VoIP Gateway Main Software Functions

AddPac

AddPac Technology

Sales and Marketing

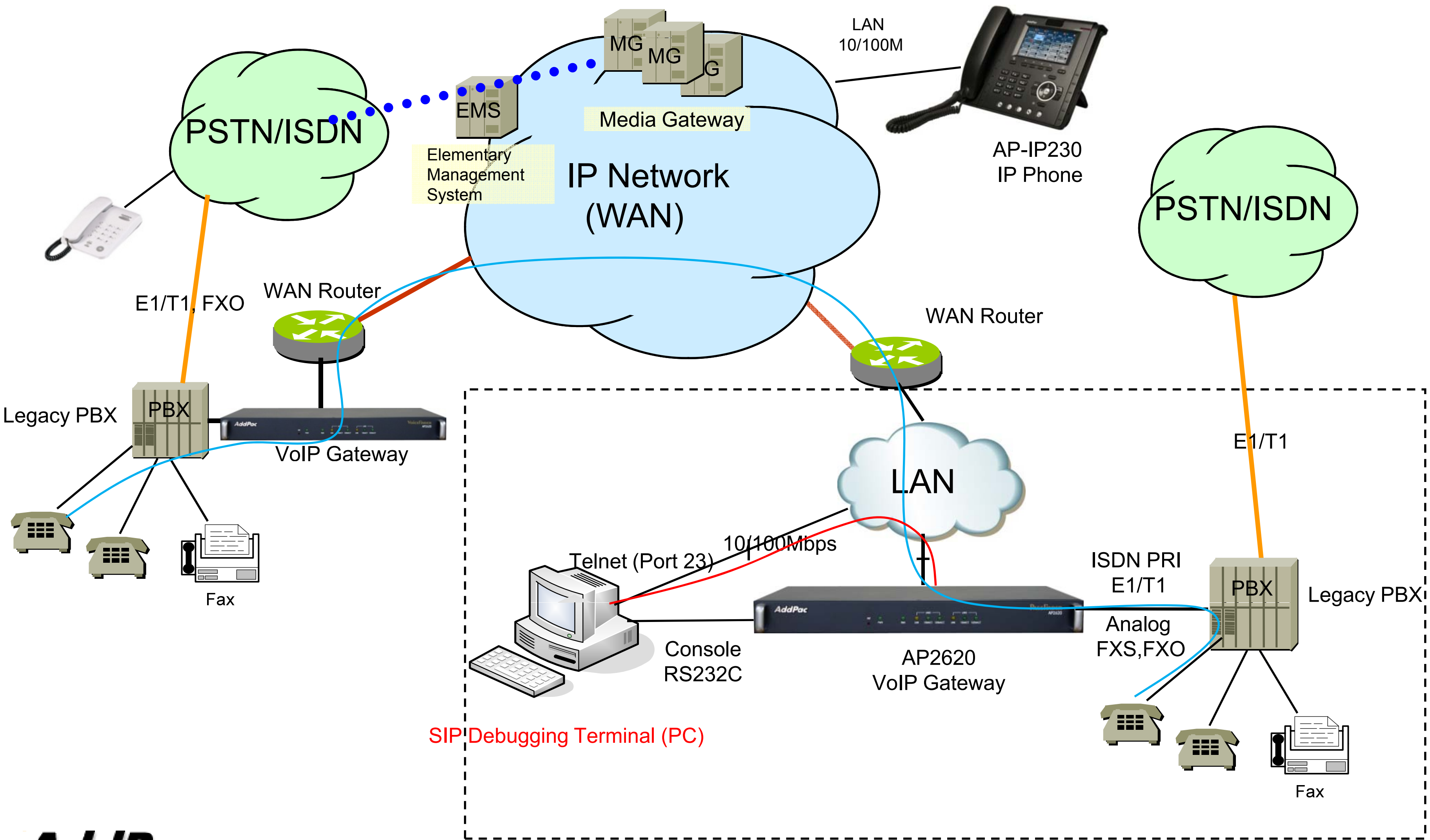
www.addpac.com

Contents

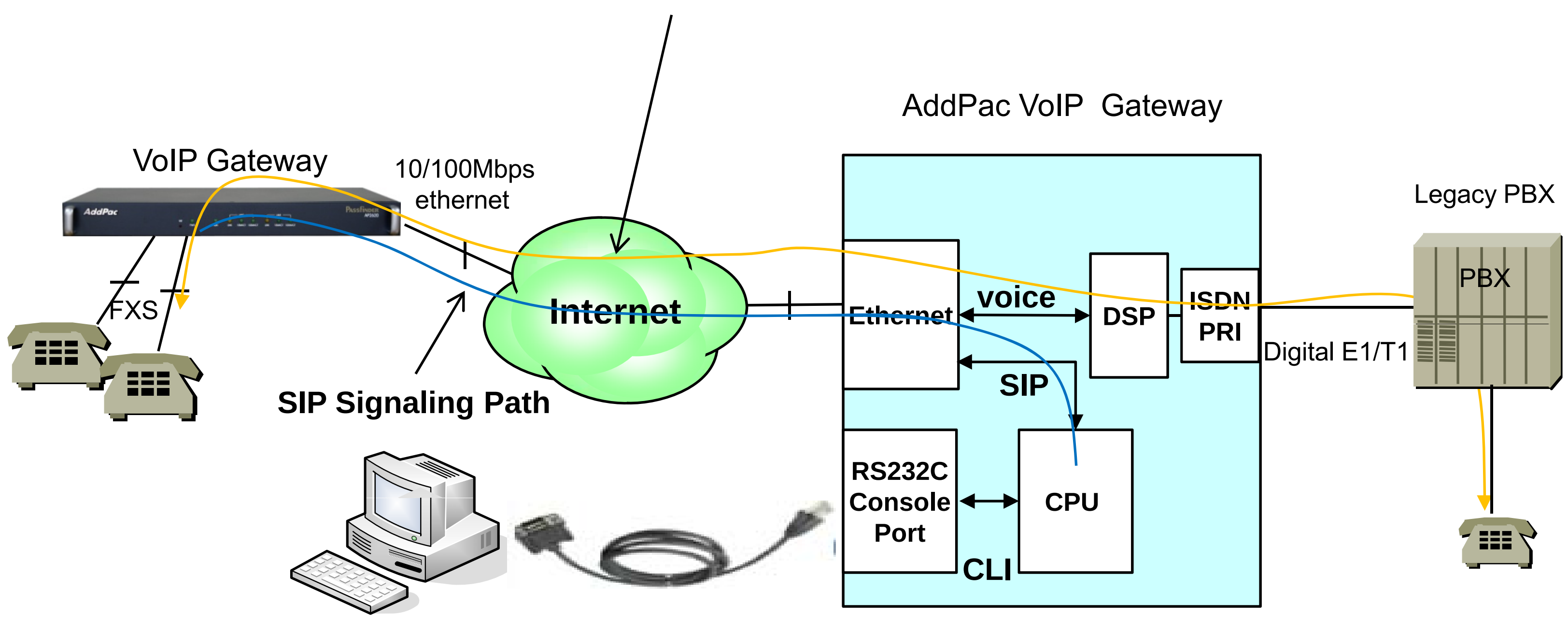
SIP Protocol Debugging Service Overview

Contents

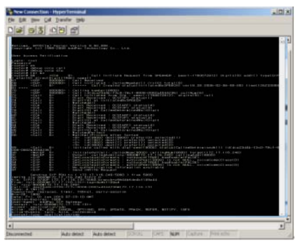
Network Diagram for SIP Debugging



SIP Debugging Access Method via Console Port



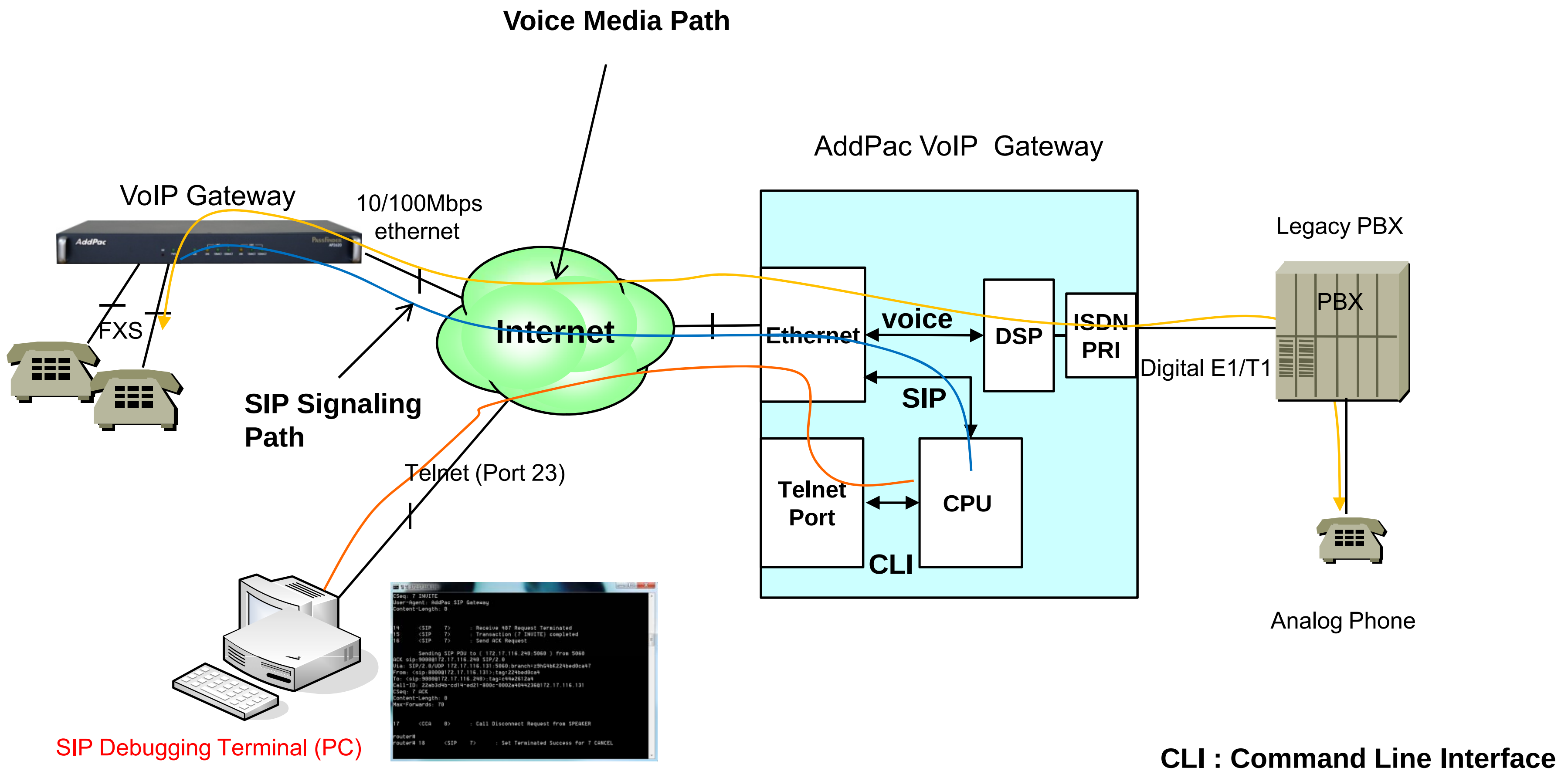
SIP Debugging Terminal (PC)



Windows HyperTerminal

CLI : Command Line Interface

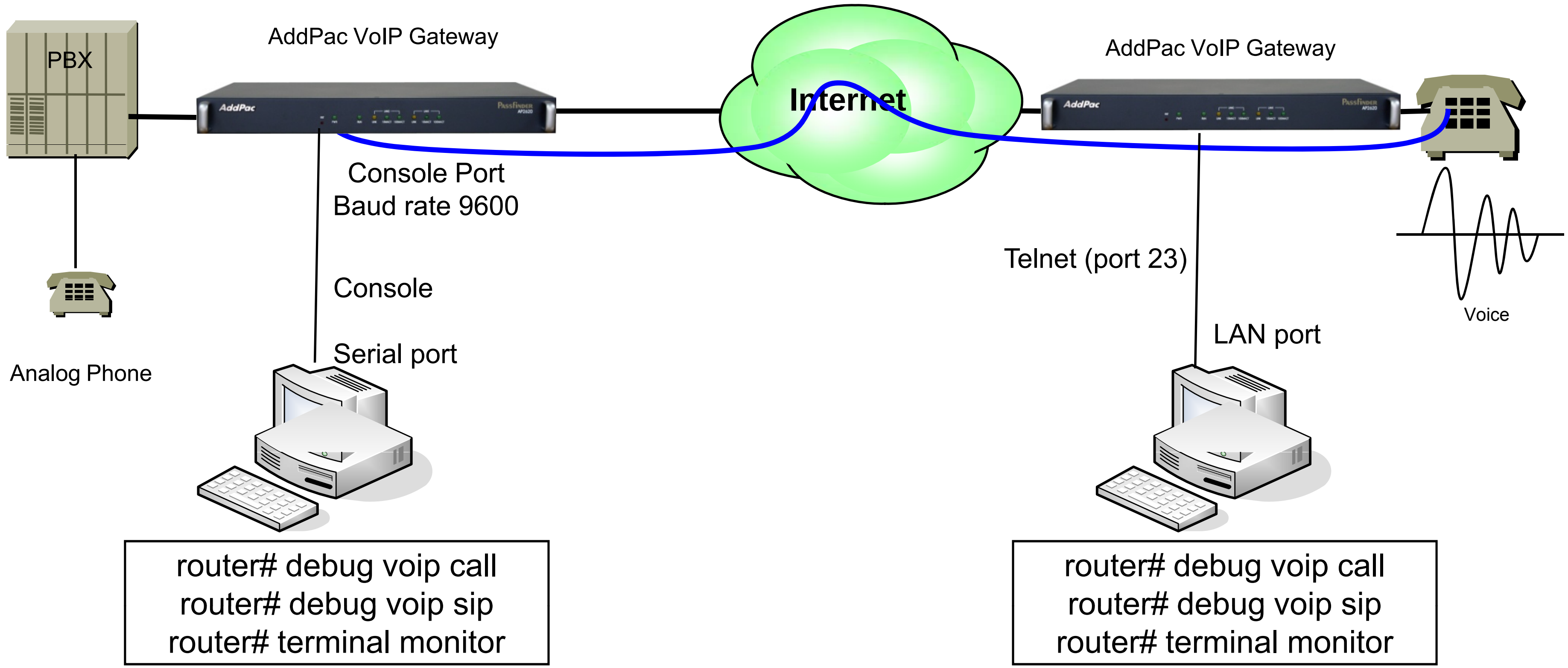
SIP Debugging Access Method via Telnet Port



Usable with telnet access program such as TeraTerm, window command, Putty, CRT

CLI : Command Line Interface

Real-time SIP Debugging Environment



VoIP Debugging Commands

Major Command

```
Login: root
Password:
router> en
router# debug voip ?                -> VoIP Debugging command
  h225-asn1   H.225 ASN.1 trace
  h245-asn1   H.245 ASN.1 trace
  ras-asn1    RAS ASN.1 trace
  call        Call trace            -> Call trace Debugging Command
  mgcp        MGCP message trace
  number      debug on a specific number (calling or called party number)
  port        debug on a specific voice port
  sip         SIP message trace     -> SIP Message Debugging
router# terminal monitor            -> Display SIP debug message through terminal
                                       Useful  when debugging by remote accessing
router# no termial monitor          -> Use when deactivate of debug command (valid when accessing telnet)
```

SIP Debugging Commands (Example)

```
Welcome, APOS(tm) Kernel Version 8.50.006.
Copyright (c) 1999-2008 AddPac Technology Co., Ltd.

User Access Verification

Login: root
Password:
router> en
router# debug voip call
router# debug voip sip
router# terminal monitor
router# 1      <CCA    0>     : Call Initiate Request from SPEAKER , peer(-
               1760673404) digits() addr() type(SIP) plar(0) directDigit(FALSE)
               name()
2      <CEP    000000> : Call Received
3      <CEP    000000> : Call Initiated : calledNumber() crv(0) total(0)
4      <Call   8>      : ****** Call Created status(InitiatedBySPEECH)
               ver(8.28:2006-02-06-00-00) time(1262390967) ****
5      <CEP    000000> : Calling number(8000)
6      <CEP    000000> : Call id(b78e3e4b-3c3f-2691-800e-0002a4044236)
               callNum(8)
7      <Call   8>      : Call Initiated from CCA : peer(-1760673404), digits(), ip()
8      <CCA    0>      : Digit Received : 9(START) status(1)
9      <CCA    0>      : Digit Received : 9(STOP) status(4)
10     <Call   8>      : Digit(9) at InitiatedBySPEECH
11     <Call   8>      : MatchedAll
12     <CCA    0>      : Digit Received : 0(START) status(4)
13     <CCA    0>      : Digit Received : 0(STOP) status(4)
14     <Call   8>      : Digit(0) at CalleeDeterminedWaitDigit
15     <Call   8>      : MatchedAll
16     <CCA    0>      : Digit Received : 0(START) status(4)
17     <CCA    0>      : Digit Received : 0(STOP) status(4)
18     <Call   8>      : Digit(0) at CalleeDeterminedWaitDigit
19     <Call   8>      : MatchedAll
20     <CCA    0>      : Digit Received : 0(START) status(4)
21     <CCA    0>      : Digit Received : 0(STOP) status(4)
22     <Call   8>      : Digit(0) at CalleeDeterminedWaitDigit
23     <Call   8>      : MatchedPerfect
24     <Call   8>      : MatchAllProcess After Sorted
```

```
<0> id(9999) dest(9000) prefer(0) selected(3)
                <1> id(1001) dest(T) prefer(0) selected(0)
                <2> id(1002) dest(T) prefer(1) selected(0)
                <3> id(3000) dest(T) prefer(2) selected(0)
25     <Call   8>      : Initiate callee with dial-peer(9000)
           status(CalleeDeterminedAll) id(b78e3e4b-3c3f-2691-800e-
           0002a4044236)
26     <NetEP  8>      : InitiateOutCall: calledNum(9000) callingNum(8000)
           target(172.17.116.240)
27     <NetEP  8>      : DoCall: calledAddr(sip:9000@172.17.116.240)
           callingAddr(8000)
28     <SIP    8>      : SetLocalAudioFormats : outbound(TRUE) hqaEnable(FALSE)
29     <SIP    8>      : SetLocalAudioFormats : myVoipPeer(9999) is not NULL,
           voiceCodecClass(0)
30     <SIP    8>      : SetLocalAudioFormats : outbound(TRUE) hqaEnable(FALSE)
31     <SIP    8>      : SetLocalAudioFormats : myVoipPeer(9999) is not NULL,
           voiceCodecClass(0)
32     <SIP    0>      : No authentication information available
33          <SIP    8>      : Send INVITE Request
 Sending SIP PDU to ( 172.17.116.240:5060 ) from 5060
INVITE sip:9000@172.17.116.240 SIP/2.0
Via: SIP/2.0/UDP 172.17.116.131:5060;branch=z9hG4bKbb4b310fa49
From: <sip:8000@172.17.116.131>;tag=bb4b310fa4
To: <sip:9000@172.17.116.240>
Call-ID: bb8e3e4b-0fa6-314b-800f-0002a4044236@172.17.116.131
CSeq: 9 INVITE
Supported: replaces, timer, 100rel, early-session
Min-SE: 1800
Date: Sat, 02 Jan 2010 00:09:31 GMT
Session-Expires: 1800
User-Agent: AddPac SIP Gateway
Contact: <sip:8000@172.17.116.131>
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE, PRACK, REFER, NOTIFY,
           INFO
Allow-Events: talk, hold, conference
Content-Type: application/sdp
Content-Length: 304
Max-Forwards: 70
```

