

PassFinder

AP2520 VoIP

Router/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]

Getting into the PassFinder AP2520 User's Manual

Chapter 1	PassFinder AP2520 Overview	13
1.1.	Introduction to the AP2520.....	13
1.2.	Main Features.....	15
1.3.	External View.....	19
Chapter 2	Before Installation	21
2.1.	Unpacking.....	21
2.2.	Installation Requirements.....	23
2.2.1.	Electrical Requirements.....	23
2.2.2.	General Requirements	24
2.2.3.	Prerequisites for Network Connection.....	25
2.2.3.1.	Synchronous Serial Cable.....	25
2.2.3.2.	Ethernet Port	27
2.2.3.3.	RS-232C Serial Console Port	27
Chapter 3	Installation and Operating Environment	28
3.1.	Installation	29
3.1.1.	Installation Procedure.....	29
3.1.2.	Console Connection.....	30
3.1.3.	Plug-In Power	33
3.2.	Environment Configuration	35
3.2.1.	User and Gateway Management Environment.....	36
3.2.2.	Interface Configuration Environment	37
3.2.3.	Routing Configuration Environment	37
3.2.4.	Security and Internet Configuration Environment.....	38
3.2.5.	System Status and Debugging Environment.....	38
3.2.6.	Voice Integration Configuration Environment.....	38
Chapter 4	Gateway Configuration and Commands	39
4.1.	Gateway Booting.....	39
4.2.	Command Usage	42
4.2.1.	Commands of the User Mode	45
4.2.2.	Commands of the Manager Mode	46

4.2.3.	Commands of the Configuration Mode.....	48
4.2.3.1.	Global Configuration(config) Commands.....	48
4.2.3.2.	Commands of the Interface Configuration Mode 1	50
4.2.3.3.	Commands of the Interface Configuration Mode 2 (IP Configuration Mode)	51
4.3.	Starting Gateway Configuration.....	52
4.4.	Ethernet Configuration	53
4.4.1.	Ethernet basic configuration	53
4.4.2.	PPPoE Configuration	57
4.5.	WAN (Serial) Interface Configuration	66
4.5.1.	HDLC Configuration	67
4.5.2.	PPP Configuration	70
4.5.3.	Frame-Relay Configuration.....	79
4.6.	Routing Configuration	88
4.6.1.	Static Routing Configuration	89
4.6.2.	RIP Configuration.....	92
4.6.3.	OSPF Configuration	98
4.7.	Filter (Access-List) Configuration.....	106
4.8.	NAT(Network Address Translation) Configuration.....	113
4.9.	DHCP(Dynamic Host Configuration Protocol) Configuration	123
4.10.	Transparent Bridging Configuration	131
4.11.	SNMP Configuration.....	136
4.12.	Gateway Management Command.....	141
4.12.1.	Command in the EXEC Mode	141
4.12.2.	Command in the Global Configuration Mode	145
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	155
4.14.1.	User Registration and Change	155
4.14.2.	Password Recovery	157
4.14.3.	Software Image Upgrade and Backup	160
4.14.4.	Configuration File의 Backup 및 Restore	163
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)	166

5.1.2.1.	Codecs.....	166
5.1.2.2.	Mean Opinion Score	167
5.1.3.	Dial Peer.....	169
5.1.4.	Voice Ports.....	171
5.2.	VoIP Interface Configuration	172
5.3.	Numbering Plan, Number Handling and Dial Peer Configuration.....	173
5.3.1.	Numbering Plan	173
5.3.2.	Dial Peer Configuration	174
5.3.2.1.	Inbound Dial Peer versus Outbound Dial Peer	174
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.....	188
5.3.4.3.	Call barring	189
5.3.5.	Prefix and Forwarding Telephone Numbers.....	191
5.3.6.	Configuration Number Expansion.....	192
5.3.6.1.	Number Expansion Table.....	192
5.3.6.2.	Configuration Number Expansion.....	193
5.3.7.	Configuration Number Translation.....	194
5.3.7.1.	Creating Translation Rules	194
5.3.7.2.	Applying Translation Rules to the Inbound POTS Calls.....	196
5.3.7.3.	Applying Translation Rules to the Inbound VoIP Calls.....	197
5.3.7.4.	Applying Translation Rules to the Outbound Calls.....	197
5.4.	Configuration Voice Ports	198
5.4.1.	Configuration Voice Ports on the AP2520 Gateway	198
5.4.2.	Voice Ports Configuration Task List and Steps.....	198
5.4.2.1.	Configuring FXS or FXO Voice Ports	198
5.4.2.2.	Configuring E&M Voice Ports.....	199
5.4.2.3.	Fine-Tuning E&M Voice Ports.....	203
5.4.2.4.	Activating/Deactivating the Voice Ports	205
5.5.	Configuring FAX Application.....	206
5.5.1.	T.38 FAX Relay using VoIP H.323	206
5.5.2.	Configuring T.38 FAX Relay for VoIP H.323.....	208
5.5.3.	FAX Relay setting by Bypass.....	209
5.6.	Other VoIP Configuration	210
5.6.1.	Setting H.323 Gateway.....	210

5.6.2.	Configuring H323 Call Start Mode	212
5.6.3.	Configuring User Class	213
5.7.	VoIP Configuration Command	215
5.7.1.	VoIP-Related whole Command.....	215
5.7.2.	Global Configuration Command	221
5.7.2.1.	dial-peer hunt.....	221
5.7.2.2.	dial-peer ipaddr-prefix.....	223
5.7.2.3.	dial-peer terminator	224
5.7.2.4.	dial-peer voice.....	226
5.7.2.5.	gateway.....	227
5.7.2.6.	num-exp	228
5.7.2.7.	translation-rule.....	231
5.7.2.8.	voice-port	232
5.7.2.9.	voice class clear-down-tone	233
5.7.2.10.	voice class codec	235
5.7.2.11.	voice class user	236
5.7.2.12.	voice service	238
5.7.2.13.	VoIP-interface	239
5.7.3.	Voice Port Configuration Command.....	242
5.7.3.1.	comfort-noise	242
5.7.3.2.	connection	243
5.7.3.3.	description (voice port)	244
5.7.3.4.	echo-cancel	245
5.7.3.5.	input gain.....	246
5.7.3.6.	Operation (E&M Voice Port Command)	248
5.7.3.7.	output gain.....	249
5.7.3.8.	polarity-inverse	250
5.7.3.9.	ring number	251
5.7.3.10.	shutdown (voice-port)	253
5.7.3.11.	signal (E&M Voice Port Command)	254
5.7.3.12.	timing delay-duration (E&M Voice Port Command)	255
5.7.3.13.	timing delay-start (E&M Voice Port Command)	256
5.7.3.14.	timing dialout-delay (E&M Voice Port Command)	257
5.7.3.15.	timing wait-wink (E&M Voice Port Command)	258
5.7.3.16.	timing wink-duration (E&M Voice Port Command)	259
5.7.3.17.	timing wink-wait (E&M Voice Port Command)	260
5.7.3.18.	Usage Guideline	260
5.7.3.19.	translate-incoming	261
5.7.3.20.	type (E&M Voice Port Command).....	262

5.7.4.	Dial Peer Commands.....	264
5.7.4.1.	answer-address.....	264
5.7.4.2.	codec.....	265
5.7.4.3.	description (dial-peer)	266
5.7.4.4.	destination-pattern	267
5.7.4.5.	dtmf-relay	270
5.7.4.6.	forward-digits	271
5.7.4.7.	huntstop	273
5.7.4.8.	port.....	274
5.7.4.9.	preference.....	275
5.7.4.10.	prefix	276
5.7.4.11.	register	277
5.7.4.12.	session target.....	279
5.7.4.13.	shutdown (Dial-Peer).....	280
5.7.4.14.	sid	281
5.7.4.15.	translate-outgoing.....	282
5.7.4.16.	vad.....	283
5.7.4.17.	voice-class codec	284
5.7.5.	Gateway, Voice Service, Voice Class and Rule Configuration Command....	286
5.7.5.1.	announcement.....	286
5.7.5.2.	codec preference	287
5.7.5.3.	counter.....	288
5.7.5.4.	discovery.....	289
5.7.5.5.	fax protocol	290
5.7.5.6.	fax rate	291
5.7.5.7.	h323 call start	293
5.7.5.8.	gkip	294
5.7.5.9.	h323-id.....	295
5.7.5.10.	lightweight-irr	296
5.7.5.11.	h323 call channel	298
5.7.5.12.	h323 call response	299
5.7.5.13.	max-digits.....	300
5.7.5.14.	password	301
5.7.5.15.	public-ip	302
5.7.5.16.	register	303
5.7.5.17.	rule	304
5.7.5.18.	security password	307
5.7.5.19.	security permit-FXO	308
5.7.5.20.	timeout	309

5.7.5.21.	translate-VoIP-incoming	310
5.7.6.	Miscellaneous Commands	313
5.7.6.1.	clear h323 call	313
5.7.6.2.	clear voice port	314
5.7.6.3.	show call active	314
5.7.6.4.	show call history	315
5.7.6.5.	show clear-down-tone	316
5.7.6.6.	show codec class	317
5.7.6.7.	show dial-peer	318
5.7.6.8.	show dialplan number	319
5.7.6.9.	show dialplan port	320
5.7.6.10.	show gateway	321
5.7.6.11.	show num-exp	322
5.7.6.12.	show translation-rule	322
5.7.6.13.	show user-class	323
5.7.6.14.	show voice port	324
5.7.6.15.	show VoIP-interface	325
5.7.6.16.	debug VoIP call	326
5.7.6.17.	debug VoIP	327
5.8.	Digital E1/T1 (ISDN PRI/R2) Installation	329
5.8.1.	General setting and installation	329
5.8.2.	PBX side configuration setting	329
5.8.3.	E1/T1 Interface Cable between PBX and APVI-1E1 Module	329
5.8.4.	Voice Port Configuration of APVI-1E1 Interface Module (Optional)	330
5.8.5.	Controller Configuration of APVI-1E1 Interface Module	331
5.8.6.	POTS peer setting of APVI-1E1 Interface Module (mandatory)	332
5.8.7.	VoIP Outgoing Call Scenario	333
5.8.8.	VoIP Incoming Call Scenario	333
5.8.9.	E1 Configuration Example	334
5.8.10.	E1 Interface Debugging	334
Appendix A. AP2520 VoIP Specifications		336
Appendix B. VoIP(Voice over IP) Config. Example		340
Appendix C AP2520 Call Finishing Cause Code		362
Appendix D Cable Specifications		366

Getting into the PassFinder AP2520 User's Manual

This chapter provides the overview of the PassFinder AP2520 Gateway user's manual and an explanation of the symbols and legends involved.

[Composition of the Manual]

The PassFinder AP2520 user's manual serves to assist the operation of the AP2520 Gateway. This manual is composed of 5 chapters and 4 Appendixes as the following :

Those experienced with Gateways may refer directly to the chapters as needed. But those less experienced are highly recommended to thoroughly understand the manual before operation of the Gateway.

- Chapter 1 『 **PassFinder AP2520 Overview** 』 provides an introduction to the hardware and software features of PassFinder AP2520 and technical support request method.
- Chapter 2 『 **Before Installation** 』 provides the installation environment and cable requirements, along with recommendations for safe operation of the equipment.
- Chapter 3 『 **Installation and Operation Environment** 』 explains the basics for connecting with LAN, WAN and Console Port
- Chapter 4 『 **Gateway Configuration and Commands** 』 explains in detail about configuring the User Interface and the corresponding commands along with configuration examples. This chapter provides important information and requires 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 『 **PassFinder AP2520 Specifications** 』 provides detail specifications for the PassFinder AP2520 Gateway.

- Appendix B 『 **Example of Gateway Port Configuration** 』 provides examples of basic PassFinder AP2520 Gateway configurations.
- Appendix C 『 **Example of VoIP Configuration** 』 provides examples of basic PassFinder AP2520 Gateway VoIP configuration.
- Appendix D 『 **Cable Specification** 』 describes the console cable, Ethernet cable specifications and Pin numbers for the PassFinder AP2520 Gateway.
- Appendix E 『 **Miscellaneous Information** 』 defines the PassFinder AP2520 Gateway certificate of quality and related policies.

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

<p>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</p>

PassFinder AP2520 Gateway User's Manual's Revision history are as follows.



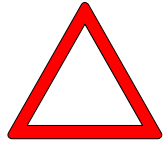

Revision No.	Date	Contents	Written By
Version 1.00	Oct. 8, 2001	Initial Released	AddPac R&D Part
Version 1.10	Mar. 2, 2002	Additional Command Released	AddPac R&D Part

[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 selection are grouped in braces({}) and are separated by Slashes(/).
- Angle brackets(< >) are required but appropriate parameters must be inputted.

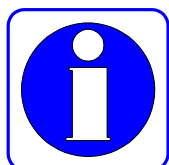
The following symbols are used for the user's reference in reading the user's manual.

Danger 	Danger This symbol signals possible danger. Misuse could result in physical injuries. In procedures with this symbol, the user is strongly advised to follow safety regulations in order to avoid electrical shock.
Warning 	Warning This symbol warns the user that misuse in this procedure could result in hardware damage of the equipment or loss of data.
Caution 	Caution This symbol calls for the user's caution. Misuse in this procedure could result in software damage of the equipment, loss of data or system configuration.
Information 	Reference This symbol indicates reference, providing detail information for understanding the user manual.

Chapter 1 PassFinder AP2520 Overview

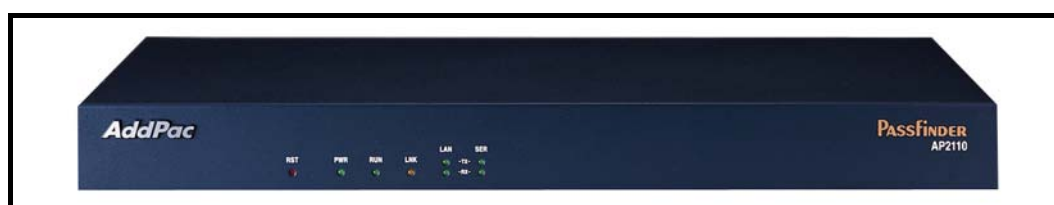
1.1. Introduction to the AP2520

Information **PassFinder AP2520** LAN-to-LAN, LAN-to-WAN high-performance VoIP router/gateway supporting VoIP service under internet or intranet environment. This network equipment, with an independent interface module slot, supports cost-efficient data and voice service in junction with PSTN networks.



Furthermore, this equipment provides a secured VPN service, a dedicated network service over a public network, and voice over IP network within an enterprise, all of which provides cost-efficient data / voice service solution.

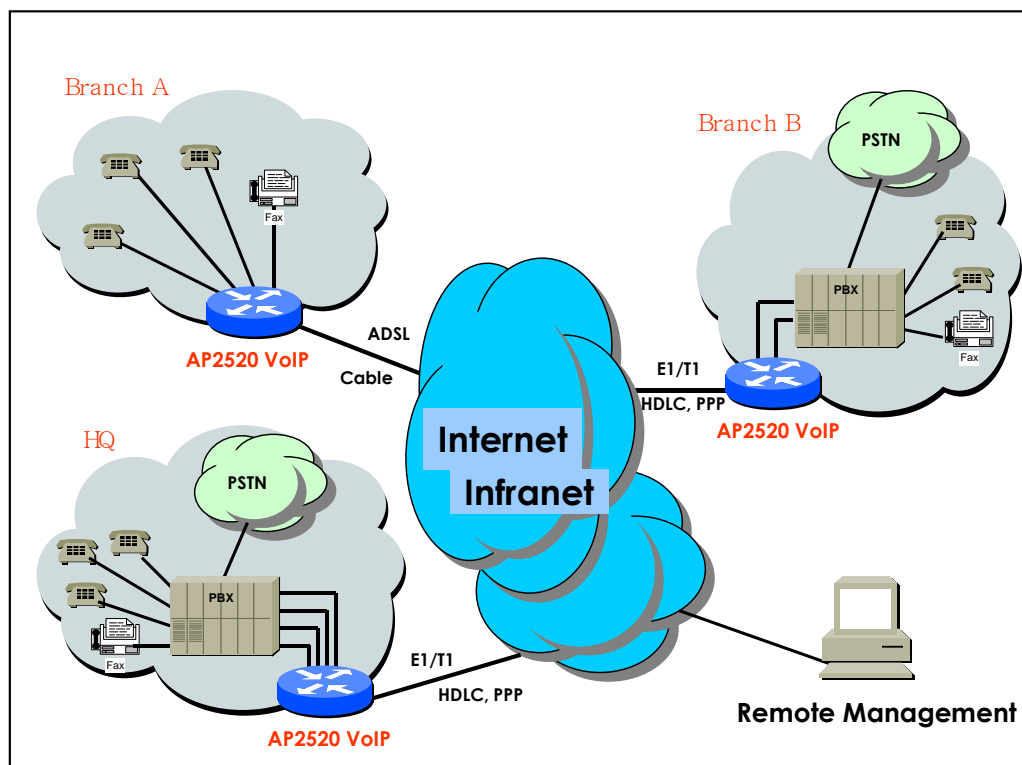
The AP2520 VoIP provides LAN-LAN or WAN – LAN internetworking connection while supporting Frame-Relay, PPP, HDLC, and other protocols. Providing manual or automatic data routing, the AP2520 VoIP also allows internet connection. The exterior is provided in the following diagram :



[Diagram 1-1 The Exterior of the PassFinder AP2520 VoIP Router]

This equipment not only supports Static, RIP v1/v2, OSPF v2 standard protocols and IEEE Spanning Tree bridging function for small-scaled networks but also shows perfect compatibility with other brands for large scaled networks such as the internet.

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

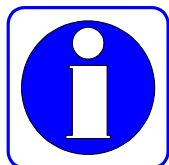


[Diagram 1-2 Network Using PassFinder AP2520 VoIP Router]

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

1.2. Main Features

Information



The PassFinder AP2520 VoIP serves not only as a dedicated-line router for enterprises, public offices, schools but also provides high-compression algorithm WAN port to utilize virtually 100% of the E1 (2,048Mbps) lines and Voice Interface Slots which can support FXS, FXO, E&M and Digital E1 at the user's request.

PassFinder AP2520 VoIP is designed to offer an exceptional, but cost-efficient, solution for SOHO and SME environment for the user's full satisfaction. The PassFinder AP2520 VoIP also supports a reliable T1/E1 service while maintaining the system user-friendly for even beginners to operate. The router supports Static, RIP v1/2, OSPF v2 protocols making it the most effective and cost saving solution.

- The PassFinder AP2520 VoIP is a module-slot designed multi-service router.
- Through various VoIP interface modules, the PassFinder AP2520 provides a high performance 32 bit RISC microprocessor structure.
- The PassFinder AP2520 VoIP supports stand-alone 2- Network Module slots.
- The PassFinder AP2520 VoIP provides 1 Fast Ethernet Port and 1 Ethernet Port or 1 Sync. Serial Port at the user's request.
- The PassFinder AP2520 VoIP provides Fixed 1-Ports Async Serial Interface (2 x RJ45)
- The PassFinder AP2520 VoIP provides 4-Ports FXS Voice Processing Network Module (4 x RJ11)
- The PassFinder AP2520 VoIP provides 4-Ports FXO Voice Processing Network Module (4 x RJ11)
- The PassFinder AP2520 VoIP provides 4-Ports E&M Voice Processing Network Module (4 x RJ11)
- The PassFinder AP2520 VoIP provides 1-Ports Digital E1 Voice Processing Network Module (1 x RJ45, ISDN-PRI and R2 Supports)
- 1U x 19" Rack Mountable Chassis with Cooling Fan
- AC Power Supply Unit
- System LEDs

Hardware Description

PassFinder AP2520 VoIP is based on the latest technique of embedded hardware and support various network interface. The major hardware specification is followings as :

- **High-performance Residential voice gateway based on WAN-to-LAN**
- **High-performance WAN-to-LAN routing solution**
- **High-performance 32bit RISC Microprocessor construction**
- Fixed 1-Port 10Mbps Ethernet for WAN Interface (RJ45)
- Fixed 1-Port 100Mbps Ethernet Interface for LAN Service (RJ45)
- Supports 2- Voice Network Module slots.
- Up-to 8-Ports FXS Voice Interface (4 x RJ11)
- Up-to 8-Ports FXO Voice Interface (4 x RJ11)
- Up-to 8-Ports E&M Voice Interface (4 x RJ48)
- Up-to 2-Ports Digital E1 Voice Interface (4 x RJ48)
- Fixed 1-Port Async Serial Interface for Console Port (RJ45)
- Power Supply Adaptor
- Various system LED function

Voice over IP Service

- The PassFinder AP2520 VoIP supports Voice over IP service.
- Support 4~8 channel Voice port, with the service in integration with operating switches(PABX), Legacy Phones, fax, and etc.
- Uses industrial standard VoIP protocol : H.323 v2, *SIP, *MGCP etc.
- Various voice compression technology such as G.723.1, G.729.A, G.711 utilizing high-performance DSP hardware.
- Auto-recognition of VAD, DTMF and FAX Tone and various voice processing functions such as CNG, Echo Cancellation.
- Supports T.38 standard G3 FAX Relay.(Out-Band and In-Band)
- High stability and convenience in integration with H.323 based Gateway, Gatekeeper etc.
- ISDN-PRI and R2 Signaling (Digital E1 Module)
- E&M Type I, II, III, IV, V in 2Wire/4Wire connection

IP Routing Protocols

The PassFinder AP2520 VoIP supports various routing/bridging protocols which are as the following.

- IP Routing (Static, Default Routing)
- RIP Version 1, Version 2
- OSPF Version 2
- Transparent Bridging (IEEE Spanning Tree Protocol)

WAN Protocols

The PassFinder AP2520 VoIP supports various WAN protocols which are as the following.

- HDLC (Cisco Propriety) at AP2520 VoIP Router
- Frame-Relay and PPP at AP2520 VoIP Router
- PPPoE(PPP over Ethernet) at AP2520 VoIP Router/Gateway
- ADSL Dynamic/Dedicated Service at AP2520 VoIP Router/Gateway
- Cable Dynamic/Dedicated Service at AP2520 VoIP Router/Gateway

Network Managements

PassFinder AP2520 VoIP supports various management functions which are as the following.

- Standard SNMP Agent, standard MIB II, Bridge MIB for systematic equipment management
- Console function support as Asynchronous port
- Telnet/ Rlogin support for remote control function
- Web based Management using http protocol
- QoS support through Traffic queuing

Security Functions

PassFinder AP2520 VoIP supports various security functions which are as the following :

- Standard & Extended IP access list support for network security
- Enable/Disable function at particular network protocol such as telnet, ftp.
- Account management function for Multi-level users
- Auto Timeout function for Telnet/Console session
- *VPN function

Operation and Managements

PassFinder AP2520 VoIP supports operation and management functions which are as the following.

- System performance analyzing function for processor, CPU and interface
- Configuration backup/ Restore function for APOS management
- Various debugging function and system auditing
- Automatic System Rebooting function with watchdog
- Data logging and management function
- IP statistics and IP accounting

Other Scalability Features

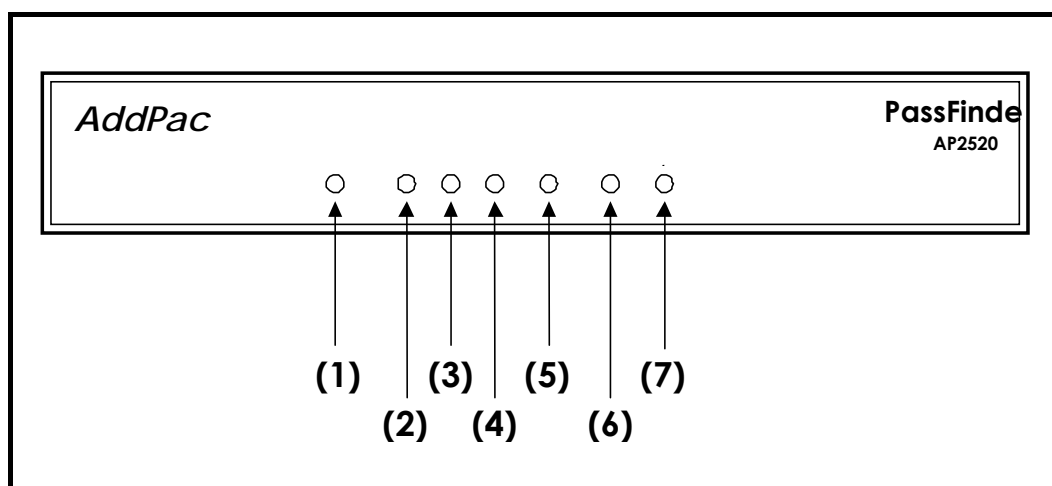
PassFinder AP2520 VoIP supports following additional features :

- DHCP Server, Client and Relay function for easy IP management
- NAT/PAT function support for efficient IP management
- Remote software upgrade support by TFTP, FTP and HTTP
- Command line interface (CLI)
- Network Time Protocol(NTP) Client support

1.3. External View

The PassFinder AP2520 VoIP Router external and its labels is as follows :

- Front View Diagram of PassFinder AP2520 VoIP Router

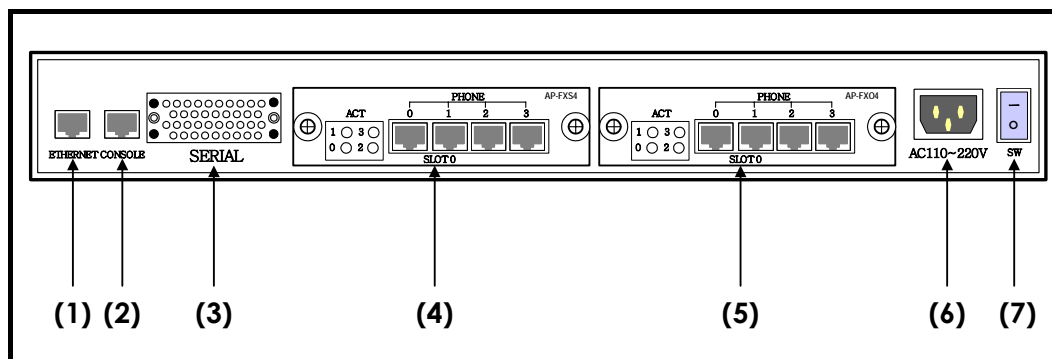


[Diagram 1-3 PassFinder AP2520 VoIP Router Front Side]

No.	Label	Description
(1)	RST	RESET switch : Resets the system by hardware.
(2)	PWR	Power LED : Indicates power supply.
(3)	RUN	RUN LED : Indicates proper functioning of the equipment.
(4)	SER (LAN1)	WAN(SERIAL) LED : Indicates WAN(SERIAL) port connection / usage for AP2520 router model. LAN1 LED : Indicates LAN 1 port connection / usage for AP2520 gateway model.
(5)	LAN	LAN LED : Indicates Ethernet port data input status.
(6)	LNK	LINK LED : Indicates proper connection of LAN.
(7)	10/100	10/100 LED : Indicates Fast Ethernet function.

[Table 1-1 PassFinder AP2520 VoIP Router Front Side Description]

- Rear View Diagram of PassFinder AP2520 VoIP Router (8-port VoIP Module)



[Diagram 1-4 PassFinder AP2520 VoIP Router / 8-ports Voice Module Rear Side]

No.	Label	Description
(1)	LAN Port	Port for connecting UTP Type 10/100BaseTx Ethernet.
(2)	Console Port	With the provided console cable, connect with the PC for equipment configuration. Mandatory for initial setting.
(3)	WAN(SERIAL)	Port for 1 WAN(SERIAL) for router model. Port for 1 LAN for gateway model.
(4)	Network Module Slot 0	4 RJ11 Type Voice Ports. (FXS) ◆ Status LEDs Provided
(5)	Network Module Slot 1	4 RJ11 Type Voice Ports. (FXO) ◆ Status LEDs Provided
(6)	Power Input Plug	Connects power cable. The AP2520 VoIP router uses both 110 and 220V AC.
(7)	Power Switch	Switch for power supply.

[Table 1-2 PassFinder AP2520 VoIP Router / 8-port Voice Module Rear Side Description]

Chapter 2 Before Installation

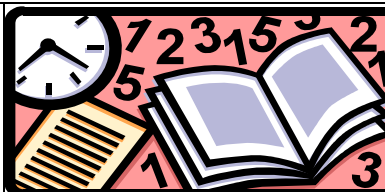
2.1. Unpacking

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

If an external damage of the packaging has been found, please contact AddPac Technology Co. Ltd. sales department (sales@addpac.com, tel : +82-2-568-3848) for an immediate exchange of product.

If no external damage has found, confirm if the following items are enclosed.

No.	Item	Content	Q'ty
1	PassFinder AP2520 Gateway/Router Main Body		1
2	LAN Cable (for RJ45 to RJ45)		1
3	Console Port Cable (for RJ45 to DB9)		1
4	Power Cord (220V Power Cord)		1
5	V.35 Cable (V.35 to V.35) (AP2520 Router Model Only)		1

6	AP2520 Operation Manual		1
---	-------------------------	--	---

[Diagram 2-1. PassFinder AP2520 Package]

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

2.2. Installation Requirements

Warning

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



- Ensure the AP2520 VoIP is in a dust-free environment before and after installation.
- Ensure the AP2520 cover is opened on a flat and safe surface.
- To prevent accidents, avoid ties, scarf, sleeves, and any other loose clothing from entangling with the Chassis.
- Avoid any actions that may effect the equipment or the operator.

2.2.1. Electrical Requirements

Danger

There are two main sources of electrical problems with the AP2520 : the power supply and static electricity.



This section describes safety recommendations for each case.

- **Electrical Safety**
 - ✓ In case of the occurrence of an electrical accident, operate at a position where immediate shut-off of power supply is possible.
 - ✓ Switch the power off when installing or taking the cover off the equipment.
 - ✓ Avoid operating the equipment alone at a 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 uncovered 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 prevent static electricity.

2.2.2. General Requirements

Warning



The PassFinder AP2520 is ready for use where electronic products are used. However, a location with the following conditions are recommended for maximum performance.

- **A level and well ventilated location is recommended.**
- **Secure the equipment safely where intended to install.**
- **Avoid placing objects on top of the equipment.**
- Install the equipment in a cool location avoiding direct sunlight.
- Maintain distance from flammable, chemical, or magnetic objects

2.2.3. Prerequisites for Network Connection

Warning



Observe EIA standards and limitations when installing the Gateway

The following section describes the synchronous serial cable, Ethernet Cable and the Console Cable PassFinder AP2520 supports.

2.2.3.1. Synchronous Serial Cable

Before connecting an equipment to the synchronous serial port, labeled "Serial" on the rear side of the router, the following must be determined.

