the fax transmission is completed, the call reverts to voice mode.

5.5.2. Configuring T.38 FAX Relay for VoIP H.323

To configure T.38 Fax Relay for VoIP H.323 for all the connections of a gateway, which is required, use the following commands in the global configuration mode:

Step	Command	Description
1	Router(config)# voice service VoIP	Enters voice-service configuration mode.
2	Router(config-vservice-VoIP)# fax protocol {t38 [redundancy value] }	Specifies the global default fax protocol. · t38 : Enable T.38 Fax relay protocol · redundancy : (Optional) Configuration Redundant T.38 Fax packet · value : Redundancy Value. Range : 0 ~ 5, Default Value : 0 .
3	Router(config-vservice-VoIP)# fax rate {2400/ 4800 / 7200 / 9600 /12000 / 14400 / disable }	Selects the maximum fax transmission speed.
4	Router(config-vservice-VoIP)# exit	Exits voice-service configuration mode and returns to the global configuration mode.

If redundancy is set as 1 or higher, not 0, in the above setting, contents of T.38 packet will be duplicated as many times as the redundancy number and transmitted.

In this case, higher bandwidth will be required. Therefore, set redundancy as 1 or higher only when there is UDP packet loss in the network. In other cases, set redundancy as 0.

Set the maximum speed for the fax rate. However, the fax rate is decided by the transmission cable quality and the transmission speeds of the VoIP gateway and two fax machines on both sides. If the fax rate is set disabled, T.38 session will not be opened.

5.5.3. FAX Relay setting by Bypass

To set fax relay with G.711 PCM clean channel in addition of T.38 fax relay, use

following commands in Global Configuration Mode. To do fax relay in this mode voice channel shall be opened with g711alaw or g711ulaw. So, codec and codec-class setting of dial-peer need to support g711alaw or g711ulaw interface and counterpart needs to set in G.711 mode.

Step	Command	Description
1	Router(config)# voice service VoIP	Converts into Voice Service Setting Mode
2	Router(config-vservice-VoIP)# fax protocol bypass	Sets Global default FAX protocol
3	Router(config-vservice-VoIP)# exit	Exits from Voice-Service Setting Mode and return to Global setting Mode

5.6. Other VoIP Configuration

5.6.1. Setting H.323 Gateway

H.323 gateway inter-works with the gatekeeper and receives the Registration Admission and Security (RAS) service. AP2120 Gateway can set static IP address in the VoIP peer and operate without any gatekeeper. Also, the AP2120 Gateway can dynamically bring the IP address (the other party's number) through the gatekeeper without setting any IP address.

For this, h323 ID of the gateway is necessary, and h323 ID is the only identifier in the gatekeeper. If VoIP IP address of the router is 211.123.1.2, the AP2120 Gateway sets the default h323 ID as VoIP.211.123.1.1. Users can set H323 ID in the gateway setup mode using "**h323-id**" command.

AP2120 Gateway uses "**gkip**" command to designate gatekeepers. With "gkip" command, users can designate more than one gatekeeper and register them by priorities. There is only one gatekeeper that can be registered at the same time.

For the security between the gateway and the gatekeeper, users can set the secure token using "**security password**" command. However, if the password is enabled, the gateway will add Crypto Token to the message and send the message to the gatekeeper. Only when CryptoH323Token is set for the gatekeeper and cryptoEPPwdHash is supported, this security setup can be made. At this time, the password is given by the administrator off line.

When the user exits the gateway setup mode by "**exit**" or "**end**" gateways start to be registered in the gatekeeper.

To cancel registration of gateway in the gatekeeper, use "**no gateway**" command in the global setup mode.

Step	Command	Description
1	Router# configure	Enters into the configuration mode.
2	Router(config)# gateway	Enters into the gateway configuration mode, and registers the gateway in the gatekeeper.
3	Router(config-gateway)# gkip <i>gatekeeper-ip-address [port] [priority]</i>	Designates the gatekeeper ip address.
4	Router(config-gateway)# h323-id <i>h323-id</i>	Designates h323 id of the gateway.
4	Router(config-gateway)# security password	Sets the H.235 security password.

	<i>password</i>	
5	Router(config-gateway)# exit	Exits configuration.

5.6.2. Configuring H323 Call Start Mode

In H.323 version2, logical channel negotiation procedures made by the fast start mode upon the start of the H.323 call is explained.

In the voice service VoIP setup mode, users can select the fast start procedures by using "**h323 call start**" command in AP2120 Gateway.

The fast start mode is the default, and H245 tunneling and the fast start is disabled when the slow start is set.

To find out the capability (T.38 fax, DTMF relay capability, etc.) of the other side in the fast start mode, users can perform H.245 procedures.

Step	Command	Description
1	Router# configure	Enters into the global configuration mode.
2	Router(config)# voice service VoIP	Enters into the voice service VoIP setup mode.
3	Router(vservice-VoIP)# h323 call start {fast slow}	Sets the fast mode or the slow start mode.

5.6.3. Configuring User Class

User-class setting is used to reject receiving calls from the unauthorized users when an incoming call arrives in the FXO from the network. When a user attempts a call to the FXO port through the network while no user-class is set, the user will have to enter the extension code digit after hearing dial tones generated by the PBX if the FXO is connected to the internal line of the PBX. However, if the FXO is connected to the PSTN, the user will hear dial tone created by the PSTN switching machine and will have to enter the other side number of the PSTN.

If any user-class is set, the user who makes the first call will hear "beep" sound instead of the dial tone. If the user enters the **password** at this time and if the password is authorized, the user can enter as many numbers as max-digits defined in the user-class. ("Beep" sound may not occur due to the gateway

on the origination side.) In this way, users can control internal calls, local calls, long-distance calls, and international calls by controlling "**max-digit**."

Users can set more than one user-classes and set call limits for other user-classes.

To keep the security of calls incoming to the FXO port through the network, users can use this command and **security permit-FXO** in the AP2120. Since it is possible to directly attempt calls to the PSTN through this FXO port or indirectly attempt calls to the PSTN through the PBX internal line, unauthorized remote users can attempt calls as well.

To prevent unauthorized users' attempting calls, the security shall be kept. Two security systems that the AP2120 Gateway provides have following advantages and disadvantages.

With "security permit-FXO" command, remote users does not need to enter the password so they can easily access the network. However, IP address of the VoIP peer on the other side shall be registered and the gatekeeper cannot be used at the same time. Also, it is not possible to bar calls of the registered peers by class.

With the "voice class user" users need to enter the password digit but stronger and multi-classed call barring is possible.

Step	Command	Description
1	Router# configure	Enters into the configuration mode.
2	Router(config)# voice class user tag	Enters into the user class configuration mode. The tag is a user class identifier.
3	Router(config-class)# password digits	Sets the password. At this time, digits include IA5 characters (0~9, #, and *) and the digit length is 4.
4	Router(config-class)# max-digits value	Sets the maximum number of digits when generating origination signals with the FXO. By adjusting the maximum number of digits, users can set PBX internal calls, local calls, long-distance calls and international calls.
5	Router(config-class)# exit	Terminates the user class configuration mode.

5.7. VoIP Configuration Command

5.7.1. VoIP-Related whole Command

```

clear      h323      call      all
           tag <0-4294967295>

voice-port <0-1>/<0-3>
           all

configure

dial-peer  hunt      <0-7>
           ipaddr-prefix #,_, n
           terminator #, *, n
           voice      tag <0-65535> pots

           destination-pattern
           n string
           forward-digits from <0-99>
           last <0-99>

           huntstop

           no destination-pattern
           forward-digits
           huntstop
           port
           preference
           prefix
           register e164
           shutdown
           translate-outgoing
           called-number
           r calling-number
           er

           slot / port
           <0-3>/<0-3>
           port
           preference <0-9>
           prefix string
           register e164
           shutdown
           translate-outgoing
           tag
           called-number <0-65535>
           tag
           calling-number <0-65535>

voip

answer-address string
              g711alaw | g711ulaw | g729 | g7231r63 |
              g7231r53
codec         g7231r53
description   string
destination-pattern
n string
              h245-alphanumeric
dtmf-relay    meric

```

```

                                huntstop
                                no
                                answer-address
                                codec
                                description
                                destination-pattern
                                dtmf-relay
                                huntstop
                                preference
                                session      target
                                shutdown
                                sid
                                translate-outgoing
                                called-number
                                calling-number
                                vad
                                voice-class  codec
                                preference    <0-9>
                                session      target      ip-address
                                                ras
                                shutdown
                                sid
                                translate-outgoing
                                called-number  tag
                                                <0-65535>
                                calling-number  tag
                                                <0-65535>
                                vad
                                voice-class  codec      tag
                                                <0-65535>

gateway
discovery
gkip      ip-address      port<0-65536>      priority<0-254>
                                <cr>
                                <cr>
lightweight-irr
h323-id    string
no         discovery
gkip      ip-address
lightweight-irr
public-ip
register
security   password

public-ip
register
security   password

no         dial-peer      hunt
                                ipaddress-prefix
                                terminator
                                voice      tag <0-65535>      pots
                                                voip

gateway
```

[illegible]

		security	permit-FXO
		timeout	t301
			t303
			tras
			tttl
			tidt
			treg
		translate-voip-inc	
		oming	called-number
			calling-number
	security	permit-FXO	
	timeout	t301	<5-600>
			default :180
		t303	<5-60>
			default :8
		tras	<2-30>
			default :6
		tttl	<10-600>
			default :60
		tidt	<1-600>
			default :10
		treg	<10-600>
			default :30
	translate-voip-inc		
	oming	called-number	tag <0-65535>
		calling-number	tag <0-65535>
voice-port	slot/port		
		comfort-noise	
	connection	plar	string
	description		string
	echo-cencel		
	input	gain	num <-13 - 31>
	no	comfort-noise	
		connection	plar
		description	string
		echo-cencel	
		input	gain
		operation	
		output	
		ring	number
		shutdown	
		signal	
		timing	dialout-delay
			delay-duration
			delay-start
			wait-wink
			wink-duration
			wink-wait
		translate-incomin	
		g	called-number
			calling-number
		type	
	operation		<u>2-wire</u> / 4-wire
	output	gain	num <-31 - 31>

			ring	number	<i>num <1-255></i>
			shutdown		
			signal	<i>delay-dial immediate <u>wink-start</u></i>	
			timing	dialout-delay	<i>num <50-5000></i>
				delay-duration	<i>num <100-5000></i>
				delay-start	<i>num <20-2000></i>
				wait-wink	<i>num <100-5000></i>
				wink-duration	<i>num <30-5000></i>
				wink-wait	<i>num <100-5000></i>
			translate-incom		
			ing	called-number	<i>tag <0-65535></i>
				calling-number	<i>tag <0-65535></i>
			type	<i><u>1</u> 2 3 5</i>	
	voip-interfa		(default	ether	
	ce	<i>interface</i>	0.0)		
show	call	active	all		
			summary		
		history	all	last	<i>num <1-100></i>
				<i><cr></i>	
	clear-down-tone				
	codec-clas				
	s	<i>tag <0-65535></i>			
		<i><cr></i>			
	dialplan	number	<i>string</i>		
		port	<i>slot / port</i>		
	dial-peer	pots	<i>tag <0-65535></i>		
			summary		
			<i><cr></i>		
		voice	<i>tag <0-65535></i>		
			summary		
			<i><cr></i>		
		voip	<i>tag <0-65535></i>		
			summary		
			<i><cr></i>		
	gateway				
	num-exp				
	translation-	<i>tag</i>			
	rule	<i><0-65535></i>	<i>string</i>		
			<i><cr></i>		
		<i><cr></i>			
	user-class				
	voice	port	<i>slot/port</i>		
			summary		
			<i><cr></i>		
	voip-interfa				
	ce				

5.7.2. Global Configuration Command

5.7.2.1. dial-peer hunt

To set the priorities for selecting the dial peer hunt, use “**dial-peer hunt**” command on the global setup mode.

To return to the default setting, use “**no**” command before this command.

dial-peer hunt *hunt-order-number*

no dial-peer hunt

5.7.2.1.1. Syntax

Keyword / Argument	Description
<i>hunt-order-number</i>	Priority algorithm 0 ~ 7 are applied as follows: 0 – (default) longest match, explicit preference, random 1 - longest match, explicit preference, sequential 2 - explicit preference, longest match, random 3 - explicit preference, longest match, sequential 4 – sequential, longest match, explicit preference 5 - sequential, explicit preference, longest match 6 – random 7 - sequential

5.7.2.1.2. Default value

0 – longest match, explicit preference, random

5.7.2.1.3. Command Mode

Global Configuratin mode

5.7.2.1.4. Usage Guideline

To select the outbound POTS going out of the Gateway or the VoIP dial peer, the called party number of the inbound call and the destination pattern of the dial peer are compared. At this time, more than one dial peers corresponding to the called party number belong to a hunt group, and dial

peers in the hunt group attempt calls according to given priorities.

In other words, the VoIP peer attempts a call to a dial peer of the hunt group when the call is failed due to network connection failure, gatekeeper failure, or gatekeeper rejection. And the POTS peer attempts a call to another dial peer of the hunt group when the call is failed due to corresponding voice port's being busy.

Factors deciding priorities to attempt calls in the hunt group include the longest match, the explicit preference, the sequential, and the random.

The longest match decides priorities by the maximum digits matched between the origination number and the destination number of the dial peer. For example, consider the origination number is 5683848, the destination number of dial peer 1 is 568T, the destination number of dial peer 2 is 568..., the destination number of dial peer 3 is 56838..., and the destination number of dial peer 4 is 5683848. Then, priorities of the dial peer by the longest match will be in order of dial peer 4 → dial peer 3 → dial peer 2 → dial peer 1.

In the explicit preference, the order set in the **preference** of the dial peer decides priorities. For example, consider the preference of dial peer 1 is 3, the preference of dial peer 2 is 2, the preference of dial peer 3 is 1, and preference of dial peer 4 is 0. Then, priorities of the dial peer is in order of dial peer 4 → dial peer 3 → dial peer 2 → dial peer 1.

The random decides the dial peer within the hunt group randomly.

The sequential decides priorities according to the selection count. The less selected, the higher priority is given.

This priority algorithm operates using all factors mentioned above. For example, operation of hunt-order-number 0 decides the first priorities according to the longest matching, checks the preference order within the same longest match priority, and then randomly selects the dial peer in the same preference order.

5.7.2.1.5. Example

In the following example, "longest match" "explicit preference" and "sequential" algorithms are applied to the hunting group.

dial-peer hunt 1

5.7.2.2. dial-peer ipaddr-prefix

To designate a special character to be used as a ipaddr-prefix for making call by ip address, use the **dial-peer ipaddr-prefix** global configuration command. Use the **no** form of this command to default setting.

dial-peer ipaddr-prefix *character*

no dial-peer ipaddr-prefix *character*

5.7.2.2.1. Syntax

Keyword / Argument	Description
character	Designates ip address prefix. Valid numbers and characters are #, *

5.7.2.2.2. Default value

Character (*)

5.7.2.2.3. Command Mode

Global Configuration mode

5.7.2.2.4. Usage Guideline

In normal case, making a remote call is handled by number digits configured at dial-peer destination pattern and session target by VoIP router operator. Although this pre-configured method is easy and secure, making a call by end-user with IP address of destination terminal is useful to call to ubiquitous VoIP terminal and gateway.

This prefix is used to discriminate normal call with number digits and direct call with IP address. To solve conflicting with terminator character, terminator character and ip address prefix character are changed automatically when configuring it.

5.7.2.2.5. Example

The following example configures * as the special ip address prefix character:

```
configure
dial-peer ipaddr-prex *
```

The following example shows digit sequence for making a call by IP address. If IP address is 127.0.1.1 and called party number is 1234 then sequence of digits to making that call is:

```
* 10 * 0 * 0 * 1 * 1234 #
```

In above sequence, the first digit is **ipaddr-prefix** and the **ipaddr-prefix** character is used to discriminate IP address dot. And the last digit is **terminator** character.

When the destination terminal is simple VoIP phone like Microsoft **Netmeeting**, sequence of digits would be:

```
* 10 * 0 * 0 * 1 #
```

5.7.2.3. dial-peer terminator

To designate a special character to be used as a terminator for variable length dialed numbers, use the **dial-peer terminator** in global configuration command. Use the **no** form of this command to default setting.

dial-peer terminator *character*

no dial-peer terminator *character*

5.7.2.3.1. Syntax

Keyword / Argument	Description
character	Designates the terminating character for a variable-length dialed number. Valid numbers and

	characters are #, *.
--	----------------------

5.7.2.3.2. Default Value

Character (#)

5.7.2.3.3. Command Mode

Global Configuration mode

5.7.2.3.4. Usage Guideline

There are certain areas in the world (for example, in certain European countries) where valid telephone numbers can vary in length. When a dialed-number string has been identified as a variable length dialed-number, the system waits until the configured value for the **timeouts interdigits** command has expired before placing the call.

To avoid waiting until the interdigit timeout value has expired, you can designate a special character as a terminator---meaning that when you dial that character, the system no longer waits for any additional digits and places the call.

Use the **dial-peer terminator** in global configuration command to designate a particular character as a terminator.

To disable the terminator, use `dial-peer terminator n`.

5.7.2.3.5. Example

The following example configures # as the special terminating character for variable-length dialed-numbers:

```
configure
dial-peer terminator #
```

5.7.2.4. dial-peer voice

To enter dial-peer configuration mode (and specify the method of voice-related encapsulation), use the **dial-peer voice** in global configuration command.

dial-peer voice *number* {voip/pots}

5.7.2.4.1. Syntax

Keyword / Argument	Description
number	Digit(s) defining a particular dial peer. Valid entries are from 1 to 2147483647.
VoIP	Indicates that this is a VoIP peer using voice encapsulation on the POTS network.
pots	Indicates that this is a POTS peer using Voice over IP encapsulation on the IP backbone.

5.7.2.4.2. Default Value

No Default Value.

5.7.2.4.3. Command Mode

Global Configuration Mode

5.7.2.4.4. Usage Guideline

Use the **dial-peer voice** global configuration command to switch to the dial-peer configuration mode from the global configuration mode. Use the **exit** command to exit the dial-peer configuration mode and return to the global configuration mode.

5.7.2.4.5. Example

The following example accesses dial-peer configuration mode and configures a POTS peer identified as dial peer 10:

```
configure
```

dial-peer voice 10 pots

5.7.2.5. gateway

To enable the H.323 Voice over IP gateway, use the **gateway** command in global configuration mode. Use the **no** form of this command to unregister this gateway with the gatekeeper.

gateway
no gateway

5.7.2.5.1. Syntax

This command has no keywords or arguments.

5.7.2.5.2. Default Value

No Default Value

5.7.2.5.3. Command Mode

Global Configuration Mode

5.7.2.5.4. Usage Guideline

Use the **gateway** command to enable H.323 VoIP gateway functionality. After you enable the gateway, it will attempt to discover a gatekeeper by using the H.323 RAS GRQ message. If you enter **no gateway**, the VoIP gateway will unregister with the gatekeeper via the H.323 RAS URQ message.

5.7.2.5.5. Example

The following example enables the gateway:

```
gateway
```

5.7.2.6. num-exp

To define how to expand an extension number into a particular destination pattern, use the **num-exp** global configuration command. Use the **no** form of this command to cancel the configured number expansion.

num-exp *extension-number expanded-number*

no num-exp *extension-number expanded-number*

5.7.2.6.1. Syntax

Keyword / Argument	Description
Extension-number	Digit(s) defining an extension number for a particular dial peer. (max length 55) Available character' s are 0-9#*%.T.
Expanded-number	Digit(s) defining the expanded telephone number or destination pattern for the extension number listed. (max length 55) Available character' s are 0-9#*%.T.

5.7.2.6.2. Default value

No Default Value

5.7.2.6.3. Command Mode

Global Configuraiton Mode

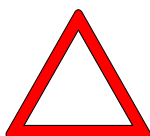
5.7.2.6.4. Usage Guideline

Use the **num-exp** global configuration command to define how to expand a particular set of numbers (for example, an extension number) into a particular destination pattern. With this command, you can map specific extensions and expanded numbers together by explicitly defining each number, or you can define extensions and expanded numbers using variables. You can also use this command to convert seven-digit numbers to numbers containing less than seven digits.

Number expansion is applied to the called party number of the inbound call. The called party number of the inbound call from the voice port or the network is translated by number expansion, and the dial peer is selected according to the translation result.

If more than one number expansions match with the called party number of the inbound call, the number expansion that matches most with the fixed pattern of the expansion-number will be selected.

Caution



It is recommended to take cautions when using number expansion with **translation-incoming** of the voice port or **translate-VoIP-incoming** of the network at the same time. If translation of the number is clear enough, it is not recommended to use two methods at the same time. If a user uses two methods, **translation-incoming** or **translate-VoIP-incoming** will be applied first and then number expansion will be applied.

Expansion-number can perform range expression. (eg. [1-9]) Also, the wildcard (.) can be used to apply number of digits of the called party number. If extension-number is configured only with (.) or (T) number translation is applied to all called-party-number.

Expanded-number is to convert fixed digits (excluding the wildcard) of the extension-number into the string of the expanded-number. There are two forms of the expanded-number. See the following:

If the expansion-number is composed only of IA5 characters (0 ~ 9, # and *) fixed digits of the extension-number will be converted into the string of the expanded-number, and other digits than the fixed digits of the called-party-number will be added at the end.

Or, if the expansion-number uses "%" form, each digit of the extension-number will be replaced by "%xx" to make a number. At this time, % values range from %01 to %99 (from the 1st digit to the 99th digit of the called-party-number.)