SIP Debugging Commands (Example)

```
v=0
o=8000 1262390971 1262390971 IN IP4 172.17.116.131
s=AddPac Gateway SDP
c=IN IP4 172.17.116.131
t=1262390971 0
m=audio 23016 RTP/AVP 0 8 18 4 2 9
a=ptime:20
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:4 G723/8000
a=rtpmap:2 G726-32/8000
a=rtpmap:9 G722/8000
 Received SIP PDU from ( 172.17.116.240:5060 )
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.17.116.131:5060;branch=z9hG4bKbb4b310fa49
From: <sip:8000@172.17.116.131>;tag=bb4b310fa4
To: <sip:9000@172.17.116.240>
Call-ID: bb8e3e4b-0fa6-314b-800f-0002a4044236@172.17.116.131
CSeq: 9 INVITE
User-Agent: AddPac SIP Gateway
Content-Length: 0
34     <SIP    8>      : Receive 100 Trying
35     <SIP    8>      : Transaction (9 INVITE) proceeding

       Received SIP PDU from ( 172.17.116.240:5060 )
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.17.116.131:5060;branch=z9hG4bKbb4b310fa49
From: <sip:8000@172.17.116.131>;tag=bb4b310fa4
To: <sip:9000@172.17.116.240>;tag=384e3113a4
Call-ID: bb8e3e4b-0fa6-314b-800f-0002a4044236@172.17.116.131
CSeq: 9 INVITE
Supported: timer, replaces, early-session
User-Agent: AddPac SIP Gateway
Contact: sip:9000@172.17.116.240
RSeq: 223744
Require: 100rel
Content-Type: application/sdp
Content-Length: 434
```

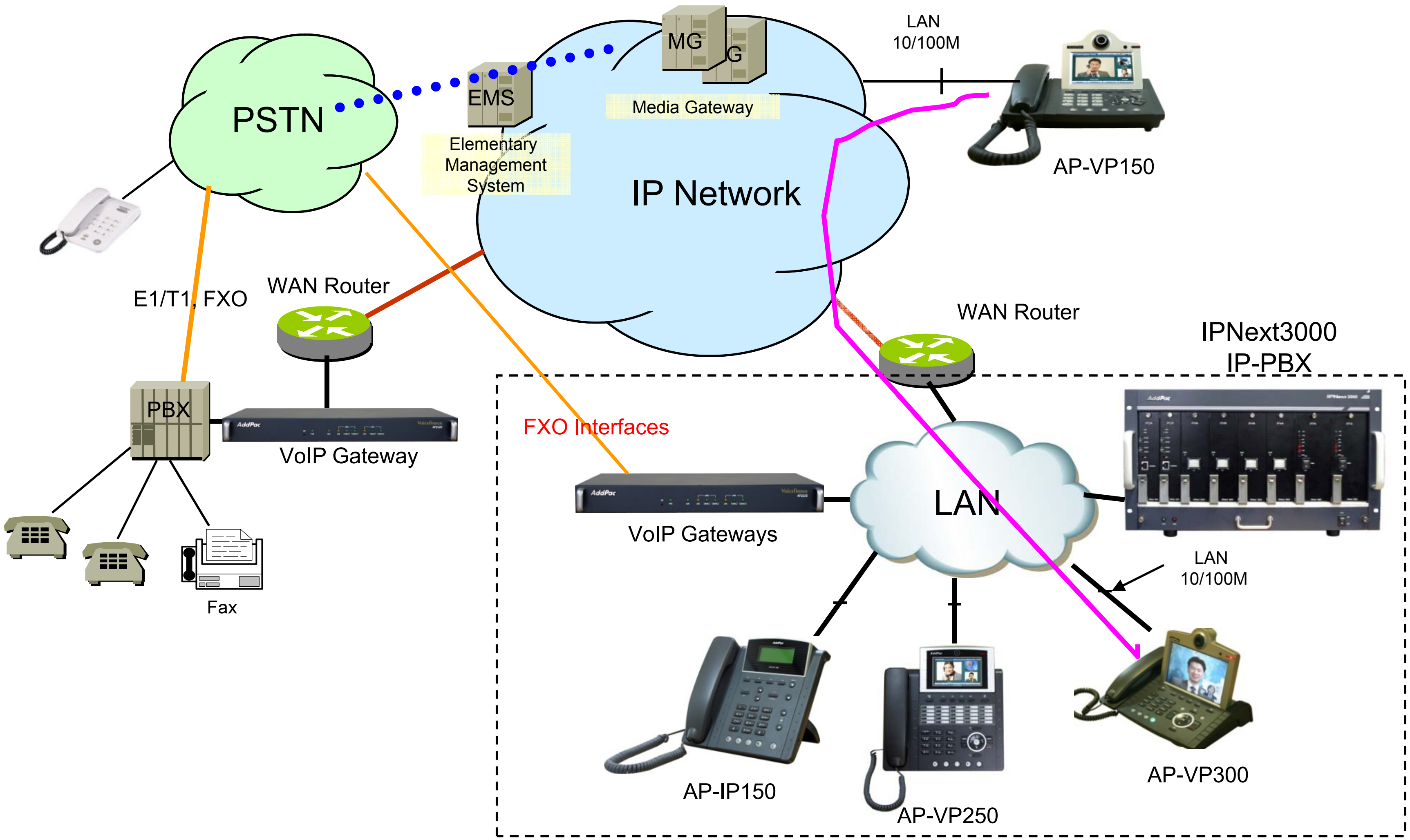
```
Received SIP PDU from ( 172.17.116.240:5060 )
SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.17.116.131:5060;branch=z9hG4bKbb4b310fa49
From: <sip:8000@172.17.116.131>;tag=bb4b310fa4
To: <sip:9000@172.17.116.240>;tag=384e3113a4
Call-ID: bb8e3e4b-0fa6-314b-800f-0002a4044236@172.17.116.131
CSeq: 9 INVITE
Supported: timer, replaces, early-session
Session-Expires: 1800;refresher=uac
User-Agent: AddPac SIP Gateway
Contact: sip:9000@172.17.116.240
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE, REFER, NOTIFY, INFO
Require: timer
Content-Length: 0


43     <SIP    8>      : Receive 200 OK
44     <SIP    8>      : Received INVITE OK response
45     <SIP    8>      : Send ACK Request

       Sending SIP PDU to ( 172.17.116.240:5060 ) from 5060
ACK sip:9000@172.17.116.240 SIP/2.0
Via: SIP/2.0/UDP 172.17.116.131:5060;branch=z9hG4bKbb4b310fa49
From: <sip:8000@172.17.116.131>;tag=bb4b310fa4
To: <sip:9000@172.17.116.240>;tag=384e3113a4
Call-ID: bb8e3e4b-0fa6-314b-800f-0002a4044236@172.17.116.131
CSeq: 9 ACK
Content-Length: 0
Max-Forwards: 70

router#
router# no terminal monitor
```

VoIP Gateway
FXO Service Features

Contents

- FXO VoIP Service Network Diagram
- FXO Service Feature List
- FXO VoIP Gateways
- FXO Port Service Feature Example
  - Polarity Inverse Detection
  - Caller-ID Detection
  - PSTN backup & busy-out function
- FXO Service Description
  - Voice-confirmed connect function
  - Clear down tone reg. and detect function
  - Hook flash timing
  - Ring number and detect timing

Network Diagram for FXO Call



FXO Service Feature List

FXO Service Features	Polarity inverse detection function
	Caller-ID detection function
	PSTN backup or busy-out function with hook off in case of power down
	Clear down tone registration and detect function
	Hook flash timing setting function
	Ring detect timeout setting function
	Ring number setting function
	Voice-confirmed connect function

FXO VoIP Gateways for SMB (4~8 Port)

Product	AP1002	AP1005	AP1100	
				
Model			Type	VoIP
			A	4 FXS, 4 FXO
			B	8 FXS
			C	8 FXO
VoIP Ports	2-Port FXS & 2-Port FXO	4-Port FXO	Up to 8-Port	
Signaling	SIP,H.323	SIP, H.323	SIP, H.323	
Module Slot	N/A	N/A	N/A	
LAN Port	2	2	2	
Console	Support	Support	Support	
Power	External Adaptor	External Adaptor	External Adaptor	

FXO VoIP Gateways (~24Port)

Product	AP1700 	AP1800 	AP2610 	AP2620 	AP2120N 	AP2330 
Available Modules	AP-FXS4 AP-FXO4 AP-FXS2O2 AP-E&M4 AP-E1	AP-N1-FXS8 AP-N1-FXO8 AP-N1-FXS4O4 AP-N1-E1	AP-FXS4 AP-FXO4 AP-FXS2O2 AP-E&M4	AP-FXS4 AP-FXO4 AP-FXS2O2 AP-E&M4 AP-E1	AP-N1-FXS8 AP-N1-FXO8 AP-N1-FXS4O4	AP-N1-FXS8 AP-N1-FXO8 AP-N1- FXS4O4
Analog Ports	Up to 8	Up to 16	Up to 4	Up to 8	Up to 16	Up to 24
Signaling	SIP, H.323	SIP, H.323	SIP, H.323	SIP, H.323	SIP, H.323	SIP, H.323
Digital E1/T1	Up to 2E1	Up to 2E1	N/A	Up to 2E1	N/A	N/A
E&M	Support	N/A*	Support	Support	Support	N/A*
Module Slot	Two(2)	Two(2)	One(1)	Two(2)	Two(2)	Three(3)
LAN Port	2	2	2	2	2	2
Console	1	1	1	1	1	1
Power	Single PSU	Single PSU	Single PSU	Single PSU	Single PSU	Single PSU

FXO VoIP Gateways (~32Port)

Product	AP2340 	AP2640 	AP2650 
Available Modules	AP-N1-FXS8 AP-N1-FXO8 AP-N1-FXS4O4	AP-FXS8 AP-FXO8 AP-FXS4O4 AP-E&M8 AP-E1	AP-FXS8 AP-FXO8 AP-FXS4O4 AP-E&M8 AP-E1
Analog Ports	Up to 32	Up to 32	Up to 32
Signaling	SIP, H.323	SIP, H.323	SIP, H.323
Digital E1/T1	N/A	Up to 2E1	Up to 2E1
E&M	N/A*	Support	Support
Module Slot	Four(4)	Four(4)	Four(4)
LAN Port	2	2	2
Console	1	1	1
Power	Single PSU	Single PSU	Dual PSU

FXO Large Capacity VoIP Gateways

Product	AP3100P	AP6500	AP6800
			
Available VoIP Modules	AP-FXS4, AP-FXO4 AP-FXS2O2, AP-E&M4	AP-N1-FXS32 AP-N1-FXO32	AP-N1-FXS32 AP-N1-FXO32
Analog Ports	Up to 60 (4Port Module x 15)	Up to 128 (32 Port Module x 4)	Up to 256 (32 Port Module x 8)
Signaling	SIP, H.323	SIP, H.323	SIP, H.323
CPU Redundancy (Dual CPU)	N/A	Support (Option)	Support (Option)
E&M	Support	N/A	N/A
Module Slot for VoIP Module	15 Slots	4 Slots	8 Slots
LAN Port	2	2	2
Console	1	1	1
Dual Power Supply (Option)	Support	Support	Support

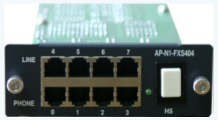
FXO VoIP Modules

DSP

Target	VoIP Modules	Module Features	Module Picture
AP1700,AP2610 AP2620,AP3100P	AP-FXO4	4-Port FXO Module	
AP1700,AP2610 AP2620,AP3100P	AP-FXS2O2	2-Port FXS&2-Port FXO Module	
AP1700,AP2610 AP2620,AP3100P	AP-FXS3O1	3-Port FXS&1-Port FXO Module	
AP2120N AP2640 AP2650	AP-FXO8	8-Port FXO Module	
AP2120N AP2640 AP2650	AP-FXS4O4	4-Port FXS&4-Port FXO Module	

FXO VoIP Modules

DSP

Target	VoIP Modules	Module Features	Module Picture
AP1800 AP2330 AP2340	AP-N1-FXO8	8-Port FXO Module	
AP1800 AP2330 AP2340	AP-N1-FXS4O4	4-Port FXS&4-Port FXO Module	
AP6500 AP6800	AP-N1-FXO32	32-Port FXO Module	

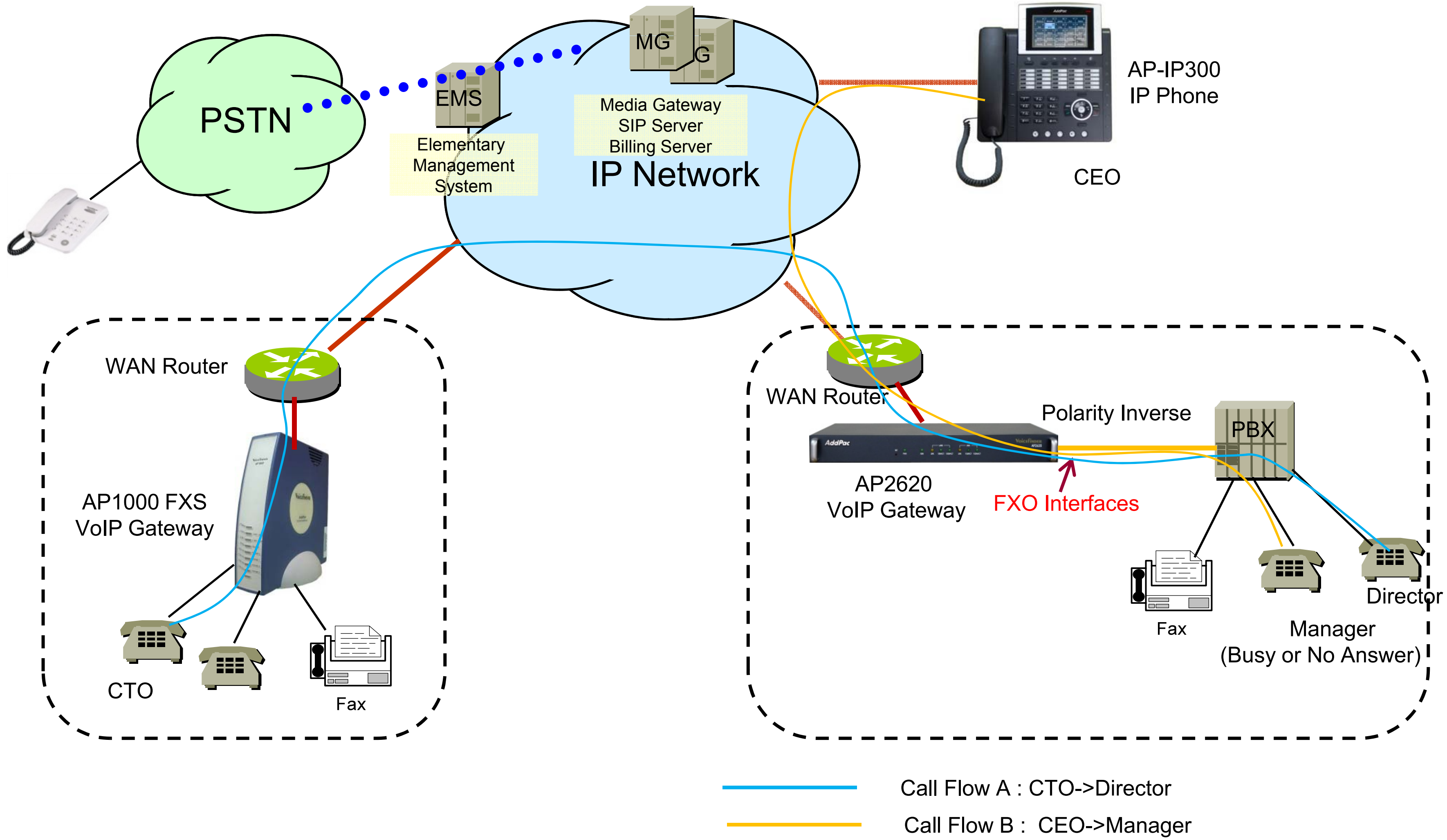
Polarity Inverse Detection Function

- Polarity inverse detection function
  - The FXO port detects the polarity inverse signal coming from Legacy PBX
  - When there is an incoming VoIP call via the FXO port to Legacy PBX, the gateway sends call connect message to Softswitch after detecting the polarity inverse signal on the FXO port.
  - Using Polarity Inverse Signal, a accurate billing service is available.