- Whether the equipment to be connected to the WAN(Serial) interface is a DTE or DCE.
- Whether the connector type is a Male or a Female.
- The required standard of the equipment.

2.2.3.1.1. DTE and DCE

The equipment communicating in connection to the synchronous Serial interface could be either DTE(Data Terminal Equipment) or DCE(Data Circuit-Terminating Equipment). The DCE equipment provides Clock Signal for communication between the router and the equipment. The DTE equipment does not provide Clock Signal. Table 2-1 describes the general DTE and DCE equipment, to be used when the difference is unclear.

Equipment Type	Connector Type	General Equipment
DTE	Male	Terminal, PC Router
DCE	Female	Modem, DSU / CSU Multiplexer

[Table 2-1 The General DTE/DCE Equipment]

2.2.3.1.2. Transfer Speed and Distance Limitations

Synchronous signals allow communication within the distance limited by the Bit Rate. Generally, the lower Data Rate allows communication to a further distance. All serial signals are subject to limitation by distance, and signals exceeding this limitation will drastically dissipate, eventually losing the signal entirely.

Table 2-2 shows the relationship between the EIA/TIA-232(RS-232c), used for the AP2520 router's console cable, signal distance and its transfer speed. This signal standard supports a maximum transfer speed of 64Kbps. Table 2-3 shows the relationship between the V.35 standard, used for the AP2520 router's WAN(Serial) cable, and its transfer speed.

Data Rate (Baud)	Distance (Feet)	Distance (Meter)
2,400	200	60
4,800	100	30
9,600	50	15
19,200	50	15
38,400	50	15
64,000	25	7.6

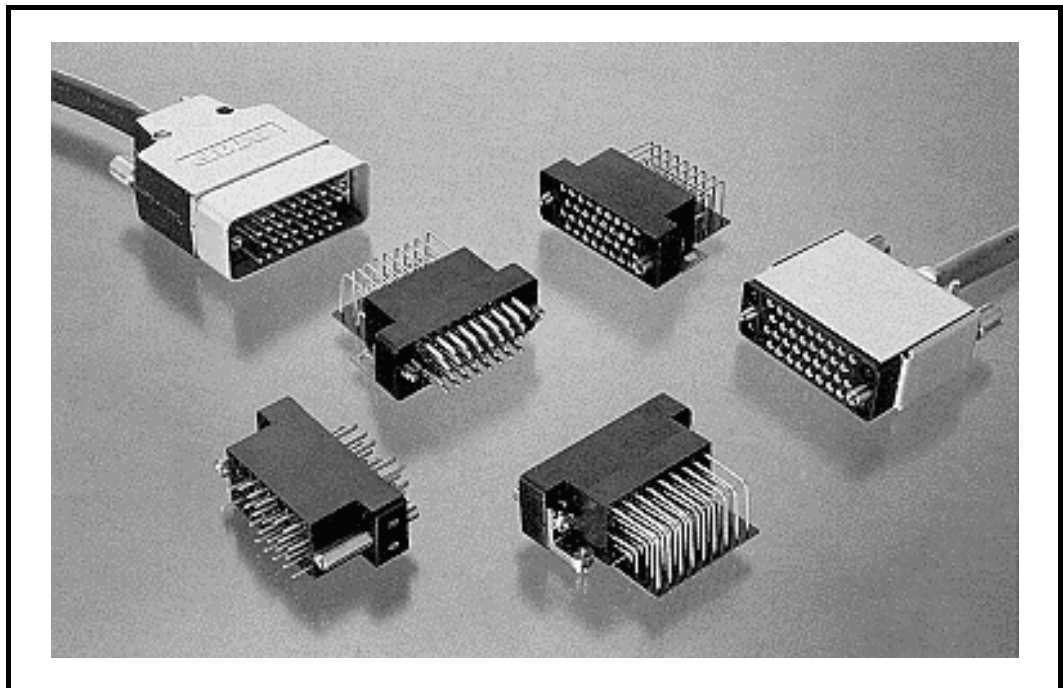
[Table 2-2 EIA/TIA-232 Transfer Speed and Distance Limitation]

Data Rate (Baud)	Distance (Feet)	Distance (Meter)
2,400	4100	1250
4,800	2050	625
9,600	1025	312
19,200	513	156
38,400	256	78
56,000	102	31

[Table 2-3 EIA/TIA-449, V.35 Transfer Speed and Distance Limitation]

2.2.3.1.3. V.35 Connection

The V.35 standard recommends a speed of less than 7Mbps. In functional usage, it is capable of transferring data at less than 4Mbps, and is used for virtually all T1/E1 (1.544Mbps/2.048Mbps) router cables. The V.35 cable uses the 34-Pin Winchester-Type connector as shown in diagram 2-4. Please refer to appendix C "Cable Specification" for detailed pin specifications.



[diagram 2-4 V.35 Serial Connector Example]

2.2.3.2. Ethernet Port

2.2.3.3. RS-232C Serial Console Port

Chapter 3 Installation and Operating Environment

This chapter provides information about the basic installation procedure of PassFinder AP2520 and related commands.

[Prerequisites] Unless a separate order is made, the tools and certain cables are not provided in the package. Prepare the following equipments and tools before installation.

- Standard screw driver set

- Cable for LAN and WAN(Serial) port connection
 - ✓ RJ-45 to RJ-45 cable for LAN port
 - ✓ V.35 cable for WAN(Serial) port for router model (1 is provided in the package)
 - ✓ RS-232c console cable with RJ-45 connector (included in equipment box)

- Cable for connecting with phone port
 - ✓ RJ-11 to RJ-11 ordinary phone-line cable

- PC with Console Terminal or Communication Emulator application (The Hyper Terminal Program in Windows will suffice. Configure as : 9,600 Baud, No Parity, 8Bit Data 1Stop Bit)

- DSU/CSU or other DCE equipment for connection with Synchronous WAN(Serial) port.

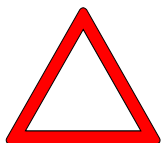
3.1. Installation

3.1.1. Installation Procedure

- Plug in the console cable and configure the console terminal. (Refer to 3.1.2 for details.)
- Connect the network to the desired port. Use RJ-45 cable with the LAN 1 port for connection with ADSL/Cable Modem or Router, and the RJ-45 cable with the LAN 0 port for connection with the HUB/Switch. (For gateway model)
- Connect the network to the desired port. Use the V.35 cable with the WAN(Serial) port for connection with DSU/CSU, and the RJ-45 cable with the LAN port for connection with the HUB/Switch. (for router model)
- Log in the Gateway after the booting message on the console with the root account. (Configuration is only possible when logged in with the root account.)
- Switch to Configuration Mode.
- For the WAN(Serial) port, configuration for mode (HDLC, PPP, Frame-Relay, etc), as well as internet address assignment, is required. (Refer to Interface Configuration.) (for router model)
- Assign an internet address to the desired port of usage. (Refer to Interface Configuration.)
- Configure the settings for the routing and VoIP related. (Refer to Chapter 4 and 5.)
- Confirm the configured settings. (Refer to the Gateway administrative

commands.)

Caution



- Save the settings on Flash Memory. **(PassFinder AP2520 immediately operates under the new settings, but under certain network environments rebooting is required.) (Refer to the following instructions for this part.)**
- Using commands such as Ping, Telnet, rlogin etc. check the status of other Gateways or PCs connected to the Gateway.
- Check the routing table to confirm if the Gateway is receiving the network information correctly.
- Use the Ping command to check other Gateways or PCs connection.
- This completes the basic configuration procedure. For optional functions, refer to the related chapter

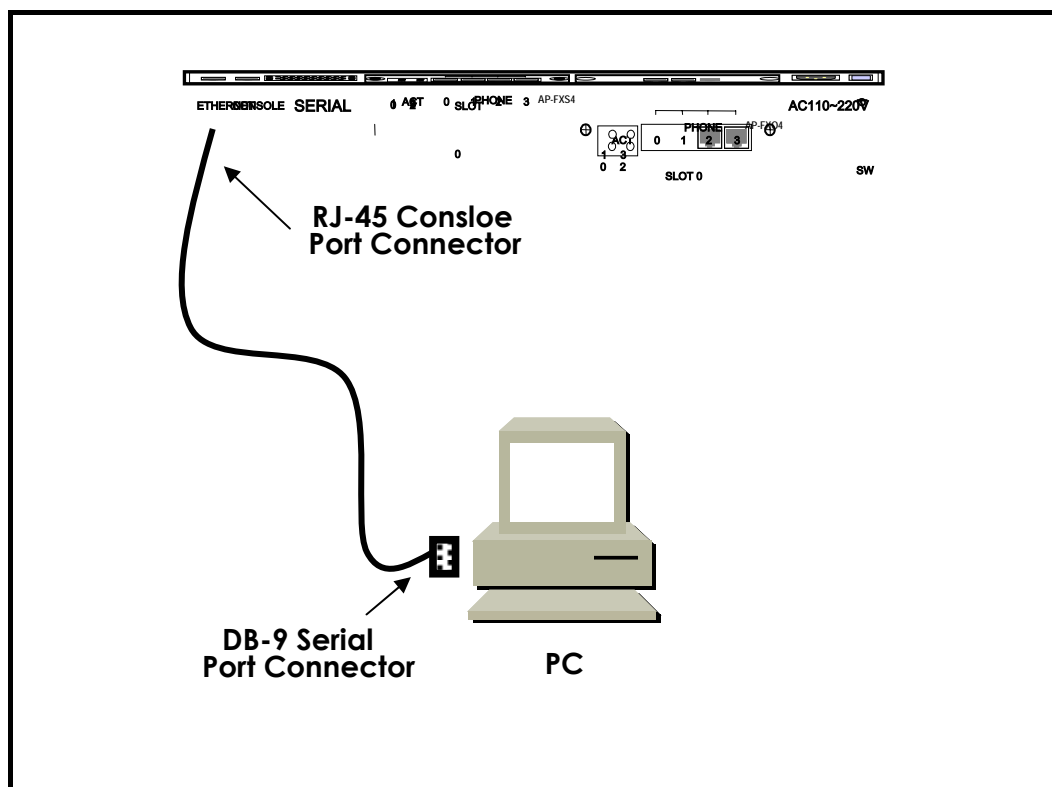
3.1.2. Console Connection

- 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 console cable provided in the package.
 - ✓ If using a PC for the console terminal, connect with the PC serial port.
- In order to use the PC as a console terminal, a communication emulator application is required. Under normal circumstances, the Hyper Terminal Program in Windows will suffice.

The console terminal should be configured as : 9,600 Baud, No Parity, 8Bits Data, One(1) Stop Bit. The PassFinder AP2520 is set to operate with the configurations above. Therefore, these settings are required for communication between the product and the console terminal. **(Refer**

to [Diagram 3-2 Hyper Terminal Configuration])

- When configuring the Hyper Terminal, select the Hyper Terminal menus in the following order: File → Configuration → Connection Target → Format and set each item.
- The console port serves the purpose of configuring the PassFinder AP2520 settings and checking its operating status.



[Diagram 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

[Diagram 3.2 Hyper Terminal Configuration]

3.1.3. Plug-In Power

Warning



- The PassFinder AP2520 Gateway is capable of recognizing and using both 110V and 220V.
- The package provides a 220V power cable. If the power supply is 110V, please use a 110V adapter.
- Switching the power switch on will turn the Power LED on the front side of the Gateway green.
- The supply of power will display the booting message on the console terminal and will turn the RUN LED green
- When the Gateway is being booted, the 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 check results, memory size and status)
 - ✓ On the display of the log-in message, input the username "root" and the password "router".
 - ✓ The completion of log-in will display the prompt "1router#" on the Gateway console terminal.
 - ✓ There are two types of prompts displayed for the PassFinder AP2520 : "1router>" and "1router#". The ">" prompt indicates that the user is not an administrator. At 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 is authorized to use all the functions and commands.

- ✓ Log-in as "Admin" allows Gateway setting configuration. Therefore, it is advised to change the Gateway password for security purposes. Refer to the Administrative contents for password change.

The display below is the message for initial booting of the PassFinder AP2520 Gateway.

```
System Boot Loader, Version 1.3.6/1
Copyright (c) by AddPac Technology Co., Ltd. Since 1999.

PassFinder Router Series (2520)
Serial Number: AP2520-ffff55
MPC855T 50MHz With 33554432 Bytes System Memory
524288 Bytes System Flash Memory
4194304 Bytes 2nd System Flash Memory
DS1742 Timekeeping RAM

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

2520 System software Revision 1.0
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 not configured yet or backup data is invalid.
Please login to system as a "root" and make configuration.

Voice Module (0): FXO
Voice Module (1): FXS

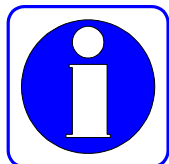
DSP S/W download
Voice Module (0): .... OK
Voice Module (1): .... OK

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

[Diagram 3.3 PassFinder AP2520 Initial Screen]

3.2. Environment Configuration

Information



The Gateway requires various configurations of parameters according to the application. This section provides important information for using the Gateway and the user is highly advised to follow the following procedures before configuring the Gateway.

- Clarify the network address according to the IP with the network diagram..
- Determine which routing protocol to use. (e.g. Static, Default, RIP, OSPF etc.) In doing so, discussion with the administrator of the connecting network is required.
- Determine the protocol to use with each WAN(Serial) port for router model. (e.g. HDLC, PPP, Frame-Relay, etc.)
- Determine the protocol to use with each LAN 1(WAN) port for gateway model. (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, settings must be reconfigured. At completion of configuration, always save the settings to prevent loss of data when switching the power on/off.

In order to log in at an unconfigured Gateway, the user must use a set username and password. The user access authority for PassFinder AP2520 is divided into 4 levels : admin, high, normal, low. All users, other than Admin is prompted "1router>" at log-in.

The user must log-in at admin level for Gateway configuration. **Factory settings for admin level log-in uses "root" for username and "router" for password. The**

user is prompted with "1Gateway#" for Admin level log-in and is allowed to configure the equipment.

PassFinder AP2520 configuration is divided into two parts : Global Configuration, which effects all the Gateways of the network, and Interface Configuration, which effects only the Gateway of configuration. By function, configuration is divided into: "User and Gateway Administration", "Interface Configuration", "Routing and Bridging Configuration", "System Status and Debugging Configuration", etc.

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. The PassFinder AP2520 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 performance, therefore the user is advised not to connect more than 10 sessions

This configuration allows the setting of the user password. The default username for PassFinder AP2520 Gateway is "root" and its password is "router". (This default setting is for "admin" level access.) When the Gateway configuration is completed, a change of password is advised. This is to prevent unauthorized users from reconfiguring the settings. The PassFinder AP2520 Gateway saves the password and the configuration in safety area.

This configuration mode allows Gateway software upgrade, and commands related to system administration such as configuration saving and backup.

It also provides commands for checking 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 an Ethernet and WAN(LAN or Serial Port) environment, an IP address must be configured for each port. For commands related to port IP address connection, refer to interface related commands. For the WAN(SERIAL) port, configuration for lower level protocols is required as well as IP address.

The LAN 1(for WAN) ports for PassFinder AP2520 are supports Legacy LAN, PPP(PPPoE) for ADSL connection. In order to connect to the network, the WAN protocol must match the one used at the other equipment, including configuration variables. Discussion with 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, DHCP information, refer to the "Configurations for Security and Internet" section.

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

3.2.3. Routing Configuration Environment

The PassFinder AP2520 Gateway supports Static, Default, RIP V1/V2 and OSPF V2 routing protocols. The routing protocol is responsible for assignment of packet route, and PassFinder AP2520 is supports multi-protocols simultaneously. Therefore it is required to configure which protocol to use. Refer to "Routing Configuration Environment" and "Interface Configuration Environment".

3.2.4. Security and Internet Configuration Environment

The PassFinder AP2520 Gateway supports additional functions for security and internet environment.

The functions provided include 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 details

3.2.5. System Status and Debugging Environment

The PassFinder AP2520 Gateway supports the "Show" command for checking the system operation status and the "Debug" command for locating system errors. The "Show" commands not only provides information about the status of interface, but also status for NAT configuration, Access-list, DHCP, registered user, buffers and all others assisting proper operation of the Gateway.

The "debug" command provides information regarding proper operation of the Gateway by displaying operating TCP/IP or Layer 2 on the terminal screen.

For more details, refer to Chapter 4.

3.2.6. Voice Integration Configuration Environment

The PassFinder AP2520 Gateway allows integration of voice applications and data. The PassFinder AP2520 Gateway provides a status check of voice and fax support / connection, voice gateway configuration, quality of voice control, PABX connection configuration, and other configuration / status report of voice related.

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

Chapter 4 Gateway Configuration and Commands

This chapter describes how to configure the PassFinder AP2520 Gateway and commands of the PassFinder AP2520 Gateway.

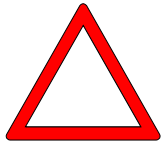
4.1. Gateway Booting

The operator can use all commands of the AP2520 through the consol or Telnet connection.

When power is supplied, the Gateway is booted as follows. :

- 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. In the default configuration, the boot loader loads Gateway software in the flash memory.
- If the boot loader does not find any 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 saved in the Gateway. 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 as using "copy running-config" command.

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

```
System Boot Loader, Version 1.3.6/1
Copyright (c) by AddPac Technology Co., Ltd. Since 1999.

PassFinder Router Series (2520)
Serial Number: AP2520-ffff55
MPC855T 50MHz With 33554432 Bytes System Memory
524288 Bytes System Flash Memory
4194304 Bytes 2nd System Flash Memory
DS1742 Timekeeping RAM

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

2520 System software Revision 1.0
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 not configured yet or backup data is invalid.
Please login to system as a "root" and make configuration.

Voice Module (0): FXO
Voice Module (1): FXS

DSP S/W download
  Voice Module (0): .... OK
  Voice Module (1): .... OK

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

```
Interface ethernet0.0, changed state to UP
login: root
password:*****
RGW - Login : root at Console on Thu Jan 1 03:14:59 1970

router#
```

4.2. Command Usage

The operator can use all commands of the VOICEFINDER AP2520 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 mode enable the operator to check configuration status of the Gateway and perform debugging. And commands of the configuration mode enable the operator to change configuration environment and set new environment.

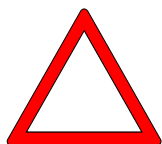
The PassFinder AP2520 Gateway has following features regarding operator's entering commands.

- Although the operator enters only a part of the command, the PassFinder AP2520 Gateway automatically recognizes the whole command. For example, if the operator enters only "sh" or "sho" instead of "show" the PassFinder AP2520 Gateway automatically recognizes "sh" or "sho" as "show."
- The PassFinder AP2520 Gateway provides an online help function so the user can check corresponding items for the command and command syntax.
- The PassFinder AP2520 Gateway provides "More" function that divides a long message into several messages so that the operator can see the whole message by scrolling the screen.
- The PassFinder AP2520 Gateway provides Help and "?" functions to display

available commands for the corresponding mode and descriptions of commands.

- The PassFinder AP2520 Gateway provides "History" function. With the history function, the operator does not need to enter the command that the operator had 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 that can be used in each mode.

Caution

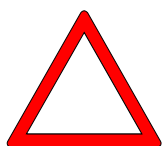


The commands indicated with "*" among the optional commands are not currently supported. They are to be supported in the higher version Gateways.

예) 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 that had been set before will return to default values.

예) 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 Gateway user
utilization	: System resource using information

4.2.1. Commands of the User Mode

Every 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 currently available and description of these commands.
clock	Indicates system time.
exit	Logs out the operator from the Gateway.
help	Explains command-using method in an interactive way.
history	Shows history of the used command lines.
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 the packet passes through to reach 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.

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 cannot use commands that are used in the user mode.

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

Commands	Description
?	Displays commands currently available and description of these commands.
clear	Clears statistical data saved in the Gateway.
clock	Indicates 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 in using the command since it can increase system load. (See "un-debug" command.)
Exit	Logs out the operator from the Gateway.
help	Explains command-using method in an interactive way.
history	Shows history of the used command lines.
load	VoIP related command. Loads the VoIP configuration script file to the VoIP Configuration of the Gateway.

no	Cancels commands entered in the command line or returns commands 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 rlogin connection that is similar to the Telnet with by original login.
save	VoIP Command. Make VoIP Configuration Script File uses Gateway VoIP Running Configuration.
show	Shows configuration status and operating status of the Gateway. However, in the user mode, "show" command shows only limited information.
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 that the packet passes through to reach a certain destination.
who	Checks users who are currently online in the Gateway, login method and login time.
write	Saves the Gateway configuration file.
undebg	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.

4.2.3. Commands of the Configuration Mode

Only the user who has the root account or equivalent authorities can access to the configuration mode. In the manager mode, the user cannot change the existing configuration of the Gateway nor make a new configuration of the Gateway.

The configuration mode can be divided into several kinds – the interface Configuration mode, the Global Configuration mode and the VoIP 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 relating 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-serial0)" 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.
Accounting-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	Display 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.
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.
tth	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.
VoIP-port	Sets the VoIP port.
VoIP-interface	Sets the VoIP Interface.

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
bridge	Sets the bridge parameters.
encapsulation	Sets and changes the encapsulation method of the interface. (AP2520 supports Ethernet, IEEE802.1q VLAN, IEEE802.3 and PPPoE Encapsulation for Ethernet, HDLC, PPP, Frame-Relay for Serial)
exit	Returns to the previous (configuration) menu.
end	Returns to the initial (Exec) mode.
Interface	Selects an interface to set additional interface.
ip	Sets IP protocol and IP service related items.
line-ctrl	Change Line Parameter settings for the interface.
no	Cancels commands entered in the command line or returns commands into default values.
mtu	Sets the size of the IP Maximum Transmission Unit (MTU.)
ppp	Sets PPP protocol related parameters.
rmon	Sets VLAN parameters for the interface.
Shutdown	Shuts down the selected interfaces.
vlan	Sets VLAN parameters for the interface.

4.2.3.3. Commands of the Interface Configuration Mode 2 (IP Configuration Mode)

The user can use IP related commands in the selected interface.

The prompt is indicated as router(config-ether0.0)#.

Command	Description
access-group	applies the access-list that has been set in the global configuration environment to the interface.
accounting	Apply IP Account List to the selected 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.
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.
proxy-arp	Enables IP proxy ARP for the corresponding interface.

4.3. Starting Gateway Configuration

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

[Procedure]

Step	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 account. (The manager's ID is  
set as "root" in the factory.)  
password:***** ➤ Enter the password. (The password is set as  
"router" in the factory.)  
AP2520 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 the PassFinderAP2520 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 the PassFinderAP2520 Gateway uses the standard ARPA encapsulation method as the default. However, if necessary, the network manager can use SNAP or IEEE 802.3 encapsulation method.

The logical port can separate the Ethernet of the PassFinderAP2520 Gateway. If the user wishes to use only one Ethernet port, the user must designate the logical port.

Do the following to use the Ethernet.

[Procedure]

Step	Operation
1	Enter into the interface configuration mode.
2	Enter into the IP configuration mode.
3	Give 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 /Serial} { 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 be set as a sub-interface.

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

1. Sets the IP address for the selected interface.
2. One of lower commands of "ip" command

[Example] Ethernet Configuration (Start)

When operating "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 address 192.20.1.1 255.255.255.0
3Router(config-ether0.0)# interface ethernet 0 1
4Router(config-ether0.1)# ip address 210.10.2.1 255.255.255.0
```

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

1. An optional command to change the encapsulation method for the current Ethernet interface
2. The default is the Ethernet.
3. VLAN supports 802.1Q VLAN.
4. PPPoE supports ADSL Service

- **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 corresponding pair of the IP address and the 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. An optional command to make the current interface up/down.
2. The Ethernet interface cannot shut down the main interface. To make a certain Ethernet interface up/down, go to the corresponding sub-interface.

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

An optional command to remove the logical interface. "If-name" represents the name of the logical interface.

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

Shows the interface status of "if-name."

[Example] Ethernet Configuration

```
Router(config)#interface ethernet 0.0
Router(config-ethernet0.0)#
Router(config-ethernet0.0)# ip address 131.12.1.1
255.255.0.0
Router(config-ethernet0.0)#no shutdown
Router(config-ethernet0.0)# mtu 2000
Router(config-ethernet0.0)# end
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.

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) protocol.

If a PPP encapsulation option is given to the PassFinder AP2520 Gateway, PPP operation is possible. 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. Software always sends the magic number configuration option. However, software sends the authentication option only when the authentication option is set.

[Procedure]

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

[Related Commands and Syntax]

- **interface { Ethernet / serial } { 0 / 1 }**

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

- **encapsulation { hdlc / ppp / frame-relay }**

Sets the serial encapsulation mode for the interface.

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

Selects the corresponding interface and enters into the IP related configuration mode.

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

1. Sets 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. Sets the PPP authentication method as CHAP or PAP in the interface configuration mode.
2. The "callin" option is to connect only incoming calls by 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 sets 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 that has been set in its local interface.

- **ppp timeout** *<second>*

1. Sets PPP negotiation timeout for PPP negotiation between two Gateways. (An optional command)
2. The default is five 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 0.0  ⚡ Enters into the
interface configuration mode.
Router(config-ether0.0)#  ⚡ Configuration is possible in this
mode.
Router(config-ether0.0)# encapsulation pppoe  ⚡ Sets the PPPoE
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] Added Commands During PAP Configuration (Server)

If the Gateway functions as a server, it means the AP2520 Gateway functions as the PPP authentication server.

```
Router(config)# user addpac password Router1 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 pppoe ☞ 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 Router, this command enables the Router 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 ☞ Exits from the configuration menu.
```

```
Router # debug ppp packet
```

```
Ethernet0 LCP: TIMEOUT
```

```
Ethernet0 LCP: O CONFREQ id=1
```

```
Ethernet0 BCP: TIMEOUT
```

```
Ethernet0 BCP: O CONFREQ id=1
```

```
Ethernet0 LCP: TIMEOUT
```

```
Ethernet0 LCP: O CONFREQ id=1
```

```
Ethernet0 BCP: TIMEOUT
```

```
Ethernet0 BCP: O CONFREQ id=1
```

```
Router # ubdebug ppp packet ☞ Stops PPP packet debugging.
```

[Example] Added Commands During PAP Configuration (Client)

This is when the AP2520 Gateway is used as a PPP CallIn on the client side.

```
Router (config)#interface ethernet0.0  ⚡ Enters into the
interface configuration mode.

Router(config-ethernet0.0)# encapsulation ppp  ⚡ Sets the PPP
mode.

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

Router(config-ethernet0.0)# ppp pap sent-username addpac
password Router1  ⚡ Sends the user name and the password that
were saved in the server during PPP connection.

Router(config-ethernet0.0)# ppp timeout 100  ⚡ Sets PPP
connection negotiation timeout value as 100 seconds.

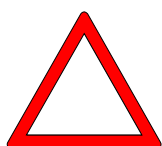
Router(config-ethernet0.0)# end  ⚡ Exits from the
configuration menu.

Router # debug ppp packet

Ethernet0 LCP: TIMEOUT
Ethernet0 LCP: O CONFREQ id=1
Ethernet0 BCP: TIMEOUT
Ethernet0 BCP: O CONFREQ id=1
Ethernet0 LCP: TIMEOUT
Ethernet0 LCP: O CONFREQ id=1
Ethernet0 BCP: TIMEOUT
Ethernet0 BCP: O CONFREQ id=1

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

Caution



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

[Example] Added Commands During CHAP Configuration (Server)

This is when the AP2520 Gateway functions as a PPP authentication server in the server side.

```
router (config)#user addpac password router1 normal ☞ Registers
the user name (addpac) and the password (router1) with the normal
priority in the server.

router (config)#interface ethernet0.0 ☞ Enters into the
interface configuration mode.

router (config-ether0.0)# encapsulation pppoe ☞ Sets the PPP
mode.

router (config- ether0.0)# ppp authentication CHAP ☞ Sets the
PPP authentication mode as CHAP 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-s 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."

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

Ethernet0 LCP: TIMEOUT
Ethernet0 LCP: O CONFREQ id=1
Ethernet0 BCP: TIMEOUT
Ethernet0 BCP: O CONFREQ id=1
Ethernet0 LCP: TIMEOUT
Ethernet0 LCP: O CONFREQ id=1
Ethernet0 BCP: TIMEOUT
Ethernet0 BCP: O CONFREQ id=1

router # undebg ppp packet ☞ Stops PPP packet debugging.
```

[Example] Added Commands During CHAP Configuration (Client)

This is when the AP2520 Gateway functions as a PPP CallIn client in the client side.