If the expanded-number is composed of (.) or (T) only, the called

-party-number is made of other digits than the fixed pattern of the extension-number.

5.7.2.6.5. Example

The following example expands the extension number 5541 to be expanded to 1408555541: In the following example, the inbound called party number 554123 is extended into 14085554123.

```
num-exp 5541 1408555541
```

In the following example, if the inbound called party number is 5551, the translation rule will not be applied. However, if the inbound called party number is 5551234, it will be translated into 14085551234.

```
num-exp 555.. 1408555
```

In the following example, if the inbound called party number is 1251234, it will be translated into 1408551234. And 3551234 will be translated into 14085551234.

```
num-exp [1-3][25]5.. 1408555
```

In the following example, if the inbound called party number is 5551234, it will be translated into 4441234.

```
num-exp 555.. 444%04%05%06%07%08%09%10%11%12
```

In the following example, if the inbound called party number is 55512, 5551234 or 555123456, it will be translated into 444.

```
num-exp 555.. 444%99
```

In the following example, if the inbound called party number is 5551234, it will be translated into 3334.

```
num-exp 555.. 111
```

```
num-exp 55512 222
```

```
num-exp 555[0-9][0-9][0-9] 333
```

In the following example, if the inbound called party number is 5551234, it will

be translated into 1234.

num-exp 555 .

num-exp 555 T

In the following example, if the inbound called party number is 5551234, it will be translated into 95551234.

num-exp . 9

num-exp T 9

5.7.2.7. translation-rule

To enter into the translation rule setup mode, use "**translation-rule**" command in the global setup mode. To delete the translation rule that has been set, use "**no**" command before "**translation-rule**" command.

translation-rule *tag*

no translation-rule *tag*

5.7.2.7.1. Syntax

Keyword / Argument	Description
tag	An identifier to designate the translation rule set

5.7.2.7.2. Default value

No Default Value

5.7.2.7.3. Command Mode

Global Configuration Mode

5.7.2.7.4. Usage Guideline

This command is to enter into a mode to set the translation rule of the called/calling party number of the inbound/outbound call.

5.7.2.7.5. Examples

The following example is to set the translation rule set 100.

```
translation-rule 100  
    rule 0 2 822
```

5.7.2.8. voice-port

To enter the voice-port configuration mode, use the **voice-port** global configuration command.

```
voice-port slot_number/port_number
```

5.7.2.8.1. Syntax

Keyword / Argument	Description
slots	Specifies the slot number in the router where the voice network module is installed. Valid entries are from 0 to 1, depending on the voice interface card you have installed.
port	Specifies the voice port. valid entries are 0 to 3.

5.7.2.8.2. Default Value

No Default Value

5.7.2.8.3. Command Mode

Global Configuration Mode

5.7.2.8.4. Usage Guideline

Use the **voice-port** configuration command to switch to the voice-port configuration mode from the global configuration mode. Use the **exit** command to exit the voice-port configuration mode and return to the global

configuration mode.

5.7.2.8.5. Example

The following example accesses the voice-port configuration mode for slot 1 and port 3:

```
configure
voice-port 1/3
```

5.7.2.9. voice class clear-down-tone

To configure clear down tone on the FXO port, use the **voice class clear-down-tone** global configuration command.

```
voice class clear-down-tone tag lowFreq highFreq onTime offTime
no voice class clear-down-tone tag
```

5.7.2.9.1. Syntax

Keyword / Argument	Description
tag	Specifies the clear down tone. Valid entries are from 0 to 1.
lowFreq	Specifies the low frequency, of Hz, of the clear-down tone provided by the local switch or PBX. The frequency range is from 300Hz to 1980 Hz
highFreq	Specifies the high frequency, of Hz, of the clear-down tone provided by the local switch or PBX. The frequency range is from 300Hz to 1980 Hz. In case of single tone, value is 0.
onTime	Specifies the on-time duration of clear down tone.
offTime	Specifies the off-time duration of clear down tone. In case of long duration tone, value is 0.

5.7.2.9.2. Default Value

No Default Value

5.7.2.9.3. Command Mode

Global Configuration Mode

5.7.2.9.4. Usage Guideline

Call termination of FXO voice-port is established through detection of clear-down tone from PSTN or PBX, which is connected with FXO port. This clear-down tone(Ex: busy tone, fast busy tone) is different from each PSTN and PB. So, handle it as registering by this command.

This command is to enable to user to set detection tones in addition to clear-down-tone provided by the system. If the default detection tone provided by the system and shown in the clear-down-tone is enough, additional setting is not necessary.

To operate newly added detection tones, reboot the system.

5.7.2.9.5. Example

Following example shows setting of clear down tone whose dual-tone 350 Hz and 420 Hz is on time 250 msec, off time 250 msec.

```
configure
voice class clear-down-tone 0 350 420 250 250
```

5.7.2.10. voice class codec

To enter voice-class configuration mode and assign an identification tag number for a codec voice class, use the **voice class codec** command in global configuration mode. To delete a codec voice class, use the **no** form of this command.

```
voice class codec tag
no voice class codec tag
```

5.7.2.10.1. Syntax

Keyword / Argument	Description
tag	The unique number you assign to the voice class. The valid range is 1 to 65,535. Each tag number must be unique on the Gateway.

5.7.2.10.2. Default Value

No Default Value.

5.7.2.10.3. Command Mode

Global Configuration Mode

5.7.2.10.4. Usage Guideline

This command only creates the voice class for codec selection preference and assigns an identification tag. Use the **codec preference** command to specify the parameters of the voice class, and use the **voice-class codec** dial-peer command to apply the voice class to a VoIP dial peer.

5.7.2.10.5. Example

The following example shows how to enter voice-class configuration mode and assign a voice class tag number starting from global configuration mode:

```
voice class codec 10
```

After you enter voice-class configuration mode for codecs, use the **codec preference** command to specify the parameters of the voice class.

The following example creates preference list 99, which can be applied to any dial peer:

```
configure
```

```
voice class codec 99
codec preference 1 g711alaw
codec preference 2 g711ulaw
codec preference 3 g729
codec preference 4 g7231r63
codec preference 5 g7231r53
exit
```

5.7.2.11. voice class user

To enter user-class configuration mode and assign an identification tag number for a user class, use the **voice class user** command in global configuration mode. To delete a user voice class, use the **no** form of this command.

voice class user *tag*

no voice class user *tag*

5.7.2.11.1. Syntax

Keyword / Argument	Description
tag	The unique number you assign to the user class. Each tag number must be unique on the Gateway. Valid entries are from 0 to 10.

5.7.2.11.2. Default Value

No Default Value

5.7.2.11.3. Command Mode

Global Configuration Mode

5.7.2.11.4. Usage Guideline

Setting of user-class uses to deny call receivance from unpermitted users when originating call is received from network. Without user-class setting, anybody, who tries to call trough network to FXO port, can hear a dial-tone from PBX,

which is connected with that port, and put desired extension number. (Or anybody, who tries to call through network to FXO port, can hear a dial-tone from PSTN exchanger, which is connected with that port, and put desired PSTN number.)

If at least one of user-class is configured, initial caller shall listen beep sound instead of dial tone and after passing password, caller can input numbers as much as max-digits, which is defined in user-class. So, using max-digit number, it is possible adjusting of extension call, intown call, local area call, long distance call, and international call.

One or more user-class can be configured. So, different call limitations are capable for different user classes.

To keep the security of calls incoming to the FXO port through the network, users can use this command and "security permit-FXO" command in the AP2120 Gateway. Since it is possible to directly attempt calls to the PSTN through this FXO port or indirectly attempt calls to the PSTN through the PBX internal line, unauthorized remote users can attempt calls as well. To prevent unauthorized users' attempting calls, the security shall be kept. Two security systems that AP1100 provides have following advantages and disadvantages.

With "security permit-FXO" command, remote users does not need to enter the password so they can easily access the network.

However, IP address of the VoIP peer on the other side shall be registered and the gatekeeper cannot be used at the same time. Also, it is impossible to bar calls of the registered peers by class.

With the "voice class user" users need to enter the password digit but stronger and multi-classed call barring is possible.

5.7.2.11.5. Example

Following example shows generation of user class 1 and setting of user class mode.

```
voice class user 1
```



```
password 1234
max-digits 10
exit
```

5.7.2.12. voice service

To specify the voice encapsulation type, use the **voice service command** in global configuration mode. To exit voice-service configuration mode, use the **exit** command.

voice service voip

5.7.2.12.1. Syntax

Keyword / Argument	Description
VoIP	Specifies Voice over IP (VoIP) parameters.

5.7.2.12.2. Default value

No Default Value

5.7.2.12.3. Command Mode

Global Configuration Mode

5.7.2.12.4. Usage Guideline

Use the **voice service** command to switch to voice-service configuration mode from global configuration mode and to specify a voice encapsulation type. Use the **exit** command to exit the voice-service configuration mode and return to the global configuration mode.

5.7.2.12.5. Example

The following example shows how to access voice-service configuration mode and specify VoIP parameters, beginning in global configuration mode:

```
voice service voip
```

5.7.2.13. voip-interface

To set an interface in which the VoIP is going to operate, use “**VoIP-interface**” command in the global setup mode.

To set the interface as the default, use “**no**” command before this command.

```
voip-interface interface-name  
no voip-interface
```

5.7.2.13.1. Syntax

Keyword / Argument	Description
<i>interface-name</i>	Designates the interface installed in the router. Interfaces include Ethernet 0.0, Ethernet 1.0, Ethernet 0 and so on.

5.7.2.13.2. Default Value

The default interface is Ethernet 0 .0.

5.7.2.13.3. Command Mode

Global Configuraiton Mode

5.7.2.13.4. Usage Guideline

With this command, users can designate the VoIP service in a certain interface.

VoIP service is provided using the IP address stored in the VoIP interface.

If no IP address is designated in the corresponding VoIP interface, VoIP-related setup or search is impossible.

5.7.2.13.5. **Example**

The following example shows how to designate the VoIP service in the Ethernet 1.0 interface.

```
configure
```

```
    voip-interface ethernet 1 0
```

The following example shows how to designate the VoIP service in the Ethernet 0 interface.

```
configure
```

```
    voip-interface Ethernet 0
```

5.7.3. Voice Port Configuration Command

5.7.3.1. comfort-noise

To generate background noise to fill silent gaps during calls if voice activity detection (VAD) is activated, use the **comfort-noise** command in voice-port configuration mode. To provide silence when the remote party is not speaking and VAD is enabled at the remote end of the connection, use the **no** form of this command.

comfort-noise

no comfort-noise

5.7.3.1.1. Syntax

This command has no arguments or keywords.

5.7.3.1.2. Default Value

Enable

5.7.3.1.3. Command Mode

Voice-port Configuration Mode

5.7.3.1.4. Usage Guideline

If the **comfort-noise** command is not enabled, and VAD is enabled at the remote end of the connection, the user will hear dead silence when the remote party is not speaking. In this case, there is no voice packet and it feels like the call is terminated. So the Gateway generates background noise to smooth the conversation- comfort noise generation. The default value is "enable". So it feels awkward or prefer silence, deactivates the function.

5.7.3.1.5. Example

The following example disables background noise on voice-port 1/0.

```
voice-port 1/0
no comfort-noise
```

5.7.3.2. connection

To specify a connection mode for a voice port, use the **connection** command in voice-port configuration mode. To disable the selected connection mode, use the **no** form of this command.

connection { **plar** } *string*

no connection { **plar** } *string*

5.7.3.2.1. Syntax

Keyword / Argument	Description
plar	Specifies a private line automatic ringdown (PLAR) connection. PLAR is an autodialing mechanism that permanently associates a voice interface with a far-end voice interface, allowing call completion to a specific telephone number or PBX without dialing. When the calling telephone goes off-hook, a predefined network dial peer is automatically matched, which sets up a call to the destination telephone or PBX.
string	Specifies the destination telephone number. Valid entries are any series of digits that specify the E.164 telephone number.

5.7.3.2.2. Default Value

No connection mode is specified.

5.7.3.2.3. Command Mode

Voice-port Configuration Mode

5.7.3.2.4. Usage Guideline

Use the **connection** command to specify a connection mode for a specific interface. For example, use the **connection plar** command to specify a PLAR

interface. The string you configure for this command is used as the called number for all calls coming in over this connection. The destination peer is determined by called number.

5.7.3.2.5. Example

The following example selects PLAR as the connection mode on the AP2120, with a destination telephone number of 555-9262: In this example, if the voice port 1/0 is hooked off, a call will be automatically sent to 5559262.

```
voice-port 1/0
connection plar 5559262
```

5.7.3.3. description (voice port)

To include a description of what this voice port is connected to, use the **description** voice-port configuration command. Use the **no** form of this command to disable this feature.

```
description string
no description
```

5.7.3.3.1. Syntax

Keyword / Argument	Description
string	Description Character String on the Port. (max length 255)

5.7.3.3.2. Default Value

Enabled with a null string

5.7.3.3.3. Command Mode

Voice-port Configuration Mode

5.7.3.3.4. Usage Guideline

Use the **description** command to include descriptive text about this voice-port connection. This information is displayed when you issue a **show** command and does not affect the operation of the interface in any way.

5.7.3.3.5. Example

The following example identifies voice port 1/0 on AP2120 as being connected to the Marketing department:

```
voice-port 1/0
description marketing_dept
```

5.7.3.4. echo-cancel

To enable the cancellation of voice that is sent out the interface and is received back on the same interface, use the **echo-cancel** command in voice-port configuration mode. To disable echo cancellation, use the **no** form of this command.

echo-cancel

no echo-cancel

5.7.3.4.1. Syntax

This command has no arguments or keywords

5.7.3.4.2. Default Value

Enable

5.7.3.4.3. Command Mode

Voice-port Configuration Mode

5.7.3.4.4. Usage Guideline

The **echo-cancel** command enables cancellation of voice that is sent out the interface and is received back on the same interface; sound that is received back in this manner is perceived by the listener as an echo. Disable echo-cancel for E&M 4-wire interface because it doesn't have echo path.

5.7.3.4.5. Example

This example disables echo-cancel for voice-port 1/0.

```
voice-port 1/0
no echo-cancel
```

5.7.3.5. input gain

To configure a specific input gain value, use the **input gain** voice-port configuration command. Use the **no** form of this command to disable the selected amount of inserted gain.

Input gain *value*
no Input gain *value*

5.7.3.5.1. Syntax

Keyword / Argument	Description
value	Specifies, in decibels, the amount of gain to be inserted at the receiver side of the interface. Acceptable value is any integer from -31 to 31.

5.7.3.5.2. Default Value

0.

5.7.3.5.3. Command Mode

Voice-Port Configuration Mode

5.7.3.5.4. Usage Guideline

A system-wide loss plan must be implemented using both **input gain** and **output gain** commands. Other equipment (including PBXs) in the system must be taken into consideration when creating a loss plan. This default value for this command assumes that a standard transmission loss plan is in effect, meaning that normally, there must be -6dB attenuation between phones. Connections are implemented to provide -6dB of attenuation when the **input gain** and **output gain** commands are configured with the default value of 0.

You can't increase the gain of a signal going out into the PSTN, but you can decrease it. Therefore, if the voice level is too high, you can decrease the volume by either decreasing the input gain value or by increasing the output attenuation

You can increase the gain of a signal coming in to the router. If the voice level is too low, you can increase the input gain.

5.7.3.5.5. Example

The following example configures a 3-decibel gain to be inserted at the receiver side of the interface in the router.

```
port 1/1
input gain 3
```

5.7.3.6. operation (E&M Voice Port Command)

To set Cabling Scheme for a certain E&M Voice port, use **operation command** at voice port configuration mode. To make the signal type back to default value, use "**no**" command. This command is for Description.

```
operation { 2-wire | 4-wire }
no operation
```

5.7.3.6.1. Syntax

Keyword / Argument	설명
2-wire	Set “ 2-wire” from E&M Cabling Scheme. Refer to the User guide.
4-wire	Set “ 4-wire” from E&M Cabling Scheme. Refer to the User guide.

5.7.3.6.2. Default Value

2-wire

5.7.3.6.3. Command Mode

Voice-port Configuration Mode (E&M)

5.7.3.6.4. Usage Guideline

“**Operation**” command is only applied to E&M voice port.

2-Wire/4-Wire Operation is done by Hardware Jumper Setting. However, the administrator/user cannot check the Hardware Jumper configuration without seeing it. To solve this problem, use “**operation**” command to add description on operation type at the gateway configuration file. So the administrator can check the E&M voice port operation with the gateway configuration File checking command..

Refer to “[Figure 5-5 E&M module Jumper Setting]” of E&M Port configuration for more detailed information.

5.7.3.6.5. Example

The following example shows adding E&M Voice Port 2-Wire Cabling Scheme description at the gateway configuration file.

```
voice-port 1/1
operation 2-wire
```

5.7.3.7. output gain

To configure a specific output gain value, use the **output gain** voice-port configuration command. Use the **no** form of this command to disable the selected output gain value.

output gain *value*

no output gain *value*

5.7.3.7.1. Syntax

Keyword / Argument	Description
value	The amount of gain in decibels at the transmit side of the interface. Acceptable value is any integer from -31 to 31. The default value for FXO, FXS, and E&M ports is 0..

5.7.3.7.2. Default Value

0

5.7.3.7.3. Command Mode

Voice-Port Configuration mode

5.7.3.7.4. Usage Guideline

A system-wide loss plan must be implemented using both **input gain** and **output gain** commands. Other equipment (including PBXs) in the system must be taken into consideration when creating a loss plan.

This default value for this command assumes that a standard transmission loss plan is in effect, meaning that normally, there must be -6 dB attenuation between phones.

Connections are implemented to provide -6 dB of attenuation when the **input gain** and **output gain** commands are configured with the default value of 0.

You can't increase the gain of a signal going out into the PSTN, but you can decrease it. Therefore, if the voice level is too high, you can decrease the volume by either decreasing the input gain value or by increasing the output attenuation.

5.7.3.7.5. **Example**

The following example on the Gateway configures a 3-decibel gain to be inserted at the transmit side of the interface:

```
port 1/1
output gain 3
```

5.7.3.8. **polarity-inverse**

To enable polarity-inverse function for a FXS voice port, use **polarity-inverse** command at voice-port configuration command. Use the **no** form of this command to disable polarity-inverse.

```
polarity-inverse
no polarity-inverse
```

5.7.3.8.1. **Syntax**

This command has no arguments or keywords

5.7.3.8.2. **Default Value**

```
disable
```

5.7.3.8.3. **Command Mode**

Voice-port Configuration Mode

5.7.3.8.4. Usage Guideline

When PBX supports billing function, the start and end point of billing are indicated by polarity-inverse. Then PBX office line connected to FXS does billing. Typically, it is not necessary to activate this function.

5.7.3.8.5. Example

To enable the polarity-inverse function to voice-port 1/0 :

```
voice-port 1/0
    polarity-inverse
```

5.7.3.9. ring number

To specify the number of rings for a specified FXO voice port, use the **ring number** voice-port configuration command. Use the **no** form of this command to restore the default value.

ring number *number*
no ring number *number*

5.7.3.9.1. Syntax

Keyword / Argument	Description
number	Number of rings detected before answering the call. Valid entries are from 1 to 255. The default is 1.

5.7.3.9.2. Default Value

One Ring

5.7.3.9.3. Command Mode

Voice-port Configuration Mode

5.7.3.9.4. Usage Guideline

Use the **ring number** command to set the maximum number of rings to be detected before answering a call over an FXO voice port. Use the **no** form of this command to reset the default value, which is one ring. Normally, the default value is recommended so that incoming calls are answered quickly. If you have other equipment available on the line to answer incoming calls, you might want to set the value higher to give the equipment sufficient time to respond. In that case, the FXO interface would answer if the equipment on line did not answer the incoming call in the configured number of rings. This command is not applicable to FXS or E&M interfaces because they do not receive ringing.

5.7.3.9.5. Example

The following example on the router sets five rings as the maximum number of rings to be detected before closing a connection over this voice port:

```
voice-port 1/0
ring number 5
```

5.7.3.10. shutdown (voice-port)

To make the voice ports for a specific voice interface card offline, use the **shutdown** voice-port configuration command. Use the **no** form of this command to put the ports back in service.

```
shutdown
no shutdown
```

5.7.3.10.1. Syntax

This command has no arguments or keywords.

5.7.3.10.2. **Default Value**

No shutdown.

5.7.3.10.3. **Command Mode**

Voice-port Configuration Mode

5.7.3.10.4. **Usage Guideline**

When you enter the **shutdown** command, all ports on the voice interface card are disabled. When you enter the **no shutdown** command, all ports on the voice interface card are enabled. A telephone connected to an interface will hear dead silence when a port is shut down.

5.7.3.10.5. **Example**

The following example makes voice port 1/3 on the Gateway offline:

```
configure
voice-port 1/3
shutdown
```

5.7.3.11. **signal (E&M Voice Port Command)**

User signal command to set Signaling type for the voice port. To apply the default signal type, use **no** command.

signal {wink-start | immediate | delay-dial }

no signal

5.7.3.11.1. Syntax

Keyword / Argument	Description
wink-start	The calling party occupies the line with off-Hook of E(Ear)-lead and stands by during “wink” instruction of M(Mouth)-lead of the called party. Then it sends address with DTMF. The command is for E&M Tie Trunk Interface. This is the default value of E&M voice port.
immediate	The calling party occupies the line with off-Hook of E(Ear)-lead and sends address with DTMF. The command is for E&M Tie Trunk Interface.
delay-dial	The calling party occupies the line with off-Hook of E(Ear)-lead. Then in a certain time, the calling party observes the called party. If the called party is On-Hook, the address is sent with Calling DTMF. If the Called party is not On-Hook. It waits until the called party becoming “Off-Hook” and sends Address information. The command is for E&M Tie Trunk Interface.