When polarity inverse function is enabled

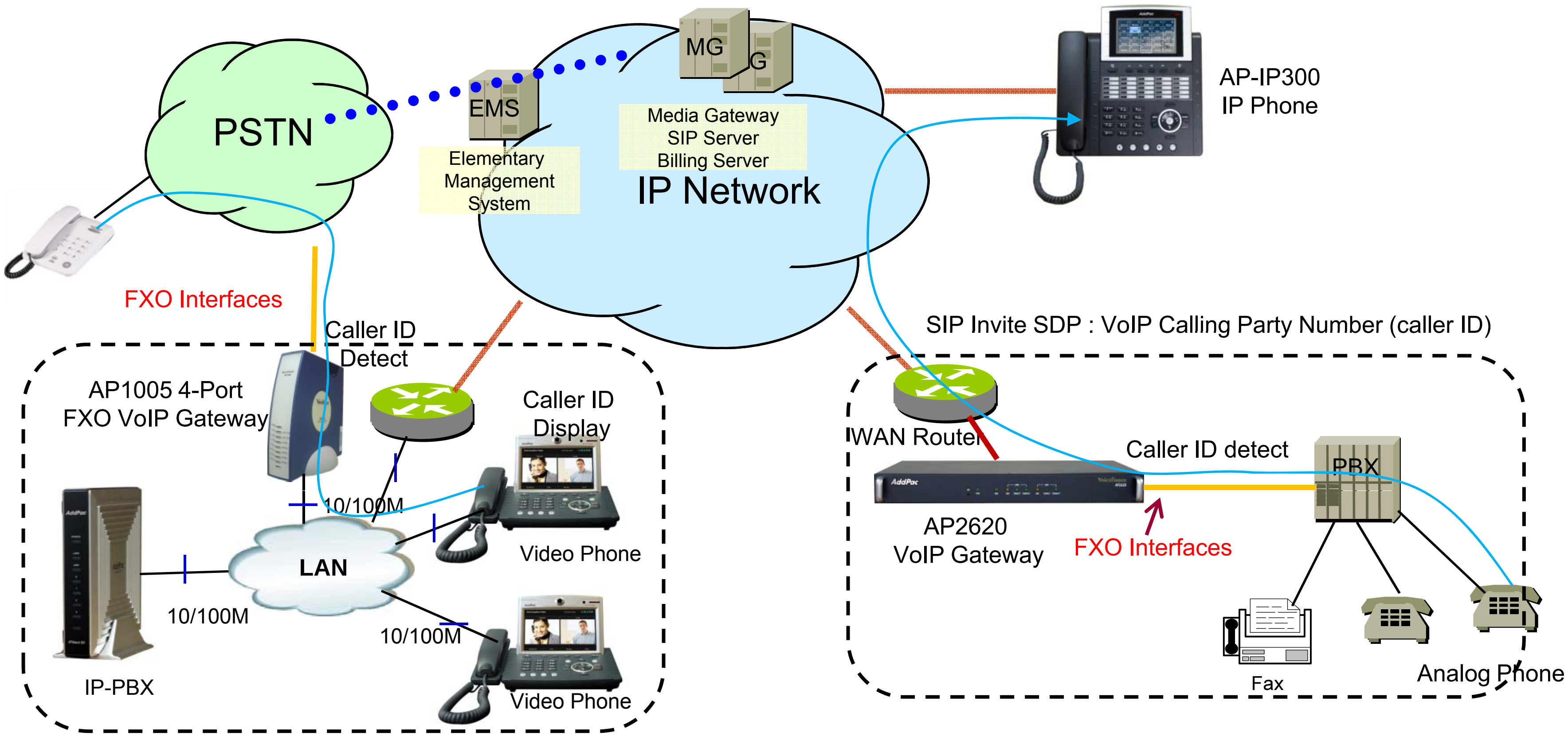
- In case of A flow, Billing is start when the director hooks off.
- In case of B flow, Billing is not start because manager port is busy or no answer

Polarity Inverse Detection Function



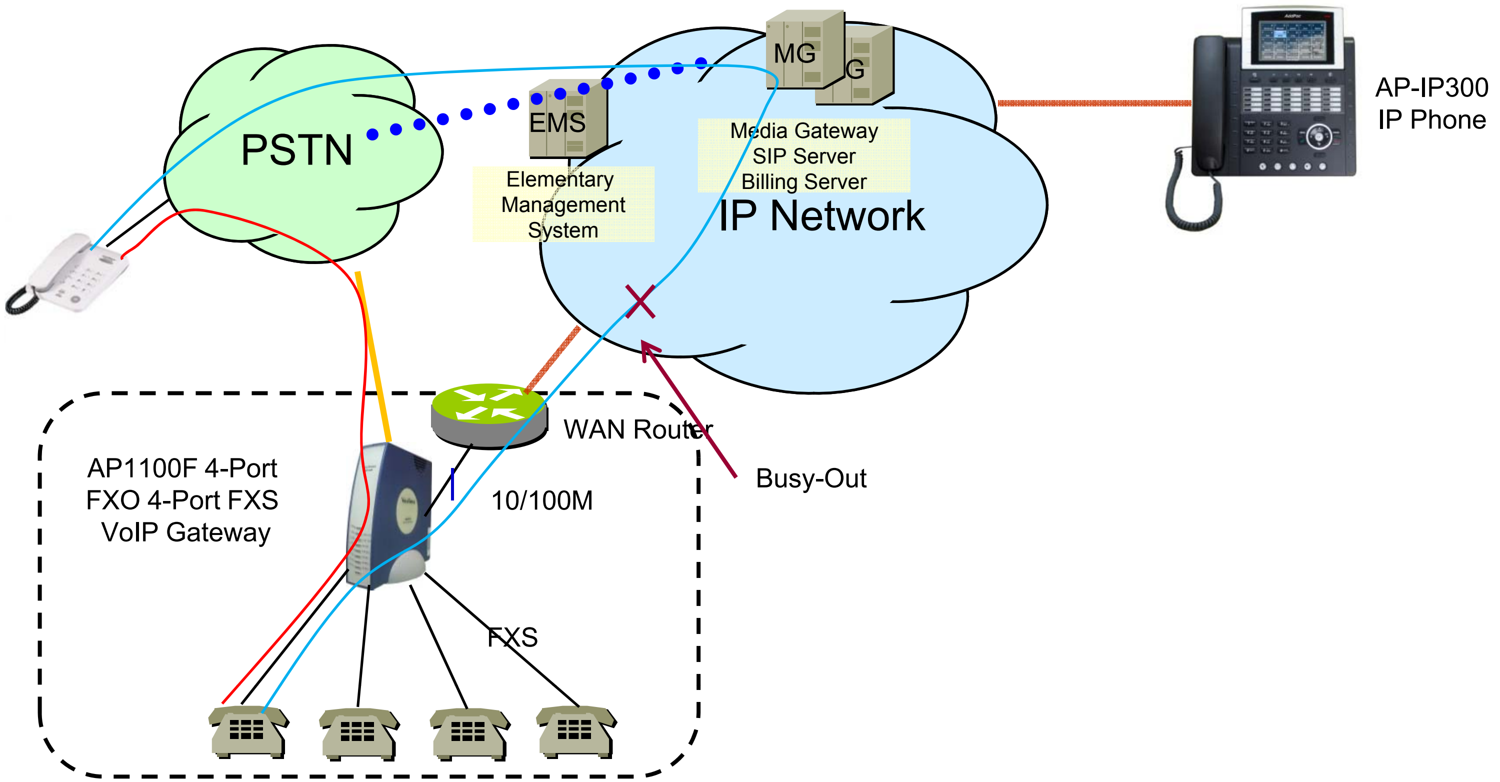
Caller ID Detect Function

- Caller-ID detection function
  - The FXO port is connected to PSTN or PBX, and is able to detect Caller-ID.
  - When a VoIP call is originated from the FXO port, the FXO port detects the caller-ID and uses the number as the VoIP calling party number.



PSTN backup or busy-out function

- PSTN backup or busy-out function
  - VoIP call can not be made when the gateway is in busy out state. User can be communicated continually using PTSN backup function.
  - Busy Out State : LAN interface is down, Softswitch is down, etc



FXO Service Description

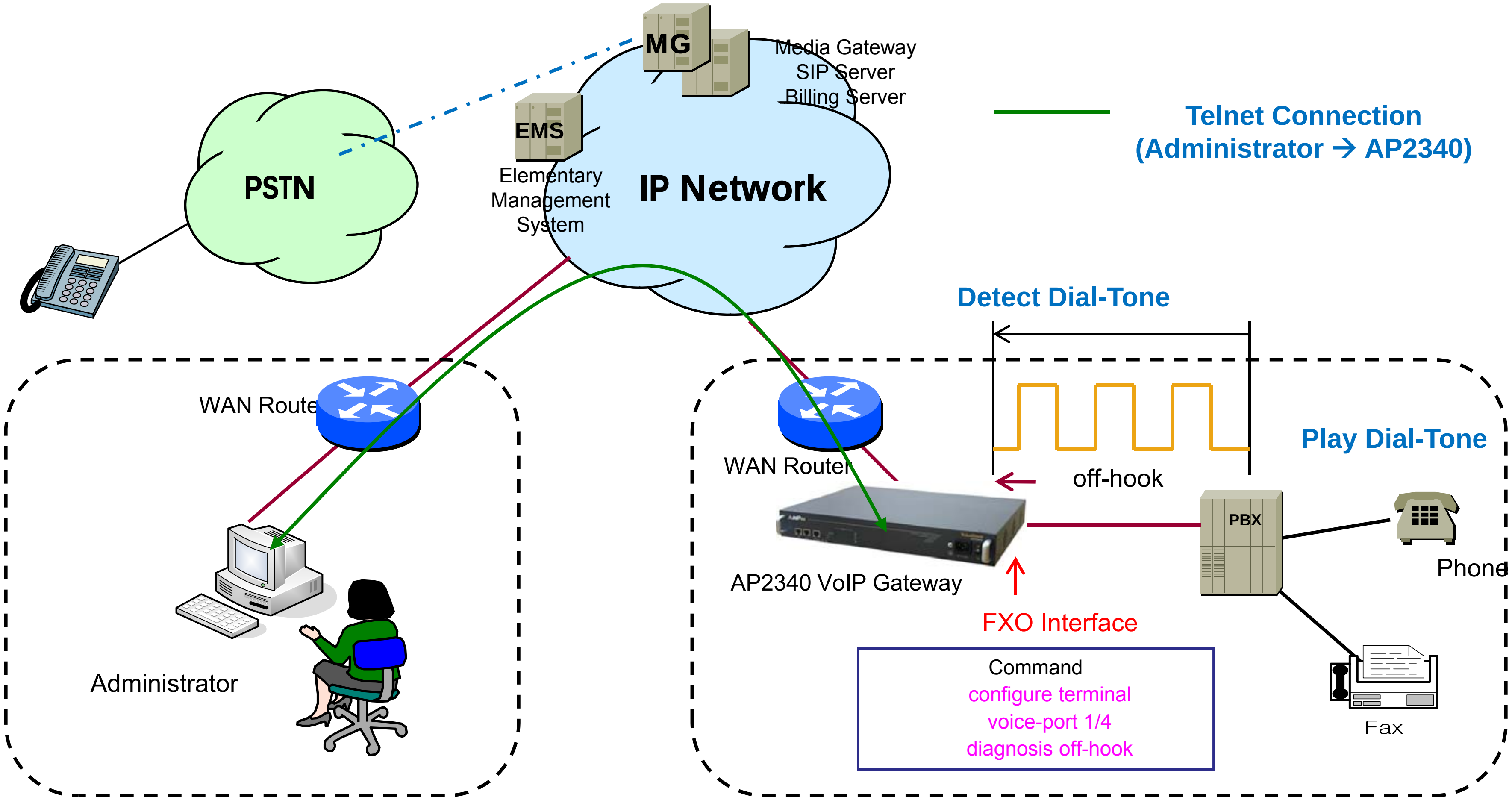
Features	Description
Voice-confirmed connect function	When FXO port is connected to PBX extension and the subscriber does take the call, connect message is not sent to sender side and billing is not included.
Ring number setting function	Use this command to set the maximum number of rings to be detected before answering a call over an FXO voice port. In that case, the FXO interface would answer if the equipment online did not answer the incoming call in the configured number of rings.
Clear down tone registration and detect function	Clear-down-tone detects call termination of FXO port connected to and generated from PSTN or PBX. The value of clear-down-tone (busy tone, fast busy tone) is different for each PSTN and PBX. So use voice class clear-down-tone for registration process in global configuration mode.
Hook flash timing setting function	Different from call-transfer, you need to press hook-flash button twice for conference call. Basically, it takes 500 ms (0.5 sec) to recognize hook-flash button from the AddPac gateway. If you think 500ms (0.5 sec) is too short, you can change hook-flash detect timeout value when hook-flash duration time of PBX is more than 500ms.

Analog Port Diagnostic Features
(FXS, FXO Port)

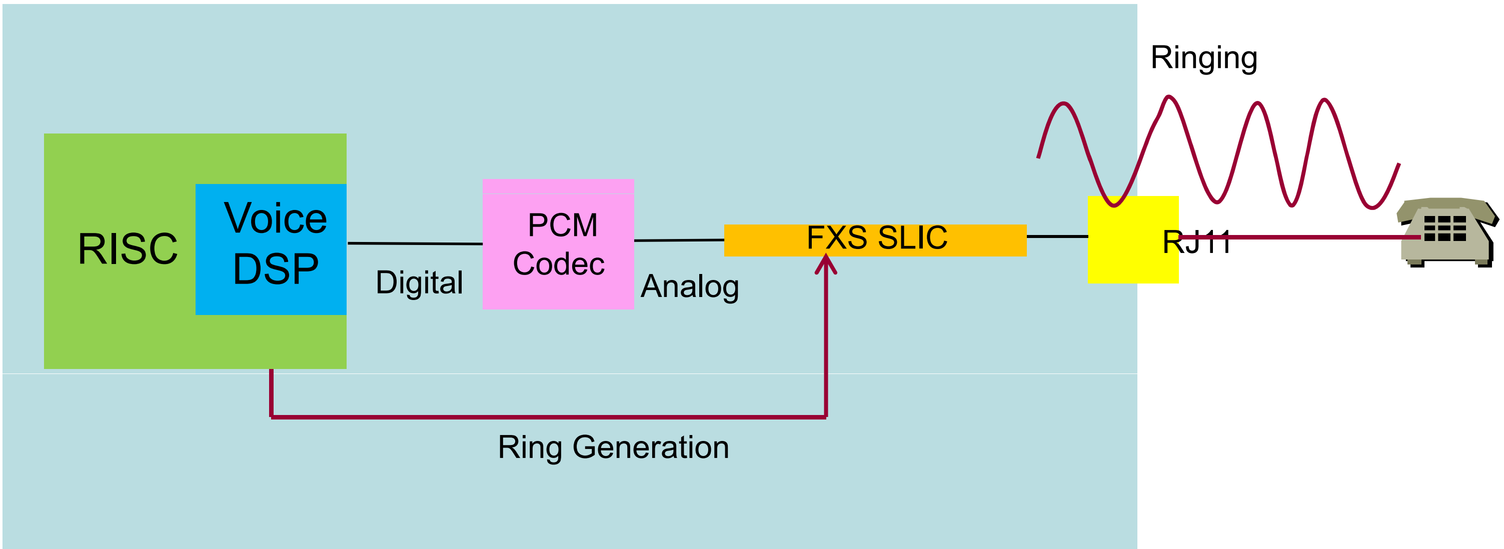
Contents

- Network Diagram for Port Diagnostic Test
- FXS Interface Diagnostic Test
  - Diagnostic Test via Ring Generation On/Off Control
- FXO Interface Diagnostic Test
  - Diagnostic Test via Hook On/Off Control
- FXO Service Feature List
- FXO Port Service Feature Example
  - Polarity Inverse Detection
  - Caller-ID Detection
  - PSTN backup & busy-out function
- FXO Service Description
  - Voice-confirmed connect function
  - Clear down tone reg. and detect function
  - Hook flash timing
  - Ring number and detect timing

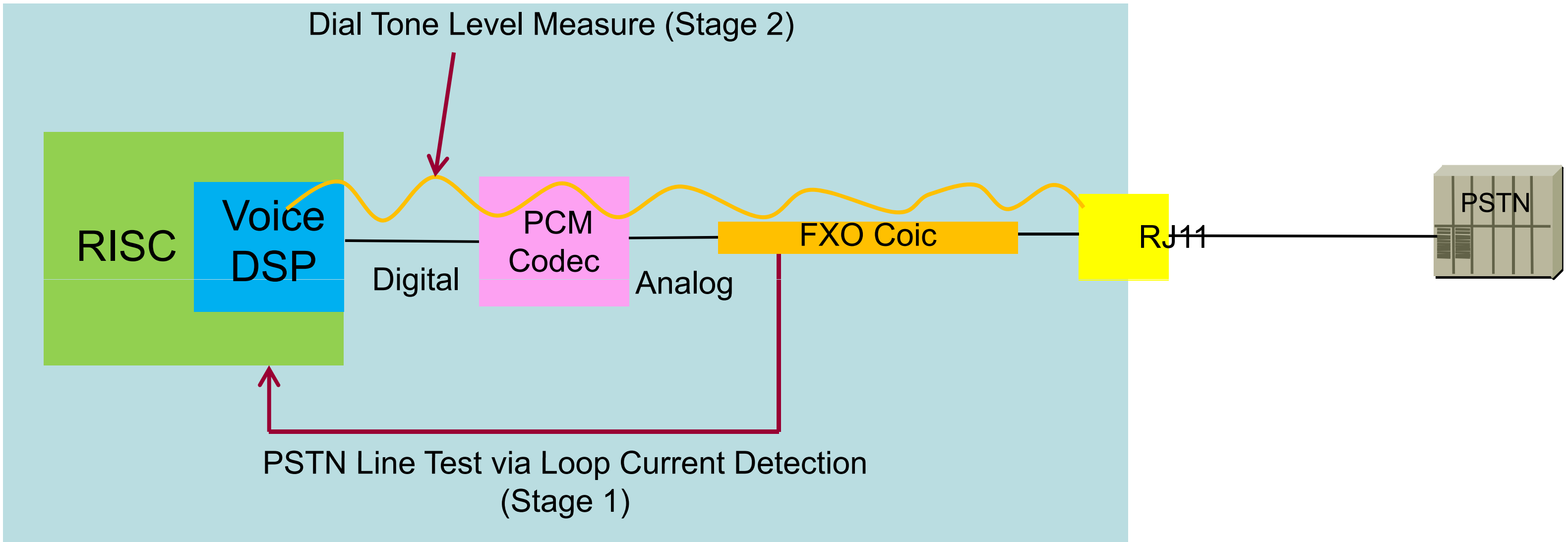
Network Diagram for Port Diagnostic



FXS Hardware Block Diagram



FXO Hardware Block Diagram



Stage 1 : PSTN Line Test by Loop Current Detection
Stage 2 : Internal FXO Hardware Test by Dial Tone Power Level Detection