```
router (config)#interface ether0.0  ⚡ Enters into the interface
configuration mode.
router (config- ether0.0)# encapsulation ppp  ⚡ Sets the PPP mode.
router (config- ether0.0)# ppp authentication CHAP  ⚡ Sets the
PPP authentication mode as CHAP for the ethernet0.0 interface.
router (config- ether0.0)# ppp CHAP hostname addpac  ⚡ If the
user name that was 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.
router (config- ether0.0)# ppp CHAP password router1  ⚡ Sets the
user name of the server side to check the password that the server
sends during PPP CHAP 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 packets.
router #
    Ethernet0.0 LCP: TIMEOUT
    Ethernet0.0 LCP: O CONFREQ id=1
    Ethernet0.0 BCP: TIMEOUT
    Ethernet0.0 BCP: O CONFREQ id=1
router # undebug ppp packet  ⚡ Stops PPP packet debugging.
```

4.5. WAN (Serial) Interface Configuration

Information



The PassFinder AP2520 router provides V.35 interface port for the WAN (serial) interface. The WAN (serial) port can be set as HDLC encapsulation, PPP encapsulation or frame-relay encapsulation according to the usage of the port, transmission line to which the router is connected, or the configuration of the router in the other side. To enable the router to normally operate, correctly set up the mode of the WAN (serial) port. How to set up each mode of the WAN (serial) port will be described later.

The WAN (serial) port of the PassFinder AP2520 router can be set as the DCE mode or the DTE mode. Basic setting is the DTE mode. In the DTE mode, the router receives clock and line speed information from the DSU/CSU. It is also possible to operate the WAN (serial) port in the DCE mode although it is not a normal case. In this case, the user must set that internal clock can be used for the WAN (serial) interface at the defined speed.

The following chapter describes how to set up HDLC and PPP frame-relay in detail.

For reader's reference, the serial interface supports the sub-interface only in the frame-relay encapsulation mode.

4.5.1. HDLC Configuration

The HDLC mode is the transmission method of the frame layer that is used in the packet data communication network. The WAN (serial) port set as the HDLC mode is applied to the physical layer and the frame layer among OSI 7 layers. In the HDLC mode, no virtual line is provided, and only one connection is provided for each physical port. Therefore, logical interface cannot be used in the HDLC mode. There is no standard specifications for the HDLC. The PassFinder AP2520 router supports same specification as the HDLC of Cisco Systems that is most widely used in the industry, and guarantees full compatibility.

[Procedure]

Step	Operation
1	Enter into the interface configuration mode.
2	Give encapsulation protocol to the interface.
3	Move to the IP configuration mode.
4	Give an IP address to the interface.
5	Make the interface up.
6	Set other necessary optional parameters.
7	Check if "show" command has been properly set up.
8	(If necessary) use "debug" command to check if the router is normally operating.

[Related Commands and Syntax]

- **configuration**

Enters into the router configuration mode.

- **interface { Ethernet / serial } { 0 / 1 }**

Selects the interface to set up, and enters into the interface configuration mode.

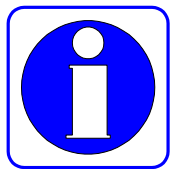
- **encapsulation { hdlc / ppp / frame-relay }**
Sets the WAN encapsulation to use for the interface.
- **ip**
Selects the corresponding interface, and enters into the IP related configuration mode.
- **address <ip_address> <net_mask>**
Sets the IP address for the selected interface.
- **clock rate < speed_value >**
If the interface is in the DCE mode, the router shall receive clocks by itself. This command is used in this case. "*Speed_value*" represents the transmission rate of the interface line. The unit of the "*speed_value*" shall be Internal in the DCE mode, or External in the DTE mode.
- **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 serial interface [0/1]**
Shows KeepAlive message in the corresponding serial interface and packet contents that are exchanged through line protocol.
- **undebug serial interface [0/1]**
Stops debugging in the corresponding serial interface.

[Example] WAN (Serial) Interface Configuration

```
router(config)# interface serial 0  ⚡  Enters into the interface
configuration mode.
router(config-serial0)#  ⚡  Configuration is possible in this mode.
router(config-serial0)#encapsulation    hdlc    ⚡    Sets    HDLC
encapsulation.
router(config-serial0)# ip address 131.12.1.1 255.255.0.0  ⚡  Sets
the IP address as "131.12.1.1/16 bit mask."
router(config-serial0)# no shutdown  ⚡  Makes the interface up.
router(config-serial0)# end  ⚡  Exists from the configuration menu and
returns to the initial manager mode.
router#show int s 0  ⚡  Shows the status of the serial 0 interface.
Interface : serial0
    IP Address : 131.12.1.1  Physical Inteface : Serial0
    Network : 131.12.1.0      Subnet Mask : 255.255.255.0
    Administrator Status =   UP   Operation Status = UP
    Network Type : HDLC      MTU : 1500
    Serial0 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 underruns
    error : 0 (0 busy)
    DCD(UP) DSR(UP) DTR(up) RTS(up) CTS(UP)
router#debug serial interface 0  ⚡  Shows line protocol exchanged
through the serial 0 interface such as KeepAlive packets and the status.
router#HDLC(O):TELNETIT_KEEPAVIVE_REQ(lseq=0, seq=0)
    HDLC(O): TELNETIT_KEEPAVIVE_REQ (lseq=0, rseq=0)
    HDLC(O): TELNETIT_KEEPAVIVE_REQ (lseq=0, rseq=0)
    HDLC(O): TELNETIT_KEEPAVIVE_REQ (lseq=0, rseq=0)
    HDLC(O): TELNETIT_KEEPAVIVE_REQ (lseq=0, rseq=0)
router#undebug serial interface 0  ⚡  Stops debugging.
```

4.5.2. PPP Configuration

Information



Point to Point Protocol (PPP) is one of standard transmission rules 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 compatibility with different manufacturers' devices.

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 loopback link faults and other faults, and automatically terminates the link.
- **Network Control Protocol (NCP):** NCP communicates with various higher layer (network layer) protocol.

If a PPP encapsulation option is given to the PassFinder AP2520 router, PPP operation is possible. Current software installed in the router supports Challenge Handshake Authentication Protocol (CHAP,) the authentication option that uses Password Authentication Protocol (PAP,) and the magic number configuration option. Software always sends the magic number configuration option. However, software sends the authentication option only when the authentication option is set.

[Procedure]

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

[Related Commands and Syntax]

- **interface { Ethernet / serial } { 0 / 1 }**

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

- **encapsulation { hdlc / ppp / frame-relay }**

Sets the serial encapsulation mode for the interface.

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

Sets the IP address for the selected interface.

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

1. Sets the login name and the password to authenticate a router that is trying to access to another router that functions as a PPP PAP/CHAP server.
2. This command functions same as the command that the router manager uses to register a login user. This is because the router shares the PPP registered user database and the router user database. The operator registers users as using the same command.
3. The difference from the registration of router 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. Sets the PPP authentication method as CHAP or PAP in the interface configuration mode.
2. The "callin" option is to connect only incoming calls by 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 router name (displayed in the router 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 sets 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 router as a PPP server and the IP address to allocate to the serial interface of the other side. (An optional command)
2. When the router receives the IP address, the router decides the subnet mask of the IP address that it received based on the IP subnet that has been set in its local interface.

- **ppp timeout *<second>***

1. Sets PPP negotiation timeout for PPP negotiation between two routers. (An optional command)
2. The default is five 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 serial 1 ➤ Enters into the interface  
configuration mode.  
router(config-serial1)# ➤ Configuration is possible in this mode.  
router(config-serial1)# encapsulation ppp ➤ Sets the PPP mode.  
router(config-serial1)# ip address 131.12.1.1 255.255.0.0 ➤ Sets  
the IP address as "131.12.1.1/16 bit mask."  
router(config-serial1)# no shutdown ➤ Makes the interface up.  
router(config-serial1)# end ➤ Exits from the configuration menu.  
router # show interface serial 1 ➤ Checks the status of the serial  
interface 1.
```

[Example] Added Commands During PAP Configuration (Server)

If the router functions as a server, it means the AP2520 router functions as the PPP authentication server.

```
router(config)# user addpac password router1 normal ☞ Registers the user name (addpac) and the password (router1) with the normal priority in the server.
```

```
router (config)#interface serial 1 ☞ Enters into the interface configuration mode.
```

```
router(config-serial1)# encapsulation ppp ☞ Sets the PPP mode.
```

```
router(config-serial1)# ppp authentication pap ☞ Sets the PPP authentication mode as PAP for the serial 1 interface.
```

```
router(config-serial1)# 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-serial1)# ppp peer default-ip address 132.12.1.2 ☞ When the other router receives the serial interface IP from this router, this command enables the router 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-serial1)# ppp timeout 100 ☞ Sets PPP connection negotiation timeout value as 100 seconds.
```

```
router(config-serial1)# end ☞ Exits from the configuration menu.
```

```
router #
```

```
Serial1 LCP: TIMEOUT
```

```
Serial1 LCP: O CONFREQ id=1
```

```
Serial1 BCP: TIMEOUT
```

```
Serial1 BCP: O CONFREQ id=1
```

```
Serial0 LCP: TIMEOUT
```

```
Serial0 LCP: O CONFREQ id=1
```

```
Serial0 BCP: TIMEOUT
```

```
Serial0 BCP: O CONFREQ id=1
```

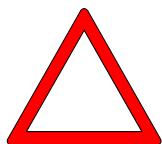
```
router # debug ppp packet ☞ Stops PPP packet debugging.
```

[Example] Added Commands During PAP Configuration (Client)

This is when the AP2520 router is used as a PPP CallIn on the client side.

```
router (config)#interface serial 1  ⚡ Enters into the interface
configuration mode.
router(config-serial1)# encapsulation ppp  ⚡ Sets the PPP mode.
router(config-serial1)# ppp authentication pap  ⚡ Sets the PPP
authentication mode as PAP for the serial 1 interface.
router(config-serial1)# ppp pap sent-username addpac password
router1  ⚡ Sends the user name and the password that were saved in the
server during PPP connection.
router(config-serial1)# ppp timeout 100  ⚡ Sets PPP connection
negotiation timeout value as 100 seconds.
router(config-serial1)# end  ⚡ Exits from the configuration menu.
router #
    Serial1 LCP: TIMEOUT
    Serial1 LCP: O CONFREQ id=1
    Serial1 BCP: TIMEOUT
    Serial1 BCP: O CONFREQ id=1
    Serial0 LCP: TIMEOUT
    Serial0 LCP: O CONFREQ id=1
    Serial0 BCP: TIMEOUT
    Serial0 BCP: O CONFREQ id=1
router # debug ppp packet  ⚡ Stops PPP packet debugging.
```

Caution



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

[Example] Added Commands During CHAP Configuration (Server)

This is when the AP2520 router functions as a PPP authentication server in the server side.

```
router(config)# user addpac password router1 normal ➤ Registers the
user name (addpac) and the password (router1) with the normal priority
in the server.

router (config)#interface serial 1 ➤ Enters into the interface
configuration mode.

router(config-serial1)# encapsulation ppp ➤ Sets the PPP mode.

router(config-serial1)# ppp authentication chap ➤ Sets the PPP
authentication mode as CHAP for the serial 1 interface.

router(config-serial1)# 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-serial1)# ppp peer default-ip address 132.12.1.2 ➤
When the other router receives the serial interface ID from this router,
this command sets the IP address as the default address "130.1.1.2."

router(config-serial1)# ppp timeout 100 ➤ Sets PPP connection
negotiation timeout value as 100 seconds.

router(config-serial1)# end ➤ Exits from the configuration menu.
router #

Serial1 LCP: TIMEOUT
Serial1 LCP: O CONFREQ id=1
Serial1 BCP: TIMEOUT
Serial1 BCP: O CONFREQ id=1
Serial0 LCP: TIMEOUT
Serial0 LCP: O CONFREQ id=1
Serial0 BCP: TIMEOUT
Serial0 BCP: O CONFREQ id=1

router # debug ppp packet ➤ Stops PPP packet debugging.
```

[Example] Added Commands During Chap Configuration (Client)

This is when the AP2520 router functions as a PPP CallIn client in the client side.

```
router (config)#interface serial 1  ⚡ Enters into the interface
configuration mode.
router(config-serial1)# encapsulation ppp  ⚡ Sets the PPP mode.
router(config-serial1)# ppp authentication chap  ⚡ Sets the PPP
authentication mode as CHAP for the serial 1 interface.
router(config-serial1)# ppp chap hostname addpac  ⚡ If the user name
that was saved in the server during PPP CHAP connection is different
from the user name of the client router, this command sends the user
name of the server side.
router(config-serial1)# ppp chap password router1  ⚡ Sets the user
name of the server side to check the password that the server sends during
PPP CHAP connection.
router(config-serial1)# ppp timeout 100  ⚡ Sets PPP connection
negotiation timeout value as 100 seconds.
router(config-serial1)# end  ⚡ Exits from the configuration menu.
router # debug ppp packet  ⚡ Decodes PPP packets.
router #
    Serial1 LCP: TIMEOUT
    Serial1 LCP: O CONFREQ id=1
    Serial1 BCP: TIMEOUT
    Serial1 BCP: O CONFREQ id=1
router # debug ppp packet  ⚡ Stops PPP packet debugging.
```

4.5.3. Frame-Relay Configuration

Information

The frame-relay mode is a transmission method of the frame layer that is used in the frame-relay data communication network. By connecting the WAN (serial) port of the PassFinder AP2520 router to the DSU/CSU, the operator can transmit frame-relay packets at the speed of T1/E1.

As the transmission line quality improves and error occurrence rate significantly drops in the transmission line, the frame-relay minimizes various control functions and the error recovery function which occupies significant amount of the data-link layer, and implements only core functions that are necessary for data transmission in the network. In this way, the frame-relay simplifies the processing steps and enables the DTE to perform other functions. As a result, the frame-relay is a kind of protocol that realizes high-speed transmission and minimum delay.

The WAN (serial) port of the PassFinder AP2520 router that is set as the frame-relay mode is applied to the physical layer and the data link layers among OSI 7 layers. Data link layers include the Link Access Procedure on the D channel (LAPD) complying with ITU-T Q.922 and Q.921 and the Link Access Protocol for Frame Relay (LAPF) complying with ITU-T Q.922. The WAN (serial) port can use several sub-interfaces in one physical link and use these sub-interfaces as virtual circuits.

The frame-relay parameters include Data Link Connection Identifier (DLCI) values that are frame-relay addresses. Communication network service providers such as Korea Telecom or Dacom (in Korea) allocate these values.

The PassFinder AP2520 router supports both of static mapping and the inverse-ARP in the frame-relay network. LMI types that the PassFinder AP2520 router supports are ANSI and Q.933a. The PassFinder AP2520 router also complies with IETF(RFC1490) standard for the encapsulation method.

The PassFinder AP2520 router functions not only as a frame-relay access router but also as a frame-relay switch. The PassFinder AP2520 router can be used under Permanent Virtual Circuit (PVC) environment.

[Procedure]

Setting the PassFinder AP2520 router as a frame-relay access router (with PVC)

Step	Operation
1	Enter into the interface configuration mode.
2	Give frame-relay encapsulation protocol to the interface.
* Configuration of the main interface	
3	Move to the IP configuration mode.
4	Give an IP address to the interface.
5	Set the static or the dynamic map.
6	Set the counter and the timer for the LMI. (Optional)
7	Set other necessary parameters.
8	Make the (main) interface up.
* Configuration of the sub-interface	
1	Create a sub-interface and enter into the corresponding configuration mode.
2	Move to the IP configuration mode.
3	Give an IP address to the interface.
4	Set the static or dynamic map.
5	Set the counter and the timer for the LMI. (Optional)
6	Set other necessary parameters.
7	Make the (main) interface up.
* Common	
1	With "show running-config" command, check if configuration has been accurately made.
2	With "show interface" command, check if the interface is normally operating.
3	(In case of a fault) use "debug" command to find and recover faults in the network connection.

[Related Commands and Syntax]

- **interface { Ethernet /serial } { 0 / 1 }**

Selects the serial interface, and enters into the interface configuration mode.

- **interface { Ethernet /serial } <X.Y>**

1. Selects the serial interface, sets the sub-interface for the selected serial interface, and enters into the interface configuration mode. (X: Main interface number, Y: Sub-interface number for the selected interface)
2. The sub-interface of the PassFinder AP2520 router shall support only the point-to-point feature. To use the multipoint feature, the operator needs to use the main interface.
3. An optional command to use a sub-interface.
4. The sub-interface is supported only when the frame-relay encapsulation is used in the serial line.

- **encapsulation { hdlc / ppp / frame-relay }**

Sets the serial mode for the interface. The PassFinder AP2520 router supports only IETF encapsulation for the frame-relay encapsulation type.

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

Sets the IP address for the interface.

- **frame-relay map { ip/bridge } [protocol_address] <dlci #>**

1. Statically maps the next-hop protocol address and the DLCI number according to that address.
2. For the bridge option using method, see "Bridging Configuration."
3. **No static map can be used as long as a sub-interface is used. In this case, use "frame-relay interface-dlci <dlci-number>" command.**

- **frame-relay interface-dlci <dlci_number>**

1. With the inverse-ARP of the frame relay, this command dynamically maps next-hop protocol address and the DLCI number that is used to

reach that address. (An optional command for dynamic mapping. Dynamic mapping cannot be made at the same time with static mapping for an interface.)

2. This command can be used for both of the main interface and the sub-interface.

- **frame-relay inverse-arp [interval <Interval-value(sec)>]**

Sets the interval that the router can send the inverse-ARP request to the frame-relay peer in the other side. (Default: 15)

- **frame-relay access-rate [<max_access_rate(bps)> [input <max_input_rate(bps)> [output <max_output_rate(bps)>]**

1. Sets the sum of CIR values in the frame-relay interface. To use a frame-relay PVC in the interface lower than E1, use this command.
2. "Input" and "Output" options decide the maximum access rate for the input and the output respectively.
3. The sum of the inputs and outputs shall not exceed total Max_Access_Rate.

- **frame-relay lmi-n391 <events(1~255)>**

Sets the polling counter for the frame-relay full status.

- **frame-relay lmi-n392 <events(1~10)>**

Sets the threshold for the frame-relay LMI error.

- **frame-relay lmi-n393 <events(1~10)>**

Sets the event counter that is monitored in the frame-relay LMI.

- **frame-relay lmi-t391 <time(5~30)>**

Sets the time-interval that is polled in the frame-relay DTE.

- **frame-relay lmi-t392 <time(5~30)>**

Sets the verification timer of the interval that is polled in the frame-relay DCE.

- **frame-relay parameter**

Enters into the parameter setting mode of the frame-relay BECN and CIR.

- **becn-enable**

Enable the Becn function in the frame-relay parameter configuration mode.

- **bc { in / out } <bc-value>**

Sets the committed burts size to input or output the corresponding port in the frame-relay parameter configuration mode.

- **be { in / out } <be-value>**

Sets the excess burst size in the frame-relay parameter configuration mode to input or output the corresponding port.

- **cir { in / out } <cir-value>**

Sets the committed information rate to input or output the corresponding port in the frame-relay parameter configuration mode.

- **mincir { in / out } <mincir-value>**

Sets the minimum acceptable CIR to input or output the corresponding port in the frame-relay parameter configuration mode.

- **frame-relay lmi-type {ansi/q.933a}** (To be implemented)

1. Sets the LMI type of the frame relay. (The default is ANSI.)
2. "q.933a" is an LMI for the frame-relay SVC service.

- **frame-relay switching** (To be implemented)

Sets the router as a frame-relay switch. (An optional command to set the router as a frame-relay PVC switch.)

- **frame-relay route <in-dlci> <out-interface> <out-dlci>** (To be implemented)

Routes the frame that came to the <In-DLCI> of the switch to the <Out-DLCI> of the <Out-Interface> when the router functions as a frame-relay switch.

- **frame-relay intf-type {dce/dte/nni}**

Designates the frame-relay interface type. (In the default, the interface type is DCE or NNI when the router functions as a frame-relay switch in the DTE mode.)

- **show running-config**

Shows current configuration.

- **show interface {Ethernet/serial} {<X.Y>}**

1. Shows the status of the interface.
2. "X" represents the main interface number, and "Y" represents the sub-interface number of the interface.

- **show frame-relay lmi**

Shows frame-relay LMI statistics for the corresponding interface.

- **show frame-relay pvc**

Shows frame-relay PVC statistics for the corresponding interface.

- **show frame-relay map**

Shows the frame-relay map table for the corresponding interface.

- **debug frame-relay { lmi/packet }**

1. Decodes and shows PPP low level packets.
2. "LMI" option decodes packets that are related with LMI data exchange.
3. "Packet" decodes PPP low level packets.

[Example] Frame-Relay Access Router Configuration (When main-interface is used)

```
router(config)# interface serial 0  ⚡ Enters into the interface
configuration mode.

router(config-serial0)#  ⚡ Configuration is possible in this mode.

router(config-serial0)# encapsulation frame-relay  ⚡ Encapsulate as
frame-relay.

router(config-serial0)# ip address 131.12.1.1 255.255.255.0  ⚡ Sets
the IP address as "131.12.1.1/24bit mask."

router(config-serial0)# no shutdown  ⚡ Makes the interface up.

router(config-serial0)# frame-relay map ip 131.12.1.2 100  ⚡ Sends
the IP traffic of which next-hop address is "131.12.1.2" to the virtual
circuit of the local DLCT No. 100.

router(config-serial0)# frame-relay interface-dlci 100  ⚡ Makes a
frame-relay map with the interval-ARP that is incoming through the DLCI
No. 100. This configuration is to perform dynamic mapping according to
the inverse-ARP. Dynamic mapping and static mapping can be used at the
same for the same port.

router(config-serial0)# frame-relay inverse-arp interval 20  ⚡ sets
the inverse-ARP request interval of the corresponding interface as 20
seconds. (The default is 15 seconds.)

router(config-serial0)# exit  ⚡ configuration mode exits.

router# show running-config  ⚡ shows assigned Configuration.

    interface ether0.0
    no ip address
    Operation is up
    !
    interface serial0
    ip address 131.12.1.1 255.255.255.0
    Encapsulation FRAME-RELAY
    Operation is up
    frame-relay map ip 131.12.1.2 100
    !
    !
    interface serial1
    no encapsulation
```

[Example] Frame-Relay Access Router Configuration

(When sub-interface is used)

```
Router(config)# interface serial 0  ⚡ Enters into the interface
configuration mode.
router(config-serial0)#  ⚡ Configuration is possible in this mode.
router(config-serial0)#encapsulation frame-relay  ⚡ Encapsulates as
the frame-relay.
router(config-serial0)# interface serial0.1  ⚡ Creates sub-interface
s0.1 and starts configuration.
router(config-serial0.1)# ip address 131.12.1.1 255.255.255.0  ⚡
Sets the IP address as "131.12.1.1/16 bit mask."
router(config-serial0.1-ip)# exit  ⚡ Returns to the previous
configuration mode.
router(config-serial0.1)# no shutdown  ⚡ Makes the interface up.
router(config-serial0.1)# frame-relay interface-dlci 100  ⚡ Uses the
inverse-ARP that is incoming through the DLCI No. 100 to set a frame-relay
map. This configuration is to perform dynamic mapping according to the
inverse-ARP. In the sub-interface, static mapping cannot be used.
router(config-serial0.1)# exit  ⚡ Exits from the configuration mode.

interface ether0.0
  no ip address
  Operation is up
!
interface serial0
  no ip address
  Encapsulation FRAME-RELAY
  Operation is up
!
!
interface serial0.1
  ip address 131.12.1.1 255.255.255.0
  Operation is up
  frame-relay interface-dlci 100
```

```
!  
!  
interface serialno  
encapsulation  
!
```

4.6. Routing Configuration

Information



The PassFinder AP2520 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 network in different manager's domain. IGP includes RIP, OSPF and IS-IS, and EGP includes BGP. The PassFinderAP2520 Gateway supports only IGP – RIP and OSPF.

To use routing protocol in the PassFinderAP2520 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 following when selecting 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 the PassFinder AP2520 Gateway at the same time. If several kinds of routing protocol is used in one Gateway, each kind of 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 order of static route, OSPF route, RIP route and default

route.

4.6.1. 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:

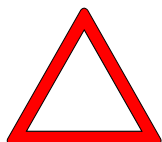
- If routing software cannot create a proper route to send packets to a certain destination
- If the network is small or is not complex so it is easy to configure a static route, Or if the user does not want to have any packet such as route update packet and so on that may give load to the network
- If the user wants to send all packets of which destinations do not appear in the routing table to a certain next-hop address as 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 the PassFinderAP2520 Gateway. Therefore, only when the Gateway does not find any path, the Gateway uses the default route.

[Procedure]

Step	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 to set during setting up the static route shall be directly connected with the Gateway to set.
2. The default route is one of static routes, and the setting method of the default route 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**

Enables or disables a certain routing process.

- **route** *<destination-IP-network>* *<address-mask>* { *<next-hop-address>* / **Ethernet** / **null** } [(0/1) / *<null_int_#>*] [*<sub_int_#>*]

1. Designates the route to send the packet to the destination address.
2. When using the candidate default (default route,) both of the destination address and the mask filed shall be zero.
3. The Gateway shall 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 that uses a null interface.

- **show route**

Check the routes in the routing table.

- **show static**

Check the static route that has been set.

[Example] Static Routing Configuration and Usage

```

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

router(config)# ip routing  Enables 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
packet, whose destination address is 130.2.0.0/24bit, 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 address
132.20.1.1. (Candidate Default; Setting of Default route)

router(config)# exit  Exit from setting mode.

router(config)# show route  Shows routing table.

```

Destination	Network-Mask	Gateway	Cost	Interface	TTL	Protocol
130.1.1.0	255.255.255.0	130.1.1.1	1	serial0	0	DIRECT
130.2.0.0	255.255.0.0	131.20.1.1	1	serial0	0	STATIC
0.0.0.0	0.0.0.0	131.20.1.1	1	serial0	0	STATIC

```

router(config)# show static  Shows routing table setted as
static.

```

Destination	Network-Mask	Gateway	Cost	Interface	TTL	Protocol
130.1.1.0	255.255.255.0	130.1.1.1	1	serial0	0	DIRECT
130.2.0.0	255.255.0.0	131.20.1.1	1	serial0	0	STATIC
0.0.0.0	0.0.0.0	131.20.1.1	1	serial0	0	STATIC

130.2.0.0	255.255.0.0	131.20.1.1	1	serial0	0	STATIC
0.0.0.0	0.0.0.0	131.20.1.1	1	serial0	0	STATIC

4.6.2. RIP Configuration

Information



Routing Information Protocol (RIP) is one of representative Interior Gateway Protocol (IGP.) Although RIP was introduced long time ago, RIP is still widely used. RIP is usually used in a small scale and homogeneous network (using a single mask.) RIP is one of most representative protocol that uses Distance-Vector, and RFC 1058 describes RIP standards.

RIP uses User Datagram Protocol (UDP) as the packet to exchange routing information, and the PassFinder AP2520 router updates routing information every 30 seconds. This process is called the advertising process. If the router does not receive updated packets from another router more than for 180 seconds, the router considers that the other router is not available any more. If the router does not receive any updated information for more than 240 seconds, the router permanently deletes the other router from the routing table.

For the metric, RIP uses the hop-count. The metric is a value that shows the difference between two paths where there are several paths from the router to the destination. The hop-count is number of routers that the route encounters to reach the destination. Therefore, the metric of the directly connected network is "0," and the maximum value of the metric that RIP can have is 15. (If the metric is 16, the network is considered unreachable.) Due to these characteristics, it is not recommended to use RIP in a large network.

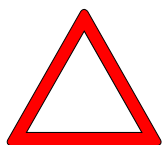
RIP sends updated information only through the interface that the manager designated. If no RIP is set in an interface, no RIP updated information can be sent through this interface. Therefore, to use RIP, the user shall make RIP related configuration in the corresponding interface.

The biggest difference between RIP version 2 and RIP version 1 is that RIP version 2 supports Variable Length Subnet Mask (VLSM) and can be used in a heterogeneous network. Besides, RIP version 2 uses the multicast for routing

update.

[Procedure]

Step	Operation
1	Go to the configuration mode.
2	Enable the RIP process.
3	Go to the interface configuration mode.
4	Enter into the IP configuration mode..
5	Enable RIP protocol in the interface in which RIP is going to be used. ((If necessary) set RIP version to use.)
6	(If necessary) change RIP related setting.
7	Set other necessary parameters (authentication and so on.)
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 a fault) use “debug” command to find fault causes and take proper measures.

Caution

1. The PassFinder AP2520 router support authentication among RIP neighbors.
(The simple text method and the MD5 encryption method.)
2. The PassFinder AP2520 router can enable/disable split-horizon, holddown-down and poison-reverse for each interface as using the RIP option.
3. RIP versions to be used in the PassFinder AP2520 router shall be defined for each interface. Unless there is any separate setting, RIP version 1 is used.

[Related Commands and Syntax]

- **router { static/rip/ospf }**
Enables or disables a certain routing process.
- **rip send {1/2/12}**
Decides to which RIP – v1, v2 or v1/v2 – to send routing information through the corresponding information.

- **rip receive {1/2/12}**

Decides which RIP – v1, v2 or v1/v2 – receives routing information through the interface.

- **rip metric <metric_value>**

1. Designates RIP metric (hop-count) for routing information that is sent through the corresponding information.
2. If the metric value is 16 or higher, RIP routing considers the network unreachable and drops the network from the routing table.

- **rip {default-information/static-information}**

1. When the router sends RIP routing information, the router re-distributes static route information or default route information to the RIP process before sending RIP routing information.
2. If the user uses this command, the user does not need to set default/static router information in every network device. Instead, the user only needs to enable RIP routing. Then, every network device will have the same route table.

- **rip auth-type {simple/md5}**

An optional command to decide whether to use authentication or not when the interface and the neighboring router exchange routing information. The manager shall set the authentication method – the simple text method or the MD4 encryption method.

- **rip auth-key <key-string>**

Sets key value for authenticating routing information exchange between the interface and the neighboring router. (This key value must be set when authentication is used, and it must be the same with the key value of the neighboring router.)

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

Enables options - split-horizon, hold-down timer and poison reverse. Normally, it is recommended to enable all these options in the RIP network. However, in the hub port equipment of the Non-Broadcast Multi-Access

(NBMA) such as frame-relay, disable the split-horizon option.

- **show route**

Checks the routes in the routing table.

- **show router**

Checks the enabled routing process.

- **show rip**

Checks RIP status of each interface.

- **debug rip**

Decodes RIP packets exchanged by the router and shows status of RIP packets.

[Example] RIP Configuration and Usage

```
router# config
router(config)# ip routing ☞ Enables IP routing.

Router(config)# router rip ☞ Enable the RIP process.

Router(config)# interface Ethernet 0.0 ☞ Enters into a configuration
mode for the sub-interface 0 of the Ethernet interface 0.

Router(config-ether0.0)# ip rip send 12 ☞ Set RIP v1/v2 through the
corresponding interface.

Router(config-ether0.0) # ip rip receive 1 ☞ Receives only RIP v1
packets among advertise packets, which come through corresponding
interface.

Router(config-ether0.0) # ip rip auth-type simple ☞ Set Simple
Authentication for RIP information exchange through corresponding
interface.

Router(config-ether0.0)# ip rip convergence split-horizon ☞ In
RIP Process, this enables Split-Horizon as Convergence Mechanism.

Router(config-ether0.0)# ip rip convergence poison-revers ☞ In
```

RIP Process, this enables poison-reverse as Convergence Mechanism.

Router(config-ether0.0)# end ☞ Exits from setting mode.

Router # show router ☞ Shows Enabled Routing Process.

Current Routing Information :

OSPF(Open Shortest Path First) : DISABLE

RIP(Routing Information Protocol) : ENABLE

Static Routing : ENABLE

Router # show rip ☞ Shows contents of configured RIP Process.

RIP Configuration : serial0

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

4.6.3. OSPF Configuration

Information



Open Shortest Path First (OSPF) is a kind of Interior Gateway Protocol (IGP) that has been developed by the OSPF working group of the Internet Engineering Task Force (IETF,) and it uses the link state algorithm. Since OSPF has been engineered to well support the IP network, OSPF supports IP subnet and toggling of exchanged routing information. Also, OSPF supports packet authentication with the neighboring router, and uses IP multicast when exchanging routing information packet.

The PassFinder AP2520 router supports OSPF version 2 specifications that are described in the Internet RFC 1583. The following is some of major functions implemented in the PassFinder AP2520 router by the OSPF.

- Stub Area: Defines the stub area.
- Route Redistribution: Acquires routing information by IP routing protocol and redistributes routing information to another routing protocol.
- Authentication: Supports plain text and MD5 authentication between neighboring routers within the same area.
- Routing Interface Parameter: Enables the manager to set interface parameters – interface output cost, retransmission interval, interface transmit delay, router priority and authentication key.
- Area Boarder Router (ABR): If the router covers more than two OSPF areas, the PassFinder AP2520 router functions as an area boarder router.