5.7.3.11.2. Default Value

wink-start

5.7.3.11.3. Command Mode

Voice-port Configuration Mode

5.7.3.11.4. Usage Guideline

“signal” is applied to only Analog voice ports.

The configuration is only applied to a certain configured port.

If E&M voice port is configured as “Immediate Signaling”, the PBX might lose the first part of the number. So use Delay-Dial Signaling instead of Immediate Signaling.

Some devices have DTMF Receiver with limited digits. With this kind of

devices, the calling side should be delayed until DTMF Receiver is available.

5.7.3.11.5. Example

The below example is the configuration of occupying the line with Off-hook of E-lead and sending DTMF information right away.

```
voice-port 1/1
signal immediate
```

5.7.3.12. timing delay-duration (E&M Voice Port Command)

Use **timing delay-duration** command to set Delay Signal Duration for the certain port. To apply the default Delay Duration, use **no** command.

```
timing delay-duration milliseconds
no timing delay-duration
```

5.7.3.12.1. Syntax

Keyword / Argument	Description
milliseconds	Set Delay Signal Duration of Delay Dial Signaling. The acceptable values are " 100~5000" .

5.7.3.12.2. Default Value

200 milliseconds

5.7.3.12.3. Command Mode

Voice-port Configuration mode

5.7.3.12.4. Usage Guideline

timing delay-dulation command is applied to the outgoing clals.

5.7.3.12.5. Examples

The below configuration is allowing 3000msec Delay Signal Duration to outgoing calls.

```
voice-port 1/0  
timing delay-dulation 3000
```

5.7.3.13. timing delay-start (E&M Voice Port Command)

To set min. Delay time between Outgoing Seizure to Out-Dial Address, use **timing delay-start** command. To apply the default value, use **no** command.

timing delay-start *milliseconds*

no timing delay-start

5.7.3.13.1. Syntax

Keyword / Argument	Description
milliseconds	Set min. Delay time from Outgoing Seizure to Outdial Address. Unit: milliseconds. The acceptable values are" 20~2000"

5.7.3.13.2. Default Value

300 milliseconds

5.7.3.13.3. Command Mode

Voice-port Configuration Mode

5.7.3.13.4. Usage Guideline

timing delay-start command sets Minimum Delay time to outing calls.

5.7.3.13.5. Example

The below configuration sets 250msec Delay-start for a voice port.

```
voice-port 1/0
timing delay-start 250
```

5.7.3.14. timing dialout-delay (E&M Voice Port Command)

To set Dial-out Delay of sending Dial Digit, use "**timing dialout-delay**" command.

To apply the default value, use **no** command.

timing dialout-delay *milliseconds*

no timing dialout-delay

5.7.3.14.1. Syntax

Keyword / Argument	Description
milliseconds	Sets Dial-out Delay for Sending numbers from E&M Immediate Trunk or for the Cut-through. The acceptable values are " 100~5000" .

5.7.3.14.2. Default Value

200 milliseconds

5.7.3.14.3. Command Mode

Voice-port Configuration Mode

5.7.3.14.4. Example

The below configuration sets 350msec Dial-out Delay for a voice port.

```
voice-port 1/0
timing dialout-delay 350
```

5.7.3.15. timing wait-wink (E&M Voice Port Command)

To set the max. Waiting Time between Outgoing Seizure and Wink Signal, use **timing wait-wink** command. To apply the default value, use **no** command.

timing wait-wink *milliseconds*

no timing wait-wink

5.7.3.15.1. Syntax

Keyword / Argument	Description
milliseconds	The max. waiting time for Wink-start signal. Unit: milliseconds. The acceptable values are “ 100~400” .

5.7.3.15.2. Default Value

550 milliseconds

5.7.3.15.3. Command Mode

Voice-port Configuration Mode

5.7.3.15.4. Example

The below configuration sets 300msec Wait-wink Duration.

```
voice-port 1/0
```

```
timing wait-wink 300
```

5.7.3.16. timing wink-duration (E&M Voice Port Command)

To set max. Wink-Signal Duration, use **timing wink-duration** command. To apply the default value, use **no** command.

timing wink-duration *milliseconds*

no timing wink-duration

5.7.3.16.1. Syntax

Keyword / Argument	Description
milliseconds	To set max. Wink-Signal Duration. Unit: milliseconds. The acceptable values" 100~400" .

5.7.3.16.2. Default Value

200 milliseconds

5.7.3.16.3. Command Mode

Voice-port Configuration Mode

5.7.3.16.4. Usage Guideline

timing wink-dulation sets Wink-start Dulation for outgoing calls.

5.7.3.16.5. Example

The below configuration sets 300msec Wink-Signal Duration for outgoing calls.

```
voice-port 1/0
timing wink-dulation 300
```

5.7.3.17. timing wink-wait (E&M Voice Port Command)

To set max. Wink-wait Duration, use **timing wink-wait** command. To apply the default value, use **no** command.

timing wink-wait *milliseconds*

no timing wink-wait

5.7.3.17.1. Syntax

Keyword / Argument	Description
--------------------	-------------

milliseconds	To set Wink-wait Duration for Wink-start signal. The acceptable values are " 100~5000" .
--------------	---

5.7.3.17.2. Default Value

200 milliseconds

5.7.3.17.3. Command Mode

Voice-port Configuration Mode

5.7.3.17.4. Usage Guideline

To set Wink-wait Duration for outgoing calls.

5.7.3.17.5. Example

The below configuration sets 300msec Wink-wait Duration for outgoing calls.

```
voice-port 1/0
timing wink-wait 300
```

5.7.3.18. translate-incoming

To apply the translation rule to the inbound POTS call coming to the corresponding voice port, use this command. To stop applying the translation rule, use "no" command before "translate-incoming" command.

```
translate-incoming { called-number | calling-number } tag
no translate-incoming { called-number | calling-number }
```

5.7.3.18.1. Syntax

Keyword / Argument	Description
called-number	Applies the translation rule to the inbound called party number.
calling-number	Applies the translation rule to the inbound calling party number.
<i>tag</i>	Refers to the rule set. Tag values range from 0 to

	65535.
--	--------

5.7.3.18.2. **Default Value**

No translation rule is applied.

5.7.3.18.3. **Command Mode**

Voice-port Configuration Mode

5.7.3.18.4. **Usage Guideline**

This command uses the number translation rules that have been set by “**translation-rule**” command for the inbound call of the corresponding voice-port.

If the translation rule is applied to the called party number and if numeric data is entered into the voice port in order, check if translation is made for every number entered. At this time, translation shall be made only once.

5.7.3.18.5. **Example**

In the following example, translation rule 10 is created and applied to the calling party number of the voice port 1/1.

Therefore, if the calling party number of the inbound call is 93450, it is translated into 9563450.

```
translation-rule 10
    rule 0 9 956
    rule 1 8 878
voice-port 1/1
    translate-incoming calling-number 10
```

5.7.3.19. **type (E&M Voice Port Command)**

To set E&M Voice port type, use “**type**” command. To apply the default value,

use **no** command.

type { 1 | 2 | 3 | 5 }

no type

5.7.3.19.1. Syntax

Keyword / Argument	설명
1	To set Type-1 for E&M voice port. Refer to the User Guideline for more detailed information.
2	To set Type-2 for E&M voice port. Refer to the User Guideline for more detailed information.
3	To set Type-3 for E&M voice port. Refer to the User Guideline for more detailed information.
5	To set Type-4 for E&M voice port. Refer to the User Guideline for more detailed information.

5.7.3.19.2. Default Value

Type-5

5.7.3.19.3. Command Mode

Voice-port Configuration Mode (E&M)

5.7.3.19.4. Usage Guideline

The command is only applied to E&M voice ports.

E&M Type 1, 2, 3, 5 configuration is doen by Hardware Jumper Setting. However, the administrator/user cannot check the E&M type without seeing it. To solve this problem, use "**type**" command to add description on the type at the gateway configuration file. So the administrator can check the E&M voice port operation with the gateway configuration File checking command..

Refer to "[Figure 5-5 E&M module Jumper Setting]" of E&M Port configuration for more detailed information.

5.7.3.19.5. **Example**

The below configuration sets Description of E&M voice port using Type-5 at the gateway configuration file.

```
voice-port 1/1  
    type 5
```

5.7.4. Dial Peer Commands

5.7.4.1. answer-address

To find the VoIP dial peer for the VoIP inbound call incoming to the network as using the calling party number of the inbound call, use "**answer-address**" command in the dial-peer setup mode. To disable the number that has been set, use "**no**" command before "**answer-address**" command.

answer-address *string*

no answer-address

5.7.4.1.1. Syntax

Keyword / Argument	Description
String	<p>Number string defined in the E.164 or private telephone number plan. Numeric data (0 to 9) "#" and "*" can be used.</p> <ul style="list-style-type: none">• (*) & (#): These characters can be found on the standard button-type telephone. They cannot be located at the first place of the string. (For example, *650 is invalid.)• (.): The period means a value that can match with any numeric entered. In other words, the period cannot be placed at the first place of the string. (For example, .650 is invalid.)• ([]): Brackets are to indicate the range. The Range is the character sequence within the bracket and only numeric data (0 to 9) can be used for the range. This is similar to the regular expression rule.

5.7.4.1.2. Default Value

Null String.

5.7.4.1.3. Command Mode

Dial-Peer configuration Mode (VoIP dial peer)

5.7.4.1.4. Usage Guideline

This command is applied to the VoIP dial peer of the AP2120 VoIP Gateway.

The **"answer-address"** command is used to find the VoIP dial peer for the VoIP inbound calls. The VoIP dial peer for the VoIP inbound call from the network is selected as follows:

Firstly, the VoIP dial peer that has the **session target** matching with the IP address of the inbound call is searched.

Secondly, if the corresponding peer is not found, the VoIP dial peer that has **answer-address** matching with the calling party number of the inbound call will be searched.

Lastly, if no peer is found, the VoIP dial peer matching with the **destination-pattern** of the inbound call will be searched.

5.7.4.1.5. Example

In the following example, if the calling party number of the inbound VoIP call is "5263848", VoIP peer 10 will be selected.

```
dial-peer voice 10 voip
answer-address 526....
```

5.7.4.2. codec

To specify the voice coder rate of speech for a dial peer, use the **codec** dial-peer configuration command. Use the **no** form of this command to reset the default value.

```
codec {g711alaw / g711ulaw / g729r8 / g7231r63 / g7231r53 }
no codec
```

5.7.4.2.1. Syntax

Keyword / Argument	Description
G711alaw	G.711 A-Law 64Kbps Codec
G711ulaw	G.711 u-Law 64Kbps Codec
G729	G.729 8Kbps Codec
G7231r63	G.723.1 6300 bps. This is the default CODEC for AP1100 Gateway.
G7231r53	G.723.1 5.3Kbps Codec

5.7.4.2.2. Default Value

G.723.1 6.3Kbps Codec

5.7.4.2.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.2.4. Usage Guideline

Use the **codec** command to define a specific voice coder rate of speech for a dial peer.

For toll quality, use **G.711.alaw** or **G.711.ulaw**. These values provide high-quality voice transmission but use a significant amount of bandwidth. For almost toll quality (and a significant savings in bandwidth), use the **G.729** or **g7231** value.

If **codec** values for the VoIP peers of a connection do not match, the call will fail.

5.7.4.2.5. Example

The following example configures a voice coder rate that provides toll quality requesting a relatively high amount of bandwidth:

```
dial-peer voice 10 voip
    codec g711alaw
```

5.7.4.3. description (dial-peer)

To include a description of what this VoIP dial peer is connected to, use the **description** at dial-peer configuration command. Use the **no** form to disable this feature.

description *string*

no description

5.7.4.3.1. Syntax

Keyword / Argument	Description
string	Character String for Dial-Peer. (max length 255)

5.7.4.3.2. Default Value

null String

5.7.4.3.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.3.4. Usage Guideline

Use the **description** command to include descriptive text about this dial-peer connection.

This information is displayed when you issue a **show** command and does not affect the operation of the interface in any way.

5.7.4.3.5. Example

The following example identifies dial peer 10 of AP2120 VoIP Gateway at the Seoul office:

```
dial-peer voice 10 voip
description Seoul_office
```

5.7.4.4. destination-pattern

To specify either the prefix or the full E.164 telephone number (depending on your dial plan) used for a dial peer, use the **destination-pattern** dial-peer configuration command. Use the **no** form of this command to disable the

configured prefix or telephone number.

destination-pattern *string* [**T**]

no destination-pattern

5.7.4.4.1. Syntax

Keyword / Argument	Description
String	Series of digits that specify the E.164 or private dialing plan telephone number. (max length 55) Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: <ul style="list-style-type: none">• The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. These characters cannot be used as leading characters in a string (for example, *650).• Period (.), which matches any entered digit (this character is used as a wildcard). The period cannot be used as a leading character in a string (for example, .650).• Brackets ([]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. This is similar to a regular expression rule.
T	(Optional) Control character indicating that the destination-pattern value is a variable length dial string

5.7.4.4.2. Default Value

Null String

5.7.4.4.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.4.4. Usage Guideline

This command is applicable to both VoIP and POTS dial peers on all platforms.

Use the **destination-pattern** command to define the E.164 telephone number for this dial peer.

This pattern is used to match dialed digits to a dial peer. The dial peer is then

used to complete the call. When a router receives voice data, it compares the called number (the full E.164 telephone number) in the packet header with the number configured as the destination pattern for the voice-telephony peer. The router then strips out the left-justified numbers corresponding to the destination pattern. If you have configured a prefix, the prefix is appended to the front of the remaining numbers, creating a dial string, which the router then dials. If all numbers in the destination pattern are stripped-out, the user receives a dial tone.

There are certain areas in the world (for example, in certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T** to indicate that a particular **destination-pattern** value is a variable-length dial-string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired.

5.7.4.4.5. Example

The following example configures the E.164 telephone number, "555-7922," for a dial peer:

```
dial-peer voice 10 pots
    destination-pattern 5557922
```

The following example shows configuration of a destination pattern in which the digit numbers range between 5553409 and 5559499:

```
dial-peer voice 3 voip
    destination-pattern 555[3-9]4[0-9]9
```

The following example shows configuration of a destination pattern in which the digit numbers of " 5551439, 5553439, 5555439, 5557439, and 5559439":

```
dial-peer voice 4 voip
    destination-pattern 555[13579]439
```

5.7.4.5. dtmf-relay

To specify how an H.323 gateway relays dual tone multi-frequency (DTMF) tones between telephony interfaces and an IP network, use the **dtmf-relay** command in dial-peer configuration mode. Use the **no** form of this command to remove all signaling options and to send the DTMF tones as part of the audio stream.

dtmf relay { h245-alphanumeric }

no dtmf relay

5.7.4.5.1. Syntax

Keyword / Argument	Description
h245-alphanumeric	(Optional) Forwards DTMF tones by using the H.245 "alphanumeric" User Input Indication method. Supports tones 0-9, *, #, and A-D.

5.7.4.5.2. Default Value

None

5.7.4.5.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.5.4. Usage Guideline

DTMF is the tone generated when you press a digit on a touch-tone phone. This tone is compressed at one end of a call; when the tone is decompressed at the other end, it can become distorted, depending on the codec used. The DTMF relay feature transports DTMF tones generated after call establishment out of band using a standard H.323 out-of-band method.

The **dtmf-relay** command determines the outgoing format of relayed DTMF tones. The gateway automatically accepts all formats.

The principal advantage of the **dtmf-relay** command is that it sends DTMF

tones with greater fidelity than is possible in-band for most low-bandwidth codecs, such as G.729 and G.723. Without the use of DTMF relay, calls established with low-bandwidth codecs may have trouble accessing automated DTMF-based systems, such as voice-mail, menu-based ACD systems, and automated banking systems.

5.7.4.5.5. Example

The following example configures DTMF relay with the h245-alphanumeric option when sending DTMF tones to dial-peer 103:

```
dial-peer voice 103 voip
    dtmf-relay h245-alphanumeric
```

The next example configures the gateway to send DTMF in-band (the default) when sending DTMF tones to dial-peer 103:

```
dial-peer voice 103 voip
    no dtmf-relay
```

5.7.4.6. forward-digits

To set the number of the forwarding digit of the outbound POTS as a random number not by using the default method, use "**forward-digits**" command in the dial-peer setup mode. To forward digits that do not match with the destination pattern by the default method, add "**no**" command.

```
forward-digits { from | last } number
no forward-digits
```

5.7.4.6.1. Syntax

Keyword / Argument	Description
from	Forwards the called party number from the designated digit.
last	Forwards last digits of the called party number as designated.
<i>number</i>	Number of digits to forward. The value ranges from 0 to 100. If the designated value is higher than the maximum digits that can be forwarded, only the digits that can be forwarded at maximum

	are forwarded.
--	----------------

5.7.4.6.2. Default Value

In default setting, if the called party number matches with the destination pattern of the outbound POTS peer, only digits that are not matched will be forwarded.

5.7.4.6.3. Command Mode

Dial-Peer Configuration Mode (POTS peer)

5.7.4.6.4. Usage Guideline

This command is a dial-peer setup mode command and applied only to the POTS peer.

This command is used to define number of digits when relaying last digits of the called party number of an inbound call as the called party number of the outbound call. The default is no forward-digit, and in the default status, number forwarding is made.

5.7.4.6.5. Example

If POTS peer 10 is decided for the outbound and if the called party number of the inbound call is 100123456789, number 123456789 will be forwarded as set in the default. This is because **"forward-digit"** has not been set.

```
dial-peer voice 10 pots
  destination-pattern 100...
```

If **"forward-digit from"** is added to the above setting, only "456789" (from the 7th digit to the last digit) will be forwarded.

```
forward-digit from 7
```

In the following example, all digits (100123456789) will be forwarded.

```
forward-digit from 1
```

In the following example, no digit will be forwarded.

forward-digit from 99

If "**forward-digit last**" is added as below, only last four digits ("6789") will be forwarded.

forward-digit last 4

In the following example, no digit is forwarded.

forward-digit last 0

In the following digit, all digits "100123456789" are forwarded.

forward-digit last 99

5.7.4.7. huntstop

To stop dial peer hunting in the hunting group, use "**huntstop**" command in the dial-peer setup mode. To use default setting, use "**no**" command before "**huntstop**" command.

huntstop

no huntstop

5.7.4.7.1. Syntax

This command has no arguments or keywords.

5.7.4.7.2. Default Value

Hunting can be made in the default state.

5.7.4.7.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.7.4. Usage Guideline

If an outbound dial peer is selected for an inbound call and if more than one

dial peers are selected, a hunting group will be made.

If a **huntstop** has been set already in a certain dial peer and if the outbound call to that dial peer fails, a call will be terminated without hunting other dial peers.

5.7.4.7.5. Example

The following example is to perform huntstop in VoIP peer 110.

```
dial-peer voice 110 voip
    huntstop
```

5.7.4.8. port

To associate a dial peer with a specific voice port, use "**port**" command at dial-peer configuration command. Use the **no** form of this command to cancel this association.

```
port slot/port
no port
```

5.7.4.8.1. Syntax

Keyword / Argument	Description
Slot	Slot number where the voice interface card is installed. Valid entries are 1 or 0.
port	Port number for voice port number of voice interface module. Valid entries are 0 to 3.

5.7.4.8.2. Default Value

No port is configured.

5.7.4.8.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.8.4. Usage Guideline

This command is applicable only to POTS peers .

Use the **port** configuration command to associate the designated voice port with the selected dial peer.

This command is used for calls incoming from a telephony interface to select an incoming dial peer and for calls coming from the VoIP network to match a port with the selected outgoing dial peer.

5.7.4.8.5. Example

The following example associates a dial peer with voice port:

```
dial-peer voice 10 pots
port 1/0
```

5.7.4.9. preference

To clearly designate priorities within the hunt group for a certain dial-peer, use “**preference**” command in the dial-peer setup mode. To use default priorities, use “**no**” command before “**preference**” command.

```
preference value
no preference
```

5.7.4.9.1. Syntax

Keyword / Argument	Description
<i>value</i>	Values range from 0 to 9, and the lower the value is, the higher the priority is.

5.7.4.9.2. Default Value

The default is 0 and has the highest priority.

5.7.4.9.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.9.4. Usage Guideline

Setting priorities within the hunt group by the preference enables users to adjust the priority of a certain dial peer.

5.7.4.9.5. Example

Let's assume that there is a dial peer as follows:

```
dial-peer voice 10 pots
  destination-pattern 5551234
  preference 3
```

```
dial-peer voice 11 pots
  destination-pattern 555....
  preference 0
```

If the called party number of the inbound call is 5551234, all dial peers will be selected. However, if the preference is prior in selecting the hunt algorithm by "dial-peer hunt" command, dial peer 11 will be selected first.

5.7.4.10. prefix

To specify the prefix of the dialed digits for this dial peer, use the **prefix** dial-peer configuration command. Use the **no** form of this command to disable this feature.

```
prefix string
no prefix
```

5.7.4.10.1. Syntax

Keyword / Argument	Description
string	Integers representing the prefix of the telephone number associated with the specified dial peer. Valid numbers are 0 through 9, and a comma (.). Use a comma to include a pause in the prefix.