Command Line Interface

- Diagnosis ring-on/off for FXS Interface Test

FXS Port Ring Generation
Check Debug message
Check Port Information

FXS Port Ring Termination

- Diagnosis off/on-hook for FXO Interface Test

FXO Port off-hook
Check PSTN Line : Loop Current Measure Instead of Voltage Level
Detection Tone Level : Power Level Measure by using Voice DSP

FXO Port Call Termination

FXS Port Diagnostic Example by CLI

```
Welcome to AddPac Gateway

login: root        ← Login
Password:
Gateway > enable
Gateway#
Gateway# configure terminal        ← Global Configuration
Gateway(config)# voice-port 1/0        ← Voice Port Configuration
Gateway(config-voice-port-1/0)# diagnosis ring-<on/off>        ← FXS Port Ring Control
Gateway(config-voice-port-1/0)# diagnosis ring-on

RTA(1/0/0) Rx CC_RING_REQ peerId(-1)
VM(1/0/0) Line Reverse
VM(1/0/0) Start ring actv        ← Check Debug message
VM(1/0/0) SW to -72V
VM(1/0/0) Gen ring idle

Gateway(config-voice-port-1/0)# show rta port
port   type codec VAD SID CNG echo iGn oGn Dial CDT MGC dbg conn   peer   state
--------------------------------------------------------------------------------
01/00/00 FXS  G711U  1   1   1   1    0   0  1    0   0   1  none   NULL   RINGING    ← Check Port Information
01/01/00 FXS  G711U  1   1   1   1    0   0  1    0   0   1  none   NULL   ON_HOOK
```

FXO Port Diagnostic Example by CLI

Welcome to AddPac Gateway

login: root ← Login
Password:
Gateway > enable
Gateway#
Gateway# configure terminal ← Global Configuration
Gateway(config)# voice-port 1/4 ← Voice Port Configuration
Gateway(config-voice-port-1/4)# diagnosis <off/on>-hook ← FXO Port Control
Gateway(config-voice-port-1/4)# diagnosis off-hook

VM(1/4/0) FXO OffHook
VM(1/4/0) Skip Tx CONNECT_CNF by mpLineTestMode
VM(1/4/0) FXO LoopCurrent detected ← PSTN Line Connect
22 22 22 22 22 22 22 23 22 22 22 22 22 22… (dBm) ← Detection Tone Level by DSP (Tone Level -22dBm)
22 22 22 22 22 22 22 23 22 22 22 22 22 22…
OR
VM(1/4/0) FXO no LoopCurrent ← PSTN Line not Connect
63 63 63 63 63 63 63 63 63 63 63 63 63 63… (dBm) ← Not Detection Tone Level by DSP
63 63 63 63 63 63 63 63 63 63 63 63 63 63 63…

Gateway(config-voice-port-1/4)# diagnosis on-hook

FXO Service Feature List

FXO Service Features	Polarity inverse detection function
	Caller-ID detection function
	PSTN backup or busy-out function with hook off in case of power down
	Clear down tone registration and detect function
	Hook flash timing setting function
	Ring detect timeout setting function
	Ring number setting function
	Voice-confirmed connect function

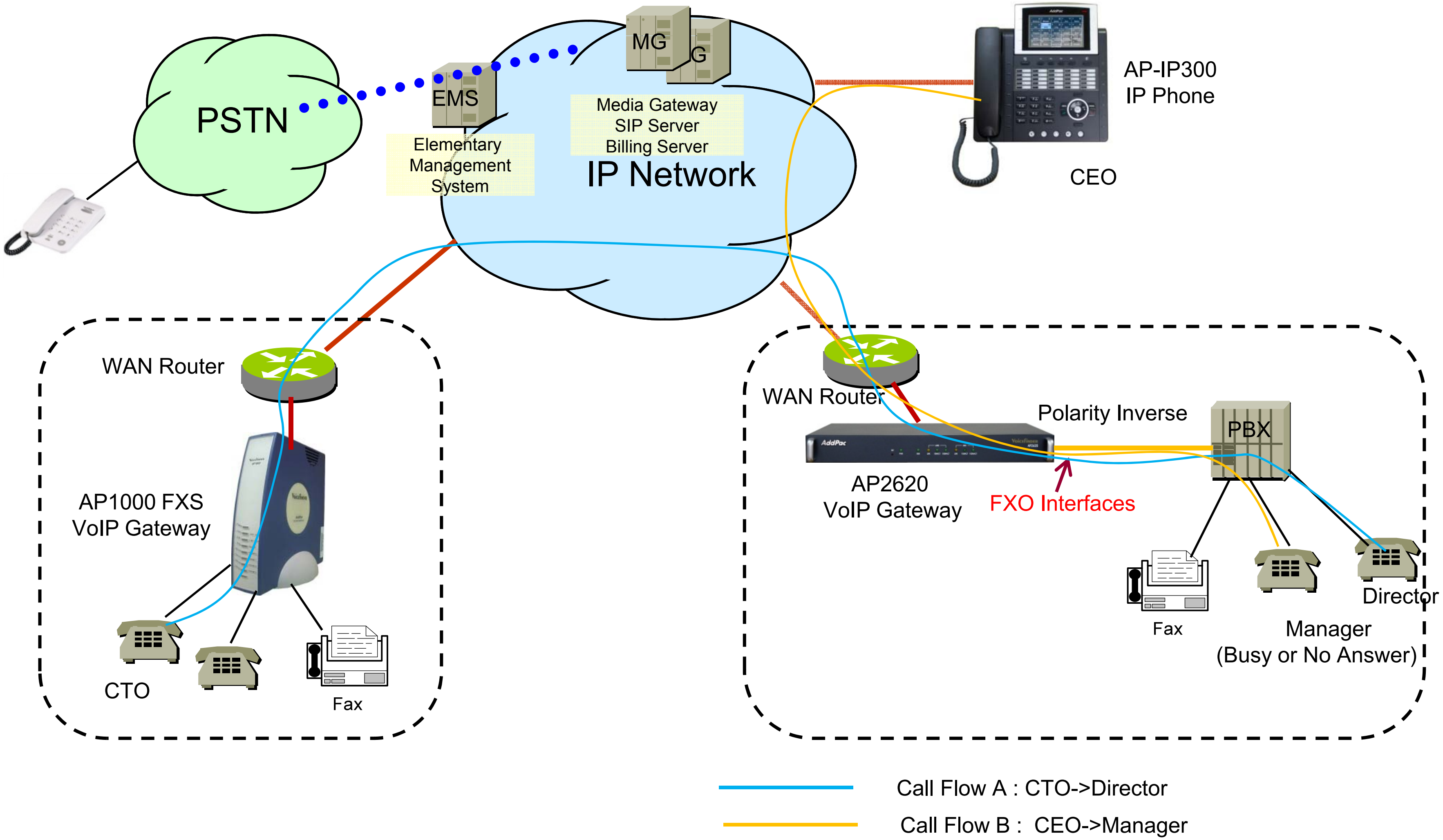
Polarity Inverse Detection Function

- Polarity inverse detection function
  - The FXO port detects the polarity inverse signal coming from Legacy PBX
  - When there is an incoming VoIP call via the FXO port to Legacy PBX, the gateway sends call connect message to Softswitch after detecting the polarity inverse signal on the FXO port.
  - Using Polarity Inverse Signal, a accurate billing service is available.

When polarity inverse function is enabled

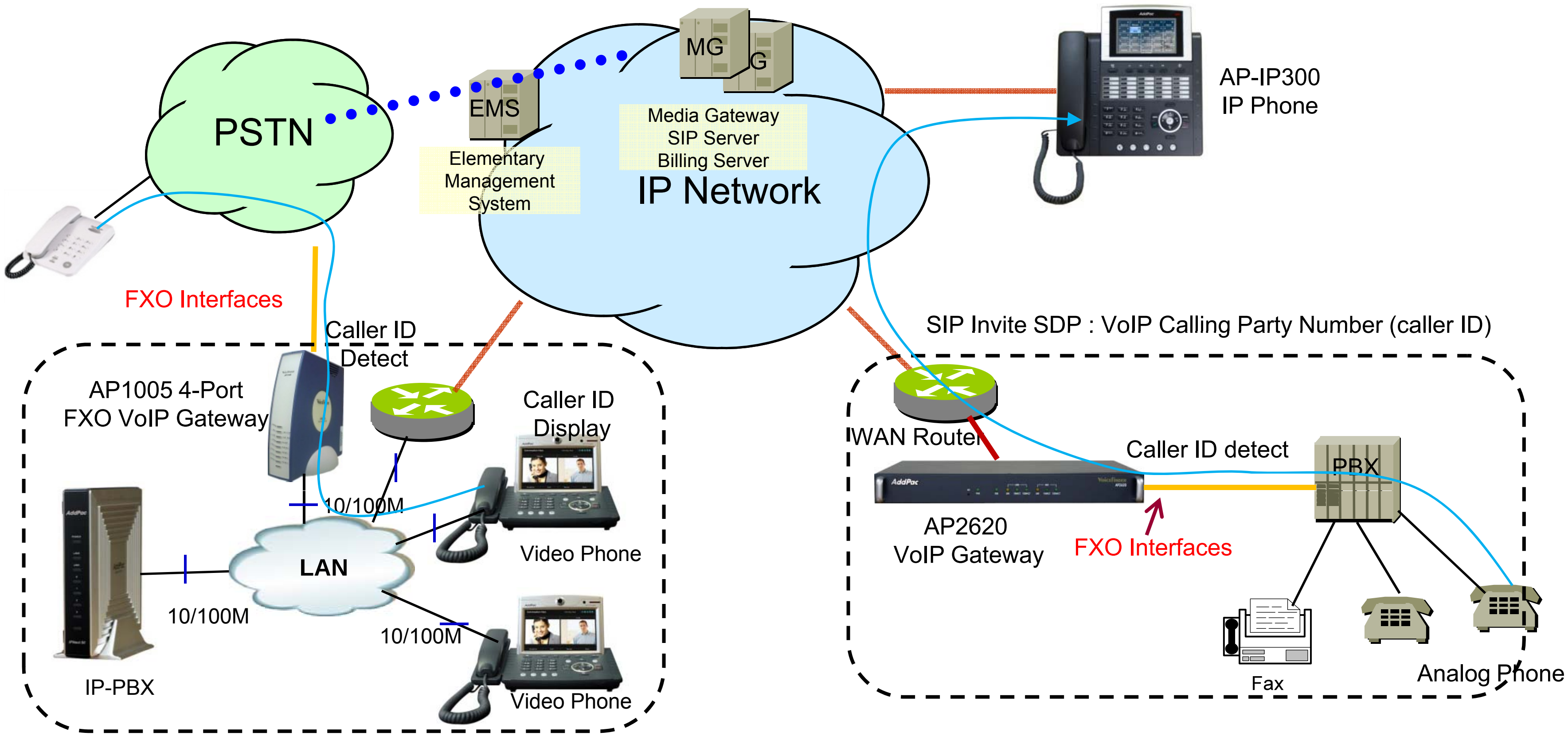
- In case of A flow, Billing is start when the director hooks off.
- In case of B flow, Billing is not start because manager port is busy or no answer

Polarity Inverse Detection Function



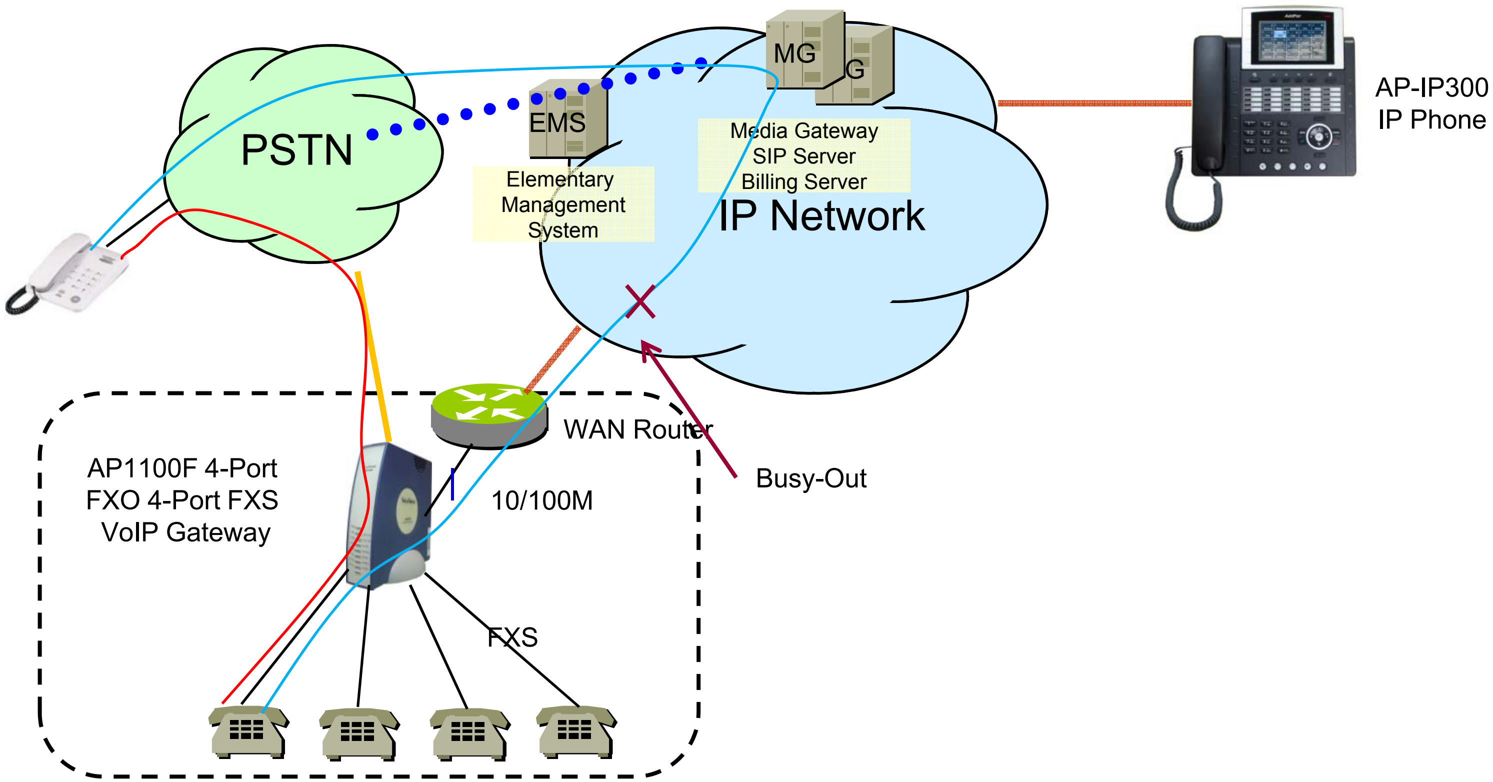
Caller ID Detect Function

- Caller-ID detection function
  - The FXO port is connected to PSTN or PBX, and is able to detect Caller-ID.
  - When a VoIP call is originated from the FXO port, the FXO port detects the caller-ID and uses the number as the VoIP calling party number.



PSTN backup or busy-out function

- PSTN backup or busy-out function
  - VoIP call can not be made when the gateway is in busy out state. User can be communicated continually using PTSN backup function.
  - Busy Out State : LAN interface is down, Softswitch is down, etc



FXO Service Description

Features	Description
Voice-confirmed connect function	When FXO port is connected to PBX extension and the subscriber does take the call, connect message is not sent to sender side and billing is not included.
Ring number setting function	Use this command to set the maximum number of rings to be detected before answering a call over an FXO voice port. In that case, the FXO interface would answer if the equipment online did not answer the incoming call in the configured number of rings.
Clear down tone registration and detect function	Clear-down-tone detects call termination of FXO port connected to and generated from PSTN or PBX. The value of clear-down-tone (busy tone, fast busy tone) is different for each PSTN and PBX. So use voice class clear-down-tone for registration process in global configuration mode.
Hook flash timing setting function	Different from call-transfer, you need to press hook-flash button twice for conference call. Basically, it takes 500 ms (0.5 sec) to recognize hook-flash button from the AddPac gateway. If you think 500ms (0.5 sec) is too short, you can change hook-flash detect timeout value when hook-flash duration time of PBX is more than 500ms.