There are several areas including the backbone area in one routing domain of the OSPF network.

- Routing Domain: The routing domain means an area that performs routing processing with single routing protocol. If a network uses separate routing protocol, OSPF considers this network as an outside network. One OSPF

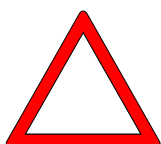
routing domain consists of one backbone area and several areas.

- Area: An area consists of several networks, and each area has a network configuration diagram called the status database. All routers in the same area have a same databases. The area can communicate with the backbone area only through Area Boarder Router (ABR.) In most cases, routers within the area have internal area paths, other area paths and external routing paths. To remove a path, the operator needs to define the area as a stub area. Then, only an internal area path will be available.
- Backbone Area: The backbone area connects areas each other, and its value is always "Area 0." Every OSPF routing domain has one backbone area, and every area shall be connected to the backbone area. However, if any area cannot be directly connected to the backbone area due to network design, the area shall be connected to the backbone area through the virtual link (a kind of OSPF tunnel.)

[Procedure]

Step	Operation
1	Go to the configuration mode.
2	Go to the interface configuration mode.
3	Enter into the IP configuration mode..
4	Enable OSPF protocol in the interface.
5	Set the area-ID to which the interface is going to belong.
6	Set other necessary parameters (authentication and so on.)
7	Make the (main) interface up.
8	Enable the OSPF process.
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 a fault) use “debug” command to find fault causes and take proper measures.

Caution



When setting the OSPF, enable the OSPF process after setting OSPF in the interface. If the user does not keep the above procedure, OSPF may not normally function.

[Related Commands and Syntax]

- **router { static/rip/ospf }**
Enables or disables a certain routing process.
- **ospf enable**
Enables the OSPF in the corresponding interface.
- **ospf area-id <ospf-area-value>**
Sets the area-ID to which the corresponding interface is going to belong.

- **ospf cost** <cost-value>

An optional command to statically set OSPF cost value for the manager.

- **ospf auth-type** { simple/md5 }

An optional command to use authentication when the interface and the router in the area where the interface belongs exchange routing information. The manager shall set the authentication method – the simple text method or MD5 encryption method.

- **ospf auth-key** <key-string>

Sets key value for authenticating routing information exchange between the interface and the neighboring router. (This key value must be set when authentication is used, and it must be the same with the key value of the router in the same area.)

- **ospf auth-id** <key-id>

Sets key identifier for authenticating routing information exchange between the interface and the neighboring router. (This key identifier must be set when authentication is used, and it must be the same with the key identifier of the neighboring router.)

- **ospf priority** <priority-value>

1. Decides the priority to become DR when the OSPF select DR/BDR/Drouter between the interface and the neighboring router. The priority range is 1 ~ 255. The higher the value is, the higher the priority is.
2. The default is 1.

- **ospf hello-interval** <interval-time>

1. Sets the hello interval that the router exchanges with a neighboring router through the interface to configure the adjacency. The hello interval shall be the same with the hello interval of the neighboring router.
2. The default is ten seconds. However, the default is 30 seconds in the frame-relay network.

- **ospf dead-interval** *<interval-time>*
 1. Sets information of the router after a neighboring router declares dead.
 2. The default is four times of the hello-interval.

- **ospf poll-interval** *<interval-time>*
 1. Sets the interval for the polling packet.
 2. The default is same with the hello-interval.

- **ospf retransmit-interval** *<interval-time>*
 1. Sets retransmission interval when the router loses link state advertisement value.
 2. The default is same with the hello-interval.

- **ospf default-router**
 1. Notifies that the router is the default router to the OSPF network.
 2. Same command as "default-information originate" of other routers.
 3. This command can be executed only when the router is an ABR.

- **ospf neighbor** *<neighbor_ip_address>*
 1. Statically sets the neighbor.
 2. Used for the HUB interface of the frame-relay network that is one of representative Non-Broadcasting Multiple Access (NBMA) networks.

- **ospf network { broadcast / non-broadcast / point-to-multipoint }**
 1. Defines interface characteristics in OSPF.
 2. Can be used only in the serial interface.
 3. Statically sets the neighbor.

- **show route**

Checks the routes in the routing table.

- **show router**

Checks the enabled routing process.

- **show ospf {area / config / debug / interface / lsdb / nbma-nbr / neighbor /**

nexthop}

1. Checks OSPF status of each option.
2. Each option has its own function as follows:
 - 1) area: Displays information of the area..
 - 2) Config: Displays information of current configuration.
 - 3) Debug: Displays currently enabled debugging function.
 - 4) interface: Shows information of the interface in which currently set OSPF is enabled.
 - 5) Isdb: Shows the database of the currently configured Link State Advertisement (LSA.)
 - 6) nbma-nbr: Shows neighbor relationship established in the NBMA network such as the frame-relay.
 - 7) neighbor: Shows the neighbor router that is currently configured and according relationship.
 - 8) nexthop: Shows information of the next-hop that has been made by the OSPF process.


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

1. Decodes OSPF packets exchanged in the network and provides operation information of the OSPF.
2. Each option has its own function as follows:
 - 1) all: Enables all debugging information that is related with OSPF that the PassFinder router supports.
 - 2) error: Decodes error packets among OSPF related packets during OSPF processing.
 - 3) event: Decodes packets for the event such as setting a neighbor and so on among OSPF related packets during OSPF processing.
 - 4) packet: Decodes all OSPF related packets.
 - 5) spf: Shows Shortest Path First (SPF) process related parts among OSPF events.

[Example] OSPF Configuration and Usage

```
Router# config
router(config)# ip routing  ☞ Enables IP routing.
router(config)# interface Ethernet 0 0  ☞ Enters into a configuration
mode for the sub-interface 0 of the Ethernet interface 0.
router(config-ether0.0)# ip address 130.1.1.1 255.255.255.0  ☞ Sets
the IP address as "130.1.1.1/24bit."
router(config-ether0.0)# ospf enable  ☞ Enables the OSPF in the
interface.
router(config-ether0.0-ip)# ospf area-id 10  ☞ Makes the Ethernet
interface belong to OSPF Area 10. Through this, the corresponding network
address enters into OSPF Process area 10.
router(config-ether0.0)# ospf priority 10  ☞ If DR is selected, sets
Priority 10 for the router to make Nego against the other router.
router(config-ether0.0)# ospf cost 5  ☞ Sets that the Cost (metric)
value should be advertised as 5.
router(config-ether0.0)# int serial 0  ☞ Enters into the serial 1
interface configuration mode.
router(config-serial0)# ip address 135.1.1.1 255.255.255.0  ☞ Sets
the IP address as "135.1.1.1/24bit."
router(config-serial0)# ospf enable  ☞ Enables OSPF in the interface.
router(config-serial0)# ospf area-id 0  ☞ Makes the serial interface
0 belong to OSPF Area 0. Through this, the corresponding network address
enters into OSPF Process area 0.
router(config-serial0)# ospf priority 1  ☞ If DR is selected, sets
Priority 1 for this router to make Nego against the other router.
router(config-serial0)# ospf cost 10  ☞ Sets that the Cost (metric)
value for the interface should be advertised as 10.
router(config-serial0)# ospf network broadcast  ☞ Sets that the
features for this interface are broadcasted.
router(config-serial0)# exit  ☞ Returns to the previous configuration
mode.
router(config)# router ospf  ☞ Enables the OSPF process. From this
point, the OSFP process operates. The user shall set this command after
```

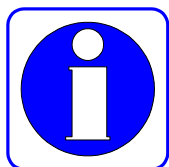
setting the OSPF for the line interface to normally operate the OSPF. If configuration for the interface changes after the OSPF process operates, use **"no router ospf"** command to disable the OSPF process and enable it again.

router(config)# exit  Returns to the previous mode (Exec mode.)

router# copy running-config  Saves the configuration file.

4.7. 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 unqualified user's access to the inside network from outside and disclosure of information.

The PassFinder AP2520 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 the PassFinderAP2520 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 to normally operating the access-list. If there is no matching condition, software rejects the corresponding packet. (Default)

The PassFinderAP2520 Gateway supports 30 standard access-lists (List # 0~29) and 30 extended access-list(List # 30 ~ 59.)

[[Procedure]

Step	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 when every condition cannot be considered.

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

As 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 또는 protocol name (Ex: TCP, ICMP, UDP IP and so on)

3) source : Source Network Address,

4) Source-wildcard : Source Address의 Inverse Mask

5) Destination : Destination Network Address

6) destination-wildcard : Destination Address의 Inverse Mask

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 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 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
```

4.8. NAT(Network Address Translation) Configuration

Information One of problems of the Internet is that available IP address space 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, certified 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 addresses.

- 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 as using 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 as using 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.

The PassFinder AP2520 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 on an external, registered IP address.

1. The PassFinder AP2520 Gateway currently supports only dynamic address translation.
2. The PassFinder AP2520 Gateway supports 256 NAT addresses.
3. The PassFinder AP2520 Gateway only static routing for NAT.

[Procedure]

Step	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 statistically 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 Nap 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>* **natstatic-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**}

As 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. To 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 during the latter half of 2000.
 4. IP-Address for PAT: The address of a terminal whose port shall be statically set. IP-Address for PAT is one of local inner network addresses. As using 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. Selects options for timeout value when the session is in idle status during PAT conversion.
 2. Details of each option are as follows:
 - 1) Fin-timeout: Sets timeout after TCP Fin. The default is 10 seconds.
 - 2) icmp-timeout: Sets timeout after ICMP Session Idle. The default is 60 seconds.
 - 3) sys-timeout: Sets timeout after TCP sync Idle. The default is 60 seconds.
 - 4) tcp-timeout: Sets timeout after TCP Session Idle. The default is 3,600 seconds.
 - 5) udp-timeout: Sets timeout after UDP Session Idle. The default is 60 seconds.

- **show nat-list** [*nat-list-number*]
 1. Shows NAT-list that has been set.
 2. If no NAT-List-Number is designated, this command will show status of all NATs.

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

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

- **show running-config**

Shows 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 ➤ Defines NAT pool that the internal
packet can take "2.2.2.X/24bit" address as the source address when
going outside.
router (config)# nat-list 0 nat static-entry 1.1.1.253
2.2.2.254 ➤ Defines NAT pool that the internal packet can take
"2.2.2.254" address when going 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 ➤ Defines NAT pool that the packet can take "2.2.2.253"
address when going outside from the host whose source is "1.1.1.254."
router (config)# nat-list 0 nat timeout 250 ➤ When session is
in Idle status, sets the time value to turn into address free state
as 250 seconds.
router (config)# interface Ethernet 0 0 ➤ Enters into the
configuration mode of the interface Ethernet 0.0
router (config-ether0.0)# ip address 1.1.1.3 255.255.255.0
➤ Allocates addresses to the Ethernet 0.0 interface. One of Indise
local addresses shall be selected.
router (config-ether0.0)# nat-group 0 nat ➤ Applies NAT pool
with NAT-list 0 to the Ethernet 0.0 interface. NAT shall be set
in the inside network always.
router (config-ether0.0)# end ➤ Exits from the configuration.
router # sh nat-list 0 ➤ Shows setting of NAT List No. 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  Shows NAT format in ethernet
interface 0.0 and present NAT table.
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  Shows 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 serial0

    ip address 132.1.1.1 255.255.255.0

    Encapsulation HDLC

    Operation is UP!









interface serial1

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  Sets PAT that the
internal packet can take IP address 2.2.2.2 as the source address
when going outside.
router (config)# nat 0 nat static-entry udp 1000 1.1.1.4 1.1.1.5
 Statically sets that packets should be sent to "1.1.1.4" and
"1.1.1.5" of internal host when Application (Dial Pad, Wow Call or
UDP No. 1000 port) tries to access to the network from outside. If
there are several internal hosts set, load is distributed in order.
router (config)# interface Ethernet 0 0  Enters into the
configuration mode of the interface Ethernet 0.0
router (config-ether0.0)# ip address 1.1.1.3 255.255.255.0
 Allocates addresses to Ethernet 0.0 interface. The address shall
be one of Indise local addresses.
router (config-ether0.0)# nat-group 5 pat  Applies PAT pool
that is NAT-list 5 to Ethernet 0.0 interface. NAT/PAT shall be set
in the inside network always.
router (config-ether0.0)# end  Exit from setting mode.
router # sh nat-list 5  Shows setting 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  Shows NAT/PAT setting in
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  Shows present 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 serial0

    ip address 132.1.1.2 255.255.255.0

    Encapsulation HDLC

    Operation is UP

interface serial1

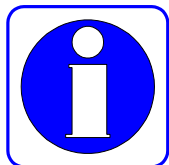
    no encapsulation

```

4.9. DHCP(Dynamic Host Configuration Protocol)

Configuration

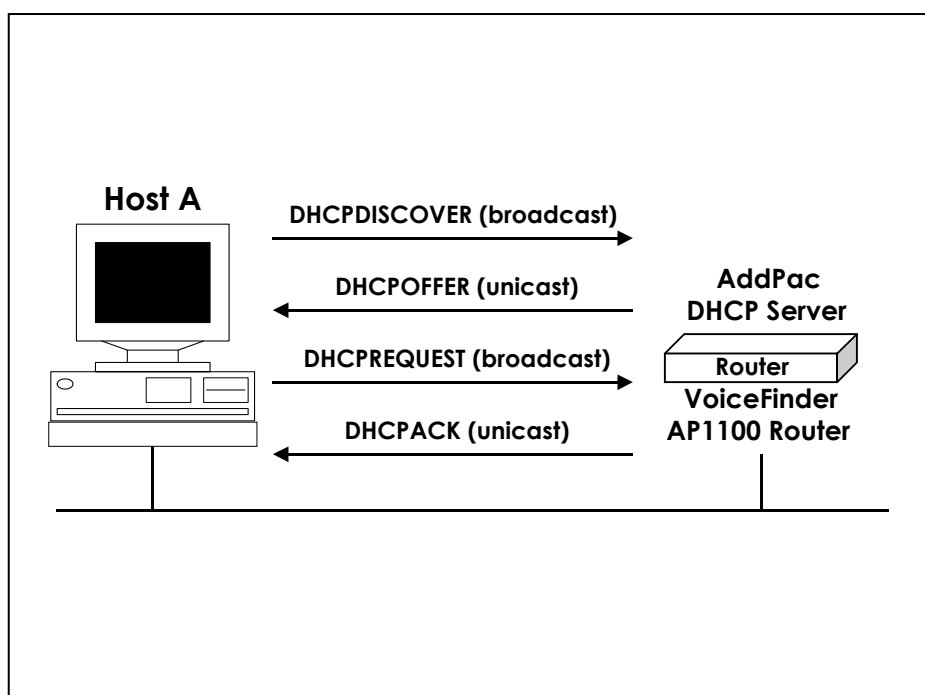
Information Dynamic Host Configuration Protocol (DHCP) automatically allocates IP addresses to DHCP clients.



The DHCP function of the PassFinder AP2520 Gateway uses the address pool that has been set in the Gateway to allocate IP addresses to DHCP clients and manage IP addresses.

If software of the PassFinder AP2520 Gateway does not 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 that the network manager has set.

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 the PassFinder AP2520 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 lower 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 use the DHCP function. (For example, servers and printers whose addresses shall be fixed.)
- If necessary, the user shall define DHCP options to use in the Gateway – the default Gateway and the DNS server.

PassFinder AP2520 supports not only DHCP Server function but also DHCP Clients and Relay functions. If it configured DHCP in address field instead IP Address, AP2520 operate in DHCP Client mode.

[Procedure-DHCP Server]

Step	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 DHCPs and 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.

[Procedure – DHCP Client]

순서	작업 내용 Description
1	Move to the configuration mode.
2	Select the interface configure as a DHCP Client
3	Apply the DHCP-Client instead of IP Address to the corresponding interface

[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. Sets 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. Sets 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>*

As an interface command, binds DHCP-list with the interface to use.

- **ip address dhcp**

Set ip address with DHCP Clients to the interface to use.

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

Shows a certain DHCP list or whole DHCP configuration.

- **show running-config**

Shows configuration contents in which DHCP is included.

Optional Commands

- **dhcp-list** *<dhcp-list-number>* **option** [option command]
 1. Sets options used in the DHCP-list set in the Gateway.
 2. Optional Commands
 - 1) **arp-cache-timeout** *<time(second)>*: Sets time value that the ARP cache table can keep the Mac address.
 - 2) **default-ip-ttl** *<time(second)>*: Sets IP TTL value of the packet.
 - 3) **dhcp-lease-time** *<time(second)>*: Sets time value to check how long each IP address allocated by the DHCP server is valid. The

default is one hour.

- 4) **dns** <*dns-address*>: Sets the addresses of the DNS server so that DHCP clients can use them.
- 5) **domain-name** <*domain-name*>: Designates 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*}: Sets that the DHCP clients should inform the Ethernet encapsulation method that the Gateway is going to use. The PassFinderAP2520 Gateway supports Ethernet Version 2 and IEEE802.2 address. *The default is Ethernet Version 2.*
- 7) **interface-mtu** <*mtu-value*>: Sets MTU value for the interface.
- 8) **name-server** <*name-server-address*>: Sets the name server address.
- 9) **ntp-server** <*ntp-server-address*>: Sets the NTP server address.
- 10) **max-lease-time** <*time(second)*>: Sets time value to check how long each IP address allocated by the DHCP server is valid. After time passes, all addresses are recovered to be free regardless of the connection status.
- 11) **smtp-server** <*smtp-server-address*>: Sets the SMTP server address.
- 12) **pop3-server** <*pop3-server-address*>: Sets POP3 mail server address.
- 13) **Gateway-option** < *default-Gateway-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*> <*Gateway-address*>: Routes an initial DHCP packet to a certain address.
- 15) **time-server** < *time-server-address* >: Sets the time server address.
- 16) **www-server** < *www-server-address* >: Sets the web server address.

[Example] DHCP Server Mode Configuration and Usage

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

router (config)# dhcp-list 0 type server ☞ Sets that the Gateway should operate as a DHCP server.

router (config)# dhcp-list 1 address server 211.1.1.1 211.1.1.125 ☞ Sets the DHCP address pool. This command sets that the DHCP address pool can allocate addresses from "211.1.1.1" till "211.1.1.125."

Router(config)# dhcp-list 1 option domain-name AddPac ☞ Sets 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 gateway-option 211.1.1.126 ☞ Sets 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 ☞ Makes the DHCP clients to enter into the configuration mode of the Ethernet 0.0 that is the interface that the DHCP clients are going to be connected.

Router(config-ether0.0)# ip address 211.1.1.126 255.255.255.127 ☞ Sets 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. IPs may overlap.

Router(config-ether0.0)# dhcp-group 0 ☞ Sets that all DHCP packets incoming through Ethernet 0.0 interface should be allocated with addressed by rules of DHCP-0 that has been set already.

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

Router# show dhcp-list 0 ☞ Shows configuration contents 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  
Gateways 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  Sets that the Gateway  
should pass DHCP broadcast packets.  
Router(config)# dhcp-list 1 address relay 151.1.12.1   
Changes 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  Enters into the  
configuration mode of the Ethernet 0.0 to which DHCP clients are  
going to be connected.  
Router(config-ether0.0)# ip address 211.1.1.126  
255.255.255.127  Sets the address of the Ethernet 0.0 interface  
as "211.1.1.126/25 Bit."  
Router(config-ether0.0)# dhcp-group 1  Relays all DHCP  
packets coming through Ethernet 0.0 interface according to rules  
of DHCP-List 1 that has been set already.  
Router(config-ether0.0)# end  Exits from the configuration  
mode.  
Router# show dhcp-list 1  Shows configuration contents of the  
DHCP List 0.  
DHCP Type = RELAY  
Next Server = 151.1.12.1  
Router# show running-config  Shows configuration contents that  
have been set.
```

[사용 예] DHCP Client 설정 및 사용의 예

```
Router# config
Router(config)# interface ether0.0  ☞ Enters into the
configuration mode of the Ethernet 0.0 that using as a DHCP clients.
Router(config-ether0.0)# ip address dhcp ☞ Set IP Address with
DHCP Client
Router(config-ether0.0)# end ☞ Exits from the configuration
mode.
Router# show run ☞ Shows configuration contents that have been
set.
interface ether0.0
    ip address dhcp

!
interface serial0
    ip address 132.1.1.2 255.255.255.0
    Encapsulation HDLC
    Operation is UP
!
interface serial1
    no encapsulation
!
```

4.10. Transparent Bridging Configuration

The PassFinder AP2520 Gateway supports transparent bridging for Ethernet and serial ports. Also, to manage networks, the PassFinder AP2520 Gateway supports Bridge MIB that is defined in RFC 1286.

The bridge functions that the PassFinder AP2520 Gateway supports 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 that adopts IEEE-based Bridged Protocol Data Unit (BPUD)

PassFinder AP2520 series Gateways only support one bridge-group. Therefore, the concept of the bridge-group is not used.

[Procedure]

Step	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**

As an interface command, sets that 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 in a way that the bridge maps can be sent through this interface.
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. 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 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 two 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**

Shows bridge forwarding database entry.

- **show bridge**

Shows spanning-tree topology that the bridge is aware of.

- **show running-config**

Shows configuration contents that have been set including bridging.

[Example] Transparent Bridging Configuration and Usage

```
router# config
router(config)# interface Ethernet 0.0  ⚡ Creates Ethernet
interface 0.0 and starts configuration.
router(config-ether0.0)# bridge  ⚡ Applies bridge to Ethernet
interface 0.0.
router(config-ether0.0)# bridge priority 2  ⚡ Sets the
spanning tree priority of the interface as 2.
router(config-ether0.0)# interface serial 0  ⚡ Enters into
the configuration mode of the interface serial 0.
router(config-serial0)# encapsulation frame-relay  ⚡
Encapsulates with the frame-relay.
router(config-serial0)# frame-relay map bridge 100  ⚡
Enables the bridge in the frame-relay interface. This command
also encapsulates the bridge packet.
router(config-serial0)# exit  ⚡ Goes back to the global
configuration mode.
router(config)# bridge forward-time 150  ⚡ Sets the bridge
forward delay interval as 150 seconds.
router(config)# bridge hello-time 5  ⚡ Sets the bridge hello
BPDU interval as five seconds.
router(config)# bridge max-age 150  ⚡ Sets the standby time
to wait until receiving BPDU from the root bridge as 150 seconds.
router(config)# exit  ⚡ Exits from the configuration mode.
router # show running-config  ⚡ Shows configuration contents.
interface ether0.0
    no ip address
    Operation is UP
    bridge
!
interface serial0
    no ip address
    Encapsulation FRAME-RELAY
```

```
Operation is UP
```

```
bridge
```

```
!
```

```
interface serial1
```

```
no encapsulation
```

router # show bridge ⇨ Bridge Forwarding Database의 Entry를 보여줍니다.

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 ⇨ Bridge(Gateway)가 알고 있는 Spanning Tree Topology를 보여줍니다.

```
Bridge is executing the IEEE compatible Spanning Tree protocol
```

```
Bridge has priority 32768, address 0000.0000.0000.0000
```

```
Configured hello 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, forward delay 30, ageing 300
```

```
Timers: hello 1, topology change 0, notification 0
```

```
Port 1(ETH0), forward status
```

```
Port path cost 0, port 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
```

4.11. SNMP Configuration

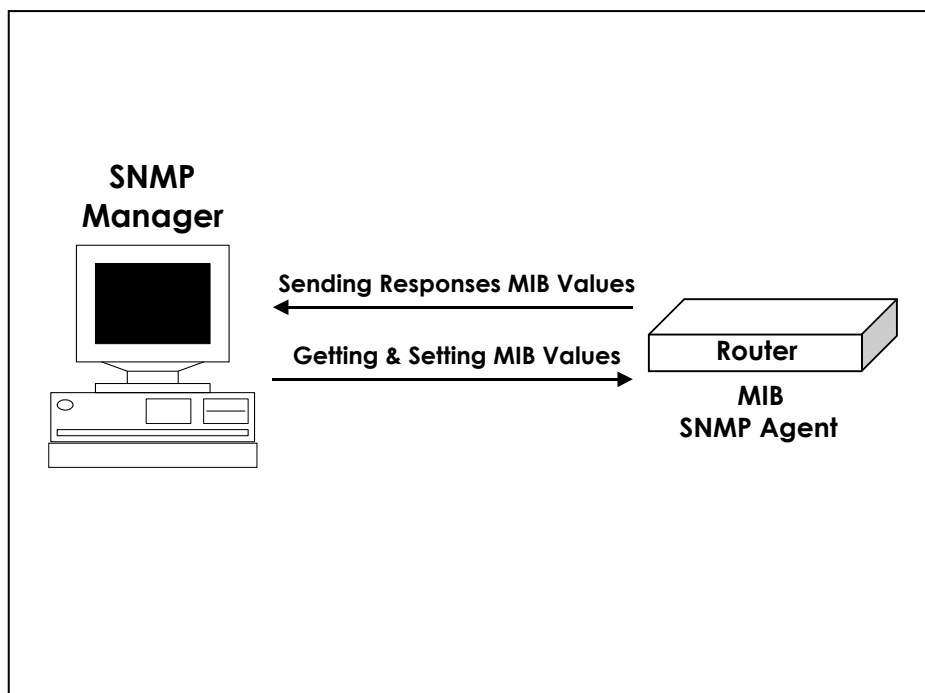
Information



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.



[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 3. 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

The PassFinder AP2520 Gateway supports both of SNMPv1 and SNMPv2C.

[Procedure]

Step	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. Registers the host to which the Gateway sends trip 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>

When the Gateway sends trap, the command indicates contact point (equipment manager) to solve trap problem.

- **snmp location** <string>

Indicates 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. Decides to shutdown (reboot) the Gateway or not by SNMP from a remote place
2. This command can greatly affect equipment operation in the network in which security is not strong. Therefore, the user shall be careful in using 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**

Shows 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
? Exchanges information with all SNMP Managers whose
community-string is AddPac-Domain1.
router(config)# snmp host 131.23.1.1 AddPac-Domain v2c ?
Sends 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 ? Sends a message
indicating that the contact point is "HongKilDong" when trap occurs
router(config)# snmp location 9FlofBuilding4 ? Sends a
message indicating that the installation location of the faulty
equipment is 9FlofBuilding4 when trap occurs
router(config)# snmp name Tac_Gateway1 ? Sends 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 ? Shows 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_Gateway1		
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 and 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. Resets certain functions or certain parts of the Gateway.
 2. Command options are as follows:
 - 1) counters: Clears counters of all interfaces.
 - 2) interface: Resets the hardware logic of a certain interface and functions as if rebooting certain interfaces.
 - 3) logging: Clears logging buffer. To be implemented later.
 - 4) utilization: Clears system utilization information of the Gateway.
- **clock [current/running/start]**
 1. Shows the system clock of the Gateway.
 2. Command options
 - 1) current: Shows current time of the Gateway.
 - 2) running: Shows total running time.
 - 3) start: Shows the time that the Gateway started operating.
 3. If there is no option, all values of the three options will be displayed.
- **configuration**

Enters into the configuration mode.

- **copy {startup-clear/running-config}**

1. Saves or deletes configuration data.
2. Command options are as follows:
 - 1) startup-clear: Deletes configuration data that is saved in the flash memory of the present Gateway.
 - 2) running-config: Saves currently running configuration information in the Gateway.

- **Debug <Option>**

1. Decodes packets passing the Gateway and indicates if the Gateway normally operates.
2. For more information and options, see "4.13 Fault Handling and Debugging."
3. When disabling Debug, use "no debug" or "Un-debug" commands.

- **exit**

1. Exits from the current mode, and enters into the next lower mode.
2. If the user uses "exit" command in the Exec mode, the user needs to log in again.

- **help**

Describes the interactive help system.

- **history**

1. Shows commands history.
2. The AP2520 Gateway keeps maximum 25 histories for each mode.
3. To use a command again used in 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. Sends echo messages.
2. Command options are as follows:
 - 1) [-f: fast send mode]
 - 2) [-l: loopback mode for HDLC]
 - 3) [-t: sends one datagram per seconds]
 - 4) [-s: specify the sending interface IP address]

- **reboot**

Reboots the Gateway system.

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

Opens the Rlogin connection.

- **show {option}**

1. Shows 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, see "4.13 Fault Handling and Debugging."

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

Opens a Telnet connection in the remote host.

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

1. Tests 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*]

Checks the path that can be accessed through a remote host.

- **undebug** <Option>
 1. Negates debugging configuration.
 2. For more information and options, see “ 4.13 Fault Handling and Debugging.”

4.12.2. Command in the Global Configuration Mode

[Command Formats and Optional Commands]

- **access-list { option }**

1. Sets the access-list for the packet.
2. For more information, see 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 AP2520 Gateways supports 10 ~ 256 size.

- **bridge { option }**

1. Sets the bridge.
2. For more information, see Bridge Configuration in the previous chapter.

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

Sets the system clock of the present Gateway.

- **dhcp-list { option }**

1. Sets the DHCP.
2. For more information, see DHCP Configuration in the previous chapter.

- **Ethernet [full-duplex]**

1. Sets the Ethernet interface as full-duplex.
2. The default is half-duplex.

- **exit**
 1. Exits from the current mode, and enters into the next lower 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**

Describes the interactive help system.
- **history**
 1. Shows history of used commands.
 2. The AP2520 Gateway keeps maximum 25 histories in each mode.
 3. To use the command again, enter "! History#."
- **hostname { host-name }**

Sets a name in the network of the Gateway.
- **interface { ethnet/null/loopback } < main-interface.sub-interface >**

Enters into a configuration mode of a certain interface.
- **logging { option }**
 1. Sets logging of the equipment.
 2. For more information, see "4.13 Fault Handling and Debugging."
- **nat-list { option }**
 1. Sets Network Address Translation (NAT.)
 2. For more information, see 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. Sets the traffic queuing.
 2. For more information, see Traffic Queuing Configuration in the previous

chapter.

- **route {option}**

1. Sets the static route.
2. For more information, see Routing Configuration in the previous chapter.

- **router static**

1. Enables or disables static routing process.
2. For more information, see Routing Configuration in the previous chapter.

- **service {ftpd/snmpd/telnetd/fttpd}**

1. Enables Application demon for a certain service.
2. To disable the service, use "**no service**" command.

- **snmp { option }**

1. Sets SNMP protocol for management.
2. For more information, see SNMP Configuration.

- **user { Option }**

1. Commands to manage Gateway users.
2. For more information, see "4.14 User, Password, Software Image and Configuration File Management."

- **utilization { cpu/Ethernet/serial } [interface] [interface-number]**

[measuring-period]

1. Checks 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 five minutes.

4.13. Fault Management and Debugging

This chapter describes how to handle and process faults while operating the PassFinder AP2520 Gateway. The AP2520 Gateway provides "show" commands, "Debug" commands and "logging" commands for fault handling.

4.13.1. Logging Command

Logging commands log 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**

Enables logging for all available destinations.

- **logging condition {option}**

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

- **logging destination {option}**

1. Sets conditions of the destination host to send logging information.
2. Option

- 1) **ip** *<destination-ip-address>*: Sets IP address of the remote host to send logging information.
- 2) **port** *[port-number]*: Defines the port number of the remote host to send logging information.
- 3) **on**: Enables 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}**: Displays option contents.
“show” command related optional commands are as follows:
- **access-list** *[access-list-number]*
 1. Shows the access-list that has been set.
 2. For more information, see Access-List Configuration in the previous chapter.
- **arp** *[ip-address for ARP entry]*
Shows the contents of the ARP table.
- **bridge**
 1. Shows forwarding/blocking database of the bridge.
 2. For more information, see Bridge Configuration in the previous chapter.
- **clock** *[current/running/start]*
Shows the system clock of the current Gateway.
- **debug-port**
show current debug terminal information.

- **dhcp-list** [*dhcp-list-number*]
 1. Shows the DHCP that has been set.
 2. For more information, see DHCP Configuration in the previous chapter.
- **ethernet**

Shows the mode and operation rate of the Ethernet interface.
- **interface** [**Ethernet/null/loopback**] [<*main-interface*>.<*sub-interface*>]

Describes the status and the configuration of the interface.
- **logging** [**history**]
 1. Shows contents of the logging buffer.
 2. History option shows the contents of the system log history table.
- **nat-list** [*nat-list-number*]
 1. Shows the NAT that has been set.
 2. For more information, see NAT Configuration in the previous chapter.
- **proxy-arp**

Indicates if the proxy ARP is enabled.
- **route** [**static**]
 1. Shows decided route information table.
 2. Static option shows each table as using the algorithm of the corresponding option.
 3. For more information, see Routing Configuration in the previous chapter.
- **router**
 1. Displays enabled routing processes.
 2. For more information, see Routing Configuration in the previous chapter.
- **running-config**

Shows currently running configuration file.

- **session**

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

- **service**

Displays enabled service processes in the current Gateway.

- **snmp**

Displays 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**

Displays static routes that are set in the Gateway.

- **system task**

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

- **tcp**

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

- **udp**

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

- **user**

Displays profiles of the users registered in the Gateway.

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

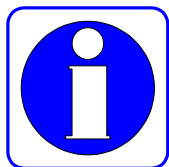
Shows utilization state and values currently set.

- **version**

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

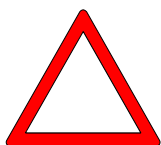
4.13.3. Debug Commands

Information



Debug commands decodes certain packets that pass through Gateway devices and indicate whether packets are normal or not to the manager. Therefore, the manager can check whether the network or device has been normally set up or not. Debug commands can be used in the Exec mode.

Caution



Note that Debug commands use a lot of system resources. Therefore, minimize the range of using Debug commands. Also, since Debug commands greatly lower general performances of the system, turn off Debug commands.

“debug” command can be used in the Exec mode, and its syntax is as follows:

- **debug {option}**: Enables debugging.
- **no debug {option}**: Enables debugging that has been set.
- **undebug {option}**: Disables debugging.

Debug related optional commands are as follows:

- **ppp {chap/error/negotiation/packet }**
 1. Decodes and shows configuration and operation status of PPP.
 2. Details of each option are as follows:
 - 1) chap: Decodes and shows information exchanged when CHAP is being set.
 - 2) error: Decodes and shows error information in the PPP process.
 - 3) negotiation: Decodes and shows PPP link negotiation information.
 - 4) packet: Decodes PPP packets.

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

1. Decodes and shows TCP/IP packets passing through the Gateway.
2. Details of each option is as follows:
 - 1) arp: Decodes and shows ARP packets.
 - 2) icmp: Decodes and shows ICMP packets.
 - 3) tcp: Decodes and shows TCP/IP packets.
 - 4) udp: Decodes and shows 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 the PassFinder AP2520 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}**: Registers of changes users.

User's command related optional commands are as follows:

- **add** <login-name> <password> [**admin/high/normal/low**]
 1. Registers Gateway users.
 2. Sets the user's authority level as admin, high, normal or low.
- **change** <login-name> <old-password> <new-password>
Changes the password of the Gateway user.
- **level** <login-name> <password> [**admin/high/normal/low**]
 1. Changes the authority level of the Gateway user.
 2. Changes 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]

Step	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 serial console port, 2 Serial 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#
```

[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 "Gateway".