5.7.4.10.2. **Default Value**

Null String.

5.7.4.10.3. **Command Mode**

Dial-Peer Configuration Mode

5.7.4.10.4. **Usage Guideline**

Use the **prefix** command to specify a prefix for a specific dial peer. When an outgoing call is initiated to this dial peer, the **prefix string** value is sent to the telephony interface first, before the telephone number associated with the dial peer.

If you want to configure different prefixes for dialed numbers on the same interface, you need to configure different dial peers.

5.7.4.10.5. **Example**

The following example specifies a prefix of "9" and then a pause for 1 sec.:

```
dial-peer voice 10 pots
prefix 9,
```

5.7.4.11. **register**

To register or deregister a fully qualified POTS dial-peer E.164 address of a Gateway with a gatekeeper, use "**register e164**" command in dial-peer configuration mode. To deregister an E.164 address, use the **no** form of this command.

register e164

no register e164

5.7.4.11.1. **Syntax**

This command has no keywords or arguments

5.7.4.11.2. **Default Value**

No default value

5.7.4.11.3. **Command Mode**

Dial-Peer Configuration Mode

5.7.4.11.4. **Usage Guideline**

Use this command to register the E.164 address of an analog telephone line attached to a Foreign Exchange Station (FXS) port of a Gateway. The gateway automatically registers fully qualified E164 addresses. Use the **no register e164** command to deregister an address. Use the **register e164** command to register a deregistered address.

Before you automatically or manually register an E.164 address with a gatekeeper, you must create a dial peer (using the **dial-peer** command), assign an FXS port to the peer (using the **port** command), and assign an E.164 address (using the **destination-pattern** command).

The E.164 address must be a fully qualified address. For example, 5551212, and 4085551212 are fully qualified addresses; 408555.... is not a fully qualified address. E.164 addresses are registered only for active interfaces—those that are not shut down. If an FXS port or its interface is shut down, the corresponding E.164 address is deregistered.

5.7.4.11.5. **Example**

The following command sequence places the gateway in dial-peer configuration mode, assigns an E.164 address to the interface, and registers that address with the gatekeeper:


```
dial-peer voice 110 pots
port 1/0
destination-pattern 5551212
register e164
```

The following commands deregister an address with the gatekeeper:

```
dial-peer voice 110 pots
no register e164
```

5.7.4.12. sid

When SID Packet transmission function is enable during silence processing under VAD function activation for call processing of specific dial-peer, use **sid** command in dial-peer configuration mode. If you want to set disable mode, add **no** command in front of **sid** command.

```
sid
no sid
```

5.7.4.12.1. Syntax

There is no any specific keyword and argument in this command.

5.7.4.12.2. Default Value

```
enable
```

5.7.4.12.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.12.4. Usage Guideline

If the VAD function is enable, the silence traffic is not transmitted via VoIP network environments, tin this time, only it is possible to aware to hear voice packet. But during silence processing, intermittently SID packet is transmitted. If you don't want this SID packet transmission function for reason of matching

problem with interoperability or unnecessary comfort noise generation, disable this function.

5.7.4.12.5. Example

The following command example is disable mode of SID packet transmission function.

```
dial-peer voice 10 voip
no sid
```

5.7.4.13. session target

To specify a network-specific address for a specified dial peer, use the **session target** of dial-peer configuration command. Use the **no** form of this command to disable this feature.

```
session target destination-address
no session target
```

5.7.4.13.1. Syntax

Keyword / Argument	Description
destination-address	IP address of the dial peer.

5.7.4.13.2. Default Value

No Default Value

5.7.4.13.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.13.4. Usage Guideline

Use the **session-target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select.

5.7.4.13.5. Example

The following example configures a session-target IP address "211.238.1.1".

```
dial-peer voice 10 voip
session-target 211.238.1.1
```

5.7.4.14. polarity-inverse

To activate polarity-inverse of FXS voice port. Use "**no**" to disable this function.

```
polarity-inverse
no polarity-inverse
```

5.7.4.14.1. Syntax

There is no any specific keyword and argument in this command.

5.7.4.14.2. Default Value

disable

5.7.4.14.3. Command Mode

Voice-port Configuration Mode

5.7.4.14.4. Usage Guideline

When PBX supports billing function and the start and end points are indicated by polarity inverse, activate this function. Then PBX Trunk line connected to FXS starts billing. Normally, the function is not necessarily to activate.

5.7.4.14.5. Example

The below configuration activates polarity- inverse at voice-port 1/0.

```
voice-port 1/0
    polarity-inverse
```

5.7.4.15. shutdown (Dial-Peer)

To change the state of the selected dial peer from up to down, use the **shutdown** dial-peer configuration command. Use the **no** form of this command to change the administrative state of this dial peer from down to up.

```
shutdown
no shutdown
```

5.7.4.15.1. Syntax

This command has no arguments or keywords.

5.7.4.15.2. Default Value

No shutdown

5.7.4.15.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.15.4. Usage Guideline

When a dial peer is shut down, you cannot initiate calls to that peer. This command is applicable to both VoIP and POTS peers.

5.7.4.15.5. Example

The following example changes the state of voice telephony dial peer 10 to down:

```
configure
dial-peer voice 10 pots
shutdown
```

5.7.4.16. translate-outgoing

To apply the translation rule to the outbound call of the corresponding dial peer, use this command. To stop applying the translation rule, add “no” command.

```
translate-outgoing { called-number | calling-number } tag
no translate-outgoing { called-number | calling-number }
```

5.7.4.16.1. Syntax

Keyword / Argument	Description
called-number	Applies the translation rule to the outbound called party number.
calling-number	Applies the translation rule to the outbound calling party number.
<i>tag</i>	Refers the rule set. Tag values range from 0 to 65535.

5.7.4.16.2. Default Value

No translation rule is applied.

5.7.4.16.3. Command Mode

Dial peer Configuration Mode

5.7.4.16.4. Usage Guideline

This command is applied to the POTS peer and the VoIP peer. Use “Translation-rule” command for the outbound call of the corresponding dial peer, and apply the number translation rule that has been set before.

5.7.4.16.5. Example

In the following example, translation rule 10 is created and it is applied to the calling party number of dial-peer 200. Therefore, if the calling party number of the outbound call is 93450, it will be translated into 9563450.

```
translation-rule 10
    rule 0 9 956
    rule 1 8 878
dial-peer voice 200 voip
    translate-outgoing calling-number 10
```

5.7.4.17. vad

To enable voice activity detection (VAD) for the calls using this dial peer, use the **vad** dial-peer configuration command. Use the **no** form of this command to disable VAD.

```
vad
no vad
```

5.7.4.17.1. Syntax

This command has no arguments or keywords.

5.7.4.17.2. Default Value

```
enable
```

5.7.4.17.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.17.4. Usage Guideline

Use the **vad** command to enable voice activity detection. With VAD, silence is not transmitted over the network, only audible speech. If you enable VAD, the sound quality is slightly degraded but the connection requires much less

bandwidth.

If you use the **no** form of this command, VAD is disabled and voice data is continuously transmitted to the IP network.

5.7.4.17.5. Example

The following example enables VAD:

```
dial-peer voice 10 voip
vad
```

5.7.4.18. voice-class codec

To assign a previously configured codec selection preference list (codec voice class) to a VoIP dial peer, enter the **voice-class codec command** in dial-peer configuration mode. To remove the codec preference assignment from the dial peer, use the **no** form of this command.

voice-class codec *tag*

no voice-class codec *tag*

5.7.4.18.1. Syntax

Keyword / Argument	Description
tag	The unique number assigned to the voice class. The valid range for this tag is 1 to 65533. The <i>tag</i> number maps to the tag number created using the voice class codec global configuration command.

5.7.4.18.2. Default Value

Dial peers have no codec voice class assigned.

5.7.4.18.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.18.4. Usage Guideline

You can assign one voice class to each VoIP dial peer. If you assign another voice class to the same dial peer, the last voice class assigned replaces the previous one.

5.7.4.18.5. Example

The following example shows how to assign a previously configured codec voice class to a dial peer:

```
dial-peer voice 100 voip
voice-class codec 10
```


5.7.5. Gateway, Voice Service, Voice Class and Rule Configuration Command

5.7.5.1. announcement

Use **announcement** command to activate voice announcement function. To disable this function, use the **no** form of this command.

announcement

no announcement

5.7.5.1.1. Syntax

There is no any keyword and argument in this command.

5.7.5.1.2. Default Value

disable

5.7.5.1.3. Command Mode

Voice Service Voip Configuration Mode

5.7.5.1.4. Usage Guideline

If voice announcement function is activated voice announcement is made in case of abnormal finishing of call processing, inputting password for FXO voice ports, and PSTN rerouting. The kind of voice announcements is different from each APOS versions. Other AP VoIP gateway may be not supports this function.

5.7.5.1.5. Example

The following command shows an example of enabling voice announcement function.

```
voice service voip
  announcement
```

5.7.5.2. codec preference

To specify a list of preferred codecs to use on a dial peer, use the **codec preference** command in voice-class configuration mode. To disable this function, use the **no** form of this command.

codec preference *value codec_type*

no codec preference *value codec_type*

5.7.5.2.1. Syntax

Keyword / Argument	Description
Value	Specifies the order of preference, with 1 being the most preferred and 5 being the least preferred.
Codec_type	Specifies the codec preferred. . G711alaw : G.711 A-Law 64Kbps Codec . G711ulaw : G.711 u-Law 64Kbps Codec . G729 : G.729 8Kbps Codec . G7231r63 : G.723.1 6.3Kbps Codec.. . G7231r53 : G.723.1 5.3Kbps Codec

5.7.5.2.2. Default Value

No default behavior or values.

5.7.5.2.3. Command Mode

Voice-class Configuration Mode

5.7.5.2.4. Usage Guideline

The gateway at the opposite end of the WAN may have to negotiate the codec selection for the network dial peers. The codec preference command specifies the order of preference for selecting a negotiated codec for the connection.

5.7.5.2.5. Example

AP2120 Gateway uses voice codec for toll-quality, high bandwidth

```
voice class codec 99
codec preference 1 g711alaw
codec preference 2 g711ulaw
codec preference 3 g723lr63
codec preference 4 g729
end
dial-peer voice 1919 voip
voice-class codec 99
```

5.7.5.3. counter

To set VoIP-related counter parameter value, use “**counter**” command in the voice service setup mode. To convert this setup into the default state, use “**no**” command before this command.

```
counter { cras } value
no counter { cras }
```

5.7.5.3.1. Syntax

Keyword / Argument	Description
cras <i>value</i>	RAS message retransmission counter with the gatekeeper. The value ranges from 1 to 5, and the default is 3.

5.7.5.3.2. Default Value

See the above.

5.7.5.3.3. Command Mode

Voice-Service Configuration Mode

5.7.5.3.4. Usage Guideline

This command is to partially set the global voice-service for the VoIP service.

The **cras** counter is to retransmit message if no reply is received during **timeout tras** after sending RAS message – GRQ, RRQ, ARQ and DRQ – to the gatekeeper.

5.7.5.3.5. Example

In the following message, the RAS message is tried two times.

```
voice service voip
  counter cras 2
```

5.7.5.4. discovery

This command is to activate the function of sending GRQ(Gatekeeper Request) message. Use the **no** form of this command to set disable mode.

discovery

no discovery

5.7.5.4.1. Syntax

There is no any keyword and argument in this command set.

5.7.5.4.2. Default Value

enable

5.7.5.4.3. Command Mode

Gateway Configuration Mode

5.7.5.4.4. Usage Guideline

When a VoIP gateway is registered with a gatekeeper, if this function is activated, the Gateway sends GRQ and receives GCF before sending RRQ. However, if this is not activated, the gateway directly sends RRG.

5.7.5.4.5. Example

The following command deactivates discovery command.

```
gateway
    no discovery
```

5.7.5.5. fax protocol

To specify the global default fax protocol for all the Voice over IP (VoIP) dial peers, use the **fax protocol** command in voice-service configuration mode. To return to the default fax protocol, use the **no** form of this command.

```
fax protocol { t38 [redundancy value] | bypass | inband-t38 [redundancy
value] }
no fax protocol
```

5.7.5.5.1. Syntax

Keyword / Argument	Description
t38	ITU-T T.38 standard fax protocol.
Inband-t38	A conversion of ITU-T T.38 standard fax protocol sending T.38 information on RTP payload.
bypass	Fax protocol on clean voice channel (i.e., G.711)
redundancy	(Optional) redundancy for the T.38 fax protocol.
value	The <i>value</i> can be from 0 to 5. The default is 0.

5.7.5.5.2. Default Value

T.38 fax protocol

5.7.5.5.3. Command Mode

Voice-Service Configuration Mode

5.7.5.5.4. Usage Guideline

Use the **fax protocol t38** command to configure T.38 Fax Relay for VoIP. The **t38** keyword enables the T.38 Fax Relay protocol.

Optional parameters **redundancy** is used to send redundant T.38 fax packets.

** inband-t38 is used by Commworks(Previously, 3Com)'s VoIP Gateway for T.38 FAX Protocol, so to user the device configure this opetion.*

5.7.5.5.5. Example

The following example shows setting T.38 fax protocol for VoIP in global configuration mode:

```
voip service voip
fax protocol t38
```

5.7.5.6. fax rate

To establish the rate at which a fax is sent to the specified dial peer, use the **fax rate** command in dial-peer configuration mode.

To reset the dial peer for voice calls, use the **no** form of the command.

```
fax rate { 2400 | 4800 | 7200 | 9600 | 12000 | 14400 | disable }
no fax rate
```

5.7.5.6.1. Syntax

Keyword / Argument	Description
2400	Specifies a fax transmission speed of 2400 bps.
4800	Specifies a fax transmission speed of 4800 bps.
7200	Specifies a fax transmission speed of 7200 bps.
9600	Specifies a fax transmission speed of 9600 bps.
12000	Specifies a fax transmission speed of 12,000 bits per second (bps).
14400	Specifies a fax transmission speed of 14,400 bps.
disable	Disables Fax Relay transmission capability.

5.7.5.6.2. **Default Value**

14400 bps

5.7.5.6.3. **Command Mode**

Voice-Service Configuration Mode

5.7.5.6.4. **Usage Guideline**

Use the **fax rate** command to specify the fax transmission rate to all dial peers.

The values for this command apply only to the fax transmission speed and do not affect the quality of the fax itself. The higher transmission speed values (14,400 bps) provide a faster transmission speed but monopolize a significantly large portion of the available bandwidth. The lower transmission speed values (2400 bps) provide a slower transmission speed and use a relatively small portion of the available bandwidth.

This command is meaningful only under T.38 Fax Relay. If the fax rate is disabled, T.38 fax relay does not operate. The fax relay made by the bypass mode performs no operation in the gateway (as it does nothing for the fax communication in the PSTN network) setting the rate does not mean anything.

Although T.38 is set as 14400 bps by this command, if two fax machines on both sides operate at 9600, actual fax rate will be 9600 bps.

5.7.5.6.5. **Example**

The following example shows a fax rate transmission speed of 9600 bps for faxes sent using a dial peer:

```
voice service voip
fax rate 9600
```

5.7.5.7. h323 call start

To force the H.323 Version 2 gateway to use Fast Connect or Slow Connect procedures for all H.323 calls, use the **h323 call start** command in voice-service configuration mode. To restore the default condition, use the **no** form of this command.

h323 call start { fast | slow | preferred-slow }

no h323 call start

5.7.5.7.1. Syntax

Keyword / Argument	Description
fast	Gateway uses H.323 Version 2 (Fast Connect) procedures
slow	Gateway uses H.323 Version 1 (Slow Connect) procedures.
preferred-slow	If you configure this option, at the time to make a call, Gateway use slow start (normal start) procedure. At the time to receive a call, Gateway use slow start (normal start) or fast start procedure depends on calling party's configuration.

5.7.5.7.2. Default Value

Fast.

5.7.5.7.3. Command Mode

Voice-Service Configuration Mode

5.7.5.7.4. Usage Guideline

This **h323 call start** command is configured as part of the global voice-service configuration for VoIP services. It does not take effect unless the **call start system** voice-class configuration command is configured in the VoIP dial peer.

5.7.5.7.5. Example

The following example selects Slow Connect procedures for the gateway:

```
voice service voip
h323 call start slow
```

5.7.5.8. gkip

To specify the gatekeeper associated with a proxy and control how the gatekeeper is discovered, use the **gkip** command in gateway configuration mode.

```
gkip ip-addr [port] [priority]
no gkip ip-addr
```

5.7.5.8.1. Syntax

Keyword / Argument	Description
<i>ip-addr</i>	The gatekeeper discovery message will be unicast to this address. and, optionally, the UDP port specified.(Default Port Value is 1719)
<i>port</i>	Optionally, the UDP port of gatekeeper specified.(Default Port Value is 1719)
<i>priority</i>	Optionally designates priorities of several alternate gatekeepers. The priority value ranges from 0 to 254, and the lower the value is, the higher the priority is. The default priority is 128.

5.7.5.8.2. Default Value

No gatekeeper is configured for the proxy.

5.7.5.8.3. Command Mode

Gateway Configuration Mode

5.7.5.8.4. Usage Guideline

The VoIP gateway is registered in the gatekeeper that is the Registration

Admission and Status (RAS) server and receives the billing service. The AP2120 VoIP Gateway can designate maximum ten gatekeepers in a gateway using this command. To view the list of the gatekeepers, use "**show gateway**" command. If more than one gateway is designated, gateways try to register themselves in the gatekeeper using the GRQ message according to their priorities. There is only one gatekeeper that can be registered at the same time. When a gateway receives the re-registration failure message or does not receive any message, the next gateway tries to register itself to the gatekeeper.

Users can designate the gatekeeper using this command or using the Alternate GK list included in the message that the currently registered gatekeeper sends. For reader's reference, official gatekeeper multicast IP address based on H.323 standard is 224.0.1.41 and the port is 1718.

5.7.5.8.5. Example

The following example sets up a unicast discovery to a gatekeeper:

```
gkip 192.7.5.1
```

In the following example, the gatekeeper has 224.0.1.41 IP address (a multicast IP address) and port 1718, and its priority is 0.

```
gkip 224.0.1.41 1718 0
```

5.7.5.9. h323 call channel

If you want to open voice channels before voice CONNECT In case of normal voice processing, use **h323 call channel early** command in voice service configuration mode. To return default configuration mode, use the **no** form of this command.

```
h323 call channel { early | late }
```

```
no h323 call channel
```

5.7.5.9.1. Syntax

Keyword / Argument	Description
early	If you want to open voice channel before voice CONNECT in case of normal(slow) voice processing, use this command.
late	If you want to open voice channel after voice CONNECT in case of normal(slow) voice processing, use this command.

5.7.5.9.2. Default Value

late

5.7.5.9.3. Command Mode

Voice-Service Configuration Mode

5.7.5.9.4. Usage Guideline

This command supports one of global voice service parts for VoIP services. This command is able to use at a point of time under transmission CONNECT of H.245 call processing based logical call using the AP2120 VoIP gateway or remote other gateway doing starting h323 call.

When the gateway or remote gateways use normal (slow) for H323 call start, the logical channel (voice channel) is opened when CONNECT is received after the other side does hook off.

It may be possible to cut a front of real voice sound in case of opening voice channel after CONNECT. To avoid this phenomenon, use **h323 call channel early** mode to open voice channel before other side hooking off.

5.7.5.9.5. Example

The following command example shows fast voice channels

```
voice service voip
  h323 call channel early
```

5.7.5.10. h323 call response

If you want to define message besides ALERT message after call proceeding message responding to Q.931 setup message, use h323 call response command in voice service configuration mode. To return default configuration mode, use the **no** form of this command.

h323 call response { alert | progress | none}

no h323 call response

5.7.5.10.1. Syntax

Keyword / Argument	Description
alert	Sending ALERT message as response message.
progress	Sending PROGRESS message as response message.
none	Sending CONNECT message as response message after CALL PROCEEDING .

5.7.5.10.2. Default Value

alert.

5.7.5.10.3. Command Mode

Voice-Service Configuration Mode

5.7.5.10.4. Usage Guideline

This command supports to setup configuration for one of global voice service parts for VoIP service. AP2120 VoIP gateway is able to send message whether gateway send ALERT or PROGRESS message according to command configuration before completing CONNECT message after sending call proceeding message when gateway operate as receiving gateway side with getting setup message. This command configuration setting recommend default mode besides special case.

5.7.5.10.5. Example

The following command example shows how to make configuration response message to change progress message.

```
voice service voip
  h323 call response progress
```

5.7.5.11. h323-id

To configure the H.323 name of the gateway identifying this gateway to its associated gatekeeper, use the **h323-id** command in gateway configuration mode.

```
h323-id h323_id
```

5.7.5.11.1. Syntax

Keyword / Argument	Description
h323-id	H.323 name (ID) used by this gateway when this gateway communicates with its associated gatekeeper. Usually, this ID is the name of the gateway with the gatekeeper domain name appended to the end: name@domain-name . (max length 95)

5.7.5.11.2. Default Value

```
voip.ip_address
```

5.7.5.11.3. Command Mode

Gateway Configuration Mode

5.7.5.11.4. Example

The following example configures the gateway ID is GW13@addpac.com

```
gateway
gkip 211.238.1.1
```

h323-id GW13@addpac.com

5.7.5.12. lightweight-irr

To send IRR(Information Request Response) message as simple information, use this command. To make disable this command, use the **no** form of this command to set disable mode.

lightweight-irr

no lightweight-irr

5.7.5.12.1. Syntax

There is no any keyword and argument in this command set.