APOS™ Upgrade with DHCP
(DHCP option 66, 67)

Contents

DHCP Option 66, 67

- DHCP Option
  - Option 66 : TFTP server name
  - Option 67 : Bootfile name

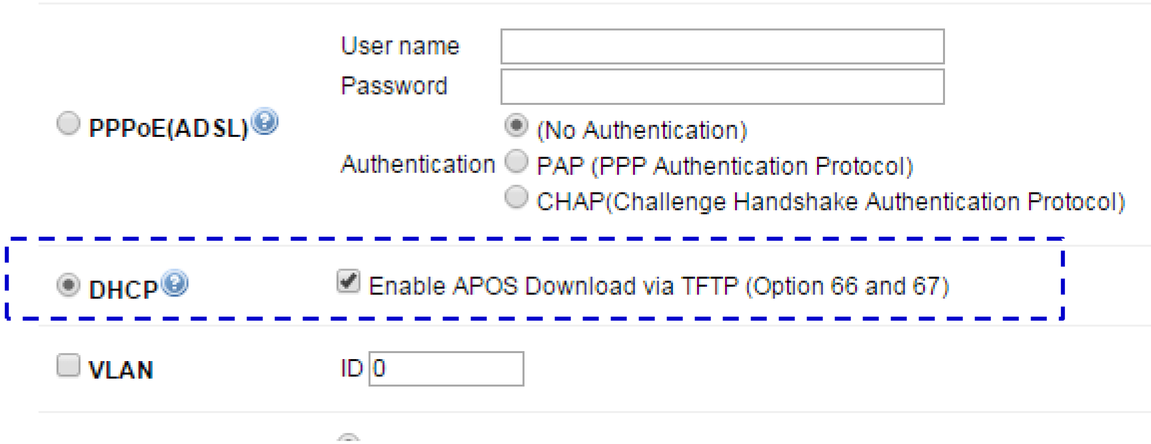
Enable DHCP Option (CLI)

- CLI

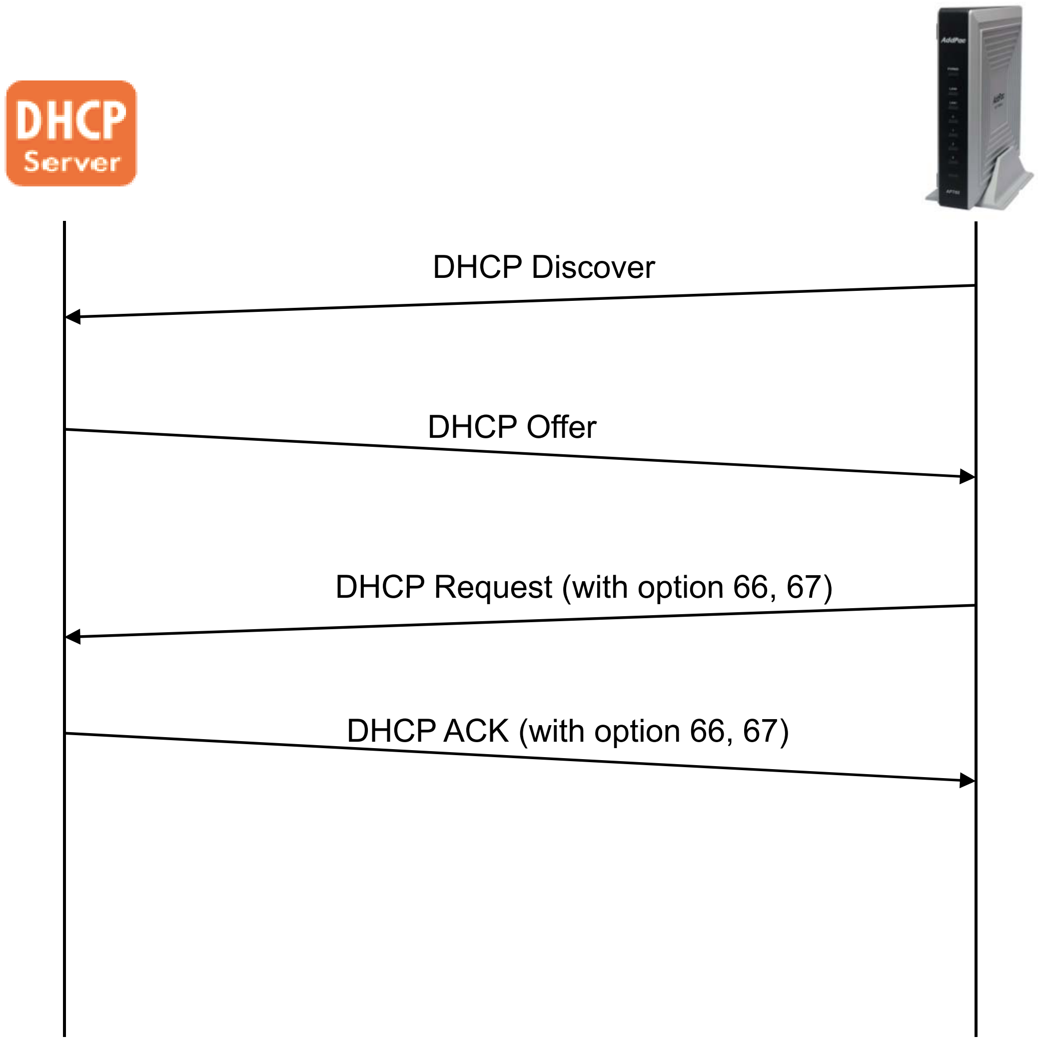
```
!
interface FastEthernet0/0
 ip address dhcp
 ip dhcp unicast
 ip dhcp request option 66
 ip dhcp request option 67
 speed auto
!
```

Enable DHCP Option (Smart Web)

- HTTP Server
  - System WAN Setup



DHCP Message Flow



Firmware Update Procedure

- Received DHCP ACK Message
  - Check DHCP Option 66 and 67
  - If option is exist
    - Check Local APOS filename and DHCP option 67 Bootfile name
    - If the name is not same, Start Download via TFTP
      - tftp://Option 66 : TFTP server name / Option 67 : Bootfile name
      - After Download, Reboot System and Restart DHCP Procedure

APOS™ SIP Server with DHCP
(DHCP option 120)

Contents

- DHCP Option
- DHCP Option Enable (CLI, Smart Web)
- DHCP Message Flow
- Firmware Update Procedure

DHCP Option 120

- DHCP Option
  - DHCP Option for Session Initiation Protocol (SIP) Servers
  - Defined at RFC3361 (Standards Track)
  - SIP Server information Encoding
    - Domain Name List (enc = 0)
    - IPv4 Address List (end = 1)

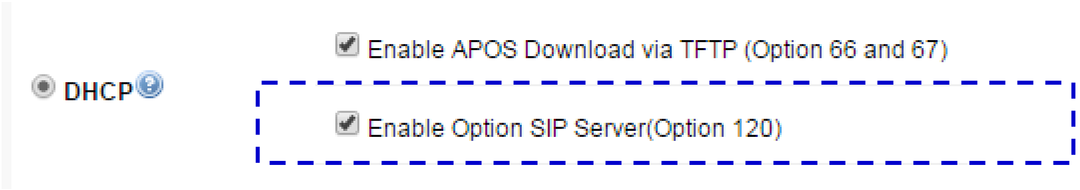
Enable DHCP Option (CLI)

- CLI

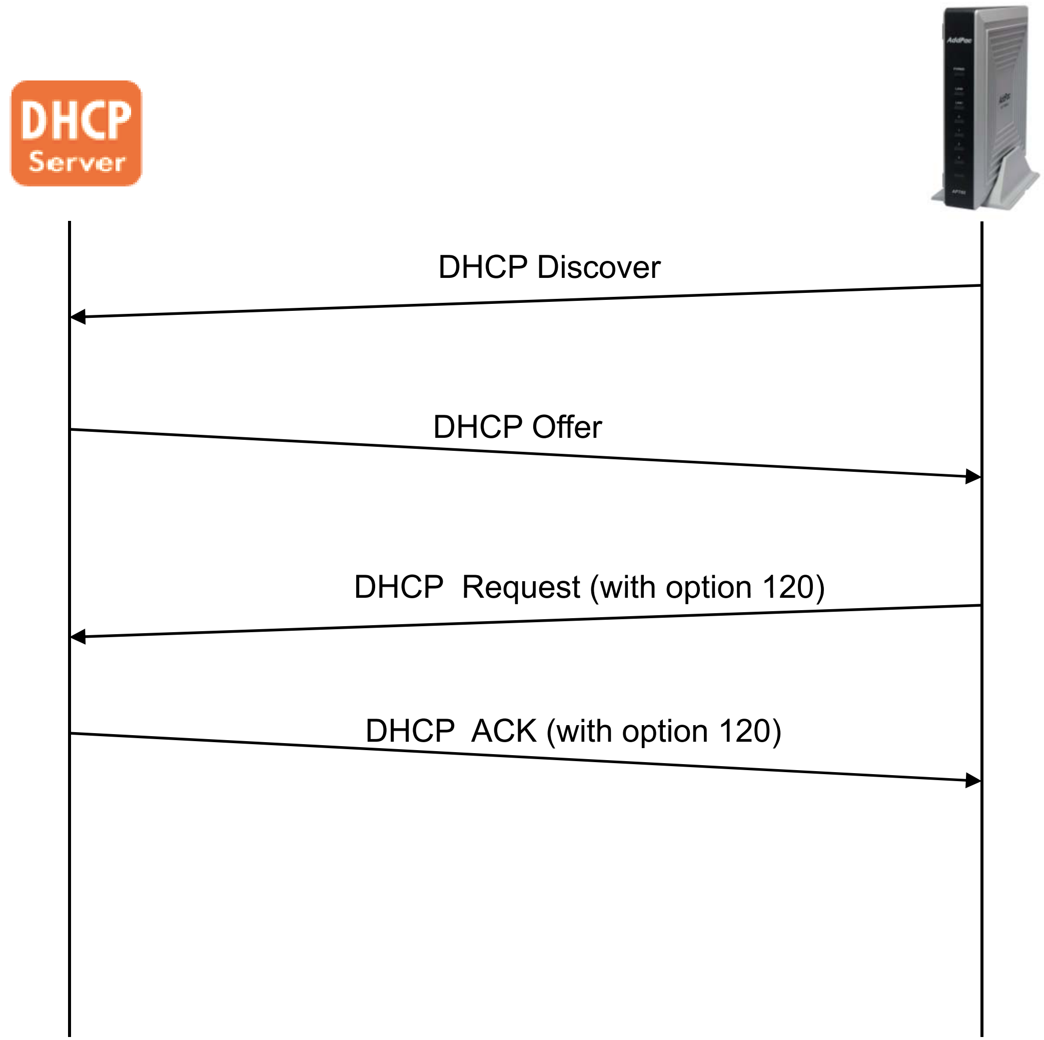
```
!
interface FastEthernet0/0
 ip address dhcp
 ip dhcp unicast
 ip dhcp request option 120
 speed auto
!
```

Enable DHCP Option (Smart Web)

- HTTP Server
  - System WAN Setup



DHCP Message Flow



Firmware Update Procedure

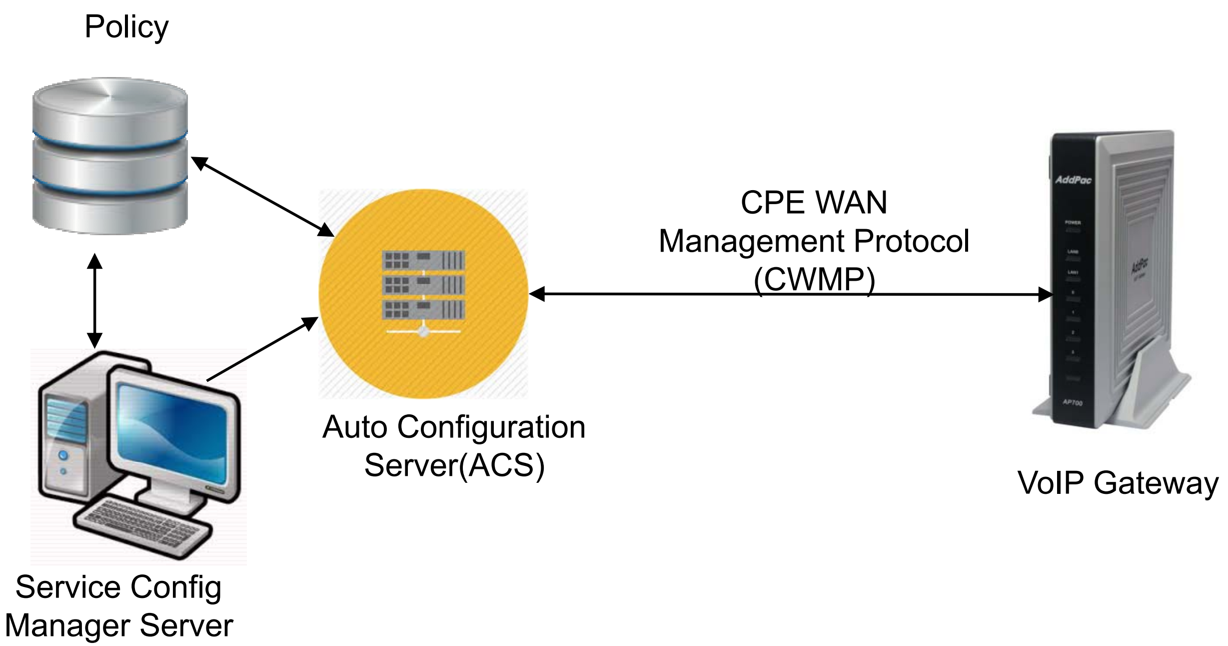
- Received DHCP ACK Message
  - Check DHCP Option 120
  - If option exist
    - Decoding SIP Server Information (enc=0 or enc=1)
    - Compare DHCP SIP Server and Local SIP Server
    - If same, no action
    - If not same
      - Unregister Current SIP Server
      - Update SIP Server using DHCP SIP Server
      - Register New SIP Server

TR-069
(CPE WAN Management Protocol)

Contents

- Protocol Architecture
- TR-069 Service Configuration (CLI, Smart Web)
- Supported Operation
- Tested High-Level Operation

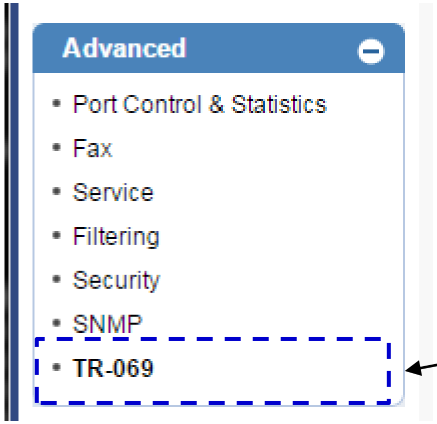
Protocol Architecture



TR-069 Service Configuration (CLI)

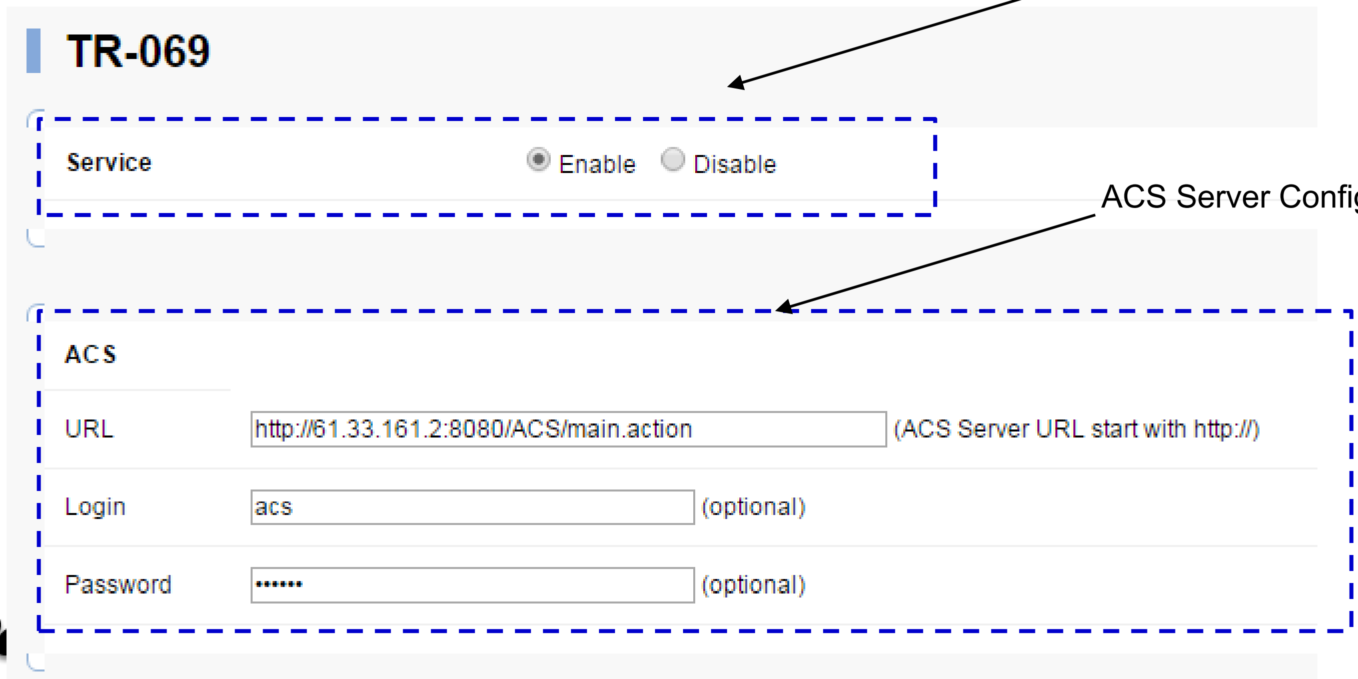
```
!
tr069
  acs url http://61.33.161.2:8080/ACS/main.action
  acs authentication login acs password ******
  httpd port 8000
  httpd authentication login cpe password ******
  cpe serial-number AP-GW-12356423
  cpe oui ADDPAC-0002A4
  service enable
!
```

TR-069 Service Configuration (Smart Web)



Select TR-069 at Advanced

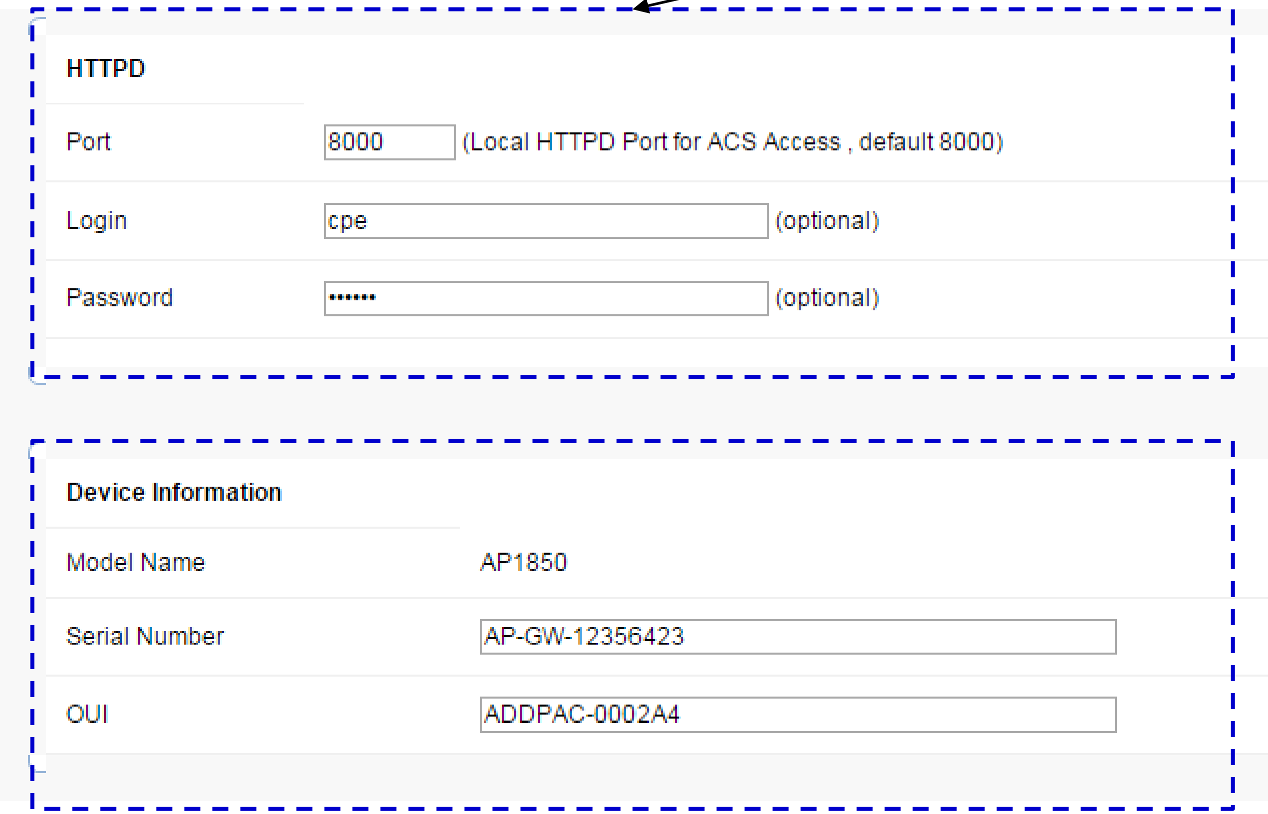
Service Enable/Disable



ACS Server Configuration

TR-069 Service Configuration (Smart Web)