3 BOOT# sh password

password = "Gateway"

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 "Gateway1".

[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 Password
3 BOOT(config)# passwd Gateway ?
    <repeat new password> New Password for confirm
4 BOOT(config)# passwd Gateway Gateway ?
    < cr >
5 BOOT(config)# passwd Gateway Gateway1
    password changed
6 BOOT(config)#
```

4.14.3. Software Image Upgrade and Backup

Software of the AP2520 Gateway is regularly upgrade according to functional upgrade or bug fix. 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 logging in the system. Firstly, 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 Gateway 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 Gateway.bin
200 PORT command successful.
150 BINARY data connection for Gateway.bin (211.170.87.99,44100).
```

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

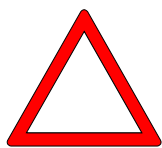
Software backup method through TFTP is same as FTP. However, login procedure is not necessary. The following is when using "put" command for software. When software upgrade is completed, "Gateway Software is updated" is displayed in the screen.

[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.

```
"software image" 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 File의 Backup 및 Restore

The AP2520 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 Gateway.cfg. The configuration file is backed up or restored through FTP/TFTP. When restoring is completed, "Config Database is updated" message is displayed in 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

```
155 sun10: #> ftp 211.170.87.221
Connected to 211.170.87.221.
220 Gateway 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 Gateway.cfg
200 PORT command successful.
150 BINARY data connection for Gateway.cfg (211.170.87.99,44100).
226 BINARY Transfer complete.
local: Gateway.cfg remote: Gateway.cfg
2016 bytes received in 0.0 seconds (375.13 Kbytes/s)
ftp> quit
```

```
221 Goodbye.  
156 sun10:/#>
```

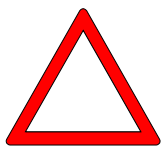
[Example] Backup and Restore of Configuration Information through TFTP

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

The following message is displayed on the 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 PassFinder AP2520.

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.

Voice over IP is primarily a software feature; however, to use this feature on a VoIP Gateway, you must install a voice interface cards, each of which is specific to a particular signaling type associated with a voice port.

5.1.2. Codecs and MOS(Mean Opinion Score)

5.1.2.1. Codecs

PCM and ADPCM are examples of "waveform" CODEC techniques. Waveform CODECs are compression techniques that exploit the redundant characteristics of the waveform itself.

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 PSap or through PBXs.
- 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.
- 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.

5.1.2.2. Mean Opinion Score

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.

Table 5-1: Compression Methods 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

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.

One of the most important design considerations in implementing voice is minimizing one-way, end-to-end delay. Voice traffic is real-time traffic; if there is too long a delay in voice packet delivery, speech will be unrecognizable. Delay is inherent in voice-networking and is caused by a number of different factors. An acceptable delay is less than 200 milliseconds.

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.

Table 5-2: CODEC-Induced Delays

CODEC	Bit Rate (kbps)	Compression Delay (ms)
G.711 PCM	64	0.75
G.726 ADPCM	32	1
G.728 LD-CELP	16	3 to 5
G.729 CS-ACELP	8	10
G.729a CS-ACELP	8	10
G.723.1 MP-MLQ	6.3	30
G.723.1 ACELP	5.3	30

5.1.3. Dial Peer

The key to understanding 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.

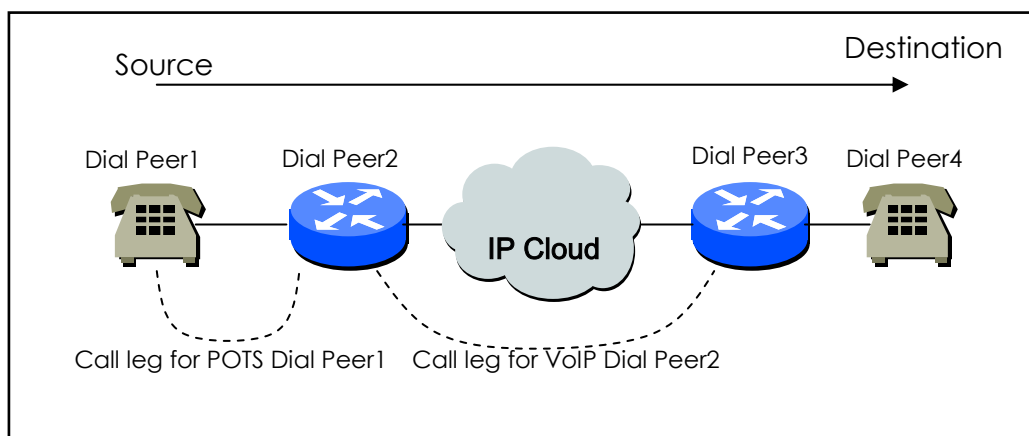


Figure 5-1: Dial Peer Call Legs from the Perspective of the Source Gateway

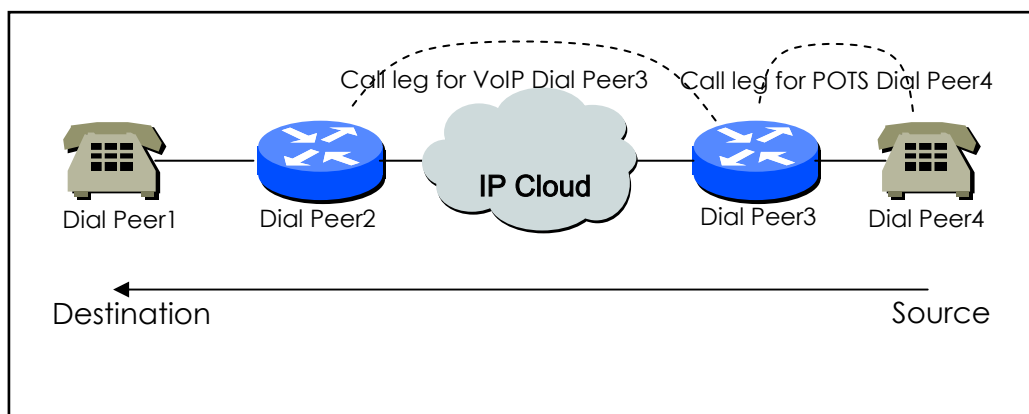


Figure 5-2: Dial Peer Call Legs from the Perspective of the Destination Gateway

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

- POTS Dial peer : POTS Dial peer describing 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 AP2520 VoIP Gateway to the local POTS network.

When configuring Voice over IP on the AP2520 VoIP Gateway, direct inward dial can be configured on a POTS dial peer. In this case, the key commands that must be configured are the **destination-pattern** and **direct-inward-dial** commands.

- Voice Network Dial peer : Voice Network Dial peer describing 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 AP2520 VoIP Gateway define the characteristics associated with a particular voice-port signaling type. Voice ports for both the AP2520 VoIP Gateway provides support for three basic voice signaling formats:

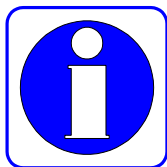
- FXO---Foreign Exchange Office interface. The FXO interface is an RJ-11 connector that allows a connection to be directed at the public switched telephone network's (PSTN's) central office (or to a standard PBX interface, if the local telecommunications authority permits). This interface is of value for off-premise extension Applications.
- FXS---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.
- E&M---The "Ear and Mouth"(or "Receive and Transmit") interface. The E&M interface is an RJ-48 connector that allows connection for PBX trunk lines (tie lines). It is a signaling technique for 2-wire and 4-wire telephone and trunk interfaces.

The AP2520 series currently provides only analog voice ports for its implementation of Voice over IP. The type of signaling associated with these analog voice ports depends on the interface module installed into the device.

The voice port syntax depends on the hardware platform is being configured. On the AP2520 series, the voice-port syntax is **voice-port slot-number/port-number**.

5.2. VoIP Interface Configuration

Information



AP2520 Gateway has various interfaces. They are Ethernet Interface and loop-back interface which are 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 connecting 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.

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 those related VoIP.

In case Ip Address of VoIP Interface is changed during VoIP service, the signal connecting 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 initiation of VoIP router (or gateway) configuration is to plan the number scable, 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 Volp network is corresponding to switcher on telephone network, have a number plan in accordance the size of VoIP network.

It is important if router is confabulated with gatekeeper in number planning. In case of being configurated with the existing gatekeeper, you should follow the number planning defined on the gatekeeper.

The simplest number configuration makes router have the public telephone number already used in the setting place of router. 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 feature, configurate network by having a private number planning.

5.3.2. Dial Peer Configuration

The key point to understanding how Voice over IP functions is to understand dial peers. Each dial peer defines 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. All the call legs for a particular connection have the same connection ID.

There are two different kinds of dial peers:

- POTS---Dial peer describing the characteristics of a traditional telephony network connection. POTS peers point to a particular voice port on a voice network device.
- VoIP---Dial peer describing the characteristics of a packet network connection; in the case of Voice over IP, this is an IP network. VoIP peers point to specific VoIP devices.

5.3.2.1. Inbound Dial Peer versus 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 *router's* perspective. An inbound call leg originates *outside* the router. An outbound call leg originates *from* the router.

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

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.

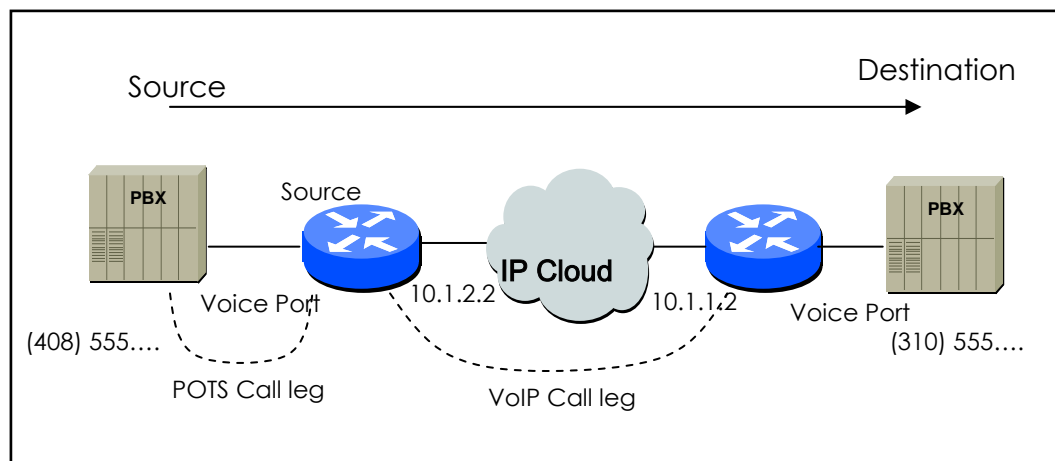


Figure 5.1 Outgoing Call in POTS Dial Peer 1's view

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 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. From access server 10.1.1.2, calling any number string that begins with the digits "1408555" will result in a connection to access server 10.1.2.2.

This implies that access server 10.1.2.2 services all numbers beginning with those digits. For more information about stripping and adding digits, see the "Outbound Dialing on POTS Peers" section.

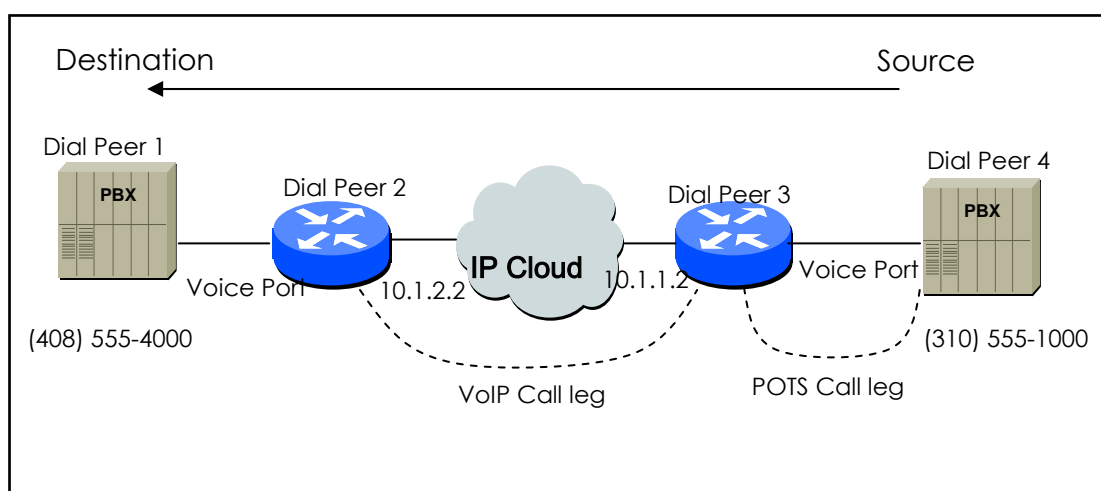


Figure 5.2 Outgoing Call in POTS Dial Peer 2's view

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 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 selection for VoIP is as follows;

- 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 string [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 location	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 string	(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 tag 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 string [T]	Enters the telephone number of the corresponding dial peer. The string 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 destination-ip-address	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 or 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 a high bandwidth or to get the highest voice quality, select **g711alaw** or **g711ulaw** from "Codec" command. These values allows better voice quality but requires 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 <i>tag</i>	Enters into the CODEC class configuration mode. The tag is an identifier of the CODEC class.
3	Router(config-class)# codec preference <i>value</i> <i>codec-type</i>	Enters into the configuration mode.
4	Router(config-class)# codec preference <i>value</i> <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 a 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 Router A attempts to make a call to the subscriber who is using PABX line #100 that is connected to the other VoIP router B.

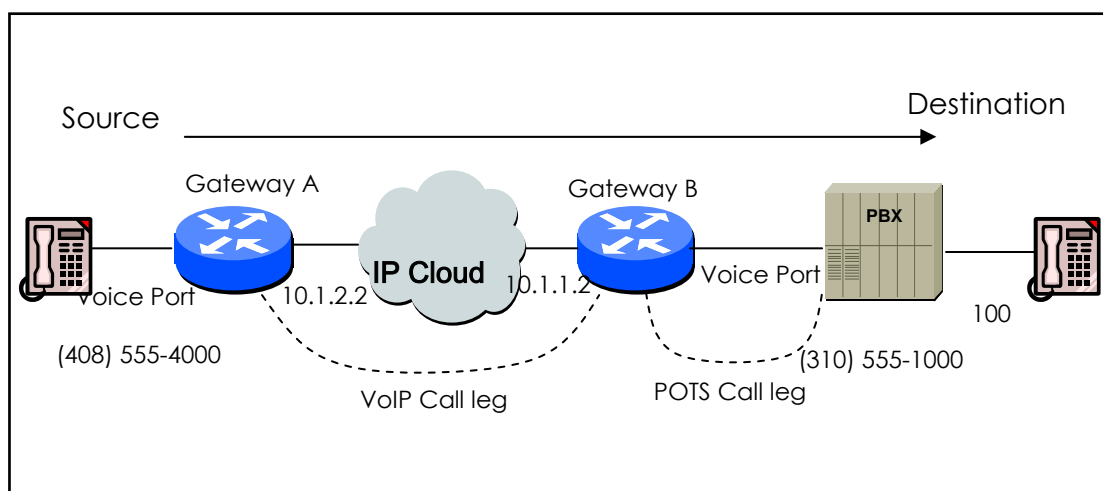


Figure 5.3 Two-Stage Dialing

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

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

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

Consider that the POTS peer setup of Router 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 Router A as follows:

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

In this kind of setup, the subscriber of Router A shall enter 3105551000100 to establish a call, and Router 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 Router A as follows:

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

In this case, if the subscriber of Router A enters the termination digit (#) after entering 31055510001234567 or if the inter-digit is timed-out, a call will be connected to Router B and Router 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 router 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 this factors. For example, operation of dial-peer hunt 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.

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 <i>[0-7]</i>	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 already 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.

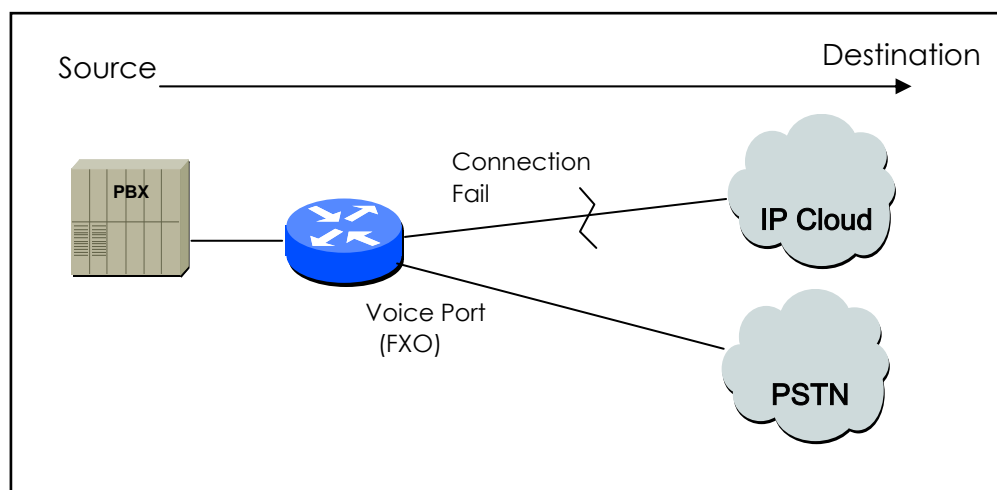


Figure 5.4 PSTN Rerouting

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 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 be 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 be 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 outputted first and 123456 is outputted 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. Configuration 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 5.7, 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 Router 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 Router 2 (located to the right of the IP cloud) is (729) 555-xxxx.

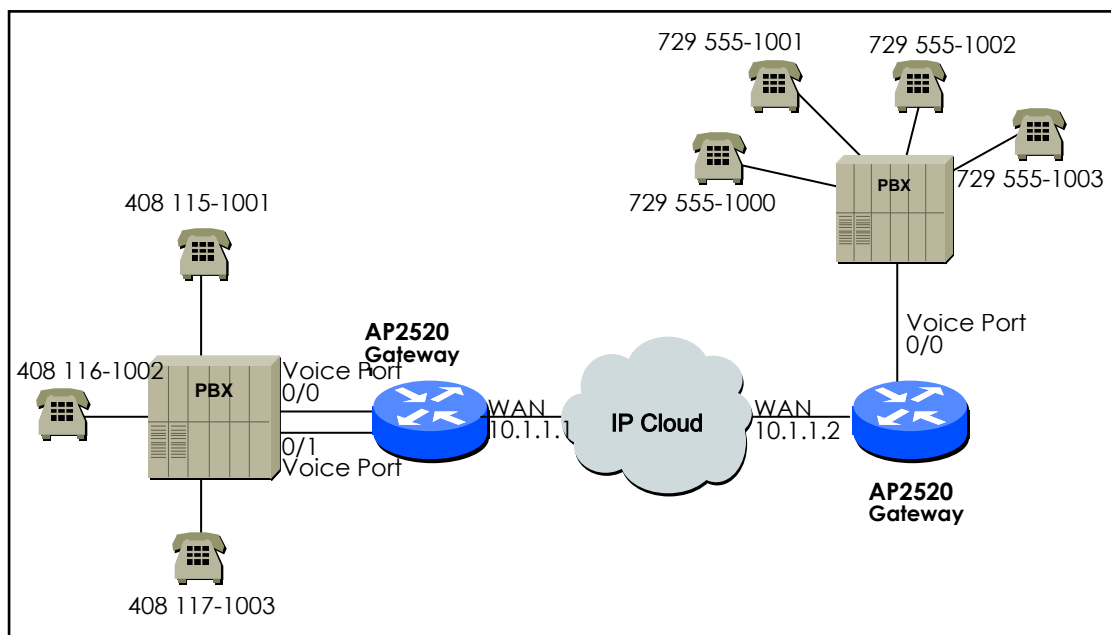


Figure 5.5 Sample VoIP Network

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 및 Gateway 2.

5.3.6.2. Configuration 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** command to verify that you have mapped the telephone numbers correctly.

5.3.7. Configuration Number Translation

5.3.7.1. Creating Translation Rules

Users can translate called/calling party number of the inbound/outbound calls in the AP2520 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 "." 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 location 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} tag	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 on the AP2520 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. Because of the inherent complexities involved with PBX networks, E&M ports might need specific voice port values configured, depending on the specifications of the devices in your telephony network.

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) 연결 모드
 - 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 <i>string</i> 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. Configuring E&M Voice Ports

Unlike FXO and FXS voice ports, the default E&M voice-port parameters most likely will not be sufficient to enable voice data transmission over your IP network. E&M voice-port values must match those specified by the particular PBX device to which it is connected.

E&M voice-port values must match those of the PBX to which it is connected. Refer to the documentation that came with your specific PBX for the appropriate E&M voice-port configuration command values.

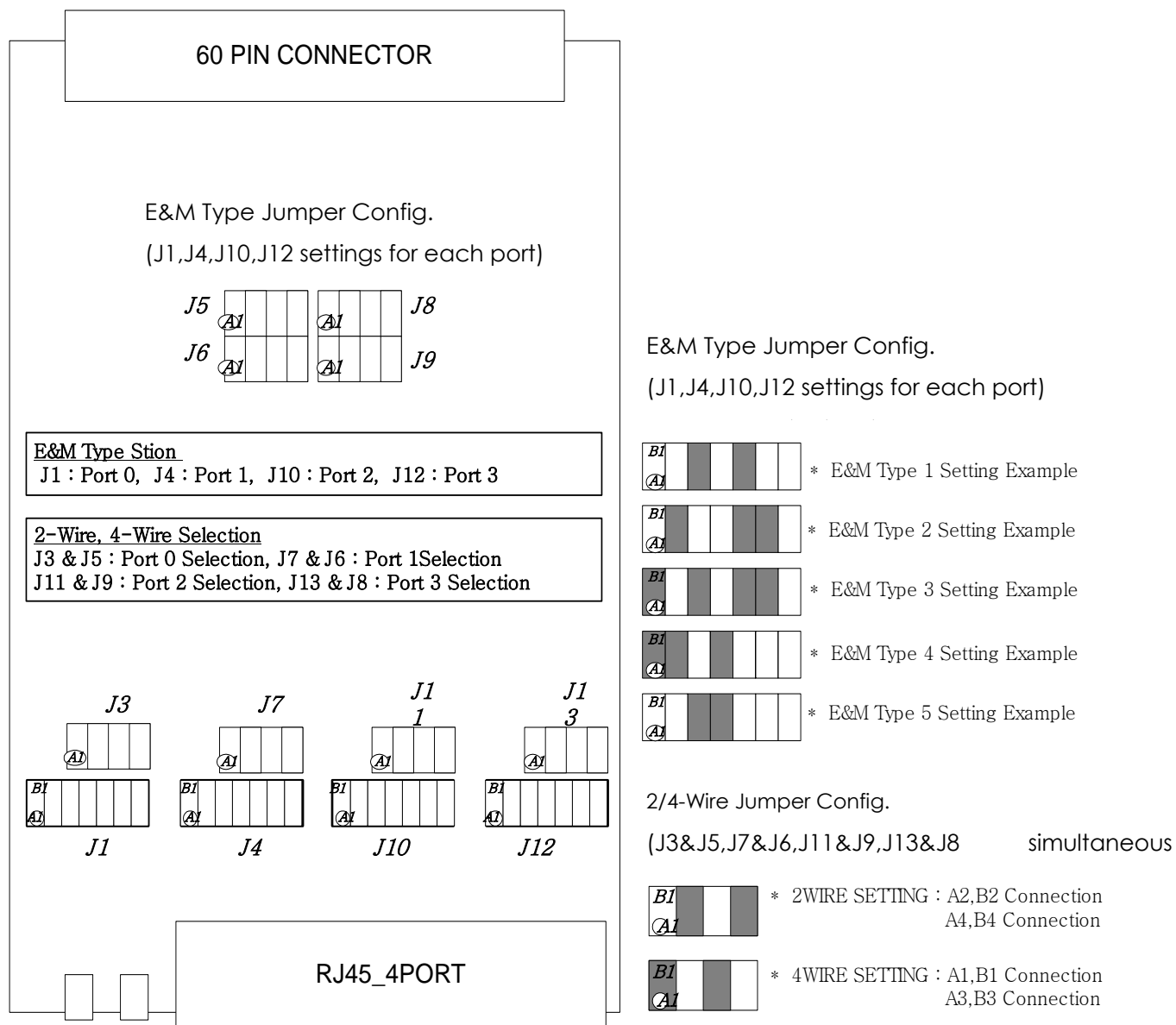
To configure an E&M voice port, perform the following tasks. The first two tasks are required; the third task is optional.

1. Identify the voice port and enter the voice-port configuration mode.
2. For each of the following required parameters, select the appropriate parameter value:
 - Signal type
 - Operation
 - Type {This part is performed as Jumper Setting}
3. Select one or more of the following optional parameters:
 - Connection mode
 - Description

To configure E&M voice ports, use the following commands beginning in Administrator command mode:

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	signal { wink-start immediate delay-dial }	Selects the appropriate signal type for this interface
4		<p>Selects a proper cabling scheme for the corresponding VoIP port. At this time, the user shall decided which wire to use – 4-wire or 2-wire. In the AP2520 router, jumper setting has been used for this matter.</p> <p>When the product is delivered to the customer from the factory, 2-wire has been set as the cabling scheme. For more information, refer to jumper setting of the E&M module.</p>
5		<p>Selects a proper E&M type for the corresponding VoIP port. At this time, the user shall select the type – Type 1, 2, 3, or 5. In the AP2520 router, jumper setting has been used for this matter.</p> <p>When the product is delivered to the customer from the factory, the E&M type has been set as Type 1. For more information, refer to jumper setting of the E&M module.</p> <p>The following shows signal configuration for each E&M type.</p> <p>Type 1</p> <ul style="list-style-type: none"> - E: output, relay to ground - M: input, referenced to ground <p>Type 2</p> <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 <p>Type 3</p> <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 <p>Type 5</p> <ul style="list-style-type: none"> - E: output, relay to ground <p>M: input, referenced to –48V</p>
6	operation { 2-wire 4-wire }	<i>This command is for information description and is not actually used. Actual operation is made according to jumper setting explained in Step 4. However, this command helps the user to easily check the wiring method without checking the jumper.</i>
7	type { 1 2 3 5 }	<i>This command is for information description and is not actually used. Actual operation is made according to jumper setting explained in Step 5. However, this command helps the user to easily check the E&M type without checking the jumper.</i>

8	connection plar <i>string</i>	(Optional) Specifies the private line auto ringdown (PLAR) connection, if this voice port is used for a PLAR connection. The <i>string</i> value specifies the destination telephone number.
9	description <i>string</i>	(Optional) Attaches descriptive text about this voice port connection.



[Figure 5.8] Jumper Setting of E&M Module

5.4.2.3. Fine-Tuning E&M Voice Ports

Depending on the specifics of your particular network, you may need to adjust voice parameters involving timing, input gain, and output gain for E&M voice ports. Collectively, these commands are referred to as voice-port tuning commands.

In most cases, the default values for voice-port tuning commands will be sufficient.

To configure voice-port tuning for E&M voice ports, perform the following tasks:

1. Identify the voice port and enter the voice-port configuration mode.
2. For each of the following parameters, select the appropriate value:
 - Input gain
 - Output gain
 - Timing other than timeout

To fine-tune E&M voice ports, use the following commands beginning in Administrator command mode:

Change voice port setup using “voice-port” command before activating/deactivating the corresponding port by “**shutdown/no shutdown**” command.

Step	Command	Description
1	configure	Enter global configuration mode.
2	voice-port slot-number/ port	Identify the voice port you want to configure and enter voice-port configuration mode.
3	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 -6 to 14.
4	output gain <i>value</i>	Specify (in decibels) the amount of gain at the transmit side of the interface. Acceptable values are from 0 to 14.
5	timing delay-duration <i>milliseconds</i>	Specify the delay signal duration for delay dial signaling. Valid entries for delay-duration are from 100 to 5000 milliseconds.

6	timing delay-start <i>milliseconds</i>	Specify the minimum delay time from outgoing seizure to outdial address. Valid entries for delay-start are from 20 to 2000 milliseconds.
7	timing wink-duration <i>milliseconds</i>	Specify the maximum wink signal duration. Valid entries for wink-duration are from 100 to 400 milliseconds.
8	timing wink-wait <i>milliseconds</i>	Specify the maximum wink-wait duration for a wink start signal. Valid entries for wink-wait are from 100 to 5000 milliseconds.
9	timing dialout-delay <i>milliseconds</i>	Sends the number to the E&M trunk or designates dial-out delay for cut-through. Values between 100 ~ 5000 msec can be used.
10	timing wait-wink <i>milliseconds</i>	Designates the maximum wait value for the wink signal. Values between 100 ~ 5000 msec can be used.

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 cycle 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.

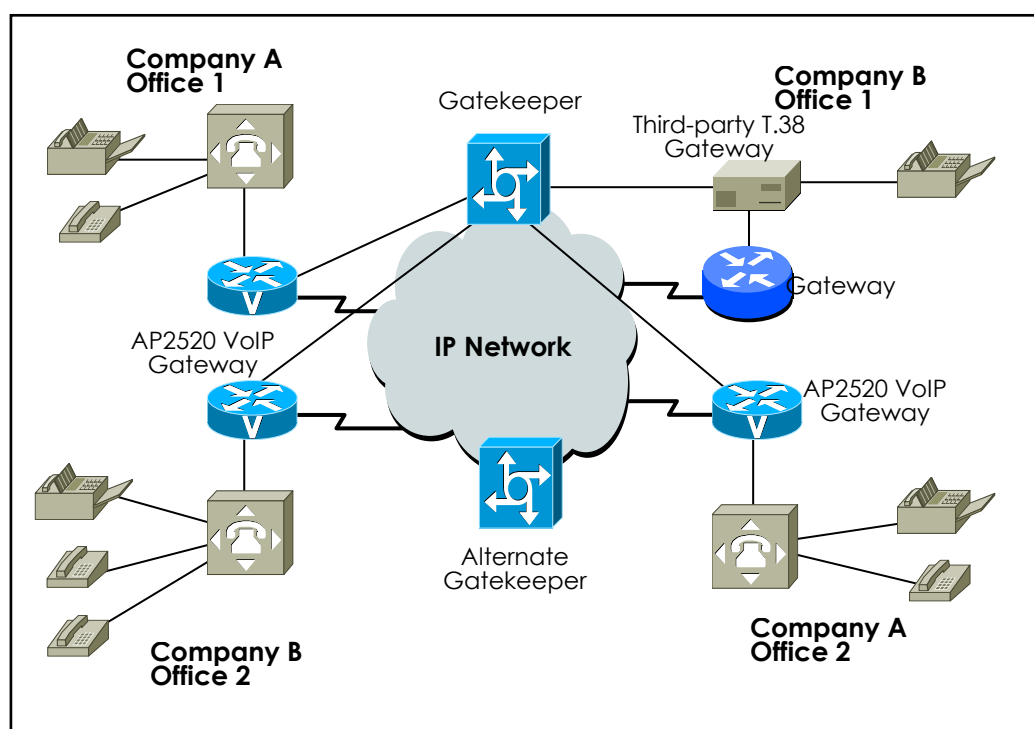
5.5. Configuring FAX Application

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 AP2520.

Because the T.38 fax relay protocol is standards based, AP2520 can interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed-vendor network when real-time fax relay capabilities are required.

Figure 5.9 shows an IP H.323 network with AP2520 routers and third-party gateways and gatekeepers using T.38 fax relay functionality. By using T.38 fax relay, all gateways and gatekeepers in this network are able to send faxes to other remote offices or to the offices of another company on the IP network.



[Figure 5-9] 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 needs 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. The AP2520 Gateway can set static IP address in the VoIP peer and operate without any gatekeeper. Also, the AP2520 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 AP2520 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.

The AP2520 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 <i>password</i>	Sets the H.235 security password.
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 the AP2520 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 origination 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 tones 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 AP2520. 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 AP2520 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 <i>tag</i>	Enters into the user class configuration mode. The tag is a user class identifier.
3	Router(config-class)# password <i>digits</i>	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 <i>value</i>	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	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	
							calling-number	
					port	slot / port <0-3>/<0-3>		
					preference	<0-9>		
					prefix	string		
					register	e164		
					shutdown			
					translate-outgoing	called-number	tag <0-65535>	
						calling-number	tag <0-65535>	
				VoIP				
					answer-address	string		
					codec	g711alaw g711ulaw g729 g7231r63 g7231r53		
					description	string		

					destination-pattern	string		
					dtmf-relay	h245-alphanumeric		
					huntstop			
					no	answer-addresses		
						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-addr	
							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-addr	port<0-65536>	priority<0-254>			
					<cr>			
				<cr>				
		lightweight-irr						
		h323-id	string					
		no	discovery					
			gkip	ip-addr				
			lightweight-irr					
			public-ip					
			register					
			security	password				
		public-ip						
		register						
		security	password					
	no	dial-peer	hunt					

			ipaddr-prefix					
			terminator					
			voice	tag <0-65535>	pots			
					VoIP			
		gateway						
		num-exp	string					
		translation-rule	tag <0-65535>					
		voice	class	clear-down-tone	tag <0-1>			
				codec	tag <0-65535>			
				user	tag <0-10>			
		VoIP-interface						
	num-exp	string	string					
	translation-rule	tag <0-65535>						
			rule	tag <0-65535>	string	string		
			no	rule	tag <0-65535>			
	voice	class	clear-down-tone	tag <0-1>	low-num <300-1980>	high-num <300-1980>	on-num <0-10000>	off-num <0-10000>
			codec	tag <0-65535>				
					codec	preference	num <1-5>	
					no	codec	preference	num <1-5>
			user	tag <0-10>				
					password	digits <4 digits>		
					max-digits	num <0-100>		
					no	password		
						max-digits		
		service	VoIP					
				announcement				
				counter	cras	<1-5> default :3		
				default				
				fax	protocol	bypass		
						t38	redundancy	num <0-5>
							<cr>	
						inband-t38	redundancy	num <0-5>
							<cr>	
					rate	2400 4800 7200 9600 12000 14400 disable		
				h323	call			
						channel	early	
							late	
						response	alert	
							progress	
							none	
						start	fast	
							slow	

							preferred-slow	
				no	announcement			
					counter	cras		
					fax	protocol		
						rate		
					h323	call	channel	
							response	
							start	
					security	permit-FXO		
					timeout	t301		
						t303		
						tras		
						tttl		
						tidt		
						treg		
					translate-VoIP-incoming	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-incoming	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	2-wire 4-wire				
			output	gain	num <31 - 31>			
			ring	number	num <1-255>			
			shutdown					
			signal	delay-dial immediate <u>wink-start</u>				
			timing	dialout-delay	num <50-5000>			
				delay-duration	num <100-5000>			
				delay-start	num <20-2000>			
				wait-wink	num <100-5000>			
				wink-duration	num <30-5000>			
				wink-wait	num <100-5000>			
			translate-incom ing	called-number	tag <0-65535>			
				calling-number	tag <0-65535>			
			type	1 2 3 5				
	VoIP-interf ace	interface	(default ether 0.0)					
show	call	active	all					
			summary					
		history	all	last	num <1-100>			
				<cr>				
	clear-down-tone							
	codec-clas s	tag <0-65535>						
		<cr>						
	dialplan	number	string					
		port	slot / port					
	dial-peer	pots	tag <0-65535>					
			summary					
			<cr>					
		voice	tag <0-65535>					
			summary					
			<cr>					
		VoIP	tag <0-65535>					
			summary					
			<cr>					
	gateway							
	num-exp							
	translation- rule	tag <0-65535>	string					

			<cr>					
		<cr>						
	user-class							
	voice	port	slot/port					
			summary					
			<cr>					
	VoIP-interf ace							

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 Configuration Mode

5.7.2.1.4. Usage Guideline

To select the outbound POTS going out of the router 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 those are 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. Examples

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** 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** global configuration command to designate a particular character as a terminator.

.

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** 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. Examples

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

The gateway is unregistered.

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.

To register the dial peer or change the number by using "**load VoIP**" command and the script file in the gateway currently operating and registered in the gatekeeper, use "**no gateway**" command. Unregister the gateway from the gatekeeper, and then load configuration or state "**no gateway**" at the beginning of the script file. Otherwise, messages between the gateway and the gatekeeper may get congested to update changed information of the gateway.

5.7.2.5.5. Examples

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 Configuration Mode

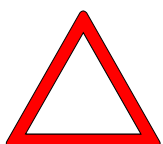
5.7.2.6.4. **Usage Guideline**

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. Examples

The following example expands the extension number 55541 to be expanded to 1408555541: In the following example, the inbound called party number 5554123 is extended into 140855554123.