5.7.5.12.2. Default Value

disable

5.7.5.12.3. Command Mode

Gateway Configuration Mode

5.7.5.12.4. Usage Guideline

AP2120 VoIP Gateway is able to send IRR message responding to IRQ message from a gatekeeper. Originally, this IRR message gives service for status confirmation of VoIP gateway with call information, and so on. However, this message sequence is able to send essential information in case of IRR message period to be short, not to need large information for call processing.

5.7.5.12.5. Example

The following command example shows to send essential information as a IRR message.

gateway

lightweight-irr

5.7.5.13. max-digits

This command is used to limit the number of digits for a user class, which in turn adds to the security of specific out-going signal to the FXO port. The "no" default value for this command is "0", meaning there is no limitation.

max-digits *number*

no max-digits

5.7.5.13.1. Syntax

Keyword / Argument	Description
number	Maximum number of digits for out-going signals

5.7.5.13.2. Default Value

0

5.7.5.13.3. Command Mode

User-Class Configuration Mode

5.7.5.13.4. Example

The following describes configuring the maximum digits for user class 1 as "10".

```
voice class user 1
max-digits 10
```

5.7.5.14. password

This command is used to configure a 4 digit security password for the security of out-going signals to FXO port. The "no" default value for this command is "null", which runs no security test for all out-going signals to the FXO port. If a security digit is configured for at least one user class, the password is checked.

password *string*

no password

5.7.5.14.1. Syntax

Keyword / Argument	Description
string	security code which could be sequence of IA5 characters. (4 digits)

5.7.5.14.2. Default Value

Null

5.7.5.14.3. Command Mode

User-Class Configuration Mode

5.7.5.14.4. Example

The following is the configuration for password "1234" for user class 1.

```
voice class user 1
password 1234
```

5.7.5.15. public-ip

To define public IP address mapped with private IP address of VoIP gateway under static NAT/PAT network environment, use this command. To disable this mode, use the **no** form of this command.

public-ip *addr*
no public-ip

5.7.5.15.1. Syntax

Keyword / Argument	Description
addr	Define IP address setting for example 211.238.72.3.

5.7.5.15.2. Default Value

Disable

5.7.5.15.3. Command Mode

Gateway Configuration Mode

5.7.5.15.4. Usage Guideline

In case of using private network environment with NAT/PAT, IP address of VoIP gateway should be set in VoIP interface of AP2120 VoIP gateway. On the other hand, using public network environment under gatekeeper and other gateway, AP2120 VoIP gateway should be defined static NAT or static PAT, and public IP address.

5.7.5.15.5. Example

The following command example shows public IP configuration mode.

```
gateway
public-ip xxx.xxx.xxx.xxx
```

5.7.5.16. register

To register a gateway to a gatekeeper, uses **register** command in gateway configuration mode. To cancel the registration, use "**no**" command before this command.

```
register
no register
```

5.7.5.16.1. Syntax

There is no any specific keyword and argument in this command set.

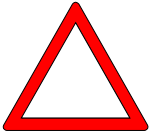
5.7.5.16.2. Default Value

disable

5.7.5.16.3. Command Mode

Gateway Configuration Mode

5.7.5.16.4. Usage Guideline



To make enable H.323 VoIP gateway functions, use register command. If VoIP gateway is enabled, this VoIP gateway try to look for gatekeeper using H.323 RAS GRQ or RRQ message. If you use no register command, AP2120 VoIP gateway is able to cancel registration from gatekeeper using H.323 RAS URG message.

If you want to change or register new dial peer using script file with operating gatekeeper, use no register (or no gateway) command in initial stage of script file or load configuration after doing un-registration from gatekeeper. Otherwise, messages may be crashed between the gateway and the gatekeeper for updating changed information

5.7.5.16.5. Example

The following command example shows setting registration mode.

```
gateway
  register
```

5.7.5.17. rule

To apply the translation rule to the calling/called party number of the inbound/outbound calls, use "**rule**" command in the translation-rule setup mode. To remove the rule that has been set, add "**no**" command to the above command.

```
rule tag input-matched-pattern substituted-pattern
no rule tag
```

5.7.5.17.1. Syntax

Keyword / Argument	Description
<i>tag</i>	An identifier to designate the rule within the rule set. Tag values range from 0 to 65535.
<i>input-matched-pattern</i>	Input digits for pattern matching. Characters that can be entered include numeric data (0 to 9) "#", "*", "[]", ".", and "T."
<i>substituted-pattern</i>	A pattern to be converted upon successful pattern matching. Characters that can be entered include numeric data (0 to 9) "#", "%", ".", and "T."

5.7.5.17.2. Default Value

There is no default value.

5.7.5.17.3. Command Mode

Translation-rule Configuration Mode

5.7.5.17.4. Usage Guideline

This command is used to apply the translation rule to the calling party/called party numbers of the inbound/outbound calls.

If one or more rules match with the called (or calling) party number, the rule which matches most with the *input-matched-pattern* will be selected.

"Input-matched-pattern" can perform range expression. (eg. [1-9]) Also, the wildcard (.) can be used to apply number of digits of the called/calling party number. If "input-matched-pattern" is configured only with (.) or (T) number translation will be applied to all called/calling-party-number.

"Substituted-pattern" is to convert fixed digits (excluding the wildcard) of the input-matched-pattern into the string. There are two forms of the *substituted-pattern*. See the following:

If the substituted-pattern is composed only of IA5 characters (0 ~ 9, # and *) fixed digits of the input-matched-pattern will be converted into the string part of the substituted-pattern and other digits than the fixed digits of the called/calling party will be attached at the end.

Or, if the substituted-pattern uses "%" form, each digit of the called/calling party number is replaced by "%xx" to make a number. At this time, % values range from %01 to %99 (from the 1st digit to the 99th digit of the called/calling party number.)

If the *substituted-pattern* is composed of (.) or (T) only, the called/calling-party-number is made of other digits than the fixed pattern of the input-matched-pattern.

5.7.5.17.5. Example

In the following example, 5554123 is extended into 140855554123.

rule 0 55541 1408555541

In the following example, the translation is not applied when the number is 5551. However, 5551234 is translated into 1408551234.

rule 0 555.. 1408555

In the following example, 1241234 is converted into 14085551234 and 3551234 is converted into 14085551234..

rule 0 [1-3][25]5.. 1408555

In the following example, 5551234 is converted into 4441234.

rule 0 555.. 444%04%05%06%07%08%09%10%11%12

In the following example, 55512 5551234 and 555123456 are all converted into 444.

rule 0 555.. 444%99

In the following example, 5551234 is converted into 3334.

rule 0 555.. 111

rule 1 55512 222

rule 2 555[0-9][0-9][0-9] 333

In the following example, 5551234 is converted into 1234.

```
rule 0 555 .
```

```
rule 0 555 T
```

In the following example, 555123 is converted into 95551234.

```
rule 0 . 9
```

```
rule 0 T 9
```

5.7.5.18. security password

To configure the secure token with gatekeeper, this **security password** command is used. If this password is enabled, this gateway add CryptoToken element to the message to gatekeeper. This CryptoToken is MD5 hashed token which also should be enabled in gatekeeper when registration, and permit call. If **no** form of this command is used, security between gateway and gatekeeper is disabled.

security password *string*

no security password

5.7.5.18.1. Syntax

Keyword / Argument	Description
string.	security code which could be sequence of ASCII characters.

5.7.5.18.2. Default Value

Disable.

5.7.5.18.3. Command Mode

Gateway Configuration Mode

5.7.5.18.4. Example

The following example set password "okok1234":

```
gateway
security password okok1234
```

5.7.5.19. security permit-FXO

For outgoing calls from remote side to PSTN or PABX route through the FXO of the gateway, the security should be concerned. To protect a call from un-secure user in remote side, when **security permit-FXO** is disabled, the call from remote side that is not registered in session target list of VoIP dial-peer will be dropped.

When session target is set to "ras" with gatekeeper, this command should be set to permit all calls to the FXO (This command is only useful without gatekeeper). If **no** form of this command is used, security is enabled and do not permit a call from unregistered VoIP peer.

```
security permit-FXO
no security permit-FXO
```

5.7.5.19.1. Syntax

This command has no arguments or keywords.

5.7.5.19.2. Default Value

Permit all calls

5.7.5.19.3. Command Mode

Voice Service Configuration Mode

5.7.5.19.4. Usage Guideline

To keep the security of the calls coming to the FXO port through the network, the AP2120 Gateway provides two methods – "Security permit-FXO" command

and the voice class user. Since it is possible to directly attempt calls to the PSTN through this FXO port or indirectly attempt calls to the PSTN through the PBX internal line, unauthorized remote users can attempt calls as well. To prevent unauthorized users' attempting calls, the security shall be kept. Two security systems that the AP2120 Gateway provides have following advantages and disadvantages.

With "security permit-FXO" command, remote users does not need to enter the password so they can easily access the network. However, IP address of the VoIP peer on the other side shall be registered and the gatekeeper cannot be used at the same time. Also, it is impossible to bar calls of the registered peers by class.

With the "voice class user" users need to enter the password digit but stronger and multi-classed call barring is possible.

5.7.5.19.5. Example

The following example permit all call to FXO:

```
voice service voip  
  
security permit-FXO
```

5.7.5.20. timeout

To set VoIP-related timer parameters, use "**timeout**" command in the voice service setup mode. To return this setup to the default state, use "**no**" command before this command.

```
timeout { t301 | t303 | tras | ttll | tidt | treg } value  
no timeout { t301 | t303 | tras | ttll | tidt | treg }
```

5.7.5.20.1. Syntax

Keyword / Argument	Description
t301 <i>value</i>	Timeout value from Q.931 Alert message reception till Connect message reception. Values range from 5 to 600, and the default is 180. T301 value is expressed in seconds.

t303 <i>value</i>	Timeout value from Q.931 Setup message transmission till initial message reception. Values range from 5 to 60 and the default value is 8. T303 value is expressed in seconds.
tras <i>value</i>	Timeout value from RAS message transmission till reply message reception. Values range from 2 to 30, and the default value is 6. Tras value is expressed in seconds.
tttl <i>value</i>	RAS time-to-live timeout value. Values range from 10 to 600, and the default value is 60. Values are expressed in seconds. This value is updated by the gatekeeper.
tidt <i>value</i>	Inter-digit timeout value to enter digits into the analog voice port. Values range from 1 to 600, and the default value is 10. Tidt value is expressed in seconds.
treg <i>value</i>	Timeout value for re-registration attempt upon registration failure in the gatekeeper. Values range from 10 to 600 and the default value is 30. Treg value is expressed in seconds.

5.7.5.20.2. Default Value

See the above.

5.7.5.20.3. Command Mode

Voice-Service Configuration Mode

5.7.5.20.4. Usage Guideline

This command is to partially set the global voice-service for the VoIP service.

A proper value has been set as the default value of the timeout. It is recommended to use the default value in most of cases.

5.7.5.20.5. Example

In the following example, the timeout value of the RAS message has been set three seconds.

```
voice service voip
  timeout tras 3
```


5.7.5.21. translate-voip-incoming

Use this command to apply the translation rule to every inbound VoIP call. To remove application of the translation rule, add "no" command to the above command.

```
translate-voip-incoming { called-number | calling-number } tag
no translate-voip-incoming { called-number | calling-number }
```

5.7.5.21.1. Syntax

Keyword / Argument	Description
called-number	Applies the translation rule to the inbound called party number.
calling-number	Applies the translation rule to the inbound calling party number.
<i>tag</i>	Refers the rule set. Ranges from 0 to 65535.

5.7.5.21.2. Default Value

No translation rule is applied.

5.7.5.21.3. Command Mode

Voice-Service Configuration Mode

5.7.5.21.4. Usage Guideline

This command is to apply the translation rule that has been set by using "translation-rule" command for the inbound VoIP call incoming from the network.

5.7.5.21.5. Example

In the following example, translation rule 10 is created and it is applied to the calling party number of the VoIP inbound calls. Therefore, if the calling party number of the inbound calls incoming from the network is 93450, it will be translated into 9563450.

```
translation-rule 10
    rule 0 9 956
    rule 1 8 878
voice service voip
    translate-voip-incoming calling-number 10
```

5.7.6. Miscellaneous Commands

5.7.6.1. clear h323 call

To force disconnection of a specific call or for all calls active with remote user, use the **clear h323 call** command in Administrator command mode. **clear h323 call { all / local_call_ID }**

5.7.6.1.1. Syntax

Keyword / Argument	Description
all	Forces all active calls currently associated with this gatekeeper to be disconnected.
local_call_ID	Specifies the local call identification number (CallID) that identifies the call to be disconnected.

5.7.6.1.2. Default Value

No Default Value

5.7.6.1.3. Command Mode

Administrator command

5.7.6.1.4. Usage Guideline

If you want to force a particular call to be disconnected (as opposed to all active calls on the gatekeeper), use the CallID number to identify that specific call. You can find the local CallID number for a specific call by using the **show call active all** command; the ID number is displayed in the CallID column.

5.7.6.1.5. Example

The following example forces all active calls:

```
clear h323 call all
```

5.7.6.2. clear voice port

To force disconnection of a call on a specific voice port, use the **clear voice port** command in Administrator command mode. If port is not specified, disconnect all calls on the system.

clear voice port *[slot/port]*

5.7.6.2.1. Syntax

Keyword / Argument	Description
port	Specifies a port to clear calls on the port..

5.7.6.2.2. Default Value

None

5.7.6.2.3. Command Mode

Administrator command

5.7.6.2.4. Usage Guideline

None

5.7.6.2.5. Example

The following example forces all active calls:

```
clear voice port
```

5.7.6.3. show call active

To display active call information for voice calls or fax transmissions in progress, use the **show call active** command in Administrator command

show call active { all/summary }

5.7.6.3.1. Syntax

Keyword / Argument	Description
all	Display all Information about all active calls
summary	Display summarized Information about all active calls.

5.7.6.3.2. Default Value

No default value

5.7.6.3.3. Command Mode

Administrator command

5.7.6.3.4. Usage Guideline

Use the **show call active** command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information.

5.7.6.3.5. Example

The following is sample output from the **show call active voice** command:

```
show call active summary
```

5.7.6.4. show call history

To display the call history table for voice calls or fax transmissions, use the **show call history** command in Administrator command.

```
show call history { all } { last number }
```

5.7.6.4.1. Syntax

Keyword / Argument	Description
--------------------	-------------

all	Displays all history information of the call history table
last	(Optional) Displays the last calls connected.
number	the number of calls that appear is defined by the <i>number</i> argument. Valid values are from 1 to 100.

5.7.6.4.2. Default Value

No Default value

5.7.6.4.3. Command Mode

Administrator command

5.7.6.4.4. Usage Guideline

The **show call history** command displays a call history. It shows call time, call setup time, called party, calling party.

5.7.6.4.5. Example

The following is sample output of the **show call history voice** command:

```
show call history all last 10
```

5.7.6.5. show clear-down-tone

To show clear-down-tone classes , use the **show clear-down-tone** command in Administrator command mode. Without number, all clear-down-tone classes will be displayed.

```
show clear-down-tone
```

5.7.6.5.1. Syntax

This command has no arguments or keywords.

5.7.6.5.2. Default Value

No Default Value

5.7.6.5.3. Command Mode

Administrator command

5.7.6.5.4. Usage Guideline

This command will display not only user added clear-down-tone by **voice class clear-down-tone** command, but also system providing clear-down-tones.

5.7.6.5.5. Example

The following is to display all Clear-down-tone class.

5.7.6.6. show codec class

To show codec classes , use the **show codec-class** command in Administrator command mode. Without number, all codec classes will be displayed.

show codec class [*number*]

5.7.6.6.1. Syntax

Keyword / Argument	Description
number	(Optional) codec class tag number.

5.7.6.6.2. Default Value

No Default Value

5.7.6.6.3. Command Mode

Administrator command

5.7.6.6.4. Example

The following is to display all Codec Class.

```
show codec class
```

5.7.6.7. show dial-peer

To display configuration information for dial peers, use the **show dial-peer voice** command. If there is no options, display all information of all Dial-Peer..

```
show dial-peer {voice | pots | voip} [ number / summary ]
```

5.7.6.7.1. Syntax

Keyword / Argument	Description
voice	Display VoIP and POTS Dial-peer information
pots	Display POTS Dial-peer information
VoIP	Display VoIP Dial-peer information
number	Optional) A specific dial peer. This option displays configuration information for a single dial peer identified by the <i>number</i> argument. Valid entries are any integers that identify a specific dial peer, from 1 to 32767.
summary	Optional) Displays a summary of all voice dial peers

5.7.6.7.2. Default Value

No Default value

5.7.6.7.3. Command Mode

Administrator command

5.7.6.7.4. Usage Guideline

Use the **show dial-peer voice** Administrator command to display the configuration of Dial-Peer both in Administrator mode and dial-peer configuration mode. This allows the user to check the latest updated information for easy configuration.

5.7.6.7.5. Example

The following is sample output from the **show dial-peer voice** command for a POTS dial peer:

```
show dial-peer voice
```

5.7.6.8. show dialplan number

To show which dial peer is reached when a particular telephone number is dialed, use the **show dialplan number** command in Administrator command mode.

```
show dialplan number dial_string
```

5.7.6.8.1. Syntax

Keyword / Argument	Description
dial_string	Specifies a particular destination pattern (telephone number).

5.7.6.8.2. Default Value

No Default Value

5.7.6.8.3. Command Mode

Administrator command

5.7.6.8.4. Usage Guideline

The **show dialplan number** command is used to test whether the dial plan configuration is valid and working as expected.

5.7.6.8.5. Example

The following is sample to show all dial-peers matching telephone number 4441234:

```
show dialplan number 4441234
```

5.7.6.9. show dialplan port

To show which POTS dial peer is matched for a specific calling number or voice port, use the **show dialplan port** command in Administrator command mode.

show dialplan port *voice-port*

5.7.6.9.1. Syntax

Keyword / Argument	Description
voice_port	Specifies the voice port location. (slot number / port number)

5.7.6.9.2. Default Value

No Default Value

5.7.6.9.3. Command Mode

Administrator command

5.7.6.9.4. Usage Guideline

Use the **show dialplan port** command as a troubleshooting tool to determine which POTS dial peer is matched to an voice-port.

5.7.6.9.5. Example

To show all dial-peers matching port 1/1:

```
show dialplan port 1/1
```

5.7.6.10. show gateway

To show gateway related information , use the **show gateway** command in

Administrator command.

show gateway

5.7.6.10.1. **Syntax**

This command has no arguments or keywords.

5.7.6.10.2. **Default Value**

No Default Value

5.7.6.10.3. **Command Mode**

Administrator command

5.7.6.10.4. **Usage Guideline**

This command will display not only gatekeeper interaction information such as gatekeeper IP address, registration status, registered aliases, but also system resource information about VoIP gateway (i.e., number of dial-peers, number of voice ports, number of codec classes, ...)

5.7.6.10.5. **Example**

To show gateway related information of this system:

show gateway

5.7.6.11. **show num-exp**

To show number expansion information, **show num-exp** Administrator command mode.

show num-exp

5.7.6.11.1. Syntax

This command has no arguments or keywords.

5.7.6.11.2. Default Value

No Default Value

5.7.6.11.3. Command Mode

Administrator command

5.7.6.11.4. Usage Guideline

Even though you create number expansion with wildcard(*), show num-exp will not display wildcard.

5.7.6.11.5. Example

To show number expansion information of this system:

```
show num-exp
```

5.7.6.12. show translation-rule

To view whole or total application result of the translation rule, use "**show translation-rule**" command that is one of administrator's commands.

```
show translation-rule [tag] [dial_string]
```

5.7.6.12.1. Syntax

Keyword / Argument	Description
<i>tag</i>	Designates a certain rule set. If not, all translation rules will be displayed..
<i>dial_string</i>	If a certain destination pattern (telephone number) is entered, application result of the rule will be shown.

5.7.6.12.2. **Default Value**

No Default Value

5.7.6.12.3. **Command Mode**

Administrator command

5.7.6.12.4. **Usage Guideline**

This command is to check if the translation rule has been properly set and to test operations of the translation rule.

5.7.6.12.5. **Example**

In the following example, the result of applying the translation rule to the telephone number 4441234 will be displayed.

```
show translation-rule 10 4441234
```

5.7.6.13. **show user-class**

To show user classes , use the **show user-class** command in Administrator command mode. All user classes will be displayed.

```
show user-class
```

5.7.6.13.1. **Syntax**

This command has no arguments or keywords.

5.7.6.13.2. **Default Value**

No Default Value

5.7.6.13.3. Command Mode

Administrator command

5.7.6.13.4. Usage Guideline

This command shows user class tag, password, and max digits can input

5.7.6.13.5. Example

To display User Class information :

```
show user-class
```

5.7.6.14. show voice port

To show voice port information , use the **show voice port** command in Administrator command mode. Without slot/port, all voice port available in this system will be displayed.

```
show voice port [summary | slot/port ]
```

5.7.6.14.1. Syntax

Keyword / Argument	Description
summary	(Optional) Brief information.
slot/port	(Optional) slot number and port number.

5.7.6.14.2. Default Value

No Default Value

5.7.6.14.3. Command Mode

Administrator command

5.7.6.14.4. **Usage Guideline**

This command can be used not only Administrator command, but also Voice-port configuration mode.

5.7.6.14.5. **Example**

To show brief voice port information of this system:

```
show voice port summary
```

5.7.6.15. **show voip-interface**

To view the VoIP interface that is currently designated, use "**show VoIP-interface**" command that is one of administrator's commands.

```
show voip-interface
```

5.7.6.15.1. **Syntax**

This command has no arguments or keywords

5.7.6.15.2. **Default Value**

No Default Value.