Local HTTP Server for ACS Server Access



Modify CPE Information (SN, OUI)

Supported Operation

Message	Description
GetParameterNames	Used to retrieve list of supported parameters from the device.
GetParameterValues	Retrieve current value of the parameters identified by keys. Could be use d to retrieve one or multiple parameters at once. The version of the call w ith object as the key allows for retrieval of all of the parameters associate d with that object
SetParameterValues	Sets the value of one or multiple parameters
GetParameterAttributes	Retrieves attributes of one or multiple parameters
SetParameterAttributes	Sets attributes of one or multiple parameters
Download	Orders CPE to download the file specified by URL and use it (depending on specified file type) as a Firmware Image, Configuration File, Ringer fil e, etc.
Upload	Orders CPE to upload specified file type to the specified destination. This could cover, for example, the current configuration file or log files.
AddObject	Adds new instance to an object
DeleteObject	Removes instance from an object

Tested High-Level Operation

- Service Re-establishment
  - ✓ Device restart
  - ✓ ACS request
- Firmware / Config Download
  - apos.bin
  - apos.cfg
- Upload
  - Event
  - Configuration (apos.cfg)
- Reboot
- Factory Reset

Firmware / Configuration Download

- Download via HTTP
- Download Argument
  - FileType :
    - “1 Firmware Upgrade Image” ➔ APOS Download
    - “3 Vendor Configuration File” ➔ Configuration Download
  - URL
    - Specify the download file location
  - TargetFileName
    - Filename of APOS Firmware

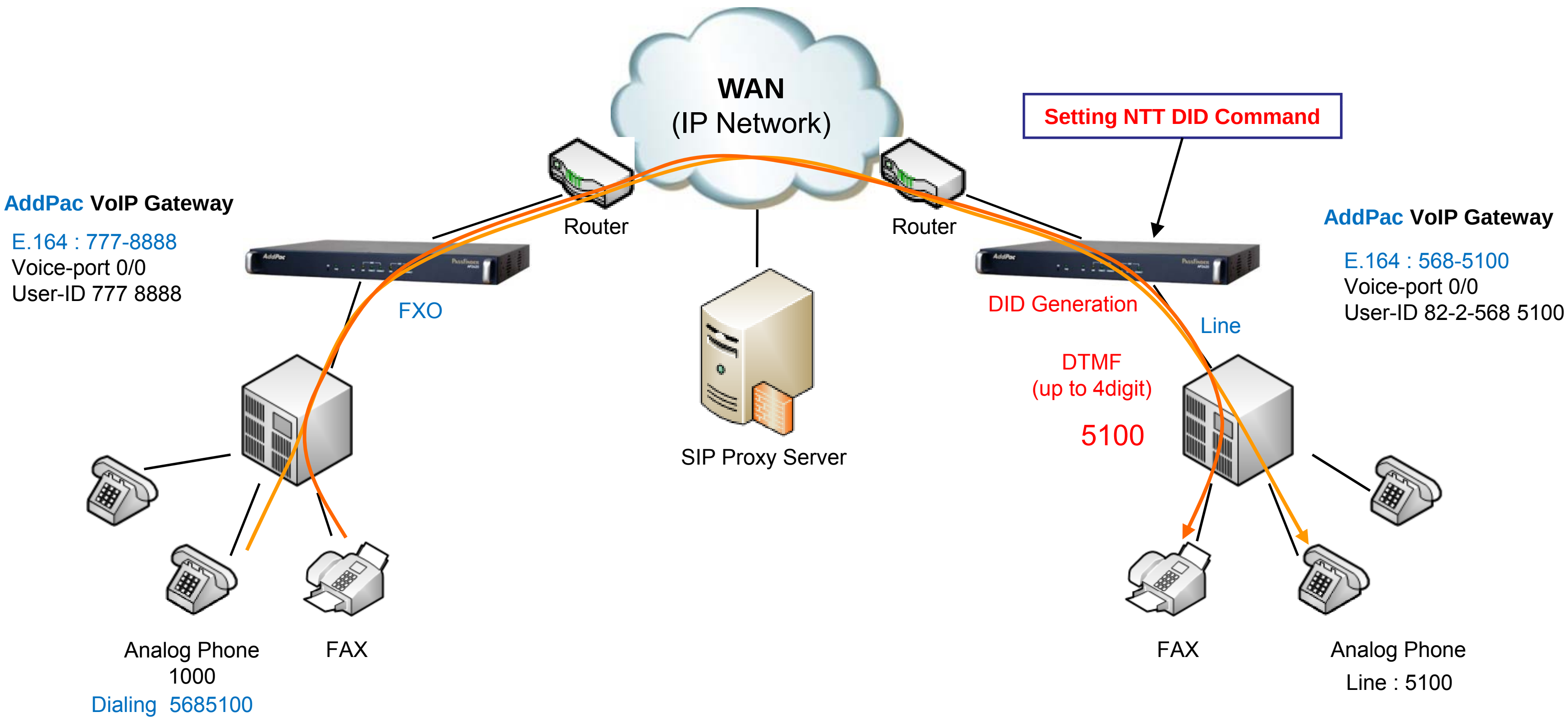
NTT DID(Direct Inward Dialing) Overview

Contents

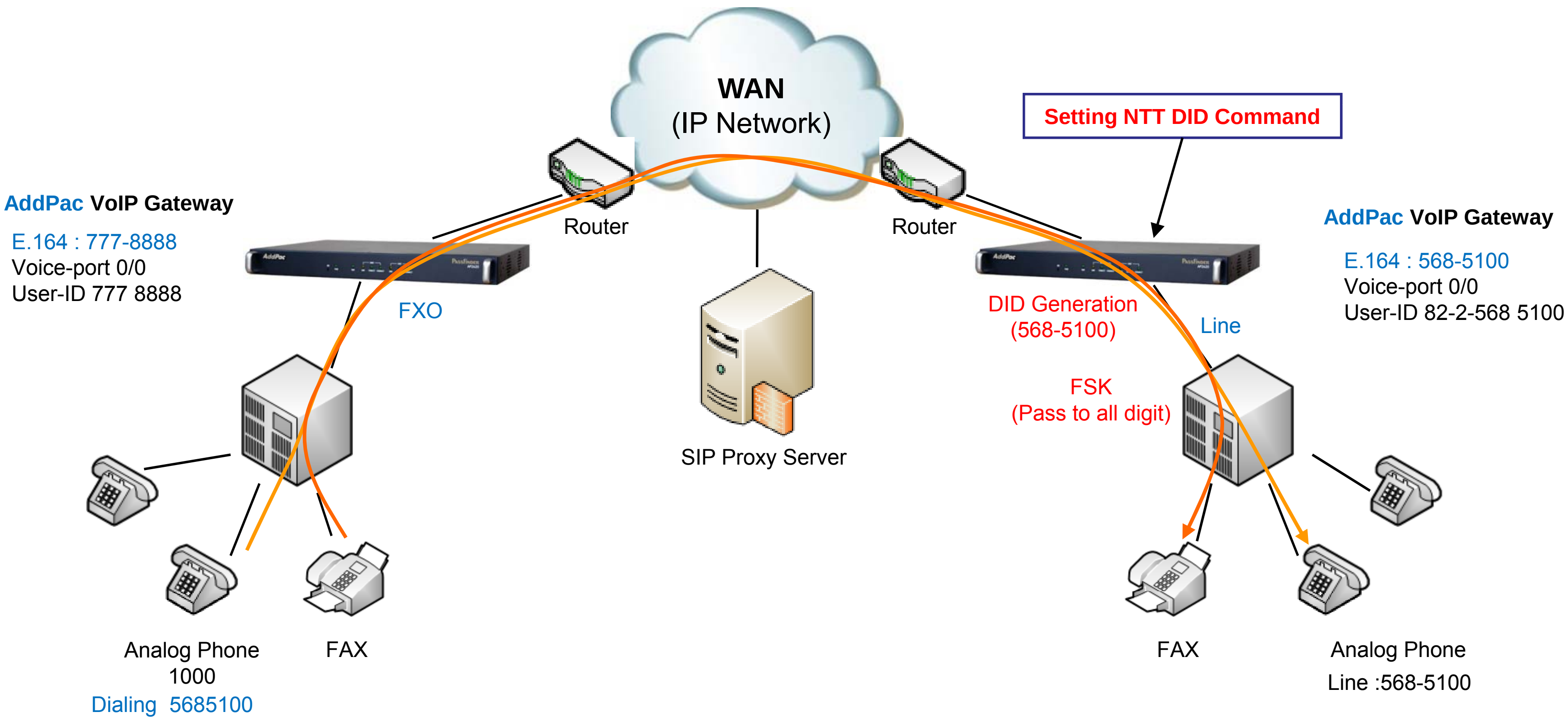
NTT DID Service

- The VoIP gateway supports DTMF, Modem and PB(Push/Button Dial Signal) types for tone generation.
- It is applied to the FXS/FXO/ISDN-PRI ports.
- DID enables callers to dial directly into an extension on a PBX without having to use an auto attendant.
- The dialed extension number is forwarded to the PBX and the call is connected to the local telephone.
- AddPac's all VoIP products supports the feature and it can be enabled/disabled by configuration.

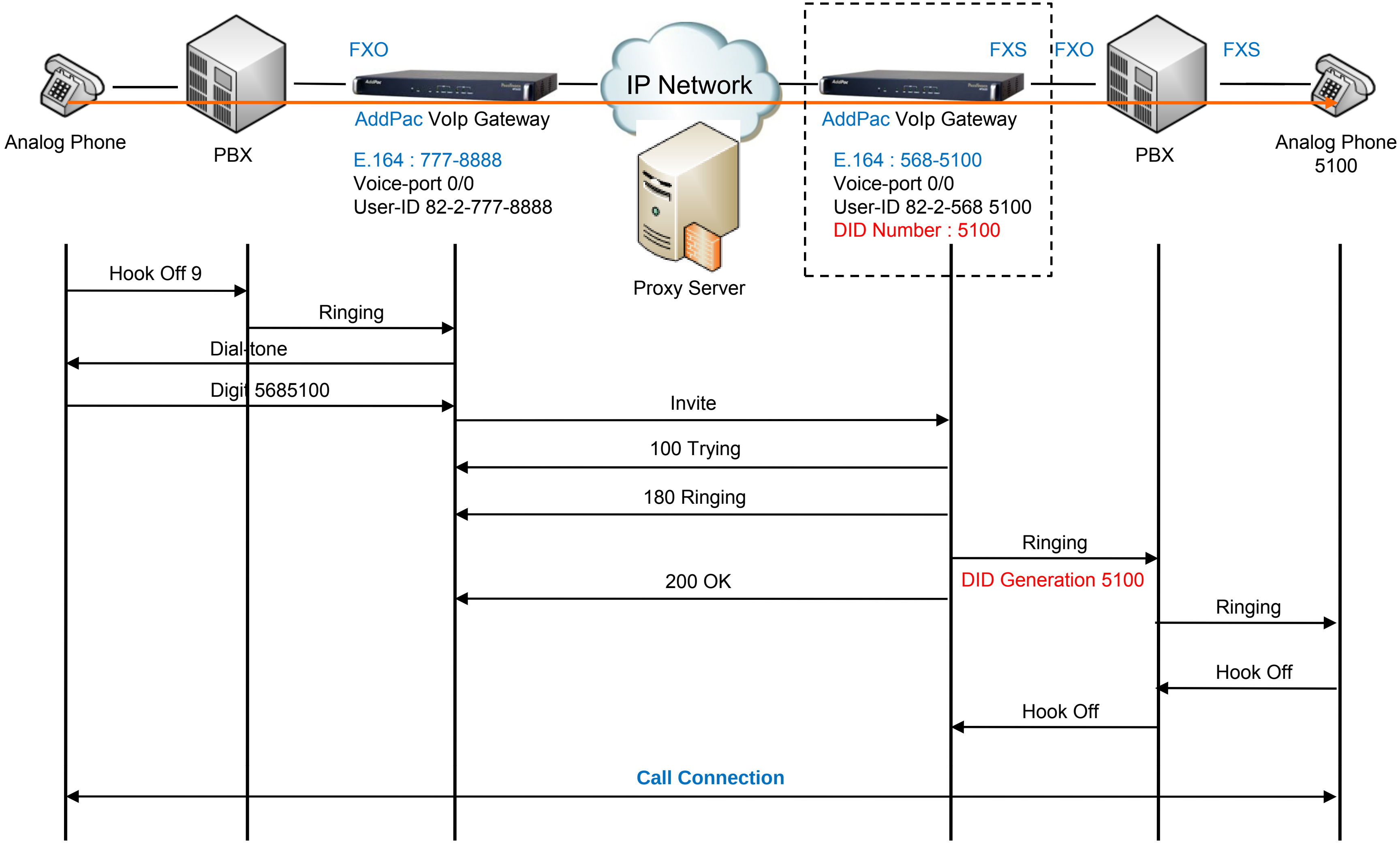
Network Diagram(NTT-PB : DTMF)



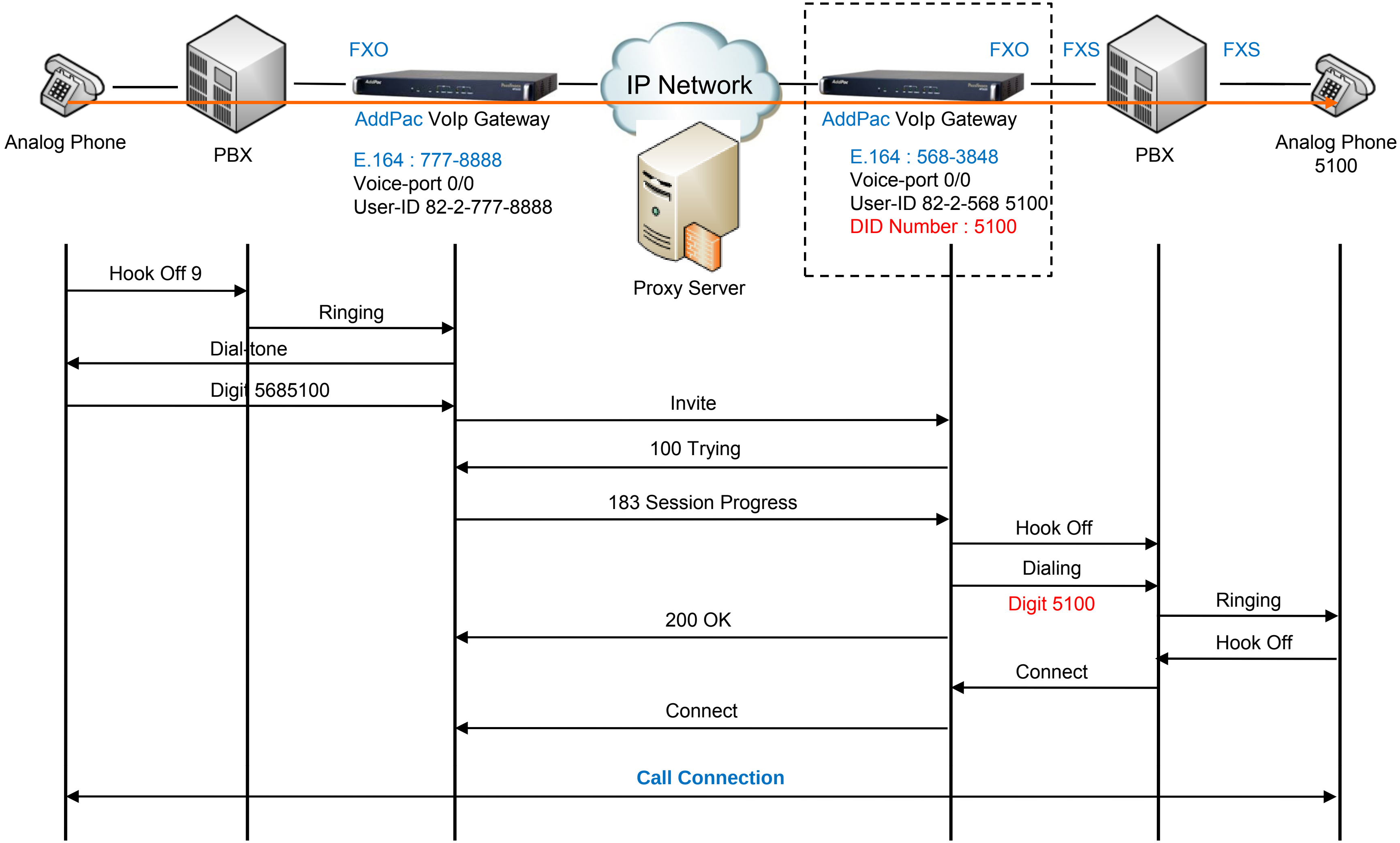
Network Diagram(NTT-Modem : FSK)