```
num-exp 55541 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 *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.

For more information about the physical characteristics of your voice network module, or how to install it, refer to the installation documentation that came with your voice network module.

5.7.2.8.5. Examples

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. Examples

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 10,000. 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. Examples

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 trough 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 AP2520 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 AP2520 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. Examples

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. Examples

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, Serial 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 Configuration 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. Examples

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 serial 0 interface.

```
configure
```

```
VoIP-interface serial 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

Enabled

5.7.3.1.3. Command Mode

Voice-port configuration Mode

5.7.3.1.4. Usage Guideline

Use the **comfort-noise** command to generate background noise to fill silent gaps during calls if VAD is activated. 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.

The configuration of the **comfort-noise** command only affects the silence generated at the local interface; it does not affect the use of VAD on either end of the connection or the silence generated at the remote end of the connection.

5.7.3.1.5. Example

The following example enables background noise on the AP2520 Gateway:

```
voice-port 1
  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. Examples

The following example selects PLAR as the connection mode on the AP2520, with a destination telephone number of 555-9262: In this example, if the receiver connected to the voice port 1/0 is hooked off, a call will be automatically sent to 5559262.

```
voice-port 1
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. Examples

The following example identifies voice port 1/0/0 on the Cisco 3600 series as being connected to the Purchasing department:

```
voice-port 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**

Enabled for all interface types.

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. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

The **echo-cancel** command does not affect the echo heard by the user on the analog side of the connection.

There is no echo path for a 4-wire ear and mouth (E&M) interface. The echo canceller should be disabled for this interface type.

5.7.3.4.5. **Examples**

The following example enables the echo cancellation feature on voice-port 3.

```
voice-port 3
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 account 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. Examples

The following example configures a 3-decibel gain to be inserted at the receiver side of the interface in the router.:

```
port 1/4
input gain 3
```

5.7.3.6. Operation (E&M Voice Port Command)

To select a specific cabling scheme for E&M ports, use the **operation** command in voice-port configuration mode. To restore the default, use the **no** form of this command.

```
operation {2-wire | 4-wire}
no operation
```

5.7.3.6.1. Syntax Description

Keyword / Argument	Description
2-wire	Specifies a 2-wire E&M cabling scheme.
4-wire	Specifies a 4-wire E&M cabling scheme.

5.7.3.6.2. Default

2-wire operation

5.7.3.6.3. Command Mode

Voice-port configuration (E&M)

5.7.3.6.4. Usage Guideline

This command (**operation**) is applied only to the E&M voice port.

2/4-wire operation setting of the AP2520 router is made through hardware jumper setting. Unless administrators/users visually check hardware jumper

setting, they cannot check the operation type. To solve this problem, administrators/users can use this command (operation) and add description of the operation method to the router setup file. After this operation, the router administrator can check the operation status of the E&M voice port using the router setup file checking command.

For hardware jumper setting, refer to "Jumper Setting of E&M Module" of "5.4.2.2 Setting E&M Port."

5.7.3.6.5. Examples

The following example specifies that an E&M port uses a 2-wire cabling scheme:

```
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 account 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. Examples

The following example on the router configures a 6-decibel gain to be inserted at the transmit side of the interface:

```
port 1/4
output gain 3
```

5.7.3.8. polarity-inverse

To enable polarity-inverse function for a FXS voice port', use the **polarity-inverse** 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

General case, there os no needs to enable this functions.

5.7.3.8.5. Examples

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 numbers 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, this command should be set to the default 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 to receive a call.

5.7.3.9.5. Examples

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 1/1
ring number 5
```

5.7.3.10. shutdown (voice-port)

To take 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. Examples

The following example takes voice port 1/3 on the router offline:

```
configure
voice-port 1/3
shutdown
```

5.7.3.11. signal (E&M Voice Port Command)

To specify the type of signaling for a voice port, use the **signal** command in voice-port configuration mode. To restore the default value for this command, use the **no** form of this command.

E&M Voice Ports

signal {wink-start | immediate | delay-dial}

no signal

5.7.3.11.1. Syntax Description

Keyword / Argument	Description
Wink-start	Indicates that the calling side seizes the line by going off-hook on its E-lead then waits for a short off-hook "wink" indication on its M-lead from the called side before sending address information as DTMF digits. Used for E&M tie trunk interfaces. This is the default setting for E&M voice ports.
Immediate	Indicates that the calling side seizes the line by going off-hook on its E-lead and sends address information as DTMF digits. Used for E&M tie trunk interfaces.
delay-dial	Indicates that the calling side seizes the line by going off-hook on its E-lead. After a timing interval, the calling side looks at the supervision from the called side. If the supervision is on-hook, the calling side starts sending information as DTMF digits; otherwise, the calling side waits until the called side goes on-hook and then starts sending address information. Used for E&M tie trunk interfaces.

5.7.3.11.2. Default

wink-start for E&M interfaces.

5.7.3.11.3. Command Modes

Voice-port configuration

5.7.3.11.4. Usage Guideline

This command (signal) applies to analog voice ports only.

Configuring this command for an E&M voice port changes only the signal value for the selected voice port.

Some PBXs will miss initial digits if the E&M voice port is configured for Immediate signaling. If this occurs, use Delay-Dial signaling instead. Some devices have a limited number of DTMF receivers. This type of equipment must delay the calling side until a DTMF receiver is available.

5.7.3.11.5. Examples

In the following example, as soon as the line is seized by the off-hook state of the E-lead for the corresponding E&M voice port, DTMF numeric data is sent.

```
voice-port 1/1
  signal immediate
```

5.7.3.12. timing delay-duration (E&M Voice Port Command)

To specify the delay signal duration for a specified voice port, use the **timing delay-duration** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

timing delay-duration *milliseconds*

no timing delay-duration

5.7.3.12.1. Syntax Description

Keyword / Argument	Description
<i>milliseconds</i>	Delay signal duration for delay dial signaling, in milliseconds. Valid entries are numbers from 100 to 5000. Supported on E&M ports only.

5.7.3.12.2. Default

200 milliseconds

5.7.3.12.3. Command Modes

Voice-port configuration

5.7.3.12.4. Usage Guideline

The call direction for the **timing delay-duration** command is out.

5.7.3.12.5. Examples

The following example configures the delay signal duration on voice port for 3000milliseconds:

```
voice-port 1/0
    timing delay-duration 3000
```

5.7.3.13. timing delay-start (E&M Voice Port Command)

To specify the minimum delay time from outgoing seizure to out-dial address for a specified voice port, use the **timing delay-start** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

timing delay-start *milliseconds*

no timing delay-start

5.7.3.13.1. Syntax Description

Keyword / Argument	Description
<i>milliseconds</i>	Minimum delay time, in milliseconds, from outgoing seizure to outdial address. Valid entries are numbers from 20 to 2000. Supported on E&M ports only.

5.7.3.13.2. Default

300 milliseconds

5.7.3.13.3. Command Modes

Voice-port configuration

5.7.3.13.4. Usage Guideline

The call direction for the **timing delay-start** command is out.

5.7.3.13.5. Examples

The following example configures the delay-start duration on a voice port for 250 milliseconds:

```
voice-port 1/0
```

```
timing delay-start 250
```

5.7.3.14. timing dialout-delay (E&M Voice Port Command)

To specify the dial-out delay for the sending digit on a specified voice port, use the **timing dialout-delay command** in voice-port configuration mode. To reset the default value, use the **no** form of this command.

timing dialout-delay *milliseconds*

no timing dialout-delay

5.7.3.14.1. Syntax Description

Keyword / Argument	Description
<i>milliseconds</i>	Dial-out delay, in milliseconds, for the sending digit or cut-through on an E&M immediate trunk. Valid entries are from 100 to 5000 milliseconds.

5.7.3.14.2. Default

200 milliseconds

5.7.3.14.3. Command Modes

Voice-port configuration

5.7.3.14.4. Examples

The following example configures the dial-out delay voice port for 350 milliseconds:

```
voice-port 1/0
    timing dialout-delay 350
```

5.7.3.15. timing wait-wink (E&M Voice Port Command)

To specify the max time to wait for wink signal after sending outgoing seizure in milliseconds, use the **timing wait-wink** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

timing wait-wink *milliseconds*

no timing wait-wink

5.7.3.15.1. Syntax Description

Keyword / Argument	Description
<i>milliseconds</i>	Maximum wait for wink signal. Valid entries are from 100 to 400 milliseconds. Supported on E&M ports only.

5.7.3.15.2. Default

550 milliseconds

5.7.3.15.3. Command Modes

Voice-port configuration

5.7.3.15.4. Examples

The following example configures the wait-wink duration on a voice port for 300 milliseconds:

```
voice-port 1/0
  timing wait-wink 300
```

5.7.3.16. timing wink-duration (E&M Voice Port Command)

To specify the maximum wink-signal duration for a specified voice port, use the **timing wink-duration** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

timing wink-duration *milliseconds*

no timing wink-duration

5.7.3.16.1. Syntax Description

Keyword / Argument	Description
<i>milliseconds</i>	Maximum wink-signal duration, in milliseconds, for a wink-start signal. Valid entries are from 100 to 400 milliseconds. Supported on E&M ports only.

5.7.3.16.2. Default

200 milliseconds

5.7.3.16.3. Command Modes

Voice-port configuration

5.7.3.16.4. Usage Guideline

The call signal direction for the **timing wink-duration** command is out.

5.7.3.16.5. Examples

The following example configures the wink-signal duration on a voice port for 300 milliseconds:

```
voice-port 1/0
  timing wink-duration 300
```

5.7.3.17. timing wink-wait (E&M Voice Port Command)

To specify the maximum wink-wait duration for a specified voice port, use the **timing wink-wait** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

timing wink-wait *milliseconds*

no timing wink-wait

5.7.3.17.1. Syntax Description

Keyword / Argument	Description
<i>milliseconds</i>	Maximum wink-wait duration, in milliseconds, for a wink start signal. Valid entries are from 100 to 5000 milliseconds. Supported on E&M ports only.

5.7.3.17.2. Default

200 milliseconds

5.7.3.17.3. Command Modes

Voice-port configuration

5.7.3.18. Usage Guideline

The call signal direction for the **timing wink-wait** command is out.

5.7.3.18.1. Examples

The following example configures the wink-wait duration on a voice port for 300 milliseconds:

voice-port 1/0
timing wink-wait 300

5.7.3.19. 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** }

5.7.3.19.1. 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.

5.7.3.19.2. Default Value

No translation rule is applied.

5.7.3.19.3. Command Mode

Voice-port configuration Mode

5.7.3.19.4. 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.

5.7.3.19.5. Examples

In the following example, translation rule set 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
    translate-incoming calling-number 10
```

5.7.3.20. type (E&M Voice Port Command)

To specify the E&M interface type, use the **type** command in voice-port configuration mode. To reset the default value, use the **no** form of this command.

This command is for description.

type {1 | 2 | 3 | 5}

no type

5.7.3.20.1. Syntax Description

Keyword / Argument	Description
1	Sets as Type-1 in the E&M voice port. To use this, refer to the Usage Guideline below.
2	Sets as Type-2 in the E&M voice port. To use this, refer to the Usage Guideline below.
3	Sets as Type-3 in the E&M voice port. To use this, refer to the Usage Guideline below.
5	Sets as Type-5 in the E&M voice port. To use this, refer to the Usage Guideline below.

5.7.3.20.2. **Default**

Type 5

5.7.3.20.3. **Command Modes**

Voice-port configuration(E&M)

5.7.3.20.4. **Usage Guideline**

This command (**type**) is applied only to the E&M voice port.

E&M type 1, 2, 3, and 5 of the AP2520 router is made through hardware jumper setting. Unless administrators/users visually check hardware jumper setting, they cannot check the operation type. To solve this problem, administrators/users can use "**type**" command and add description of the operation method to the router setup file. After this operation, the router administrator can check the operation status of the E&M voice port using the router setup file checking command.

For hardware jumper setting, refer to "Jumper Setting of E&M Module" of "5.3.3.2 Setting E&M Port."

5.7.3.20.5. **Examples**

In the following example, Type 5 is selected as the interface type of the voice port.

```
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

The default is null string.

5.7.4.1.3. Command Mode

Dial-peer setup mode (VoIP dial peer)

5.7.4.1.4. Usage Guideline

This command is applied to the VoIP dial peer of the AP2520 VoIP Gateway.

The “**answer-address**” command is used to find the VoIP dial peer for the VoIP inbound call incoming to the network.

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. Examples

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 AP2520 Gateway.

G7231r53	G.723.1 5.3Kbps Codec
----------	-----------------------

5.7.4.2.2. Default Value

G.723.1 6.3Kbps

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** value.

If **codec** values for the VoIP peers of a connection do not match, the call will fail.

5.7.4.2.5. Examples

The following example configures a voice coder rate that provides toll quality and uses 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** dial-peer configuration command. Use the **no** form of this command 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

Enabled with a 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. Examples

The following example identifies dial peer 10 of 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) to be 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

enabled with a 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. Examples

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 range between 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

No default behavior or values.

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. Examples

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 the default, 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. Examples

If POTS peer 10 is decided for the outbound, call 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. Examples

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 the **port** 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 1 to 7.

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. Examples

The following example associates a dial peer with voice port:

```
dial-peer voice 10 pots
port 1/1
```

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. Examples

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. (max length 55)

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. Examples

The following example specifies a prefix of "9" and then a pause:

```
dial-peer voice 10 pots
prefix 9,
```

5.7.4.11. register

To configure a gateway to register or deregister a fully qualified POTS dial-peer

E.164 address with a gatekeeper, use the **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 on a router. 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. Examples

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
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. session target

To specify a network-specific address for a specified dial peer, use the **session target** dial-peer configuration command. Use the **no** form of this command to disable this feature.

session target *destination-address*
no session target

5.7.4.12.1. Syntax

Keyword / Argument	Description
destination-address	IP address of the dial peer.

5.7.4.12.2. Default Value

No Default Value

5.7.4.12.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.12.4. 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.

5.7.4.12.5. Examples

The following example configures a session-target IP address "211.238.1.1".

```
dial-peer voice 10 VoIP
session-target 211.238.1.1
```

5.7.4.13. shutdown (Dial-Peer)

To change the administrative 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

5.7.4.13.1. Syntax

This command has no arguments or keywords.

5.7.4.13.2. Default Value

No shutdown

5.7.4.13.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.13.4. 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.

5.7.4.13.5. Examples

The following example changes the administrative state of voice telephony dial peer 10 to down:

```
configure
dial-peer voice 10 pots
shutdown
```

5.7.4.14. 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
```

5.7.4.14.1. Syntax

Keyword / Argument	Description
There is no any specific keyword and argument in this command.	

5.7.4.14.2. Default Value

The default value is enable mode status.

5.7.4.14.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.14.4. 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, do disable command for this function non activation mode.

5.7.4.14.5. Examples

The following command example is disable mode of SID packet transmission function.

```
dial-peer voice 10 VoIP
no sid
```

5.7.4.15. 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 }
```

5.7.4.15.1. 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.

5.7.4.15.2. Default Value

No translation rule is applied.

5.7.4.15.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.15.4. 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.

5.7.4.15.5. Examples

In the following example, translation rule set 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
```

5.7.4.16. 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

5.7.4.16.1. Syntax

This command has no arguments or keywords.

5.7.4.16.2. Default Value

Enable

5.7.4.16.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.16.4. 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 monopolizes much less bandwidth.

If you use the **no** form of this command, VAD is disabled and voice data is continuously transmitted to the IP backbone.

5.7.4.16.5. Examples

The following example enables VAD:

```
dial-peer voice 10 VoIP
vad
```

5.7.4.17. 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*

5.7.4.17.1. Syntax

Keyword / Argument	Description
tag	The unique number assigned to the voice class. The valid range for this tag is 1 to 10,000. The <i>tag</i> number maps to the tag number created using the voice class codec global configuration command.

5.7.4.17.2. Default Value

Dial peers have no codec voice class assigned.

5.7.4.17.3. Command Mode

Dial-Peer Configuration Mode

5.7.4.17.4. Usage Guideline

You can assign one voice class to each VoIP dial peer. If you assign another voice class to a dial peer, the last voice class assigned replaces the previous voice class.

5.7.4.17.5. Examples

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

To use following command for voice announcement function, use this command. To make disable this functionality, use the **no** form of this command.

announcement

no announcement

5.7.5.1.1. Syntax

Keyword / Argument	Description
There is no any keyword and argument in this command.	

5.7.5.1.2. Default Value

Default value is disable status mode.

5.7.5.1.3. Command Mode

Voice Service VoIP Configuration Mode

5.7.5.1.4. Usage Guideline

If voice announcement function is applied to voice configuration with abnormal finishing of call processing, inputting password for FXO voice ports, and PSTN rerouting, AP2520 VoIP gateway could process voice announcement during 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. Examples

The following command example is voice announcement function for enable mode.

```
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 make disable this functionality, 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 opposite ends 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. Examples

The following example creates codec preference list 99 and applies it to dial peer 1919:

```
voice class codec 99
voice class codec 99
codec preference 1 g711alaw
codec preference 2 g711ulaw
codec preference 3 g7231r63
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. Examples

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 applicable to message transmission function for GRQ(Gatekeeper Request). Use the **no** form of this command to set disable mode.

discovery

no discovery

5.7.5.4.1. Syntax

Keyword / Argument	Description
There is no any keyword and argument in this command set.	

5.7.5.4.2. Default Value

The default status is enable mode setting.

5.7.5.4.3. Command Mode

Gateway Configuration Mode

5.7.5.4.4. Usage Guideline

When the VoIP gateway is registered gatekeeper, if this function is activated, after sending GRQ, and then receiving GCF, and finally sending RRQ. However, if this is not activated, directly send RRG.

5.7.5.4.5. Examples

The following command example is to perform disable 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. The <i>value</i> can be from 0 to 5. The default is 0..
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.

5.7.5.5.5. Examples

The following example shows T.38 fax protocol for VoIP, beginning 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 smaller 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. Examples

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

The default is **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. Examples

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 charging service. The AP2520 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 in 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. Examples

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-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*

5.7.5.9.1. 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)

5.7.5.9.2. Default Value

VoIP.*ip_address*

5.7.5.9.3. Command Mode

Gateway Configuration Mode

5.7.5.9.4. Examples

The following example configures the gateway ID is GW13@addpac.com

```
gateway
gkip 211.238.1.1
h323-id GW13@addpac.com
```

5.7.5.10. lightweight-irr

To send IRR(Information Request Response) message transmission 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

5.7.5.10.1. Syntax

Keyword / Argument	Description
There is no any keyword and argument in this command set.	

5.7.5.10.2. Default Value

The default status is disable mode.

Default로 disable 되어있습니다.

5.7.5.10.3. Command Mode

Gateway Configuration Mode

5.7.5.10.4. Usage Guideline

AP2520 VoIP gateway is able to send IRR message for response IRQ message from 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 shot, not to need large information for call processing.

5.7.5.10.5. Examples

The following command example shows to send essential information as a IRR message.

```
gateway
    lightweight-irr
```

5.7.5.11. 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

5.7.5.11.1. 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.

5.7.5.11.2. Default Value

The default status value is late mode.

5.7.5.11.3. Command Mode

Voice-Service Configuration Mode

5.7.5.11.4. 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 AP2520 VoIP gateway or remote other gateway doing starting h323 call.

It may be possible to cut a front of real voice sound in case of opening voice channel after CONNECT message with hooking off other side under default configuration late mode. To avoid this phenomenon, use **h323 call channel early** mode to open voice channel before other side hooking off.

5.7.5.11.5. Examples

The following command example shows fast voice channels

```
voice service VoIP
  h323 call channel early
```

5.7.5.12. h323 call response

If you want to define message besides ALERT message after call proceeding message about response 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

5.7.5.12.1. 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.

5.7.5.12.2. Default Value

The default status value is alert mode.

5.7.5.12.3. Command Mode

Voice-Service Configuration Mode

5.7.5.12.4. Usage Guideline

This command supports to setup configuration for one of global voice service parts for VoIP service. The AP2520 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.

5.7.5.12.5. Examples

The following command example shows how to make configuration response message to change progress message.

```
voice service VoIP
  h323 call response progress
```

5.7.5.13. 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

The default value is number 0 digit.

5.7.5.13.3. Command Mode

User-class configuration Mode

5.7.5.13.4. Examples

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. Examples

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 with mapping private IP address of VoIP gateway under static NAT/PAT network environment, use this command. To make disable 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

The default status value is disable mode.