5.7.6.15.3. **Command Mode**

Administrator command

5.7.6.15.4. **Usage Guideline**

Shows the VoIP interface currently in service.

5.7.6.15.5. **Example**

In the following example, VoIP interface information of the corresponding

system will be displayed.

```
show voip-interface
```

5.7.6.16. debug voip call

To trace VoIP related events, use the **debug VoIP call** command in Administrator command mode.

```
debug voip call
```

```
no debug voip call
```

5.7.6.16.1. Syntax

This command has no arguments or keywords

5.7.6.16.2. Default Value

No Default Value

5.7.6.16.3. Command Mode

Administrator command

5.7.6.16.4. Usage Guideline

The trace will be displayed by console port. Q.931 events, H.245 events, User interface events will be displayed. This trace makes system performance degraded. This should be disabled on normal operational state.

5.7.6.16.5. Example

To trace VoIP events:

```
debug voip call
```

To stop trace:


```
undebg voip call
```

5.7.6.17. debug voip

To trace events related to VoIP ASN.1, use the administrator command mode “debug VoIP”

```
debug voip { h225-asn1 | h245-asn1 | ras-asn1 }  
no debug voip { h225-asn1 | h245-asn1 | ras-asn1 }
```

5.7.6.17.1. Syntax

Keyword / Argument	Description
h225-asn1.	Trace H.225 ASN.1 event
h245-asn1	Trace H.245 ASN.1 event.
ras-asn1	Trace RAS ASN.1 event

5.7.6.17.2. Default Value

No Default Value

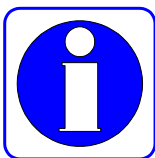
5.7.6.17.3. Command Mode

Administrator command

5.7.6.17.4. Usage Guideline

This command traces H.225 ASN.1, H.245 ASN.1, and RAS ASN.1 events, to display it on the console port. This command may effect system performance, therefore it is advised to disable this function under normal circumstances.

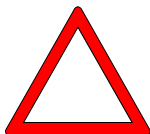
Information Users can see VoIP-related messages and call tracing through the console port.



This is default setting. However, if the user wishes to view call tracing through the telnet terminal from a remote place, the user shall use “debug-port” command (one of the global commands) from the remote terminal. Message tracing operates either in the console or in the remote terminal wherever “debug-port” command has been used. If the telnet terminal is terminated,

message tracing will automatically operate in the console. "No debug-port" displays call tracing on the default display console.

Caution



Message tracing using the debug command gives a high load to the router so it is recommended not to use the debug command under normal conditions. After tracing in the telnet terminal, exit the terminal with "no debug" or "undebug" command. Otherwise, message tracing will be displayed in the console.

5.7.6.17.5. Example

The following is an example of tracing an H.225 ASN.1 event for the system.

```
debug voip h225-asn1
```

The following is an example of switching an enabled H.245 ASN.1 Debugging function off for the system.

```
undebug voip h245-asn1
```


Appendix A. AP1100 VoIP Gateway Specifications

A-1 Voice over IP (VoIP) Service

Specification	Support (●)	Remark
1. VoIP Protocol		
ITU-T H.323 v2 Protocol	●	
Session Initiation Protocol (SIP)	●	H.323과 Dual Stack
2. Voice Compression		
G.723.1 MP-MLQ, 6.3Kbps, 5.3Kbps	●	
G.729.A CS-ACELP, 8Kbps	●	
G.711 PCM, 64Kbps	●	
G.726	●	
G.727	●	
3. Voice Processing		
Voice Activity Detection (VAD)	●	
T.38 Protocol	●	
Dual Tone Multi Frequency (DTMF)	●	
Comfort Noise Generation (CNG)	●	
Echo Cancellation	●	
4. Voice Line Interface		
FXO	●	RJ11 Interface
FXS	●	RJ11 Interface
E&M	●	RJ45 Interface
5. Others		
ITU-T H.323 Gateway Support	●	
ITU-T H.323 Gatekeeper Support	●	
ITU-T H.235 Security Support	●	

A-2 LAN/WAN Service

Specification	Support (●)	Remark
1. Ethernet Interface		
10BaseT	●	
100BaseTx	●	
Auto Sensing	●	10/100BaseTx (Automatic detection)
2. WAN Service		
PPPoE	●	
Cable Network	●	
ADSL Static IP	●	
ADSL Dynamic IP	●	
3. Port Configuration management	●	
4. Telnet service	●	
5. MTU size change	●	64 ~ 1,500byte
6. ARP Entry Revalidate	●	
7. SW Up/Down Load	●	FTP, TFTP
8. Routing Protocol & related		
Static Routing/Default	●	
RIP v1/v2	●	
OSPF v2	●	
VLAN Routing	●	IEEE802.1Q
NAT/PAT	●	For Dial-Pad, Waw Call
DHCP	●	For Server and Relay
9. Guaranteed Ethernet IP Packet transmission quality	●	
10. Transparent Bridging	●	IEEE Spanning Tree Algorithm
11. IP Access List	●	Standard & Extended
12. IP Secondary Address	●	

A-3 Operation management & other features

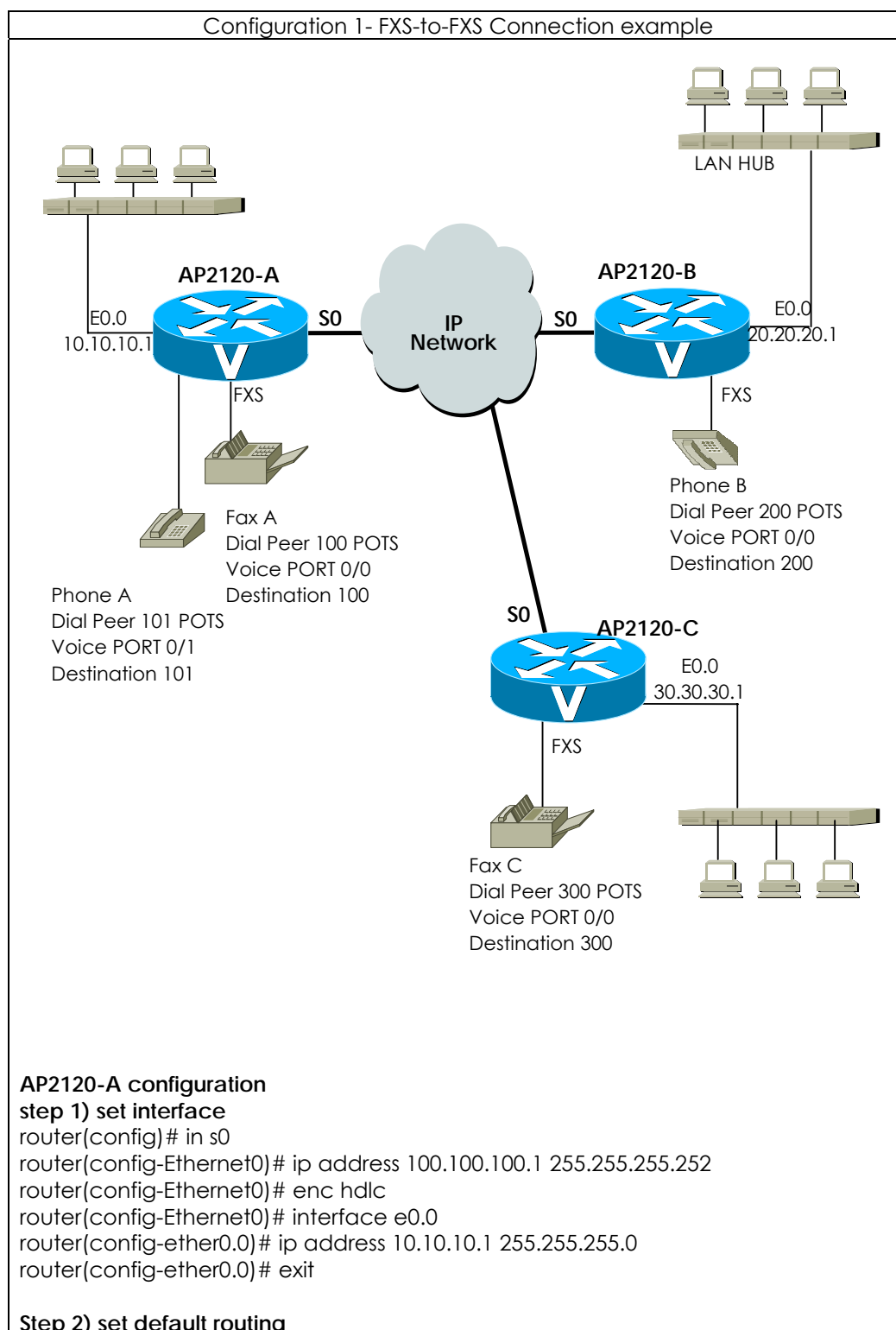
Features	Support (●)	Remark
1. Boot & reboot	●	Cold booting 20 sec, Warm booting 18 sec
2. System Backup & remote loading	●	
3. System LED indication	●	
4. SNMP	●	Support SNMP Agent MIB-II
5. Configuration delete, save	●	
6. Process Check	●	
7. CPU & Line operation rate Check	●	
8. Console port	●	
9. Security (Packet Filtering, Multi-level User Authenticcation)	●	
10. Debugging	●	
11. Traffic statistics	●	
12. ARP Table Management	●	
13. Web Based Management	●	

A-4 AP2120 VoIP Router H/W specification

ITEM	Specification	Remark
1. CPU	32bit RISC Microprocessor	
2. Fixed LAN Port	1-port 10/100Mbps Ethernet	
3. Fixed WAN Port	1-port 10/100Mbps Ethernet	
4. Fixed Console Port	1-port Async. Ethernet (RS-232C)	RJ45 Type
5. Network Module Slot	One(2) Interface Module Slot	
6. Memory		
Flash Memory	4Mbyte	
SDRAM (Main Memory)	32/64Mbyte	
Boot Memory	512Kbyte	
7. VoIP Module A	8-port FXS Interface support Provides Status LEDs	RJ-11 Type
8. VoIP Module B	8-port FXO Interface support Provides Status LEDs	RJ-11 Type
9. VoIP Module C	8-port E&M Interface support Provides Status LEDs	RJ-45 Type
10. VoIP Module D	4-port FXS and 4-port FXO Interface support Provides Status LEDs	RJ-11 Type
11. Dimension (W x D x H)	435mm x 205mm x 43mm	19" Rack Mountable Chassis
12. Power supply	110/220 VAC supported 50/60Hz – 15Watt	
13. Others	Cooling FAN Installed	

VoIP(Voice over IP) Config. Example

This parts explains several examples of VoiceFinder AP2120 Gateway configuration.




```
router(config)# route 0 0 se 0
```

Step 3) set POTS Peer

```
router(config)# dial-peer voice 100 pots
router(config-dialpeer-pots-100)# port 0/0
router(config-dialpeer-pots-100)# destination-pattern 100
router(config-dialpeer-pots-100)# dial-peer voice 101 pots
router(config-dialpeer-pots-101)# port 0/1
router(config-dialpeer-pots-101)# destination-pattern 101
router(config-dialpeer-pots-101)# exit
```

Step 4) set VoIP Peer

```
router(config)# dial-peer voice 200 voip
router(config-dialpeer-voip-200)# destination-pattern 2..
router(config-dialpeer-voip-200)# session target 20.20.20.1
router(config-dialpeer-voip-200)# dial-peer voice 300 voip
router(config-dialpeer-voip-300)# destination-pattern 3..
router(config-dialpeer-voip-300)# session target 30.30.30.1
router(config-dialpeer-voip-300)# exit
```

Step 5) Check the configuration

```
router(config)# show run
interface loopback0
  ip address 127.0.0.1 255.0.0.0
!
interface ether0.0
  ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0
  ip address 100.100.100.1 255.255.255.252
  Encapsulation HDLC
  Operation is DOWN
!
!
```

```
router(config)# sh route
```

Destination	Network-Mask	Gateway	Interface	Protocol
0.0.0.0	0.0.0.0		Ethernet0	STATIC
10.10.10.0	255.255.255.0	10.10.10.1	ether0.0	DIRECT
100.100.100.0	255.255.255.252	100.100.100.1	Ethernet0	DIRECT
127.0.0.0	255.0.0.0	127.0.0.1	loopback0	DIRECT

```
router(config)# show dial-peer voice
POTS Peers :
```

```
Pots peer 100
```

```
  dest-pattern = 100
  port = 0/0 (0)
  prefix =
  register E.164 = yes
  administrative status = up
```

```
Pots peer 101
```

```
  dest-pattern = 101
```

```
port = 0/1 (1)
prefix =
register E.164 = yes
administrative status = up
```

VoIP Peers :

VoIP peer 300

```
dest-pattern = 3..
session-target = 30.30.30.1
codec = default
codecClass = default
dtmfRelay = h245-alphanumeric
vad = yes
translation-outgoing called-number = -1
translation-outgoing calling-number = -1
description =
administrative status = up
```

VoIP peer 200

```
dest-pattern = 2..
session-target = 20.20.20.1
codec = default
codecClass = default
dtmfRelay = h245-alphanumeric
vad = yes
translation-outgoing called-number = -1
translation-outgoing calling-number = -1
description =
administrative status = up
```

AP2120-C configuration

step 1) set interface

```
router(config)# in s0
router(config-Ethernet0)# ip address 100.100.102.1 255.255.255.252
router(config-Ethernet0)# enc hdlc
router(config-Ethernet0)# interface e0.0
router(config-ether0.0)# ip address 30.30.30.1 255.255.255.0
router(config-ether0.0)# exit
```

Step 2) set default routing

```
router(config)# route 0 0 se 0
```

Step 3) set POTS Peer

```
router(config)# dial-peer voice 300 pots
router(config-dialpeer-pots-300)# port 0/0
router(config-dialpeer-pots-300)# destination-pattern 300
router(config-dialpeer-pots-300)# exit
```

Step 4) set VoIP Peer

```
router(config)# dial-peer voice 100 voip
router(config-dialpeer-voip-100)# destination-pattern 1..
router(config-dialpeer-voip-100)# session target 10.10.10.1
router(config-dialpeer-voip-100)# dial-peer voice 300 voip
```

```

router(config-dialpeer-voip-200)# destination-pattern 2..
router(config-dialpeer-voip-200)# session target 20.20.20.1
router(config-dialpeer-voip-200)# exit

```

Step 5) Check the configuration

```

router(config)# show run
interface loopback0
  ip address 127.0.0.1 255.0.0.0
!
interface ether0.0
  ip address 30.30.30.1 255.255.255.0
!
interface Ethernet0
  ip address 100.100.102.1 255.255.255.252
  Encapsulation HDLC
  Operation is DOWN
!
!

```

```

router(config)# sh route

```

Destination	Network-Mask	Gateway	Interface	Protocol
0.0.0.0	0.0.0.0		Ethernet0	STATIC
30.30.30.0	255.255.255.0	30.30.30.1	ether0.0	DIRECT
100.100.102.0	255.255.255.252	100.100.102.1	Ethernet0	DIRECT
127.0.0.0	255.0.0.0	127.0.0.1	loopback0	DIRECT

```

router(config)# show dial-peer voice
POTS Peers :

```

```

Pots peer 300
  dest-pattern = 300
  port = 0/0 (0)
  prefix =
  register E.164 = yes
  administrative status = up

```

VoIP Peers :

```

VoIP peer 200
  dest-pattern = 2..
  session-target = 20.20.20.1
  codec = default
  codecClass = default
  dtmfRelay = h245-alphanumeric
  vad = yes
  translation-outgoing called-number = -1
  translation-outgoing calling-number = -1
  description =
  administrative status = up

```

```

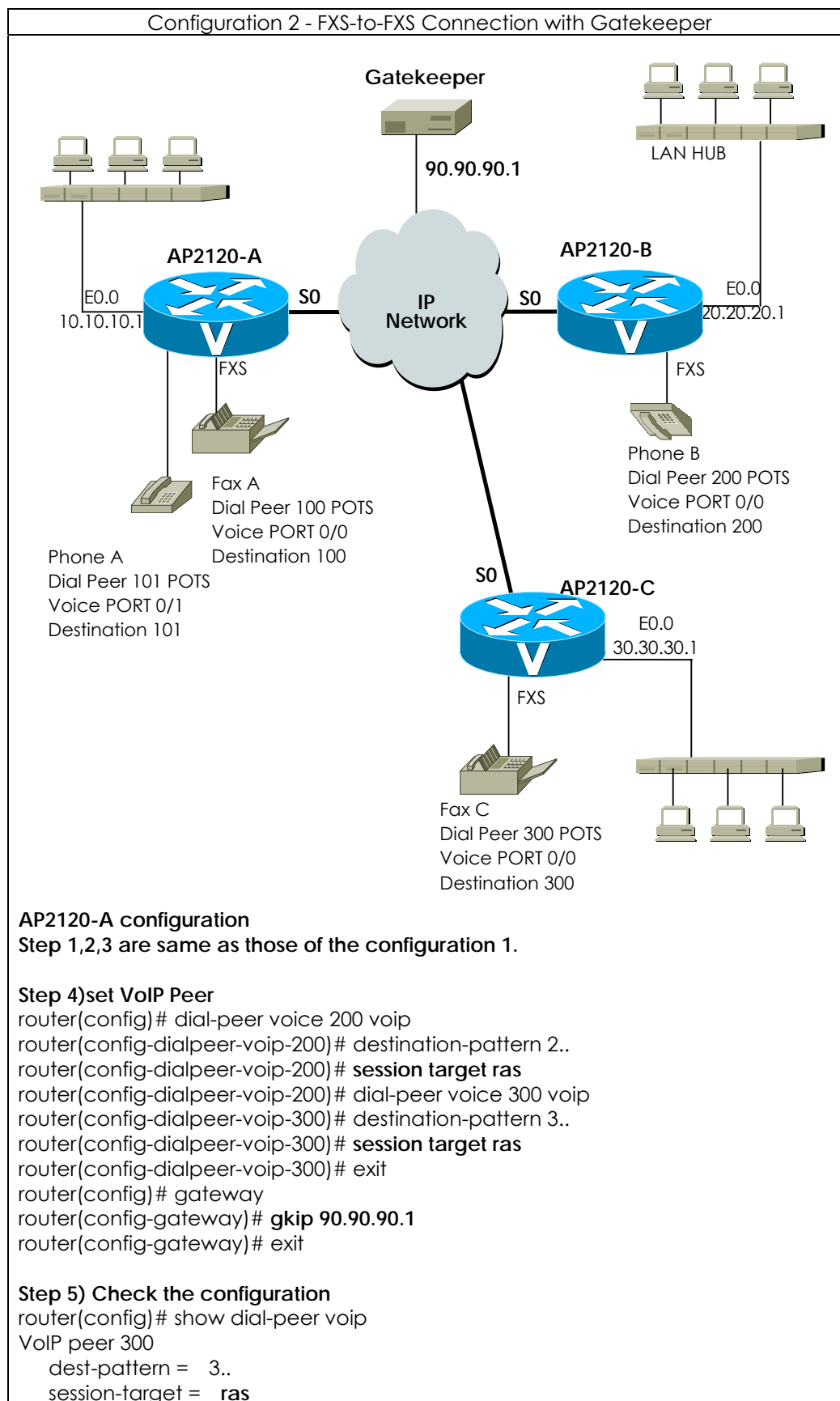
VoIP peer 100
  dest-pattern = 1..
  session-target = 10.10.10.1
  codec = default

```

```
codecClass = default
dtmfRelay = h245-alphanumeric
vad = yes
translation-outgoing called-number = -1
translation-outgoing calling-number = -1
description =
administrative status = up
```

Call Scenario

- 1) Phone A and Phone B connection
 - Phone A user picks up the phone.
 - Dials "200" for Phone B.
 - There is ring on Phone B.
 - Phone B user picks up the phone
 - In conversation
 - Phone A,B users hang up the phone.
- 2) Fax A and FAX C connection
 - Insert the paper to send to FAX C at fax B.
 - Dial "300" for fax C.
 - Confirm transmission and FAX quality



```
codec = default
codecClass = default
dtmfRelay = h245-alphanumeric
vad = yes
translation-outgoing called-number = -1
translation-outgoing calling-number = -1
description =
administrative status = up
```

VoIP peer 200

```
dest-pattern = 2..
session-target = ras
codec = default
codecClass = default
dtmfRelay = h245-alphanumeric
vad = yes
translation-outgoing called-number = -1
translation-outgoing calling-number = -1
description =
administrative status = up
```

router(config)# show gateway

Gatekeeper Registration Information

```
this gateway's H.323 id = voip.10.10.10.1
gatekeeper registration option = yes
gatekeeper registration status :
    not registered.
gatekeeper address = 90.90.90.1
gatekeeper security = disabled
local aliases
    [1] voip.10.10.10.1
    [2] 100
    [3] 101
```

Gateway Information

```
number of ports = 8
number of pots peers = 2
number of voip peers = 2
number of number expansions = 0
number of codec classes = 0
number of user classes = 0
number of current calls = 0
end of digit = #
ip address prefix = *
permit unregistered h323 incoming call to FXO = yes
h323 call start mode = fast
system fax mode = t38
system fax rate = 14400 bps
system T.38 fax redundancy = 0
```