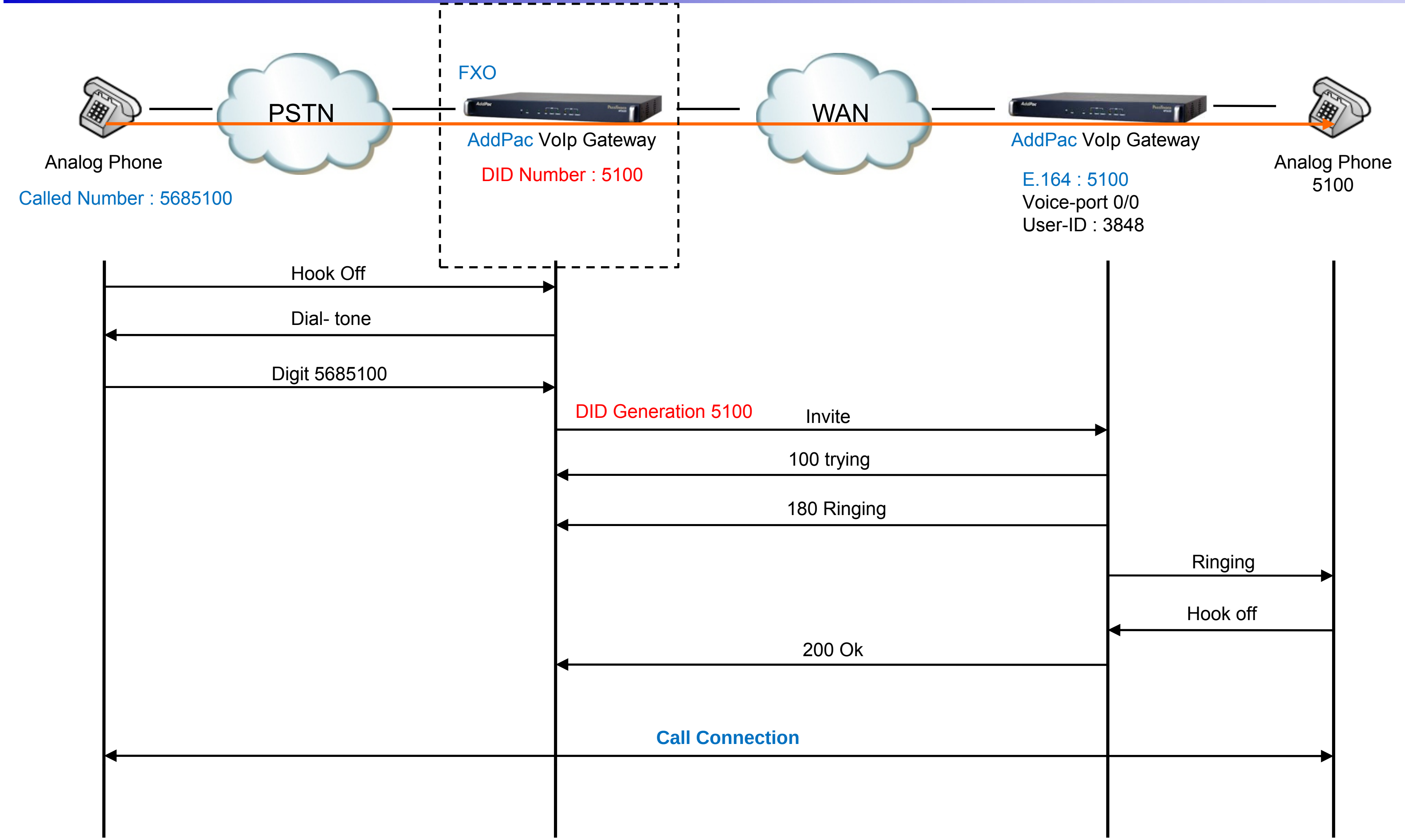
Signaling Flow - FXS



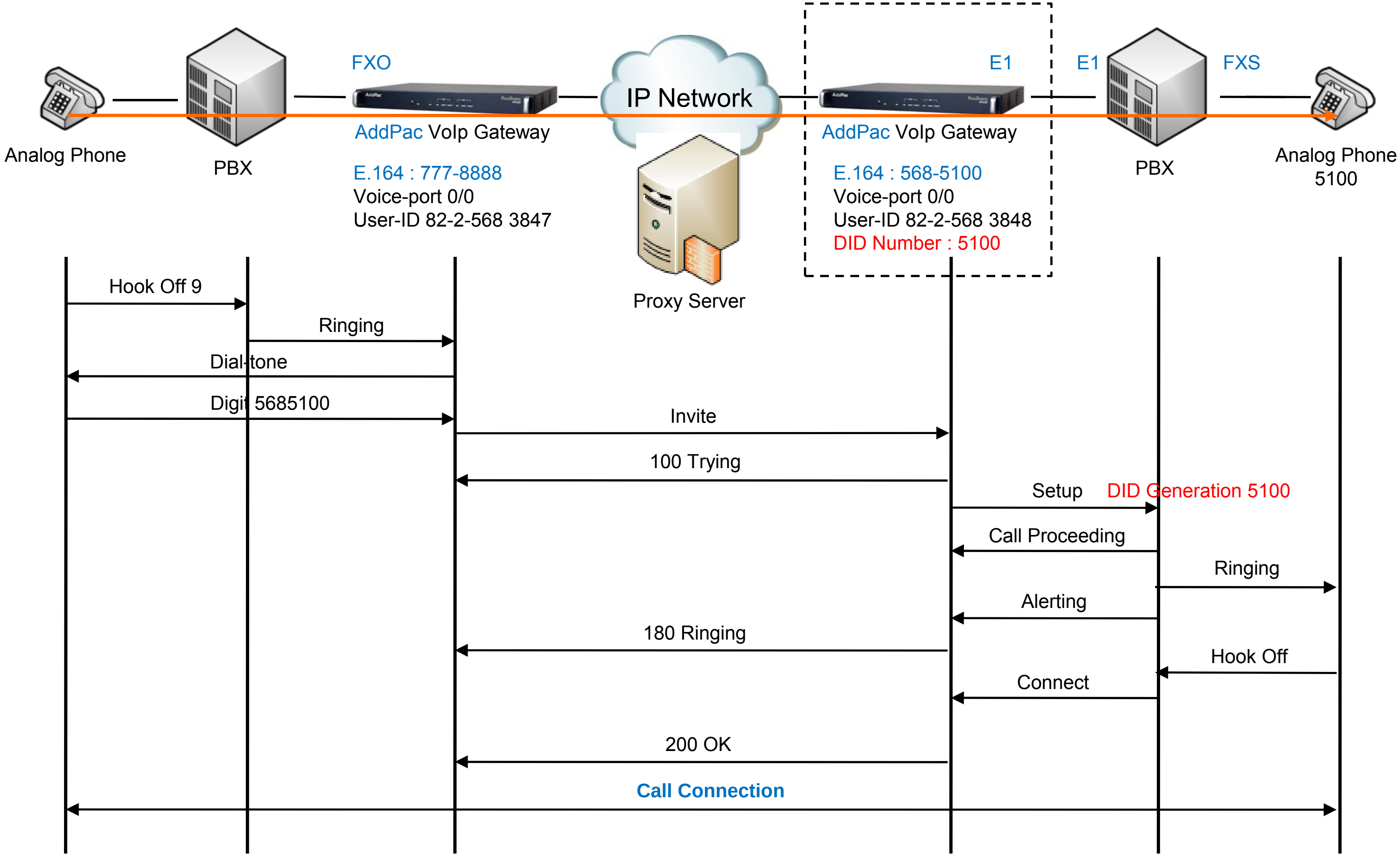
Signaling Flow - FXO



Signaling Flow - FXO



Signaling Flow – ISDN PRI



Command Line Interface

FXS, ISDN DID Configuration Command (Default : Disable)

1. Normal : DTMF Type Digit Transmission (forward digits after hook off.)
2. None : Disable DID Feature
3. NTT-PB : NTT-PB Type Digit Transmission
4. NTT-Modem : FSK Modem Type

- CID function should be enabled for NTT-Modem DID service plus CID service.
- CID function is disabled as a default value.

Command Line Interface

```
Welcome to AP2620 !

login: root        ← Login
Password:

AP2620  -  Login  : root at tty/1 on Tue Jan 10 10:33:06 2012
AP2620_A#
AP2620_A# configure terminal     ← Global Configuration
  Enter configuration commands, one per line. End with CNTL/Z
AP2620_A(config)# voice-port <slot>/<port>        ← Voice-Port  Interface Configuration
AP2620_A(config-voice-port-0/0)# did { none | normal | ntt-modem | ntt-pb }   ← DID Command
 normal          set normal mode (default : forward digits after hook off.)
 none            set none forward digit mode
 ntt-modem       set NTT modem mode
 ntt-pb          set NTT PB mode
AP2620_A#
```

Command Line Interface

- Transmission All Digit

```
AP2620_A#
AP2620_A# dial-peer voice 0 pots          ← Pots Peer Configuration
AP2620_A# destination-pattern 5683848     ← Destination Pattern Configuration Command
AP2620_A# port 0/0                        ← Port Configuration Command
AP2620_A# forward-digit from 0            ← Digit Transmit from 0 th Digit Position
AP2620_A#
```

- Transmission Part of Digit – forward digit from

```
AP2620_A#
AP2620_A# dial-peer voice 0 pots          ← Pots Peer Configuration
AP2620_A# destination-pattern 5683848     ← Destination Pattern Configuration Command
AP2620_A# port 0/0                        ← Port  Configuration Command
AP2620_A# forward-digit from 4            ← Digit Transmit from 4 th Digit Position(3848)
AP2620_A#
```

Command Line Interface

- Transmission Part of Digit– forward digit last

```
AP2620_A#
AP2620_A# dial-peer voice 0 pots            ← Pots Peer Configuration
AP2620_A# destination-pattern 5683848      ← Destination Pattern Configuration Command
AP2620_A# port 0/0                          ← Port Configuration Command
AP2620_A# forward-digit last 4              ← Digit Transmit from last 4 digit position
AP2620_A#
```

- Transmission Part of Digit - Prefix

```
AP2620_A#
AP2620_A# dial-peer voice 0 pots            ← Pots Peer Configuration
AP2620_A# destination-pattern 5683848      ← Destination Pattern Configuration Command
AP2620_A# port 0/0                          ← Port Configuration Command
AP2620_A# Prefix 2000                       ← Transmit Digit 2000 to PBX
AP2620_A#
```

VoIP Gateway SNMP MIB Overview

Contents

- SNMP MIBs

SNMP MIBs

SNMP MIBs

- MIB-II
- RMON MIBs (Statistsics, History, Alarm, Hosts Group)
- RFC2465 Management Information Base for IP Version 6: Textual Conventions and General Group
- RFC2466 Management Information Base for IP Version 6: ICMPv6 Group
- RFC2452 IP Version 6 Management Information Base for the Transmission Control Protocol
- RFC2454 IP Version 6 Management Information Base for the User Datagram Protocol
- AddPac Enterprise MIBs
- etc

AddPac Enterprise VoIP MIBs

AddPac Enterprise VoIP SNMP MIBs

- VOIP-GLOBAL –MIB
  ◦ Manages the Global setting and status.
- VOICE-IF-MIB
  ◦ Manages the voice related parameters for both voice analog and ISDN interfaces.
- VOIP-POTS-PEER-MIB
  ◦ Manages the POTS dial peer related parameters for POTS.
- VOIP-VOIP-PEER-MIB
  ◦ Manages the VOIP dial peer related parameters for VOIP.
- VOIP-MISC-MIB
  ◦ Manages the Translation rule Table, Codec Class Table, User Class Table, Alternate Gatekeeper Table, Number Expansion Table.
- VOIP-STAT-MIB
  ◦ Shows call statistics of current active calls and call history

VoIP Gateway Service Feature for Multiple MCU Redundancy Service

Call-hunt-group Service Overview

VoIP Gateway AP2340

Audio MCU AP-MC1500

Contents

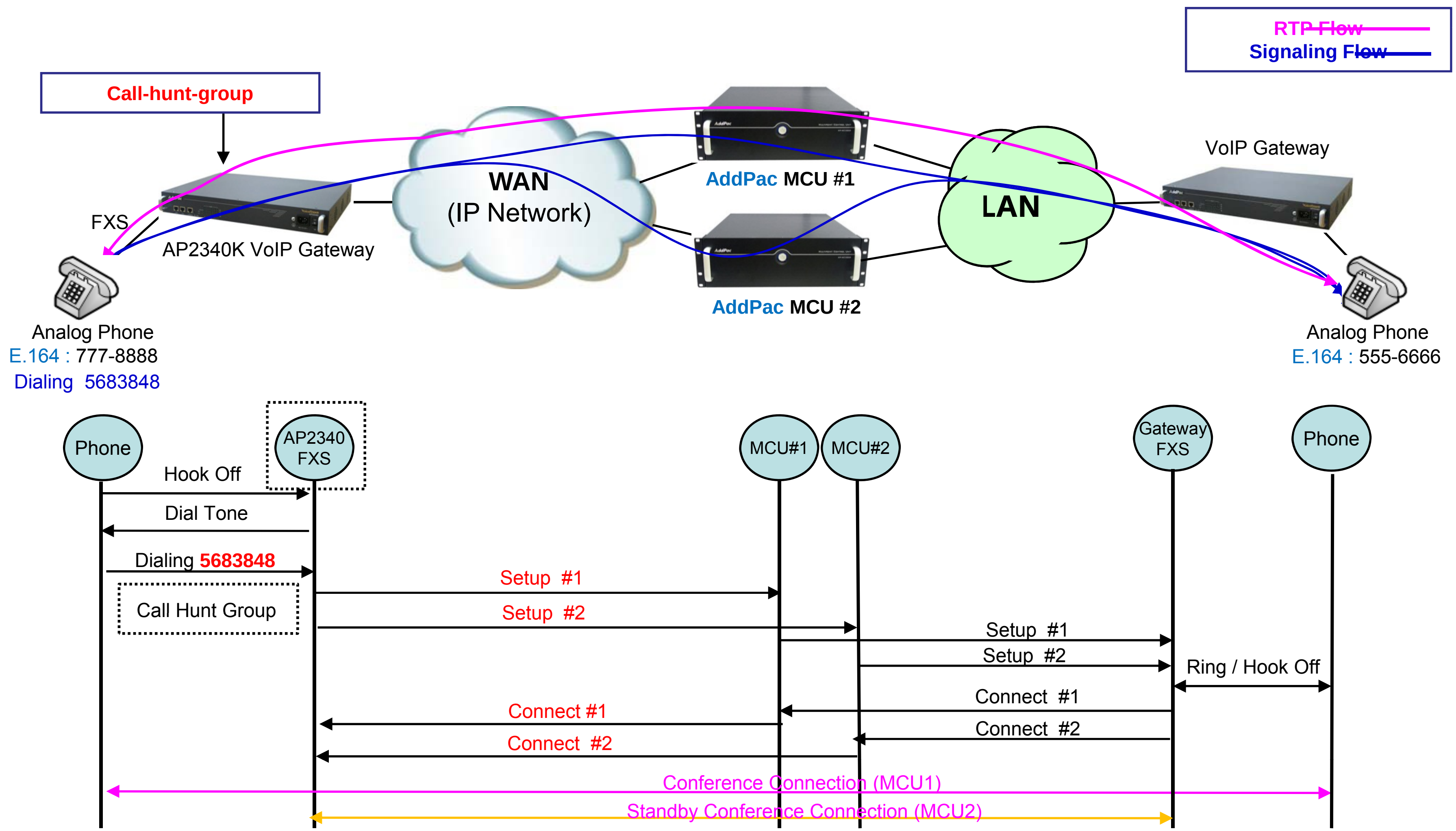
- Overview
- Signaling Flow
  - VoIP Gateway to MCU
  - VoIP Gateway to Gateway
- Command Line Interface

Overview

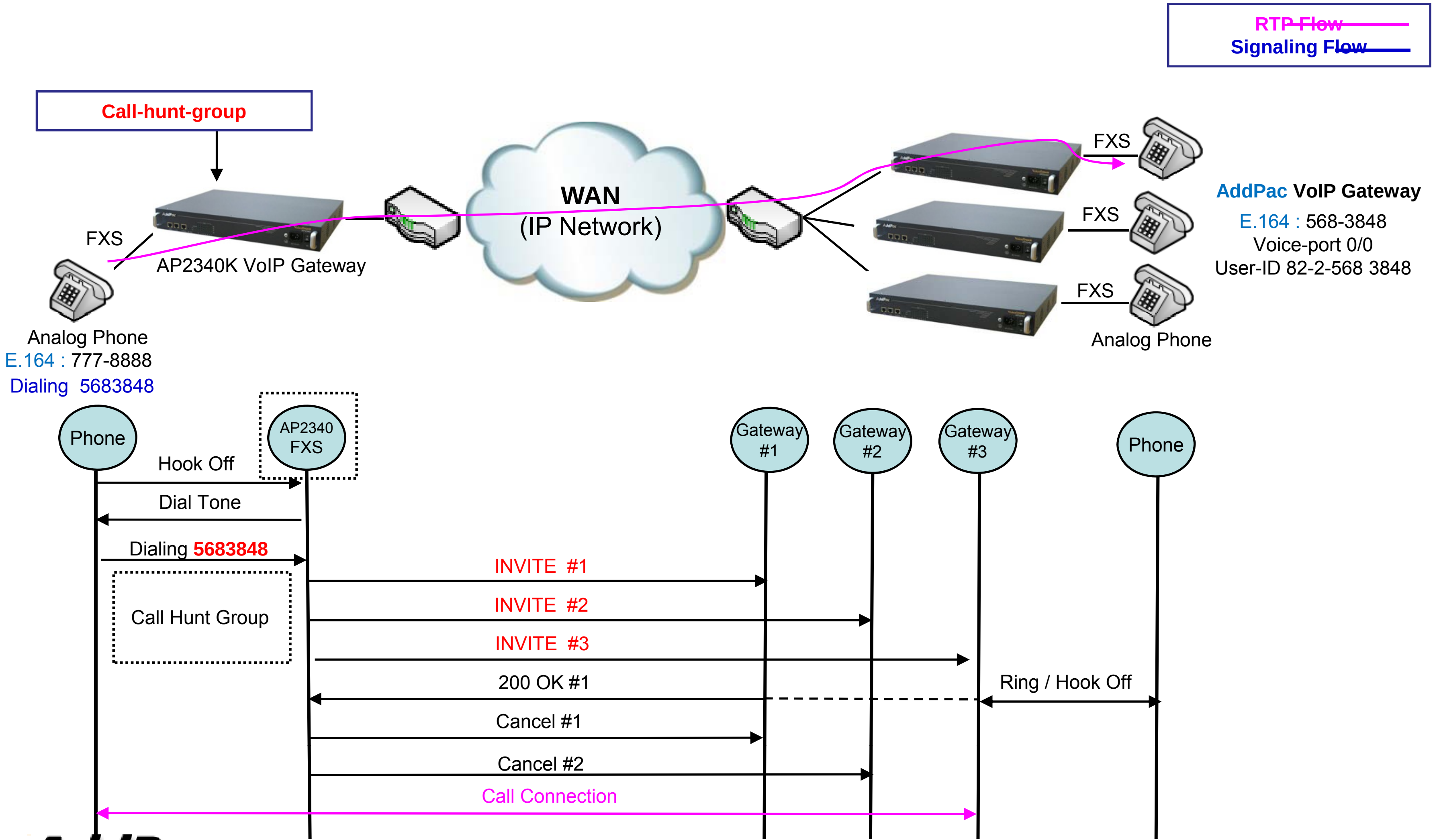
What`s Call-hunt-group

- Send multiple setup (h.323) or Invite (sip) message concurrently
- Send setup (h.323) or Invite (sip) message in order
- Call connection scheme for concurrent multiple call inbound from MCU
  - Call Arrival Time (First Incoming Call Service)
  - Preference Setting
  - RTP session change by Specific DTMF Transmission