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 AP2520 VoIP gateway. On the other hand, using public network environment under gatekeeper and other gateway, AP2520 VoIP gateway should be defined static NAT or static PAT, and public IP address.

5.7.5.15.5. Examples

The following command example shows public IP configuration mode.

```
gateway
public-ip xxx.xxx.xxx.xxx
```

5.7.5.16. register

To make registration into gatekeeper, uses **register** command in gateway configuration mode. To cancel registration into gatekeeper, use “no” command before this command.

```
register
no register
```

5.7.5.16.1. Syntax

Keyword / Argument	Description
There is no any specific keyword and argument in this command set.	

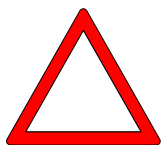
5.7.5.16.2. Default Value

The default status is disable mode.

5.7.5.16.3. Command Mode

Gateway Configuration Mode

5.7.5.16.4. Usage Guideline



To make enable function for H.323 VoIP gateway, uses register command. If VoIP gateway is enable, this VoIP gateway try to look for gatekeeper using H.323 RAS GRQ or RRQ message. If you use no register command, AP2520 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 loading configuration after doing un-registration from gatekeeper. Otherwise, messages may be crashed between gateway and gatekeeper for updating changing information

5.7.5.16.5. Examples

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 call, 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.

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 number of the inbound/outbound call.

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. Examples

In the following example, 5554123 is extended into 14085554123.

```
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. (max length 55)

5.7.5.18.2. Default Value

Disabled

5.7.5.18.3. Command Mode

Gateway Configuration Mode

5.7.5.18.4. Examples

The following example set password "okok1234":

```
gateway
```

```
security password okok1234
```

5.7.5.19. security permit-FXO

The outgoing call from remote side to FXO of this system to PSTN or PABX route is security 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 call 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 AP2520 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 AP2520 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. Examples

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** | **tttl** | **tidt** | **treg** } *value*

no timeout { **t301** | **t303** | **tras** | **tttl** | **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. Examples

In the following example, the timeout value of the RAS message has been set as 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. Examples

In the following example, translation rule set 10 is created and it is applied to the calling party number of the VoIP inbound call. Therefore, if the calling party number of the inbound call 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 a disconnect on 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. Examples

The following example forces all active calls:

```
clear h323 call all
```

5.7.6.2. clear voice port

To force a disconnect on 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 *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. Examples

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 behavior or values..

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. Examples

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 behavior or values

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 table containing a list of voice or fax calls connected through the Gateway in descending time order. Each call record is aged out of the table after a configurable number of minutes has elapsed,

5.7.6.4.5. Examples

The following is sample output from 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 behavior or values

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. Examples

The following is to display all Clear-down-tone Class.

```
show clear-down-tone
```

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 behavior or values

5.7.6.6.3. Command Mode

Administrator command

5.7.6.6.4. Examples

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 behavior or values

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 for all Voice over IP (VoIP) and plain old telephone service (POTS) dial peers configured for the router. To show configuration information for only one specific dial peer, use the argument *number* to identify the dial peer.

5.7.6.7.5. Examples

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 behavior or values.

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. Examples

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 behavior or values.

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. Examples

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 behavior or values.

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 which are 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. Examples

To show gateway related information of this system:

```
show gateway
```

5.7.6.11. show num-exp

To show all number expansions 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 behavior or values.

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. Examples

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>dia_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 behavior or values.

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. Examples

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 behavior or values.

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. Examples

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 behavior or values.

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. Examples

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 behavior or values.

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. Examples

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 behavior or values.

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. Examples

To trace VoIP events:

```
debug VoIP call
```

To stop trace:

```
undebug 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 behavior or values.

5.7.6.17.3. Command Mode

Administrator command

5.7.6.17.4. Usage Guideline

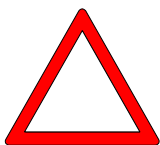
This command traces H.225 ASN.1, H.245 ASN.1, and RAS ASN.1 events, to display it on the console port. This command may effect system performance, therefore it is advised to disable this function under normal circumstances.

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 with 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, do not exit the terminal without using "no debug" or "undebug" command. Otherwise, message tracing will be displayed in the console.

5.7.6.17.5. Examples

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
```

5.8. Digital E1/T1 (ISDN PRI/R2) Installation

5.8.1. General setting and installation

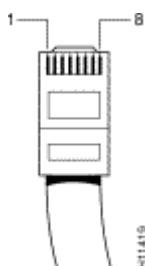
- All general and VoIP configuration setting procedure except ISDN PRI/R2 is almost same with other AddPac VoIP gateway model such as AP1100, etc.
- Currently, only AP2110, AP2520G/R, AP2830, AP2850 VoIP equipments support the Digital E1/T1 VoIP Interface module.
- Following explanation is mainly focused on E1 interface, but T1 interface is applicable also.

5.8.2. PBX side configuration setting

- Check the E1/T1 interface signaling types (ISDN PRI or R2) of PBX side. In general, ISDN PRI and R2 H/W board type is different physically.
- The 30 voice channels in E1 interface or 24 channels (T1 interface) are assigned to trunk group. And a user can bind a specific prefix number (example, 9 or 8 digit number) to this trunk group.
- In case of ISDN PRI interface, a user can configure the ISDN digit input procedures such as enbloc or overlap procedures. AddPac APV1-1E1 digital Interface supports the enbloc or overlap ISDN digit input procedure method both.
- Confirm the PCM companding type such as A-law or U-law. A-law PCM companding type is a default mode setting.

5.8.3. E1/T1 Interface Cable between PBX and APVI-1E1 Module

- AddPac APVI-1E1 VoIP digital E1 interface module support only the RJ-45 connector type. Following table show the pin configuration diagram of RJ-45 connector.



Pinouts for T1/E1 Trunk and Digital Voice Port (RJ-45) Pin	Signal
1	RX (tip)
2	RX (ring)
3	-
4	TX (tip)
5	TX (ring)
6	-
7	-
8	-

5.8.4. Voice Port Configuration of APVI-1E1 Interface Module (Optional)

- If APVI-1E1 is installed on slot0 of AP2520 VoIP equipment, voice port is 0/0. If APVI-1E1 is installed on slot1 of AP2520 VoIP equipment, voice port is 1/0.
- The VoIP configuration setting of E1 voice port is same with analog FXS/FXO configuration setting procedures. Following example show the input gain setting procedures of APVI-E1 VoIP digital E1 interface module installed on slot0. In this example, -3 means the 3dB gain.

```
router# config
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
router(config)# voice-port 0/0
```

```
router(config-voice-ports-0/0)# input gain -3
```

- As digital E1 or T1 specific command, **compand-type** command can be used for PCM quantization parameter setting. Using this command, a user can change the default a-law mode to u-law mode. (Notice: PBX peer side must be changed as u-law mode.)

```
router(config)# voice-port 0/0
router(config-voice-ports-0/0)# compand-type u-law
```

- To check the parameter setting of voice port, use the **show voice port 0/0** command. If a user uses this command, a user can see the channel parameter setting of digital E1/T1 interface module.

5.8.5. Controller Configuration of APVI-1E1 Interface Module

- **signaling mode setting (mandatory):** In AP2520G/R VoIP equipments, available signaling types are ISDN PRI, R2 and DTMF signaling types. Among the signaling types, DTMF signaling method use the CAS signaling for channel allocation like as R2 signaling type, and use the DTMF tone for digit transmission. The default signaling type is ISDN PRI signaling type. To change the signaling type, a user should use the **reboot** command after parameter setting like as following example.

```
router(config)# controller e1 0/0
router(config-controller-e1-0/0)# signaling-type r2
router# reboot
```

- **channel group setting (mandatory):** This configuration setting can be used for selecting the voice channels among the E1 interface voice channels. Following example show the voice channel selection configuration as a digital E1 VoIP interface module is installed slot0. The 16th channel configuration is ignored in channel group setting because the 16th channel is used as a signaling channel.

```
router(config)# controller e1 0/0
router(config-controller-e1-0/0)# channel-group timeslots 1-31
```

If a user want to select the channel number 1,2,3,8,20, 21 as voice channels, a following command can be used for this configuration setting.

```
router(config-controller-e1-0/0)# channel-group timeslots
1-3,8,20,21
```

- **Channel selection order (optional)** : In APVI-1E1 digital E1 VoIP interface module, when VoIP calls are started via E1 or T1 interface module, the channel allocation can be allocated among 30 or 24 free channels as a ascending order from 1th channel or descending order from 31th channel. This command can be used to determine the channel selection order. The default mode is descending order from 31th channel. We recommend that channel selection order should be opposite direction with PBX side.

```
router(config-controller-e1-0/0)# chan-number-order descending
```

- **clock source (optional)** :The clock source of AddPac E1 or T1 digital VoIP module is configurable as a master clock mode or slave clock mode. The default mode is master clock mode. To change the clock mode, AP2520G/R VoIP gateway provides the **clock-source** command.

```
router(config-controller-e1-0/0)# clock-source slave
```

- **R2 related setting (optional)** : In case of R2 signaling, to get the **calling party number** information, the following command configuration is necessary.

```
router(config-controller-e1-0/0)# r2 get-calling-number
```

- **ISDN related setting (optional)** : In ISDN signaling interface, one side is network mode, the other side is user mode. The ISDN interface mode of PBX is user mode; the peer side (VoIP gateway part) is network mode. The default mode in AddPac PRI VoIP module is network side. To change the USER/NETWORK interface mode, **isdn protocol-emulate** command can be used.

```
router(config-controller-e1-0/0)# isdn protocol-emulate user
```

Also, ISDN Q.931 timer parameter (T303, T310, N303) is changeable by user requirements

5.8.6. POTS peer setting of APVI-1E1 Interface Module (mandatory)

- In AddPac VoIP equipments, POTS peer must be existed for VoIP communication. Like as analog interface such as FXS, FXO, the POTS peer setting of digital VoIP interface can be performed using commands shown in following example.

```
router(config)#  
router(config)# dial-peer voice 0 pots  
router(config-dialpeer-pots-0)# destination-pattern 100  
router(config-dialpeer-pots-0)# port 0/0
```

In case of above example, if calling number "1001234" is received from network side, number "1234" is transmitted to peer side via ISDN PRI or R2 signaling interface.

- If a user does not want to register the E.164 number of peer side in gatekeeper, use the following command.

```
router(config-dialpeer-pots-0)# no register e164
```

5.8.7. VoIP Outgoing Call Scenario

- At first, a PBX internal-line user presses the prefix KEY number (example, 9,etc) after off-hook. After prefix KEY input, PRI line is hunted, if digit input method is overlap, a user can hear the dial-tone from VoIP gateway. After hearing the dial-tone, a user presses the called party number. If PBX digit input method is enbloc mode, END OF DIGIT # key must be pressed after dialing. In case of overlap mode, END OF DIGIT # key input is optional.
- AddPac VoIP gateway performs the H.323 outgoing call procedure according to dial-plan using called party address number received from PBX signaling interface. In this time, calling party address is internal-line number received from PBX signaling interface as a default mode. If a user want to change the calling party number, number translation of voice port or voice peer is necessary. As an example, if a user want that calling party number of all outgoing call is translated as " 2002000" number, it will be solved by following command procedures.

```
router(config)# translation-rule 0  
router(config-translation-rule#0)# rule 0 . 2002000%88  
router(config-translation-rule#0)# exit  
router(config)# dial-peer voice 1000 voip  
router(config-dialpeer-voip-1000)# translate-outgoing calling-number 0
```

5.8.8. VoIP Incoming Call Scenario

- VoIP incoming call uses the enbloc digit transmission method. If destination pattern of dial-peer

is address number " 100" and a user want to connect with internal-line number " 300" subscriber using DID method, calling party user must generates the VoIP call using called party address number " 100300" .

- In AP2520 VoIP equipment, if called party address "100300" is received from Internet, number "300" address except prefix address "200" is transmitted to PBX side.

5.8.9. E1 Configuration Example

Following command lists are simple configuration example.

In following example, digital E1 VoIP module is installed on slot0 of AP2520G/R VoIP equipment, for digital E1 PSTN interface, clock is received from peer side, AP2520 is user side, and peer side of AP2520 is network side configuration. For digital E1 PBX interface, PBX is user side, and AP2520 is network side.

In this example, number "2000" is allocated as E1 interface. So, if called party address is received from Internet through H.323 signaling procedure, E1 port is selected, except prefixed address "2000", number "1000" is transmitted to peer side via digital VoIP signaling interface.

```
! PRI controller configuration
!
controller e1 1/0
  clock-source slave
  channel-group timeslots 1-31
  isdn protocol-emulate user
!
!
dial-peer voice 4 pots
  destination-pattern 2000
  port 1/0
!
```

5.8.10. E1 Interface Debugging

Following commands are applicable for E1 interface debugging.

```
ap2520-A# debug rta ?
```

e1t1 E1/T1 Link
r2 E1/T1 CAS/R2 Signaling
q921 ISDN Q921 Packet
q931 ISDN Q931 Packet

Appendix A. AP2520 VoIP Specifications

This chapter explains the technical specification of PassFinder AP2520 VoIP Gateway/Router

IP Routing Service

IP Routing Protocols	Static and Default route
	Routing Information Protocol (RIP) v1/2
	Open Shortest Path First (OSPF) v2 Protocol
	IEEE 802.1Q VLAN Routing
	IEEE Transparent Bridging

LAN Service

Ethernet Interface	10/100Mbps Ethernet Interface
	10Mbps Ethernet for WAN Connection (Gateway Model)
Ethernet Interface Configuration	Port configuration
	Secondary/Subnet
	MTU size alteration
	ARP Entry Revalidate
	Telnet connection service

WAN Service

WAN Interface	V.35 Serial Interface for WAN (Router Model)
	10Mbps Ethernet for WAN Connection (Gateway Model)
WAN Protocol	HDLC (Cisco Compatible)
	PPP
	Frame Relay
	PPPoE for ADSL

Voice over IP Service

VoIP Protocols	ITU-T H.323 v2 Protocol with ITU-T H.235 Security Feature
	Session Initiation Protocol (SIP)
Vocie Compression	G.723.1 MP-MLQ, 6.3Kbps, 5.3Kbps
	G.729.A CS-ACELP, 8Kbps
	G.711 PCM, 64Kbps
Voice Processing	Voice Activity Detection (VAD)
	T.38 Protocol (FAX) (Out-Band / In-Band)
	Dual Tone Multi Frequency (DTMF)
	Comfort Noise Generation (CNG)
	Echo Cancellation

Network Managements

SNMP	Standard SNMP Agent MIB v2
RMON	Remote Monitoring, RFC1271 Support
Web	Web Based Management using HTTP Server Interface
Others	QoS for RTP, RTCP

Security Functions

IP Access List	Standard and Extended IP Access List, IP Packet Filtering
PPP User Authentication	Password Authentication Protocol (PAP)
	Challenge Handshake Authentication Protocol (CHAP)
Others	Access Control and Data Protections
	Enable/Disable for Specific Protocols
	Multi-level User Account Management
	Auto-disconnect for Telnet/Console Sessions

Operation and Managements

Console Port	RS-232C Based Async Serial Interface Support
Remote Manegement	Console, Rlogin, Telnet
System Performance Analysis	Process, CPU, and Connection Interface
APOS Management	APOS Configuration Back-up and Restore Remote Upgrade Function using FTP/TFTP
Others	Debugging and System Auditing
	Data Logging and Diagnostics
	System Booting, Auto-rebooting with Watch-dog Timer
	IP Traffic Statistics with Accounting

Other Scalability Features

DHCP	Dynamic Host Configuration Protocol (DHCP) Server and Relay Functions
NAT/PAT	Network Address Translation (NAT) Protocol 지원
	Port Address Translation (PAT) Protocol 지원
Bridging	IEEE Standard Spanning Tree Bridging Protocol
	Remote Bridging Support
	Concurrent Bridging Support
User Interface	Industry Standard Command Line Interface (CLI)
Others	Network Time Protocol (NTP) Support

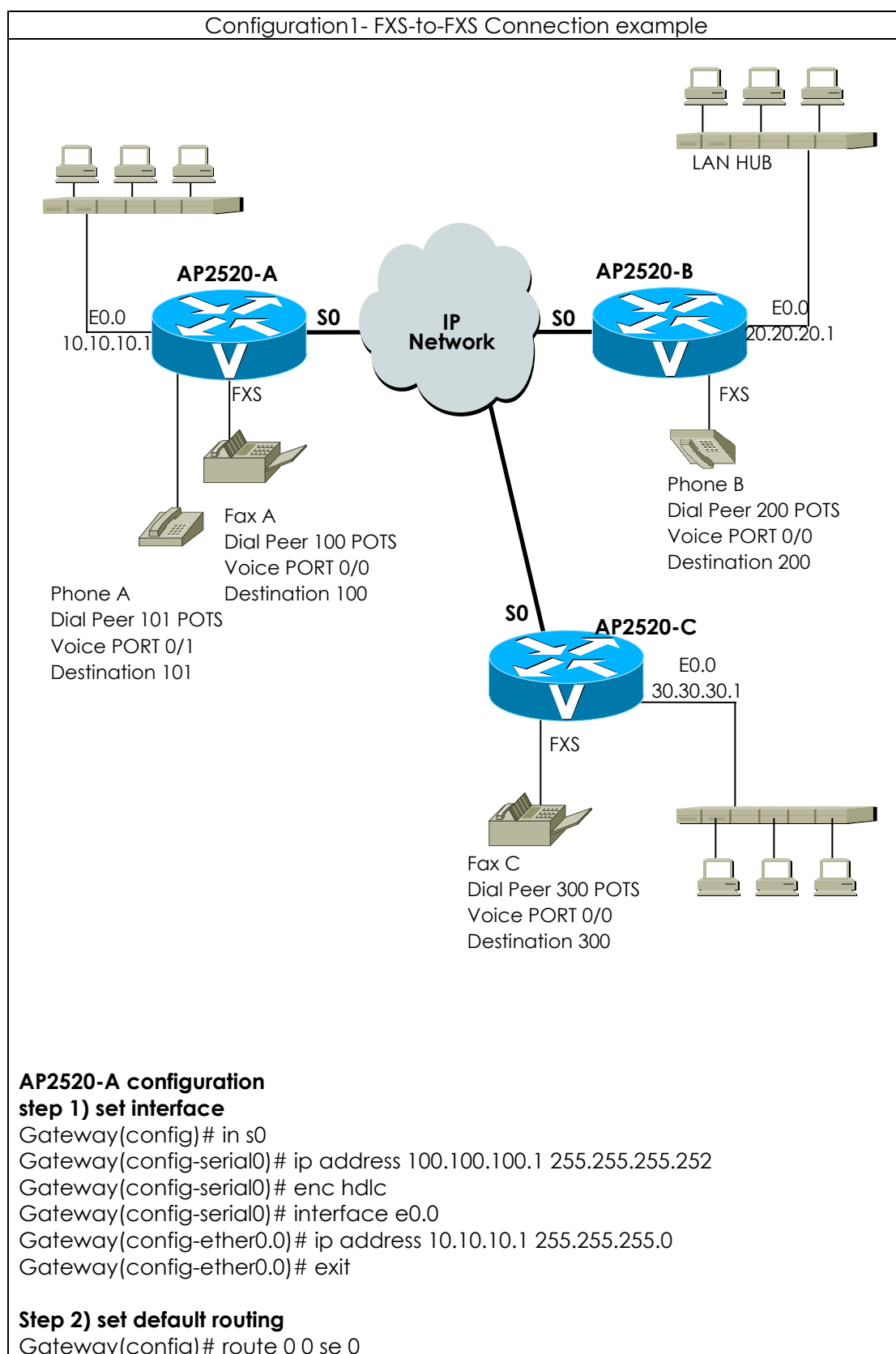
Interoperability Features

Voice Gateway	CISCO AS5300 Series
	CISCO 2600 Series
	3Com Total Control Series
	Clarent Gateway 3.0 Series
	Lucent Media Gateway Series
	Other Major Vendor

Hardware Specification

Microprocessor	32bit RISC Microprocessor
Fixed Network Interface (Gateway Model)	1-Ports 10Mbps Ethernet Interface for WAN (RJ45)
	1-Port 10Mbps Ethernet Interface for LAN (RJ45)
	1-Port Async Serial Interface for RS-232C Console Port (RJ45)
Fixed Network Interface (Router Model)	1-Ports 10Mbps Ethernet Interface for LAN (RJ45)
	1-Port Synchronous Serial Interface for WAN (V.35)
	1-Port Async Serial Interface for RS-232C Console Port (RJ45)
Supported Voice Slot	2 Slots for Voice Interface
Supported Voice Module	4-Port FXS Voice Interface (4 x RJ11) (Up to 8Ports)
	4-Port FXO Voice Interface (4 x RJ11) (Up to 8Ports)
	4-Port E&M Voice Interface (4 x RJ48) (Up to 8Ports)
	1-Port Digital E1 Voice Interface (1 x RJ48) (Up to 2Ports / MFC R2 and ISDN PRI Signaling Support)
Memory	8MB Flash Memory
	32MB SDRAM / Main Memory (Expanded to 64MB)
	512KB Boot Flash Memory
System LED	WAN, LAN, Power LED Support
Power	Free Voltage (110/220, 50/60Hz)
Power Consumption	15 Watt
Operation temperature	0°C ~ 55°C
Storage temperature	-40°C ~ 85°C
Relative humidity	5% ~ 95%
Protection against heat	Cooling Fan
W x H x D	435mm x 43mm x 205mm 1U x 19" Rack Mountable Chassis
Weight	2,418Kg

Appendix B. VoIP(Voice over IP) Config. Example



Step 3) set POTS Peer

```

Gateway(config)# dial-peer voice 100 pots
Gateway(config-dialpeer-pots-100)# port 0/0
Gateway(config-dialpeer-pots-100)# destination-pattern 100
Gateway(config-dialpeer-pots-100)# dial-peer voice 101 pots
Gateway(config-dialpeer-pots-101)# port 0/1
Gateway(config-dialpeer-pots-101)# destination-pattern 101
Gateway(config-dialpeer-pots-101)# exit

```

Step 4) set VoIP Peer

```

Gateway(config)# dial-peer voice 200 VoIP
Gateway(config-dialpeer-VoIP-200)# destination-pattern 2..
Gateway(config-dialpeer-VoIP-200)# session target 20.20.20.1
Gateway(config-dialpeer-VoIP-200)# dial-peer voice 300 VoIP
Gateway(config-dialpeer-VoIP-300)# destination-pattern 3..
Gateway(config-dialpeer-VoIP-300)# session target 30.30.30.1
Gateway(config-dialpeer-VoIP-300)# exit

```

Step 5) configuration Confirmation

```

Gateway(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 serial0
  ip address 100.100.100.1 255.255.255.252
  Encapsulation HDLC
  Operation is DOWN
!
!

```

```

Gateway(config)# sh route

```

Destination	Network-Mask	Gateway	Interface	Protocol
0.0.0.0	0.0.0.0		serial0	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	serial0	DIRECT
127.0.0.0	255.0.0.0	127.0.0.1	loopback0	DIRECT

```

Gateway(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
```

AP2520-C configuration

step 1) set interface

```
Gateway(config)# in s0  
Gateway(config-serial0)# ip address 100.100.102.1 255.255.255.252  
Gateway(config-serial0)# enc hdlc  
Gateway(config-serial0)# interface e0.0  
Gateway(config-ether0.0)# ip address 30.30.30.1 255.255.255.0  
Gateway(config-ether0.0)# exit
```

Step 2) set default routing

```
Gateway(config)# route 0 0 se 0
```

Step 3) set POTS Peer

```
Gateway(config)# dial-peer voice 300 pots  
Gateway(config-dialpeer-pots-300)# port 0/0  
Gateway(config-dialpeer-pots-300)# destination-pattern 300  
Gateway(config-dialpeer-pots-300)# exit
```

Step 4) set VoIP Peer

```
Gateway(config)# dial-peer voice 100 VoIP  
Gateway(config-dialpeer-VoIP-100)# destination-pattern 1..  
Gateway(config-dialpeer-VoIP-100)# session target 10.10.10.1  
Gateway(config-dialpeer-VoIP-100)# dial-peer voice 300 VoIP  
Gateway(config-dialpeer-VoIP-200)# destination-pattern 2..
```

```
Gateway(config-dialpeer-VoIP-200)# session target 20.20.20.1
Gateway(config-dialpeer-VoIP-200)# exit
```

Step 5) configuration Confirmation

```
Gateway(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 serial0
  ip address 100.100.102.1 255.255.255.252
  Encapsulation HDLC
  Operation is DOWN
!
!
```

```
Gateway(config)# sh route
```

Destination	Network-Mask	Gateway	Interface	Protocol
0.0.0.0	0.0.0.0		serial0	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	serial0	DIRECT
127.0.0.0	255.0.0.0	127.0.0.1	loopback0	DIRECT

```
Gateway(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
```

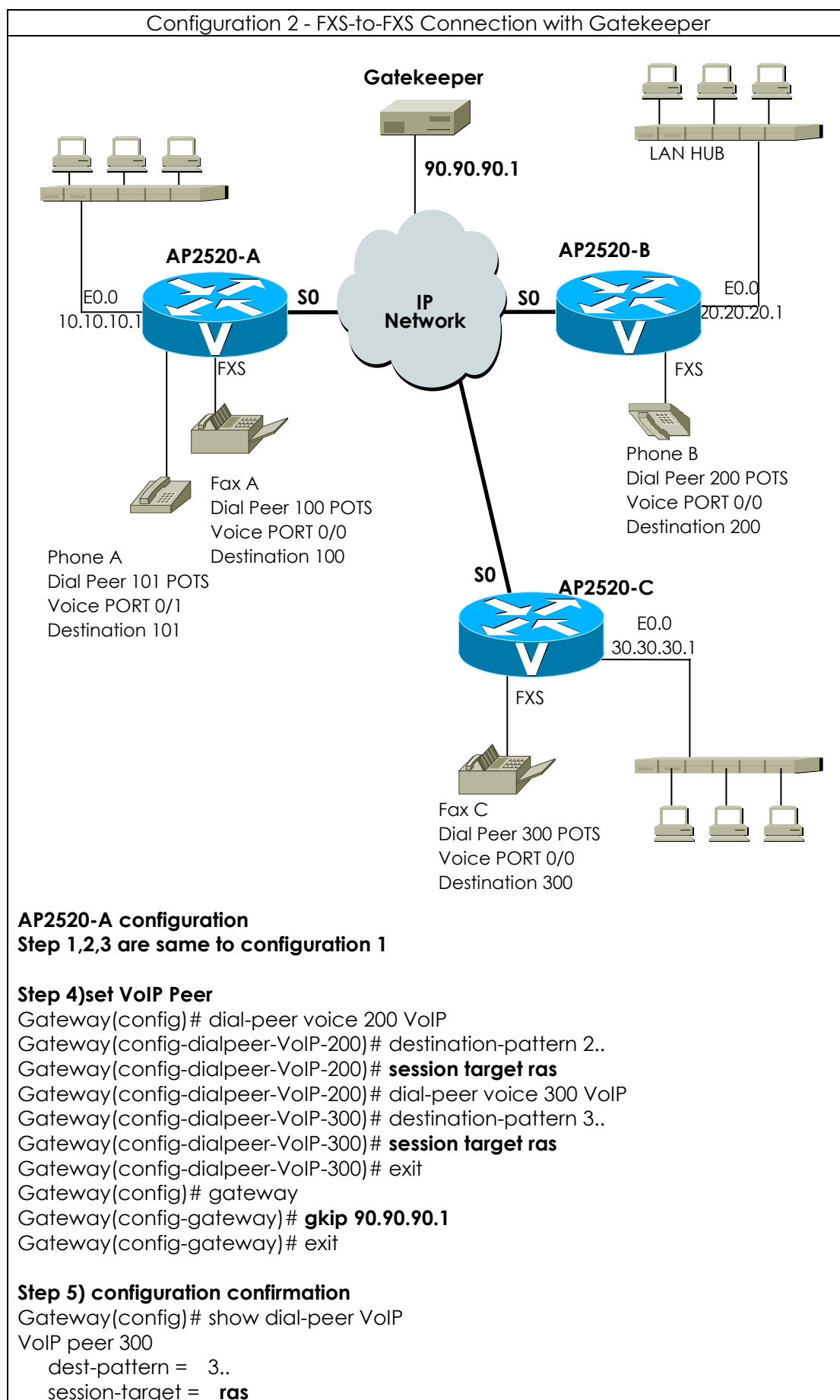
```
dtmfRelay = h245-alphanumeric  
vad = yes  
translation-outgoing called-number = -1  
translation-outgoing calling-number = -1  
description =  
administrative status = up
```

Call Scenario**1) Phone A and Phone B connection**

- User A hangs up phone A.
- user A press No. 200 dial up.
- Confirm RING sound.
- User B hangs up phone B.
- Speak over the telephone.
- Finish speaking out.

2) Fax A and FAX C connection

- Insert paper for transmission from FAX B to FAX C.
- Press No. 300 dial up from FAX B to 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
```