AP2120-B configuration

Step 1,2,3 are same as those of configuration 1

Step 4) set VoIP Peer

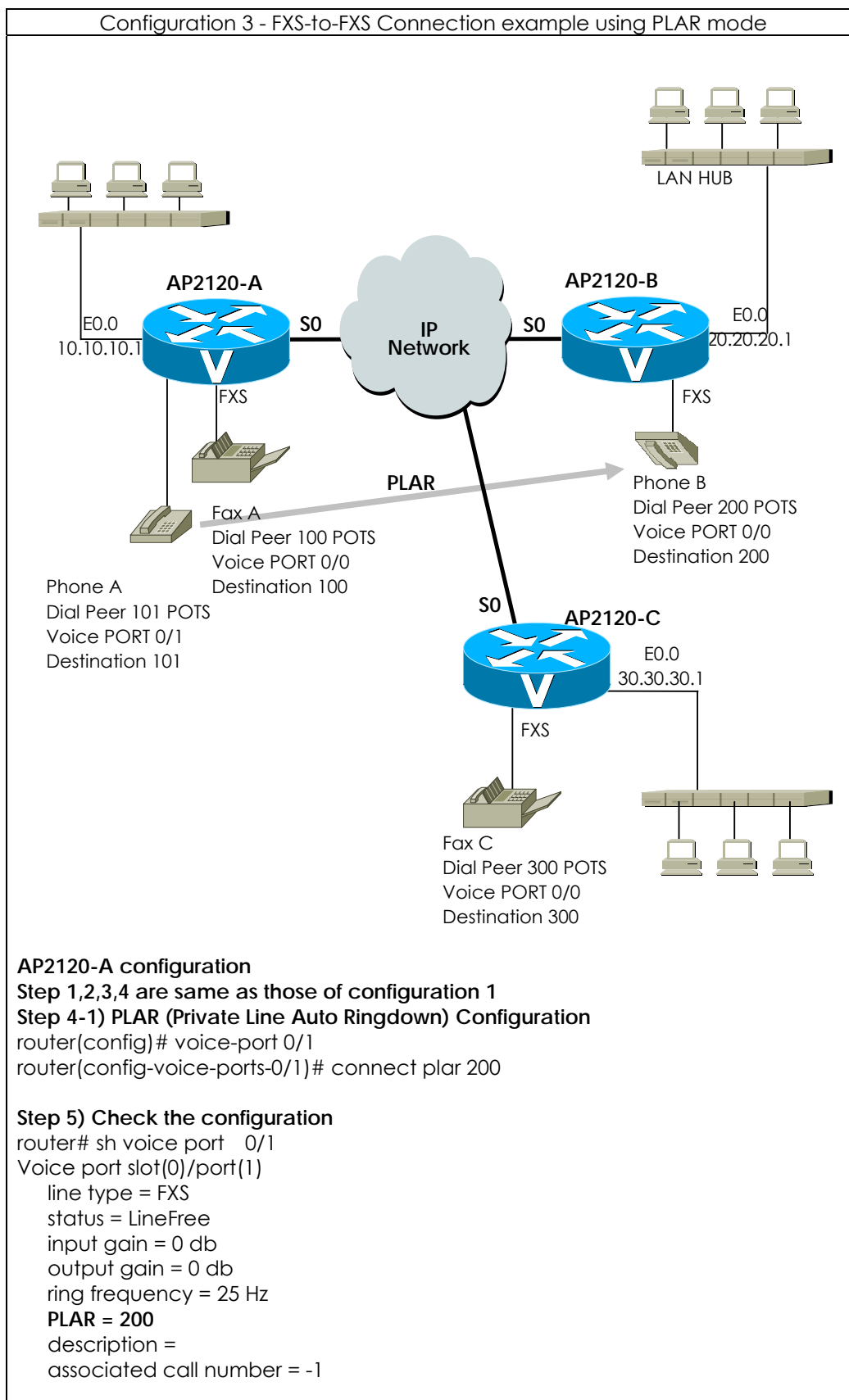
```
router(config)# dial-peer voice 100 voip
router(config-dialpeer-voip-100)# destination-pattern 2..
router(config-dialpeer-voip-100)# session target ras
router(config-dialpeer-voip-200)# dial-peer voice 300 voip
router(config-dialpeer-voip-300)# destination-pattern 3..
router(config-dialpeer-voip-300)# session target ras
router(config-dialpeer-voip-300)# exit
router(config)# gateway
router(config-gateway)# gkip 90.90.90.1
```

AP2120-C configuration

Refer to Router A,B configuration.

Call Scenario

Same as that of configuration 1.



AP2120-B configuration

Same as that of configuration 1

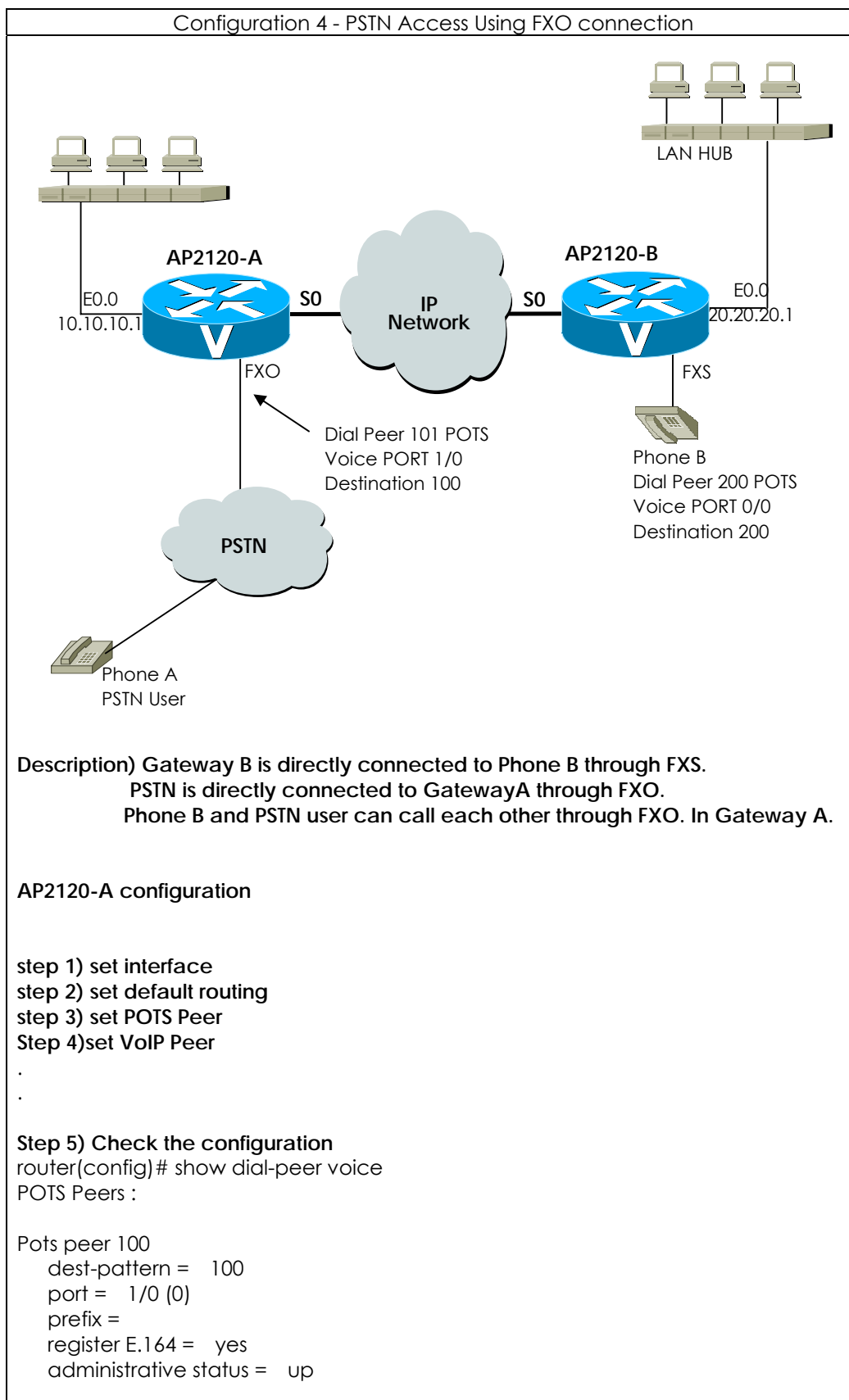
AP2120-C configuration

Same as that of configuration 1

Call Scenario

1) Phone A and Phone B connection

- Phone A user picks up the phone.
- There is ring on Phone B.
- Phone B user picks up the phone
- In conversation
- Phone A,B users hang up the phone.



VoIP Peers :

VoIP peer 200

```
dest-pattern = 2..  
session-target = 20.20.20.1  
codec = default  
codecClass = default  
dtmfRelay = h245-alphanumeric  
vad = yes  
translation-outgoing called-number = -1  
translation-outgoing calling-number = -1  
description =  
administrative status = up
```

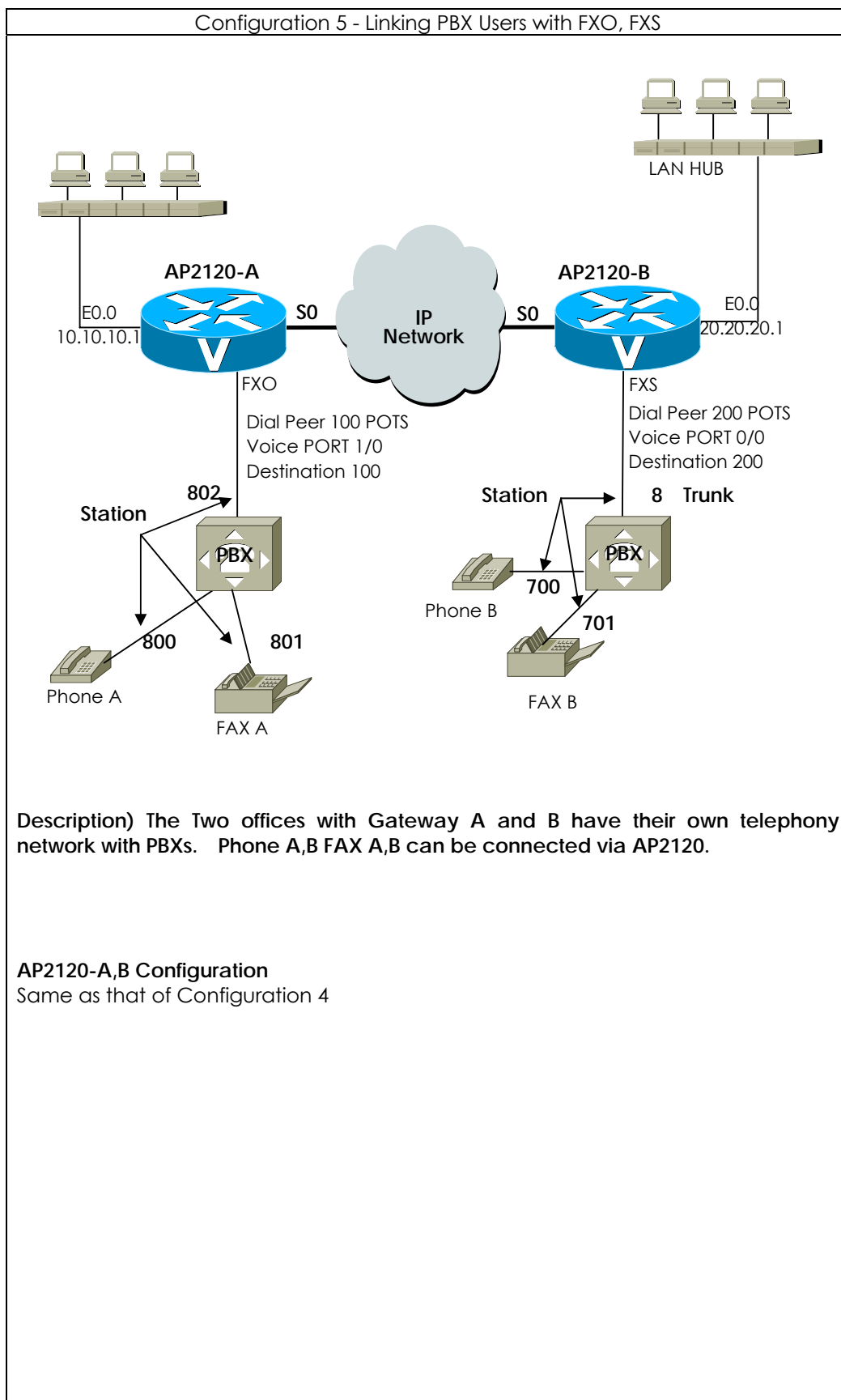
AP2120-B configuration

Same as that of configuration 1

Call Scenario

Call Scenario

- 1) Call Connection from Phone A to Phone B under PSTN
 - Press dial No. 568-3848 in connecting PSTN phone.
 - Listen dial tone, press dial No. 200 of phone B.
 - Confirm RING sound.
 - Pick up phone B.
 - Speak over the telephone.
 - Finish speaking.
- 2) Call Connection from Phone B to PSTN user Phone
 - Pick up Phone B.
 - Press dial No. 100 in connecting VoIP gateway FXO voice port 1/0 under PSTN.
 - Confirm dial tone sound, and press PSTN dial number.
 - Speak over the telephone.
 - Finish speaking.



Call Scenario

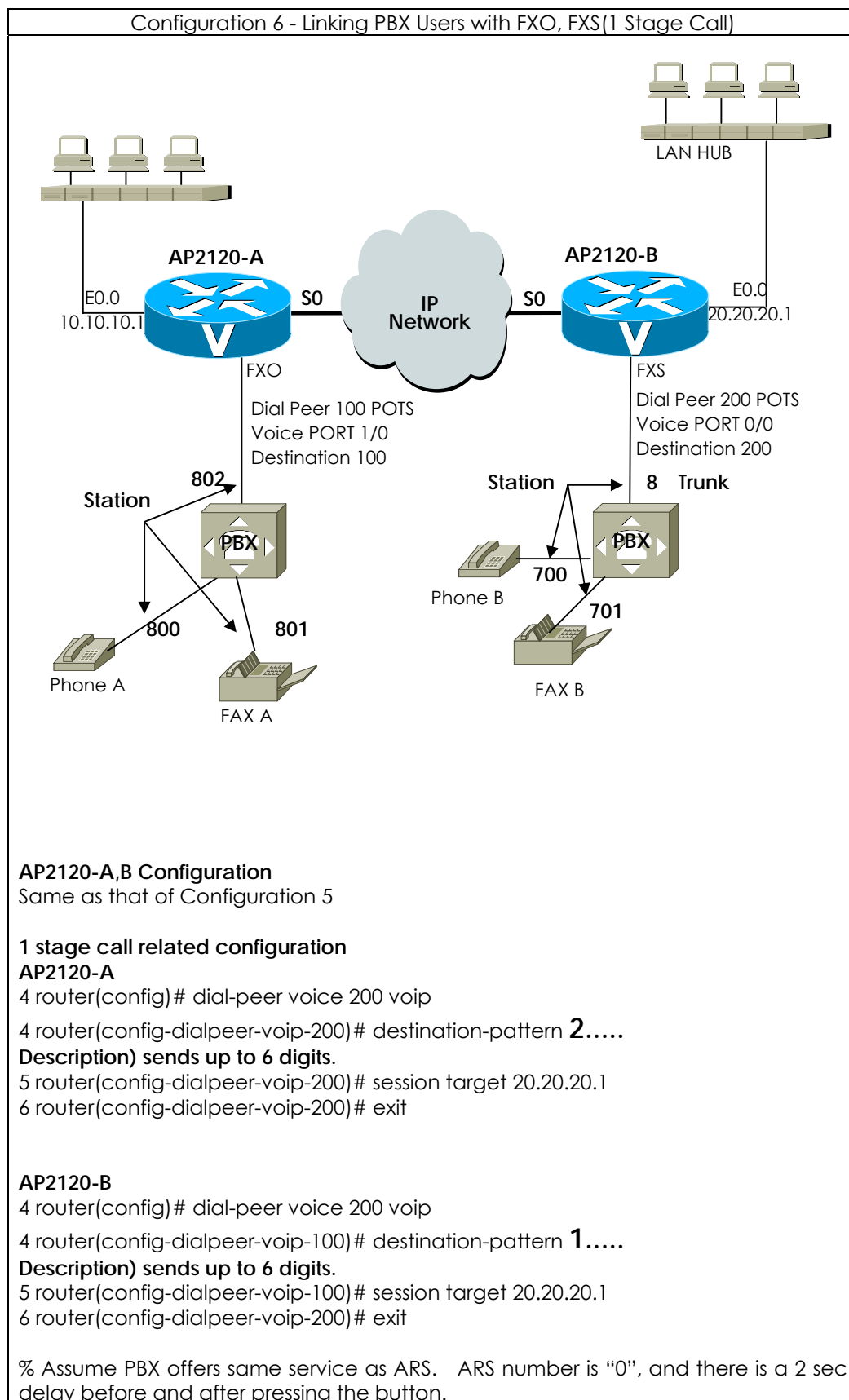
1) Phone A To Phone B connection

- Pick up Phone A.
- Listen dial tone sound of PBX A machine, and then press dial No. 802 in connecting VoIP gateway A.
- Listen dial tone sound of gateway A, and then press dial No. 200 in connecting VoIP gateway FXS voice port.
- Listen dial tone sound of PBX B machine, and then press dial No. 700 (internal Number)
- Pick up Phone B
- Speak over the telephone.
- Finish conversation.

2) Phone B To Phone A connection

- Pick up Phone B.
- Listen dial tone sound of PBX B machine, and then press dial No. 8 in connecting VoIP gateway FXO port.
- Listen dial tone sound of VoIP gateway, and then press dial No. 100 in connecting VoIP gateway A FXO port.
- Listen dial tone sound of PBX A machine, and then press dial No. 800 (internal number)
- Speak over the telephone.
- Finish conversation.

Note : Each call scenario is made up setting of PBX configuration.



Prefix can be added to Voice port configuration

```
router(config-dialpeer-pots-100)# prefix ,,0,,
```

Description) Enter "100200" from Phone B.

Router A uses "100" -> Connected to PBX.

2 sec. delay

router A dials "0" to PBX

2 sec. delay

router A dials "200" to PBX

....

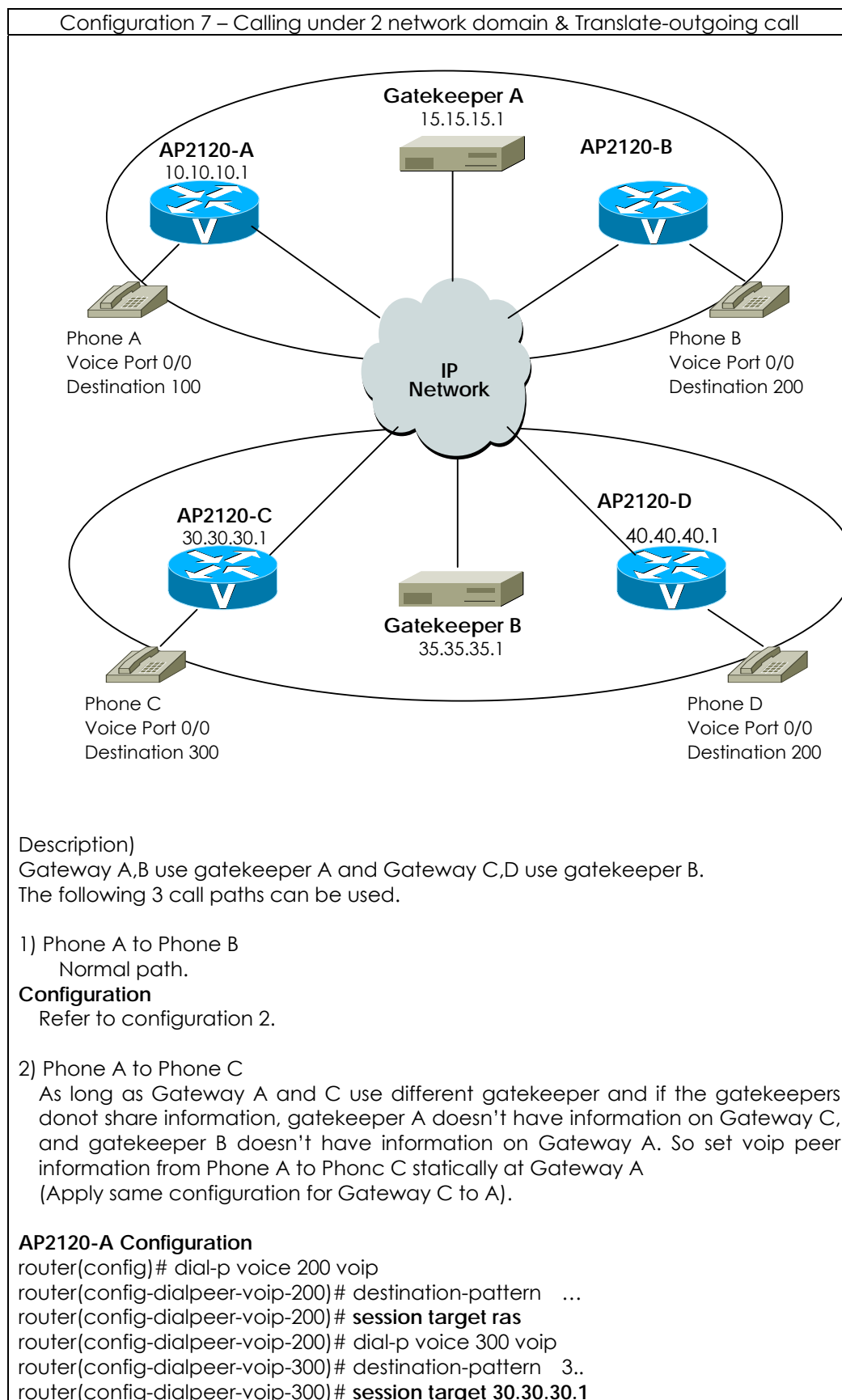
Call Scenario

1) Phone A To Phone B connection

- Pick up Phone A.
- There is dial tone from PBX. Press the number assigned for FXO port of Gateway A "802" (1 stage)
- There is dial tone from Gateway A. Press the number assigned for FXS port of the Gateway B ("200") and the extension number of Phone B ("700"). (2 stage)
- Phone B rings. Pick up Phone B.
- In conversation
- Hang up Phone A,B.

2) Phone B To Phone A connection

- Pick up Phone B.
- There is dial tone from PBX B. Press the number assigned for FXO port fo the Gateway ("8").
- There is dial tone from Gateway B. Press the number assigned for FXO port of the Gateway A ("100") and the extension number of Phone A ("800")
- Phone B rings. Pick up Phone B.
- In conversation
- Hang up Phone A,B.




```
router(config-dialpeer-voip-300)# exit
router(config)# gateway
router(config-gateway)# gkip 15.15.15.1
router(config-gateway)# exit
```

3) Phone A to Phone D

Basically, Configuraiton 2) requires number translation. When making a call from Phone A to Phone D, there is "200" at the local domain. When configuring Gateway A, to distinguish from local domain, set translate-outgoing called-number as "8XX". At this time, when "8xx" is pressed, the called party number field is converted to "2xx" and sends to Gateway B.

AP2120-A Configuration (add)

```
router (config)# translation-rule 1
router (config-trans-rule-0)# rule 0 8.. 2
router (config-trans-rule-0)# exit
router (config)# dial-p voice 800 voip
router (config-dialpeer-voip-800)# destination-pattern 8..
router (config-dialpeer-voip-800)# session target 40.40.40.1
router (config-dialpeer-voip-800)# translate-outgoing called-number 1
```

Call Scenario

1) Making a call from Phone A to Phone B

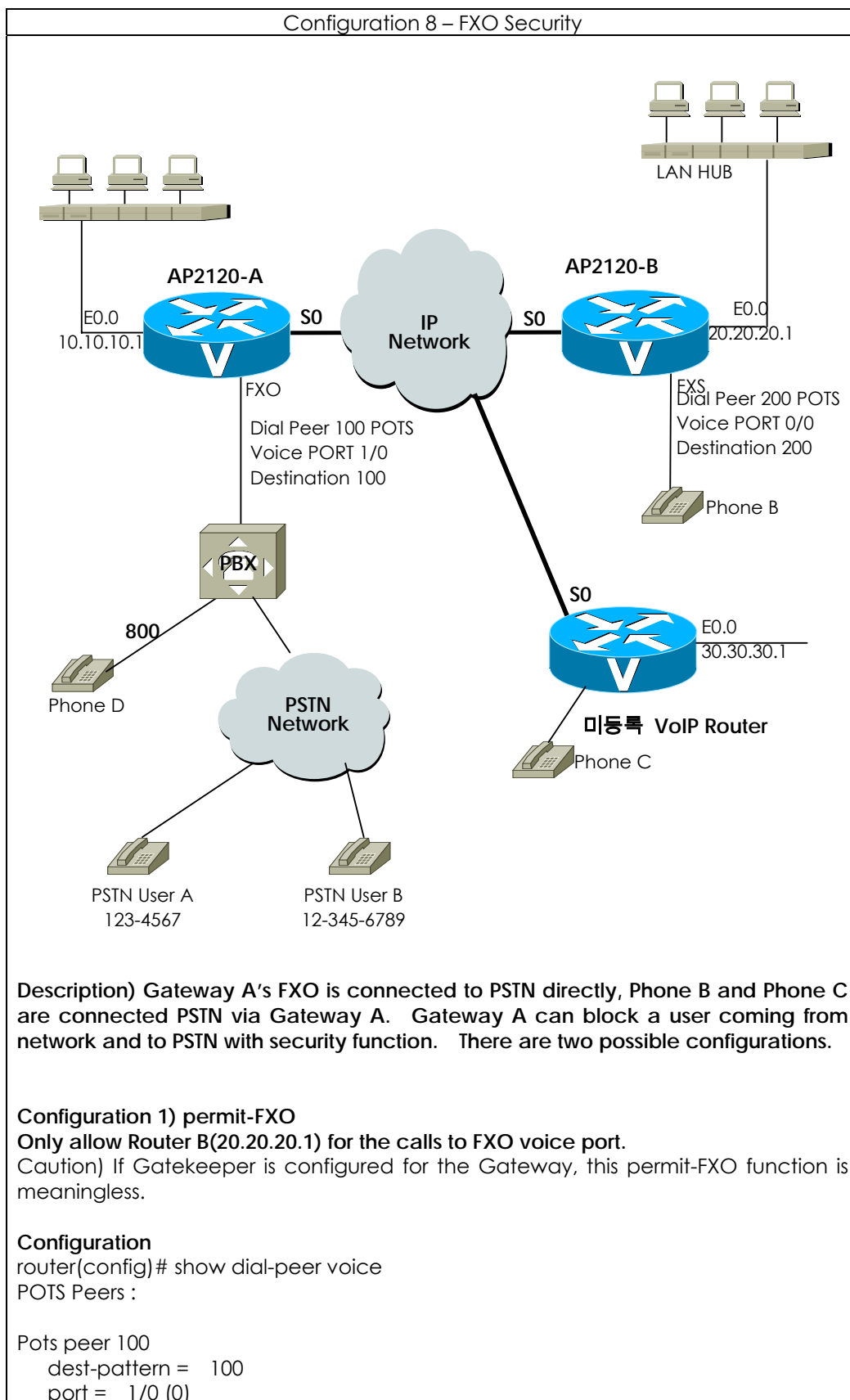
- Pick up Phone A
- Press "200" for Phone B.
- Phone B rings.
- Pick up Phone B.
- In conversation
- Hang up Phone A,B.

2) Making a call from Phone B to Phone C

- Pick up Phone A
- Press "300" for Phone C.
- Phone C rings.
- Pick up Phone C.
- In conversation.
- Hang up Phone A,C.

3) Making a call from Phone B to Phone D

- Pick up Phone A
- Press "800" for Phone D.
- Phone D rings
- Pick up Phone D
- In conversation
- Hang up Phone A,D.



```
prefix =  
register E.164 = yes  
administrative status = up
```

VoIP Peers :

```
VoIP peer 200  
dest-pattern = 2..  
session-target = 20.20.20.1  
codec = default  
codecClass = default  
dtmfRelay = h245-alphanumeric  
vad = yes  
translation-outgoing called-number = -1  
translation-outgoing calling-number = -1  
description =  
administrative status = up
```

```
router(config)# voice service voip  
router(config-vservice-voip)# no security permit-FXO  
% default Value: permit-FXO
```

call scenario)

- 1) call Phone B to Phone D
 - Pick up Phone A
 - Press the extension number of Phone B (FXO, "100").
 - Press the extension number of Phone D ("800").
 - In conversation
 - Hang up Phone B.
- 2) call Phone C to Phone D
 - Pick up Phone C
 - Press the FXO number of Phone C ("100").
 - There is no dial tone from Phone C
 - Hang up Phone B.

Configuration 2) User Class Configuration.

Check password for the calls coming from Network to the FXO voice port of Gateway A.

Configuration)

Configuration

```
router(config)# show dial-peer voice  
POTS Peers :
```

```
Pots peer 100  
dest-pattern = 100  
port = 1/0 (0)  
prefix =  
register E.164 = yes  
administrative status = up
```

VoIP Peers :

```
VoIP peer 200
```

```

dest-pattern = 2..
session-target = 20.20.20.1
codec = default
codecClass = default
dtmfRelay = h245-alphanumeric
vad = yes
translation-outgoing called-number = -1
translation-outgoing calling-number = -1
description =
administrative status = up

```

VoIP peer 300

```

dest-pattern = 3..
session-target = 30.30.30.1
codec = default
codecClass = default
dtmfRelay = h245-alphanumeric
vad = yes
translation-outgoing called-number = -1
translation-outgoing calling-number = -1
description =
administrative status = up

```

```

router(config)# voice class user 1
router(config-vclass-user#1)# password 1234
router(config-vclass-user#1)# max-digits 3
router(config-vclass-user#1)# exit
router(config)# voice class user 2
router(config-vclass-user#2)# password 4567
router(config-vclass-user#2)# max-digits 8
router(config-vclass-user#2)# exit
router(config)# voice class user 3
router(config-vclass-user#2)# password 7890
router(config-vclass-user#2)# max-digits 0
router(config-vclass-user#2)# exit

```

Description) For the users with the password "1234", only allow 3 digits for key. For the users with the password "3456", only allow 8 digits for key. For the users with the password "7890", there is no limit.

call scenario)

1) Phone B to PSTN user A using user class 1

- Pick up Phone B
- Press FXO number of Phone B ("100").
- There is signal form Phone B. Enter the password of user class 1 ("1234").
- There is dial tone from Phone B. Press the extension number ("800"). (3 digit)
- In conversation
- Hang up Phone B.

2) Phone B to PSTN user A using user class 1

- Pick up Phone B.
- Press FXO number of Phone B ("100").
- There is signal from Phone B. Enter the password for user class 1 ("1234").
- There is a dial tone from Phone B. Enter "9" to connect outside PSTN. (1

digit)

- Enter the PSTN number of user A ("1234567").

(7 digit)

Description) With the password "1234", only 3 digits are allowed. So only the number "9" and "12" are processed. So the call cannot be established.

- Hang up Phone B.

3) Phone B to PSTN user A using user class 2

- Pick up Phone B.
- Press the FXO number of Phone B ("100").
- There is signal from Phone B. Enter the password of user class 2 "4567"
- There is a dial tone from Phone B. Enter "9" to connect outside PSTN. (1 digit)
- Enter the PSTN number of user A ("1234567").

(7 digit)

Description) With the password "3456", only 8 digits are allowed. So the number "9" and "1234567" are processed. So the call can be established.

- In conversation
- Hang up Phone B.

4) Phone B to PSTN user B using user class 3

- Pick up Phone B.
- Press the FXO number of Phone B ("100").
There is signal from Phone B. Enter the password of user class 3 "7890"
- There is a dial tone from Phone B. Enter "9" to connect outside PSTN. (1 digit)
Enter the PSTN number of user A ("123456789").

Description) With the password "7890", there is no limit.

- In conversation.
- Hang up Phone B.

Appendix C AP1100 Call Finishing Cause Code

The following table shows description for call finishing cause code and mapping information for Q.931 cause or H.225 cause.

The Call Finish Cause Codes can be displayed with call tracing or **show call history all**.

AP1100 Call Finishing Cause Code	Call Finishing Master	Reason of Call Finishing	Defined Code
RemoteNoBandwidth	remote side	RELCOM* receiving cause noBandwidth(H225) NoCircuitChannelAvailable (Q931:34)	RELCOM transmission cause H225 destinationRejection
RemoteGatekeeperResourceUnavailable	remote side	RELCOM receiving cause gatekeeperResources(H225) ResourceUnavailable (Q931:47)	RELCOM transmission cause H225 destinationRejection
RemoteUnreachableDestination	remote side	RELCOM receiving cause unreachableDestination (H225) NoRouteToDestination (Q931: 3)	RELCOM transmission cause H225 destinationRejection
RemoteCallClear	remote side	RELCOM receiving cause destinationRejection (H225) NormalCallClearing (Q931: 16)	RELCOM transmission cause H225 destinationRejection
RemoteIncompatibleDestination	remote side	RELCOM receiving cause invalidRevision (H225) IncompatibleDestination (Q931: 88)	RELCOM transmission cause H225 destinationRejection
RemoteNoPermission	remote side	RELCOM receiving cause noPermission (H225) InterworkingUnspecified (Q931: 127)	RELCOM transmission cause H225 destinationRejection
RemoteUnreachableGatekeeper	remote side	RELCOM receiving cause unreachableGatekeeper (H225) NetworkOutOfOrder (Q931: 38)	RELCOM transmission cause H225 destinationRejection
RemoteResourceUnavailable	remote side	RELCOM receiving cause gatewayResources (H225) SwitchingEquipmentCongestion (Q931: 42)	RELCOM transmission cause H225 destinationRejection
RemoteInvalidNumber	remote side	RELCOM receiving cause badFormatAddress (H225) InvalidNumberFormat (Q931: 28)	RELCOM transmission cause H225 destinationRejection
RemoteAdaptiveBusy	remote side	RELCOM receiving cause adaptiveBusy (H225) TemporaryFailure (Q931: 41)	RELCOM transmission cause H225 destinationRejection
RemoteUserBusy	remote side	RELCOM receiving cause inConf (H225) UserBusy (Q931: 17)	RELCOM transmission cause H225 destinationRejection
RemoteUnknown	remote side	RELCOM receiving cause	RELCOM transmission cause

		undefinedReason (H225) NormalUnspecified (Q931: 31) or unspecified reason from remote side	H225 destinationRejection
RemoteCallDeflection	remote side	RELCOM receiving cause facilityCallDeflection (H225)	RELCOM transmission cause H225 destinationRejection
RemoteSecurityDenial	remote side	RELCOM receiving cause securityDenied (H225)	RELCOM transmission cause H225 destinationRejection
RemoteCalledPartyNotRegistered	remote side	RELCOM receiving cause calledPartyNotRegistered (H225) SubscriberAbsent (Q931: 20)	RELCOM transmission cause H225 destinationRejection
RemoteCallerNotRegistered	remote side	RELCOM receiving cause callerNotRegistered (H225)	RELCOM transmission cause H225 destinationRejection
GkCalledPartyNotRegistered	gatekeeper	Gatekeeper ARJ ** cause calledPartyNotRegistered	RELCOM transmission cause H225 alledPartyNotRegistered
GkInvalidPermission	gatekeeper	Gatekeeper ARJ cause invalidPermission	RELCOM transmission cause H225 noPermission
GkRequestDenied	gatekeeper	Gatekeeper ARJ cause requestDenied	RELCOM transmission cause H225 noPermission
GkUndefinedReason	gatekeeper	Gatekeeper ARJ cause undefinedReason	RELCOM transmission cause H225 undefinedReason
GkCallerNotRegistered	gatekeeper	Gatekeeper ARJ cause callerNotRegistered	RELCOM transmission cause H225 callerNotRegistered
GkRouteCallToGatekeeper	gatekeeper	Gatekeeper ARJ cause routeCallToGatekeeper	RELCOM transmission cause H225 unreachableGatekeeper
GkInvalidEndpointIdentifier	gatekeeper	Gatekeeper ARJ cause invalidEndpointIdentifier	RELCOM transmission cause H225 undefinedReason
GkResourceUnavailable	gatekeeper	Gatekeeper ARJ cause resourceUnavailable	RELCOM transmission cause H225 gatekeeperResources
GkSecurityDenial	gatekeeper	Gatekeeper ARJ cause securityDenial	RELCOM transmission cause H225 securityDenied
GkQosControlNotSupported	gatekeeper	Gatekeeper ARJ cause qosControlNotSupported	RELCOM transmission cause H225 gatekeeperResources
GkIncompleteAddress	gatekeeper	Gatekeeper ARJ cause incompleteAddress	RELCOM transmission cause H225 badFormatAddress
GkAliasesInconsistent	gatekeeper	Gatekeeper ARJ cause aliasesInconsistent	RELCOM transmission cause H225 undefinedReason
GkDisengageRequested	gatekeeper	Gatekeeper DRQ	RELCOM transmission cause H225 undefinedReason
LocalCallClear	local side	Hang on in normal local voice port	RELCOM transmission cause H225 destinationRejection
LocalResourceUnavailable	local side	Required local resources (exceed Max. opening call processing)	RELCOM transmission cause H225 gatewayResources
LocalPortBusy	local side	busy condition on local voice port	RELCOM transmission cause H225 inConf
LocalPortNoConnect	local side	No response voice port (ringing timer expired)	RELCOM transmission cause H225 destinationRejection

LocalPortShutdowned	local side	shutdown condition on local voice port	RELCOM transmission cause H225 unreachableDestination
LocalPeerShutdowned	local side	shutdown condition on local dial peer	RELCOM transmission cause H225 unreachableDestination
LocalInterdigitTimerExpired	local side	Local inter-digit timer expired	N/A
LocalSecurityDenial	local side	Call finishing by local security	RELCOM transmission cause H225 securityDenial
LocalInvalidGatekeeperRoute	local side	Local gateway decide abnormal condition on transport address from receiving gatekeeper.	RELCOM transmission cause H225 unreachableGatekeeper
LocalUnreachableGatekeeper	local side	Local gateway could not operate call processing due to registration failure in gatekeeper.	RELCOM transmission cause H225 unreachableGatekeeper
LocalUnreachableDestination	local side	Local gateway connecting failure on other side gateway	N/A
LocalNoAnswerFromDestination	local side	Local gateway receiving message failure from other side gateway(T303 Expired)	N/A
LocalNoConnectFromDestination	local side	Local gateway CONNECT message receiving message failure from other side gateway (T301 Expired)	RELCOM transmission cause H225 destinationRejection
LocalUnknown	local side	Local unknown reason	RELCOM transmission cause H225 undefinedReason
LocalProtocolError	local side	Message & protocol error on local side	RELCOM transmission cause H225 undefinedReason
LocalInvalidNumber	local side	Invalid number on local side	RELCOM transmission cause H225 badFormatAddress
LocalT38FaxError	local side	T.38 fax error on local side	RELCOM transmission cause H225 undefinedReason
LocalManagement	local side	Call finishing by management on local side	RELCOM transmission cause H225 undefinedReason
LocalUnavailableDestination	local side	Call finishing by destination invalid on local side (Ex. Call for FXO – FXO, Call for H323 – H323)	RELCOM transmission cause H225 undefinedReason
LocalAbortedDestination	local side	Local gateway aborting call connection to other side gateway	N/A
LocalCapabilityNegotiationFail	local side	Local gateway capability negotiation failure to other side gateway	RELCOM transmission cause H225 undefinedReason

*RELCOM : Q.931 Release Complete message

**ARJ : H.225 Admission Reject message

For your reference, the following table shows recommendation of ITU-T for H.225 cause and Q.931 cause mapping for H.323.

H225 Cause	Q931 Cause
noBandwidth	NoCircuitChannelAvailable (34)
gatekeeperResources	ResourceUnavailable (47)
unreachableDestination	NoRouteToDestination (3)
destinationRejection	NormalCallClearing (16)
invalidRevision	IncompatibleDestination (88)
noPermission	InterworkingUnspecified (127)
unreachableGatekeeper	NetworkOutOfOrder (38)
gatewayResources	SwitchingEquipmentCongestion (42)
badFormatAddress	InvalidNumberFormat (28)
adaptiveBusy	TemporaryFailure (41)
inConf	UserBusy (17)
undefinedReason	NormalUnspecified (31)
facilityCallDeflection	NormalCallClearing (16)
securityDenied	NormalUnspecified (31)
calledPartyNotRegistered	SubscriberAbsent (20)
callerNotRegistered	NormalUnspecified (31)

Appendix D Cable Specifications

This Appendix provides information about the Pinout specifications of the following cables used with the VoiceFinder 2120 Gateway.

- Console Port Signal and Pinout(RJ-45 to DB9)
- Ethernet Cable Assemble(RJ-45 to RJ-45) Pinout
- Async. Ethernet Cable Assemble(V.35 to V.35)의 Pinout

[Console Port Signal & Pinout]

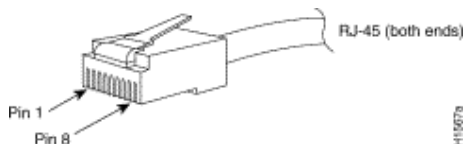
In order to connect the Gateway console port with the Terminal Emulating PC, the RJ-45 to DB9(Female DTE Connector) cable is used. The transferred signal and Pinout specifications are enlisted in the following Table C-1 "Console Port Signal and Pinout".

Router Console (DTE)	RJ-45	DB-9	Console Device (PC)
Signal	RJ-45 Pin	DB-9 Pin	Signal
RTS	1	8	CTS
DTR	2	6	DSR
TxD	3	2	RxD
GND	4	5	GND
GND	5	5	GND
RxD	6	3	TxD
DSR	7	4	DTR
CTS	8	7	RTS

Table D-1 Console port Signal and Pinout

[Ethernet Cable Assemble(RJ-45 to RJ-45) Pinout]

In order to connect the Gateway with other equipments (i.e. HUB), the RJ-45 to RJ-45 Ethernet Cable is used. The RJ-45 Connector Pin sequence is provided in Diagram C-1 and the transferred signal and Pinout specifications are enlisted in Table C-2 "Serial Ethernet Cable Signal and Pinout".



[Diagram D-1 10Base-T RJ-45 Connector]

RJ-45	Signal	Direction	RJ-45 Pin
1	Tx +	→	1
2	Tx -	→	2
3	Rx +	←	3
4	-	-	4
5	-	-	5
6	Rx -	←	6
7	-	-	7
8	-	-	8

1. These specifications are for serial cables connecting the Gateway and the HUB.
2. For Gateway to Gateway or Gateway to PC connection, the Cross Cable must be used.

[Table D-2 Serial Ethernet Cable Signal and Pinout]