Gateway(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
```

AP2520-B configuration

Step 1,2,3 are same to configuration 1

Step 4)set VoIP Peer

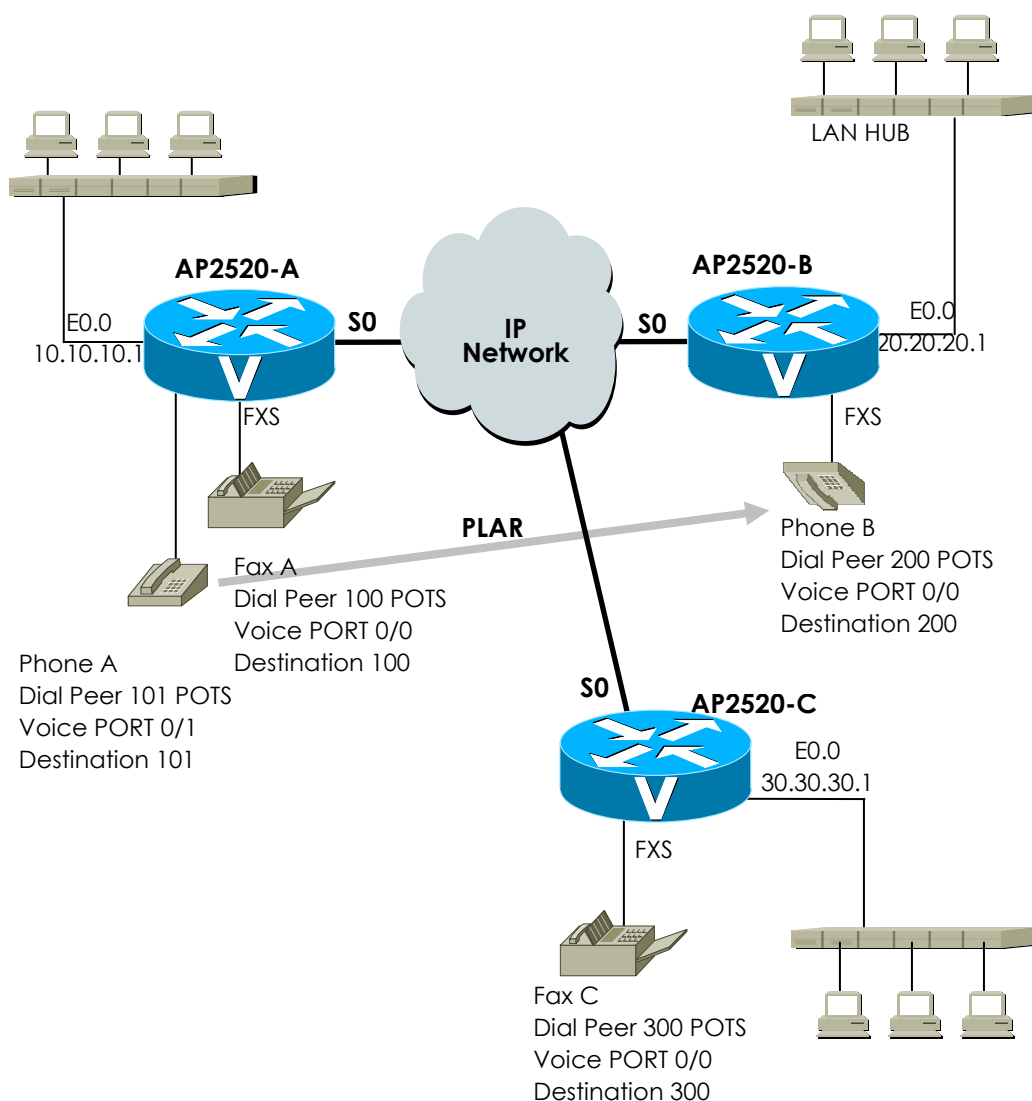
```
Gateway(config)# dial-peer voice 100 VoIP
Gateway(config-dialpeer-VoIP-100)# destination-pattern 2..
Gateway(config-dialpeer-VoIP-100)# session target ras
Gateway(config-dialpeer-VoIP-200)# dial-peer voice 300 VoIP
Gateway(config-dialpeer-VoIP-300)# destination-pattern 3..
Gateway(config-dialpeer-VoIP-300)# session target ras
Gateway(config-dialpeer-VoIP-300)# exit
Gateway(config)# gateway
Gateway(config-gateway)# gkip 90.90.90.1
```

AP2520-C configuration

Reference Gateway A,B configuration

Call Scenario

Configuration 3 - FXS-to-FXS Connection example using PLAR mode

**AP2520-A configuration**

Step 1,2,3,4 are same to configuration 1

Step 4-1) PLAR (Private Line Auto Ringdown) Configuration

Gateway(config)# voice-port 0/1

Gateway(config-voice-ports-0/1)# connect plar 200

Step 5) configuration 확인

Gateway# sh voice port 0/1

Voice port slot(0)/port(1)

line type = FXS

status = LineFree

input gain = 0 db

output gain = 0 db

ring frequency = 25 Hz

PLAR = 200

description =

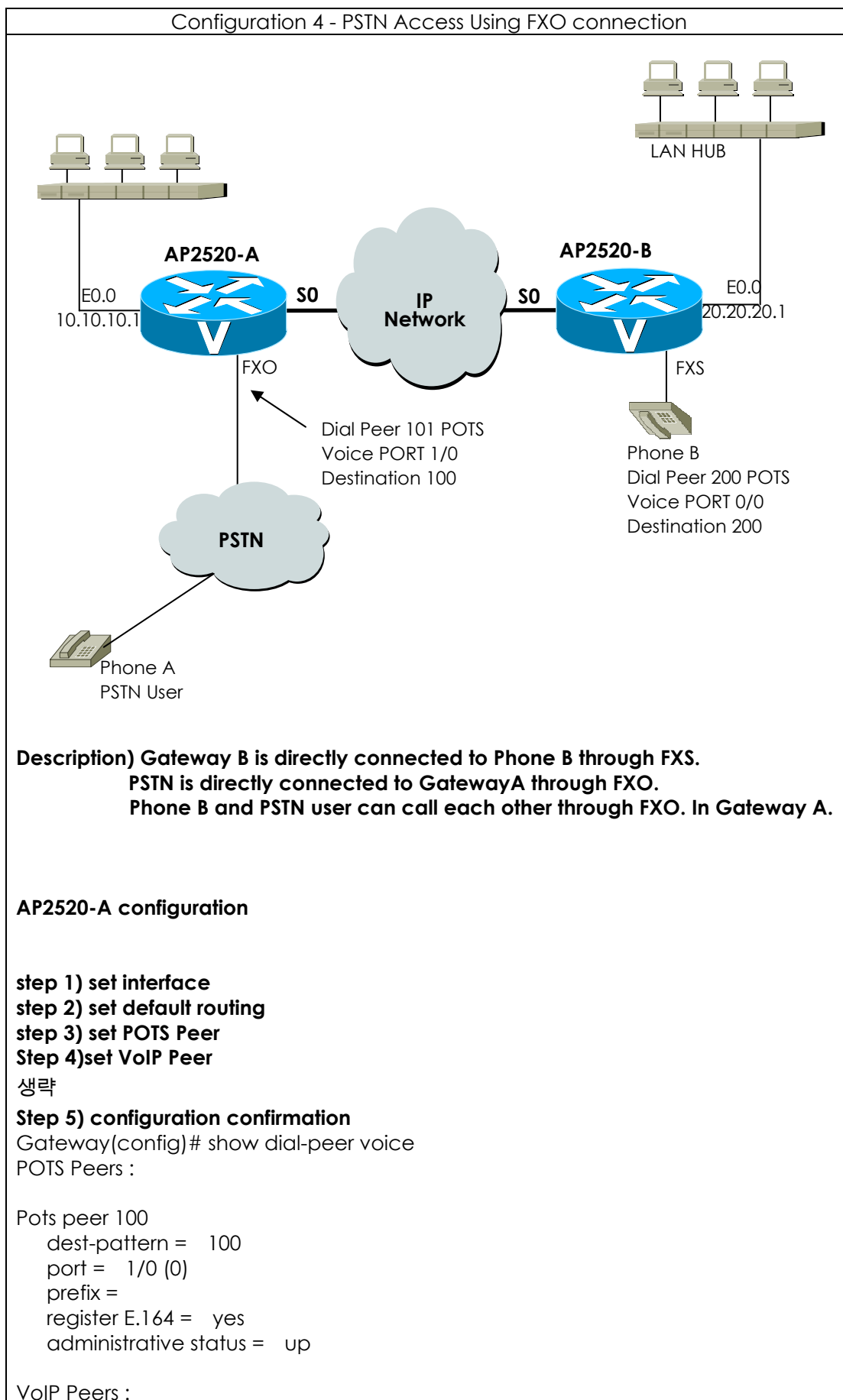
associated call number = -1

**AP2520-B configuration
same to configuration 1**

**AP2520-C configuration
same to configuration 1**

Call Scenario

1) Phone A and Phone B connection



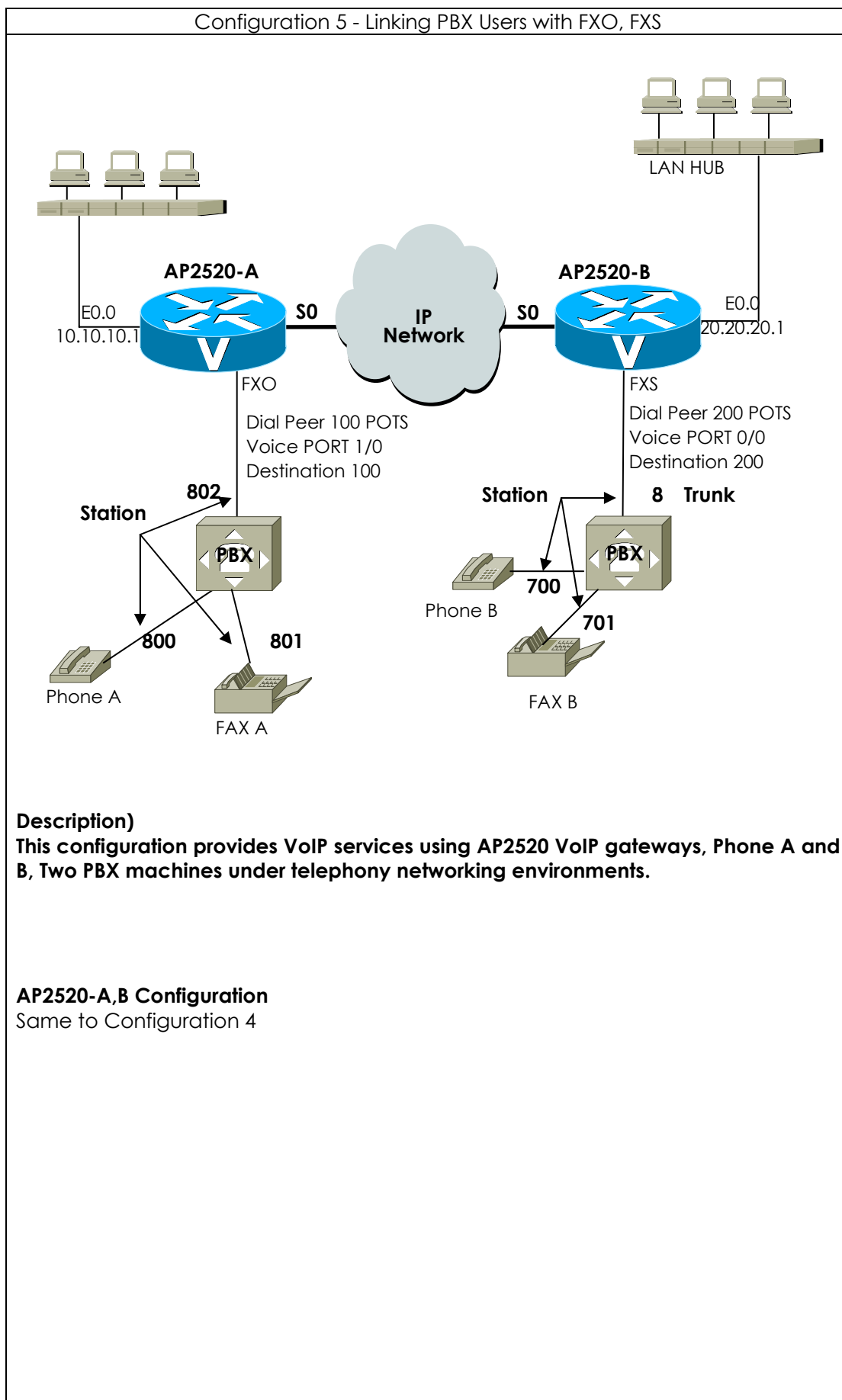
```
VoIP peer 200
  dest-pattern = 2..
  session-target = 20.20.20.1
  codec = default
  codecClass = default
  dtmfRelay = h245-alphanumeric
  vad = yes
  translation-outgoing called-number = -1
  translation-outgoing calling-number = -1
  description =
  administrative status = up
```

AP2520-B configuration

Same to configuration 1

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.
 - Hand up phone B.
 - Speak over the telephone.
 - Finish speaking out.
- 2) Call Connection from Phone B to PSTN user Phone
 - Hang 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 out.



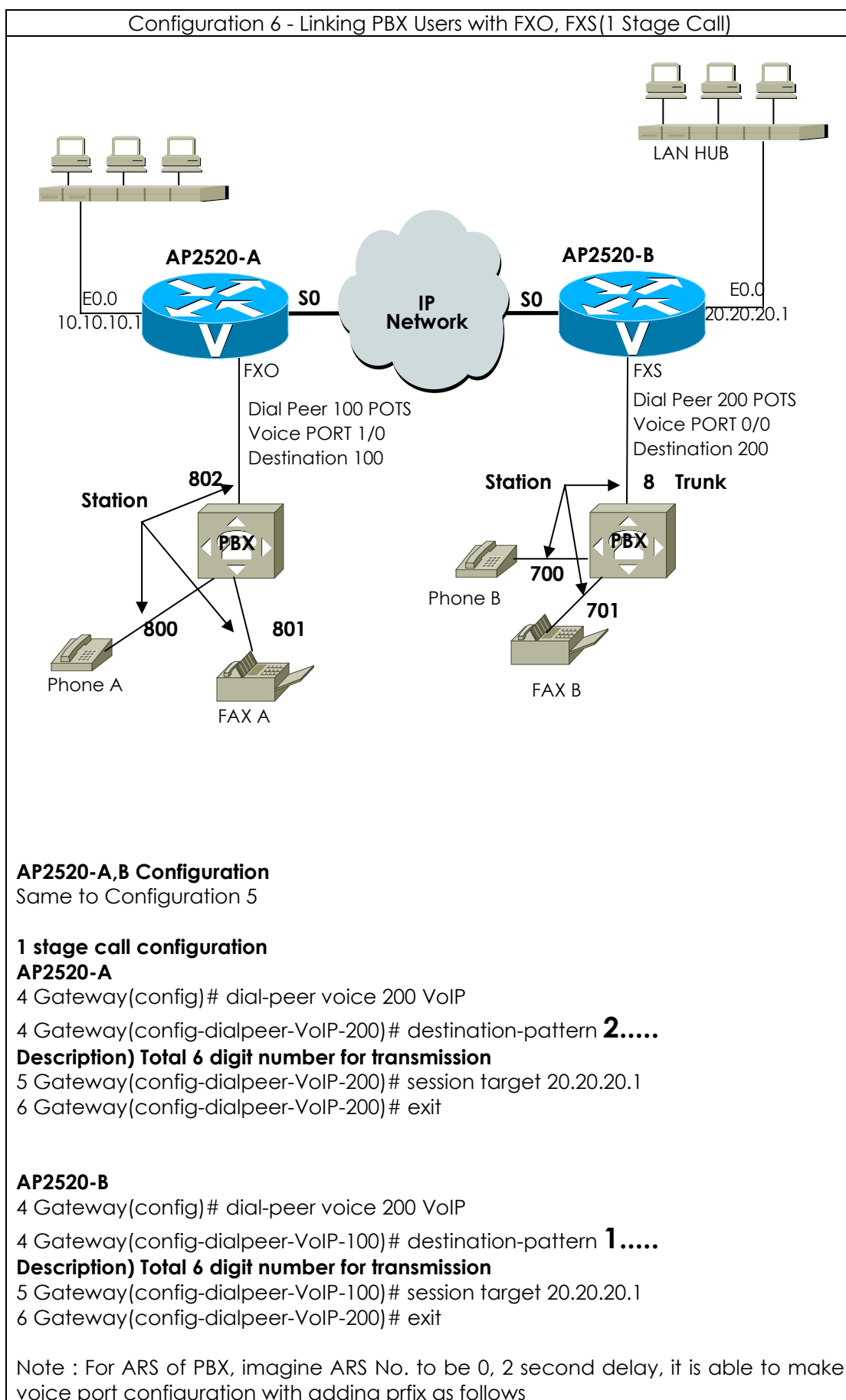
Call Scenario**1) Phone A To Phone B connection**

- Hang 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)
- Hang up Phone B
- Speak over the telephone.
- Finish speaking out.

2) Phone B To Phone A connection

- Hang 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 speaking out.

Note : Each call scenario is made up setting of PBX configuration.



Gateway(config-dialpeer-pots-100)# prefix „0,,

Description) Press 100200 at Phone B

Gateway A use No. "100"-> PBX connecting

2second delay

Gateway A dial up "0" to PBX

2 second delay

Gateway A dial up "200" to PBX

....

Call Scenario

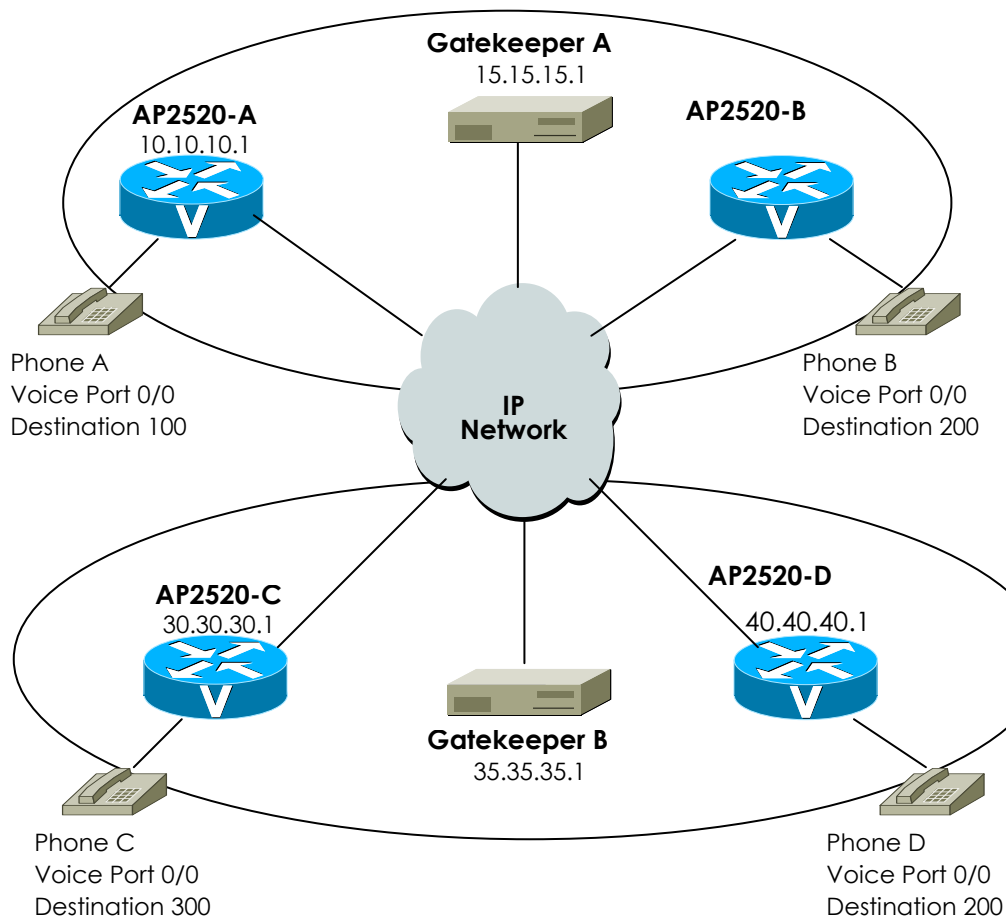
1) Phone A To Phone B connection

- Hang up Phone A.
- Listen dial tone sound of PBX machine, and then press dial No. 802 in connecting VoIP gateway A FXO port.
- Listen dial tone sound of VoIP gateway A, and then press dial No. **200700** in connecting part of VoIP gateway FXS voice port phone No. 200 and other connecting part of PBX internal phone number 700. (2 stage)
- Confirm RING sound.
- Speak over the telephone.
- Finish speaking out.

2) Phone B To Phone A connection

- Hang up Phone B.
- Listen dial tone sound of PBX B, and then press No. 8 in connecting VoIP gateway FXO voice port.
- Listen dial tone sound of VoIP gateway, and then press No. 100800 in connecting part of VoIP gateway FXO voice port phone No. 100, and other connecting part of PBX internal phone No. 800.
- Confirm RING sound.
- Speak over the telephone.
- Finish speaking out.

Configuration 7 – Calling under 2 network domain & Translate-outgoing call



Configuration & Description)

VoIP gateway A and B uses gatekeeper A, VoIP gateway C and D uses gatekeeper B. There are 3 way following call path as follows.

- 1) Phone A to Phone B
Normal path.

Configuration

Refer to Configuration 2

- 2) Phone A to Phone C

VoIP gateway A and C is connected different gatekeeper each other. To connect from phone A to phone C, gateway configuration should be setup static VoIP peer to peer configuration for each other gateway and gatekeeper.

AP2520-A Configuration

```
Gateway(config)# dial-peer voice 200 VoIP
Gateway(config-dialpeer-VoIP-200)# destination-pattern ...
Gateway(config-dialpeer-VoIP-200)# session target ras
Gateway(config-dialpeer-VoIP-200)# dial-peer voice 300 VoIP
Gateway(config-dialpeer-VoIP-300)# destination-pattern 3..
Gateway(config-dialpeer-VoIP-300)# session target 30.30.30.1
Gateway(config-dialpeer-VoIP-300)# exit
```

```
Gateway(config)# gateway
Gateway(config-gateway)# gkip 15.15.15.1
Gateway(config-gateway)# exit
```

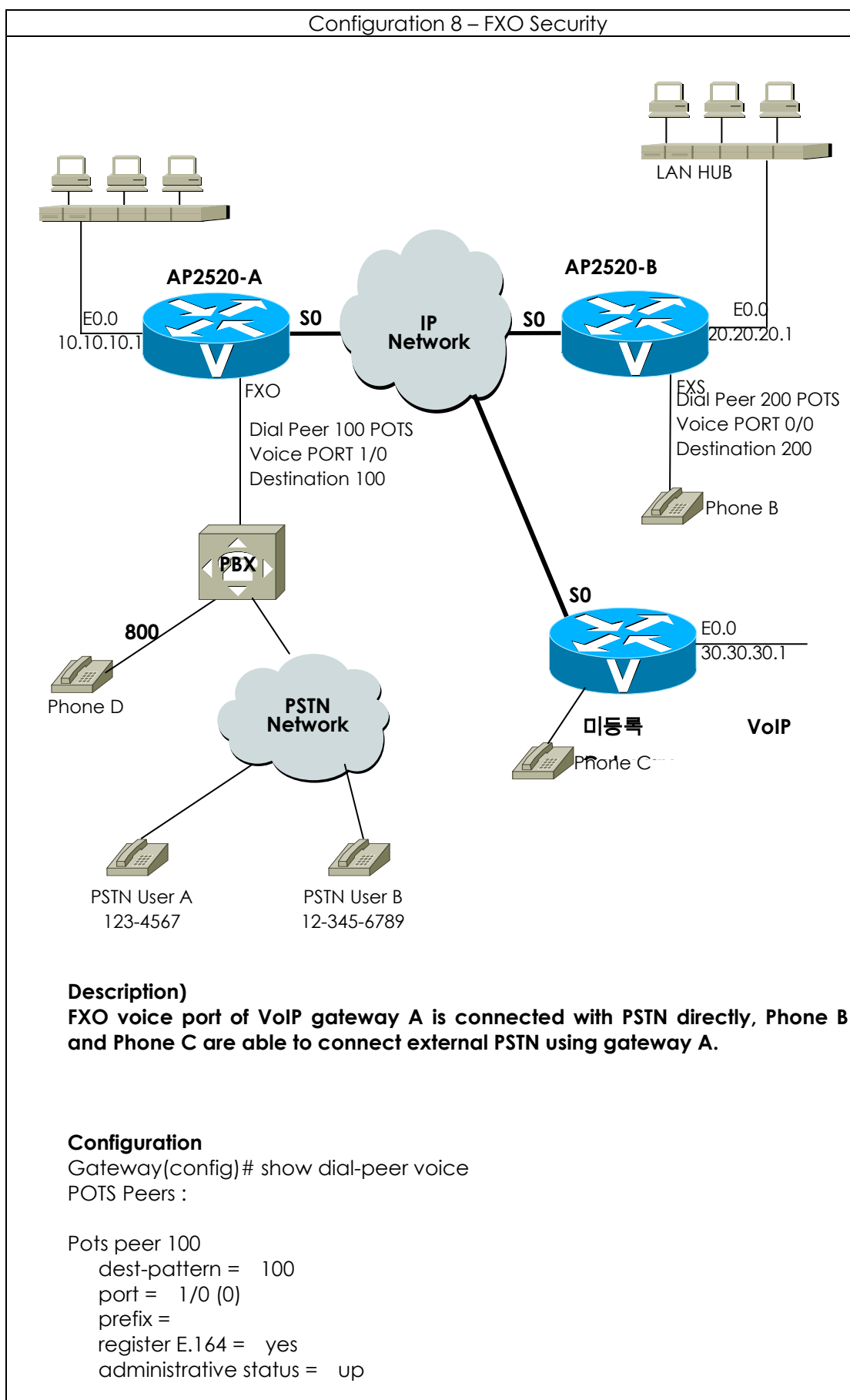
3) Phone A to Phone D

AP2520-A Configuration (추가)

```
Gateway (config)# translation-rule 1
Gateway (config-trans-rule-0)# rule 0 8.. 2
Gateway (config-trans-rule-0)# exit
Gateway (config)# dial-p voice 800 VoIP
Gateway (config-dialpeer-VoIP-800)# destination-pattern 8..
Gateway (config-dialpeer-VoIP-800)# session target 40.40.40.1
Gateway (config-dialpeer-VoIP-800)# translate-outgoing called-number 1
```

Call Scenario

- 1) Call from Phone A to Phone B
 - Hang up Phone A.
 - Press dial No. 200 of Phone B
 - Confirm RING sound of Phone B
 - Hang up Phone B
 - Speak over the telephone.
 - Finish speaking out.
- 2) Call from Phone B to Phone C
 - Hang up Phone B.
 - Press dial No. 300 of Phone C.
 - Confirm RING sound of Phone C.
 - Hang up Phone C
 - Speak over the telephone.
 - Finish speaking out.
- 3) Call from Phone A to Phone D
 - Hang up Phone A.
 - Press dial No. 800 of Phone D.
 - Confirm RING sound of Phone D.
 - Hang up Phone D.
 - Speak over the telephone.
 - Finish speaking out.



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
```

Gateway(config)# **voice service VoIP**

Gateway(config-vservice-VoIP)# **no security permit-FXO**

% default is permit-FXO

call scenario)

- 1) call Phone B to Phone D
 - Hang up Phone A
 - Press dial No. 100 of Phone B FXO voice port phone number.
 - Press dial No. 800 of PBX machine internal phone number.
 - Speak over the telephone.
 - Finish speaking out.
- 2) call Phone C to Phone D
 - Hang up Phone C
 - Press dial No. 100 of Phone C FXO voice port phone number.
 - Confirm silence sound
 - Finishing

설정 2) User Class Configuration.

Password check for every call under VoIP gateway A FXO voice port

Configuration)

Configuration

Gateway(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
```

```
Gateway(config)# voice class user 1
Gateway(config-vclass-user#1)# password 1234
Gateway(config-vclass-user#1)# max-digits 3
Gateway(config-vclass-user#1)# exit
Gateway(config)# voice class user 2
Gateway(config-vclass-user#2)# password 4567
Gateway(config-vclass-user#2)# max-digits 8
Gateway(config-vclass-user#2)# exit
Gateway(config)# voice class user 3
Gateway(config-vclass-user#2)# password 7890
Gateway(config-vclass-user#2)# max-digits 0
Gateway(config-vclass-user#2)# exit
```

call scenario)

- 1) Phone B to PSTN user A using user class 1
 - Hang up Phone B.
 - Press dial No. 100 of Phone B
 - Listen shot dial tone, and then press password No. 1234 as user class 1
 - Listen normal dial tone of PBX machine, and then press dial No. 800
 - Speak over the telephone
 - Finish speaking out.
- 2) Phone B to PSTN user A using user class 1
 - Hang up Phone B
 - Press dial No. 100 of Phone B FXO
 - Listen shot dial tone, and then press password No. 1234 as user class 1
 - Listen normal dial tone of PBX machine, and then press dial No. 9 for external PSTN connection
 - Listen dial tone, and then press dial No. 1234567 for PSTN call.
 - Speak over the telephone
 - Finish speaking out.
- 3) Phone B to PSTN user A using user class 2
 - Hang up Phone B
 - Press dial No. 100 of Phone B FXO voice port
 - Listen shot dial tone, and then press password No. 4567 as user class 2.

- Listen normal dial tone of PBX machine, and then press dial No. 9 for external PSTN connection.
 - Listen dial tone, and then press dial No. 12345678 for PSTN call.
 - Speak over the telephone
 - Finish speaking out.
 -
- 4) Phone B to PSTN user B using user class 3
- Hang up Phone B
 - Press dial No. 100 of Phone B FXO voice port
 - Listen shot dial tone, and then press password No. 7890 as user class 3.
 - Listen normal dial tone of PBX machine, and then press dial No. 9 for external PSTN connection.
 - Listen dial tone, and then press dial No. 123456789 for PSTN call.
 - Speak over the telephone
 - Finish speaking out.

Appendix C AP2520 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.

AP2520 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) 또는 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 PassFinder AP2520 Gateway.

- Console Port Signal and Pinout(RJ-45 to DB9)
- Ethernet Cable Assemble(RJ-45 to RJ-45) Pinout
- Synchronous Serial Cable Assemble(V.35 to V.35) Pinout

[Console Port Signal and Pinout]

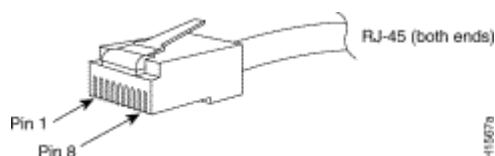
In order to connect the Gateway console port with the Terminal Emulating PC, the RJ-45 to DB9(Female DTE Connector) cable is used. The transferred signal and Pinout specifications are enlisted in the following Table C-1 "Console Port Signal and Pinout".

Gateway 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]

[Synchronous Serial Cable Assemble (V.35 to V.35) Pinout]

In order to connect the router with WAN DCE equipments (i.e. DSU/CSU), the V.35 to V.35 (DTE(Male) to DTE(Male)) cable is used. The cable transfer signal follow EIA/TIA-449 specifications and the connectors follow 34Pin J2 standards. The signals and the Pinout specifications are provided in the following Table C-3 "V.35 to V.35 Signal and Pinout".

34Pin V.35 (Router)	5.8.10.1.1.1. Signal	Direction	34Pin V.35 (CSU/DSU)
J2-A	Frame GND	-	J2-A
J2-B	Circuit GND	-	J2-B
J2-C	RTS	→	J2-C
J2-D	CTS	←	J2-D
J2-E	DSR	←	J2-E
J2-F	RLSD	←	J2-F
J2-H	DTR	→	J2-H
J2-K	LT	→	J2-K
J2-P	SD+	→	J2-P
J2-S	SD-	→	J2-S
J2-R	RD+	←	J2-R
J2-T	RD-	←	J2-T
J2-U	SCTE+	→	J2-U
J2-W	SCTE-	→	J2-W
J2-V	SCR+	←	J2-V
J2-X	SCR-	←	J2-X
J2-Y	SCR+	←	J2-Y
J2-AA	SCR-	←	J2-AA

[Table D-3 V.35 to V.35 Signal and Pinout]