Signaling Flow #1
(Gateway to MCU)



Signaling Flow #2
(VoIP Gateway to VoIP Gateway)



Command Line Interface

Multiple Setup or Invite Configuration Command (Default : Disable)

- Call-hunt-group

  Group Configuration to send multiple SETUP (H.323), INVITE (SIP)
  Setup identical call-hunt-group in Voice Port and VoIP Peer

- Call-hunt-group [Option]

  - Disconnect-policy
    Call Termination Policy Configuration

  - Timeout hunt
    Hunting Configuration to send setup or invite message

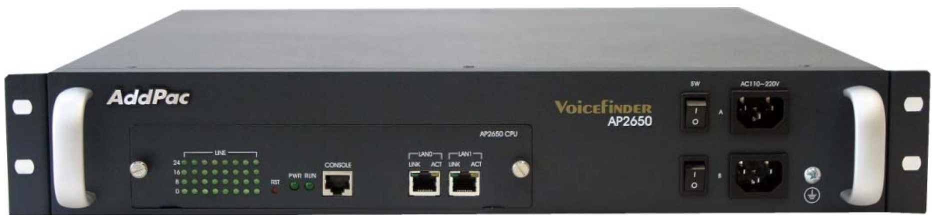
  - Session-change-dtmf
    DTMF Configuration to change RTP session change in hunt-group

Command Line Interface

Welcome to AddPac Gateway

login: root ← Login
Password:
Gateway > enable
Gateway#
Gateway# configure terminal ← Global Configuration
Gateway(config)# call-hunt-group <tag> ← Call-hunt-group Configuration
Gateway(call-hunt-group)# disconnect-policy
[active-session | individual | priority-based]
Gateway(call-hunt-group)# timeout hunt
[0-10] (0: simultaneous mode, 1-10: hunting mode)
Gateway(call-hunt-group)# session-change-dtmf
[<0-9> <#> <*>]

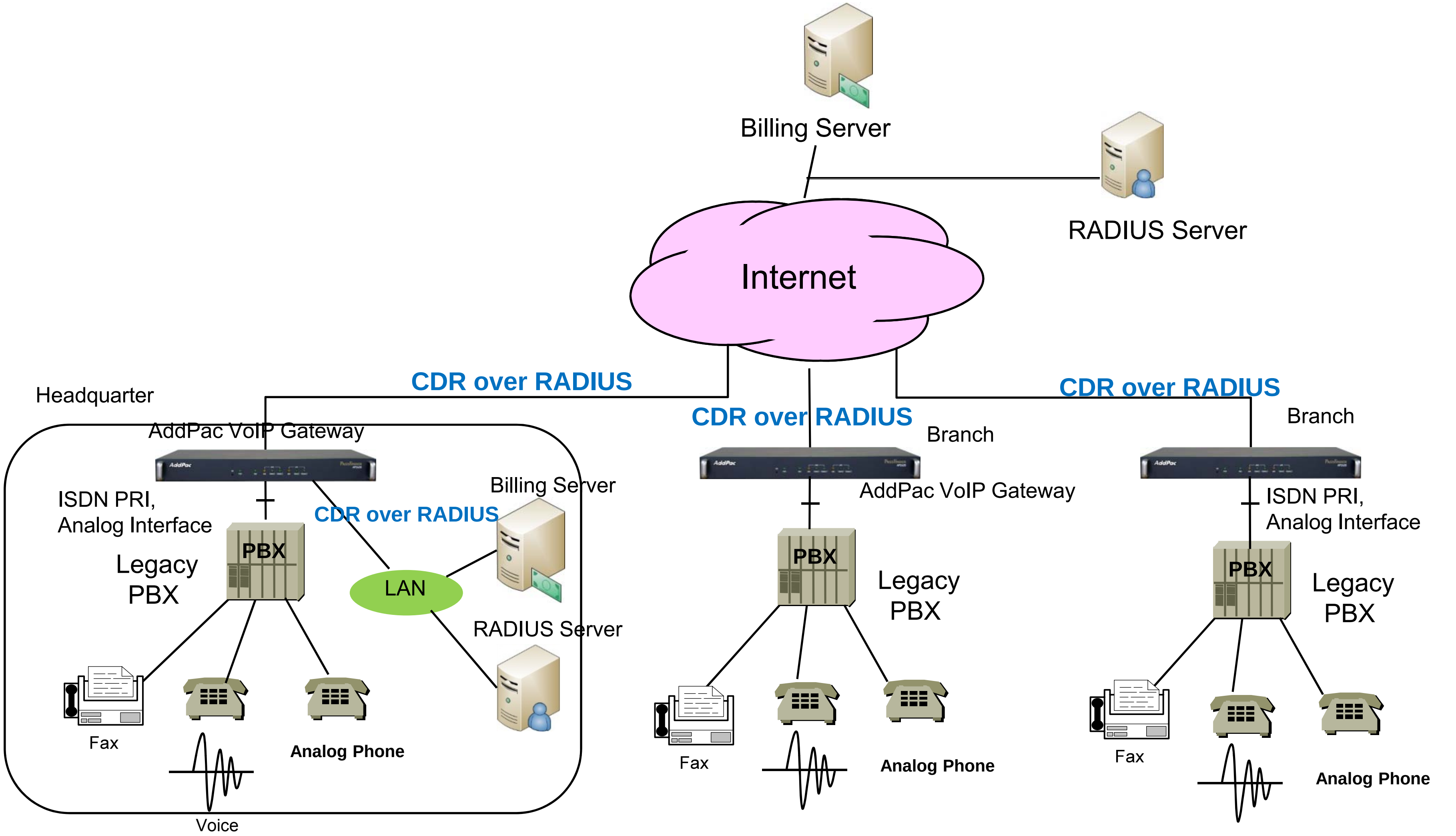
CDR(Call Detail Record) Service Features



Contents

- Network Diagram for CDR Service
- VoIP Gateway CDR Features
- CDR over RADIUS Features
- CDR Data Field

Network Diagram

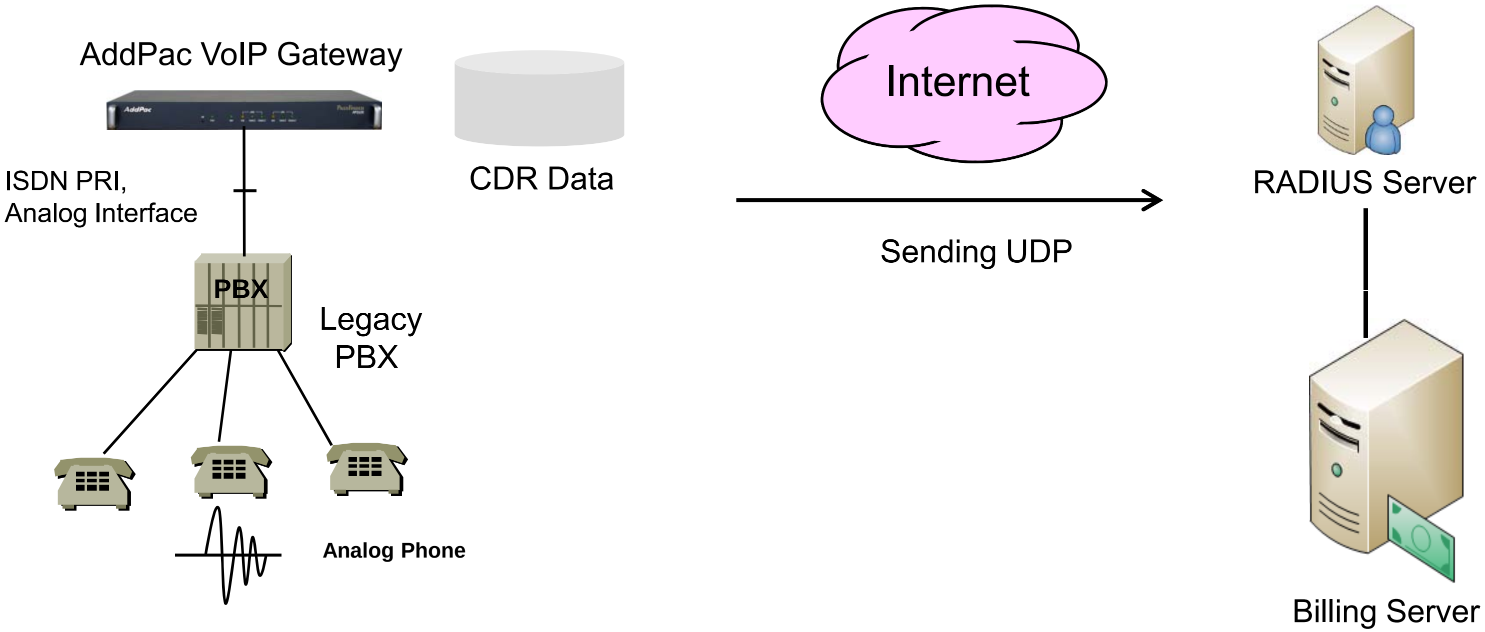


VoIP Gateway CDR Features

- AddPac VoIP Gateway Products support a feature of CDR(Call Detail Records)
  - CDR field parameters for RAIDUS Server
  - One CDR information is created when the call ends. It is composed of 60 data field values

CDR over RADIUS Features

CDR can be transmitted to RADIUS server by using VoIP Gateway Series RADIUS message.



CDR Data Field

Data Field Names	Description
cdrRecordType globalCallId_ClusterID globalCallId_callManagerId globalCallId_callId	**Call Identifier (mandatory)**
dateTimeOrigination dateTimeConnect dateTimeDisconnect duration	**Timestamp and Duration**
callingPartyNumber lastRedirectDn origCalledPartyNumber finalCalledPartyNumber	**Extension Number**
callingPartyNumberPartition lastRedirectDnPartition origCalledPartyNumberPartition finalCalledPartyNumberPartition	**Partition Information**
callingPartyLoginUserId finalCalledPartyLoginUserId	**User Information**
origDeviceName origNetAddr origNetPort origNodeId origSpan destDeviceName destNodeId destSpan destNetAddr destNetPort	**Device Information**

Data Field Names	Description
origMediaTransportAddress origMediaTransportPort origMediaCap_PayloadCapability origMediaCap_MaxFramePerPacket origVideoCap_Codec origVideoCap_Bandwidth origVideoCap_Resolution origVideoTransportAddress origVideoTransportPort destMediaTransportAddress destMediaTransportPort destMediaCap_PayloadCapability destMediaCap_MaxFramePerPacket destVideoCap_Codec destVideoCap_Bandwidth destVideoCap_Resolution destVideoTransportAddress destVideoTransportPort	**Media Channel Information**
origLegCallIdentifier destLegIdentifier destConversationId	**Call Leg Identifier**
origCause_Value origCallTerminationOnBehalfOf lastRedirectRedirectOnBehalfOf lastRedirectReason joinOnBehalfOf destCallTerminationOnBehalfOf origCalledPartyRedirectReason origCalledPartyRedirectOnBehalfOf destCause_Value comment	**State Transition Reason**

DNS UPDATE Features

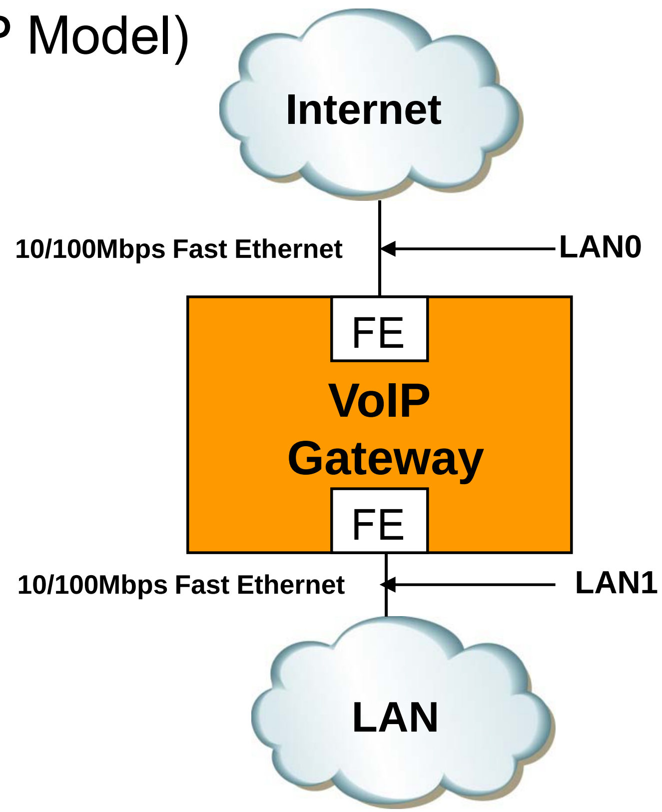
(Dynamic Updates in the Domain Name System)

Contents

- AP100 H/W Specification
- What is DNS Update?
- Network Service Diagram
- APOS Commands for DNS Update

AP100 VoIP Gateway H/W Spec.

- **RISC+DSP (Audio Codec) Microprocessor Computing Power (Dual Processor Architecture)**
- **VoIP Interface**
  - 1-Port FXS Interface
- Optional PSTN Backup Interface (AP100P Model)
- **Network Interface**
  - Two(2) 10/100Mbps Fast Ethernet
  - One(1) RS-232C Console(RJ45)
- **Power Supply**
  - External Power Adaptor (5V, 2A)
  - Power ON/OFF Switch

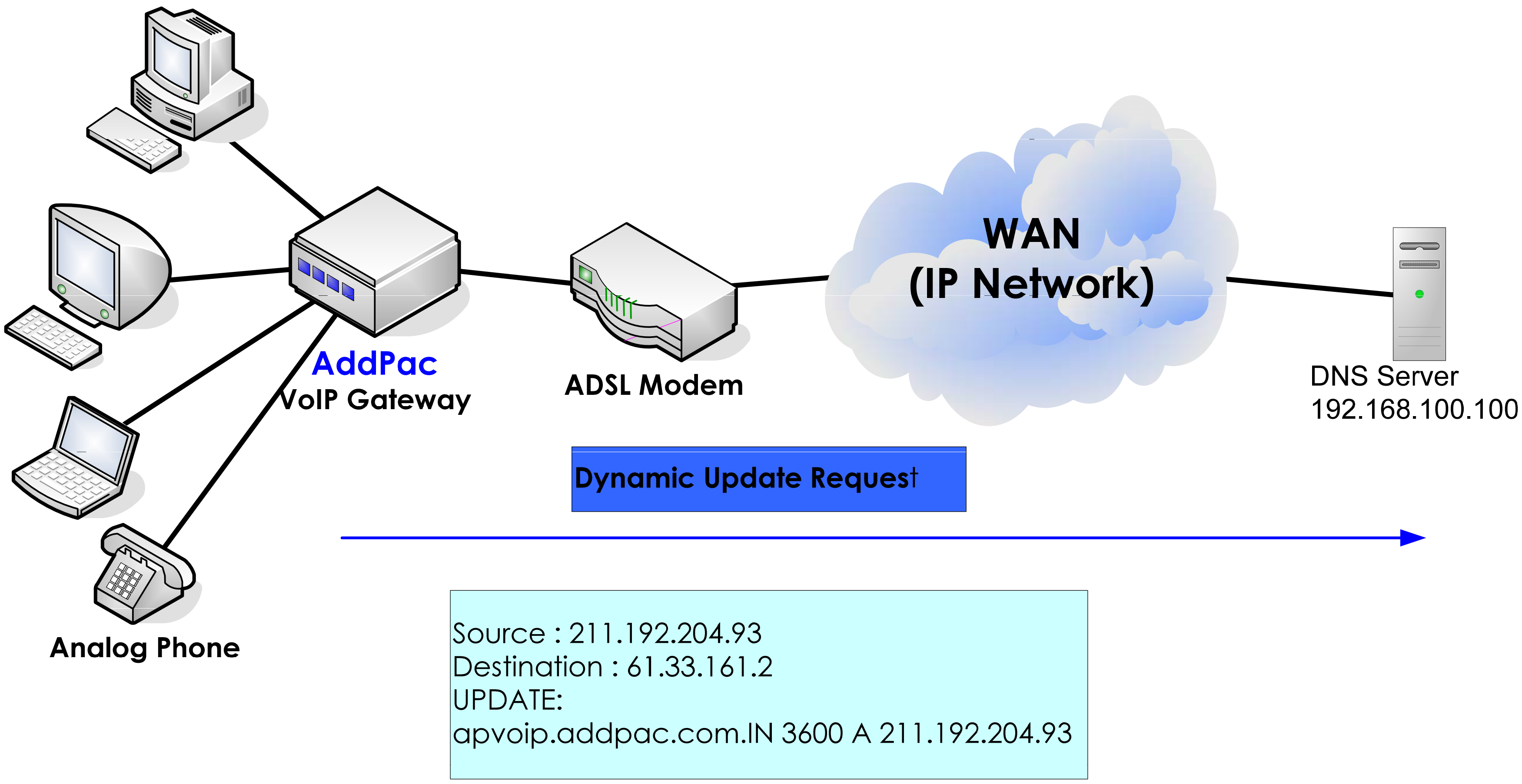


What is DNS UPDATE?

- DNS UPDATE is used to submit Dynamic DNS Update Requests as defined in RFC2136 to a name server

- DNS UPDATE packet is sent to the name server when the interface address is changed.

Network Service Diagram



APOS Commands for DNS Update

```
nsupdate domain-name apvoip.addpac.com
nsupdate nameserver 61.33.161.2
nsupdate ttl 10
!
interface ether0.0
 no ip address
 encapsulation pppoe
 ppp authentication pap callin
 ppp pap sent-username ****** password ******
 ppp echo interval 20
 ppp ipcp ms-dns
 ppp ipcp default-route
 ip nsupdate
!
```

DNS Proxy Features

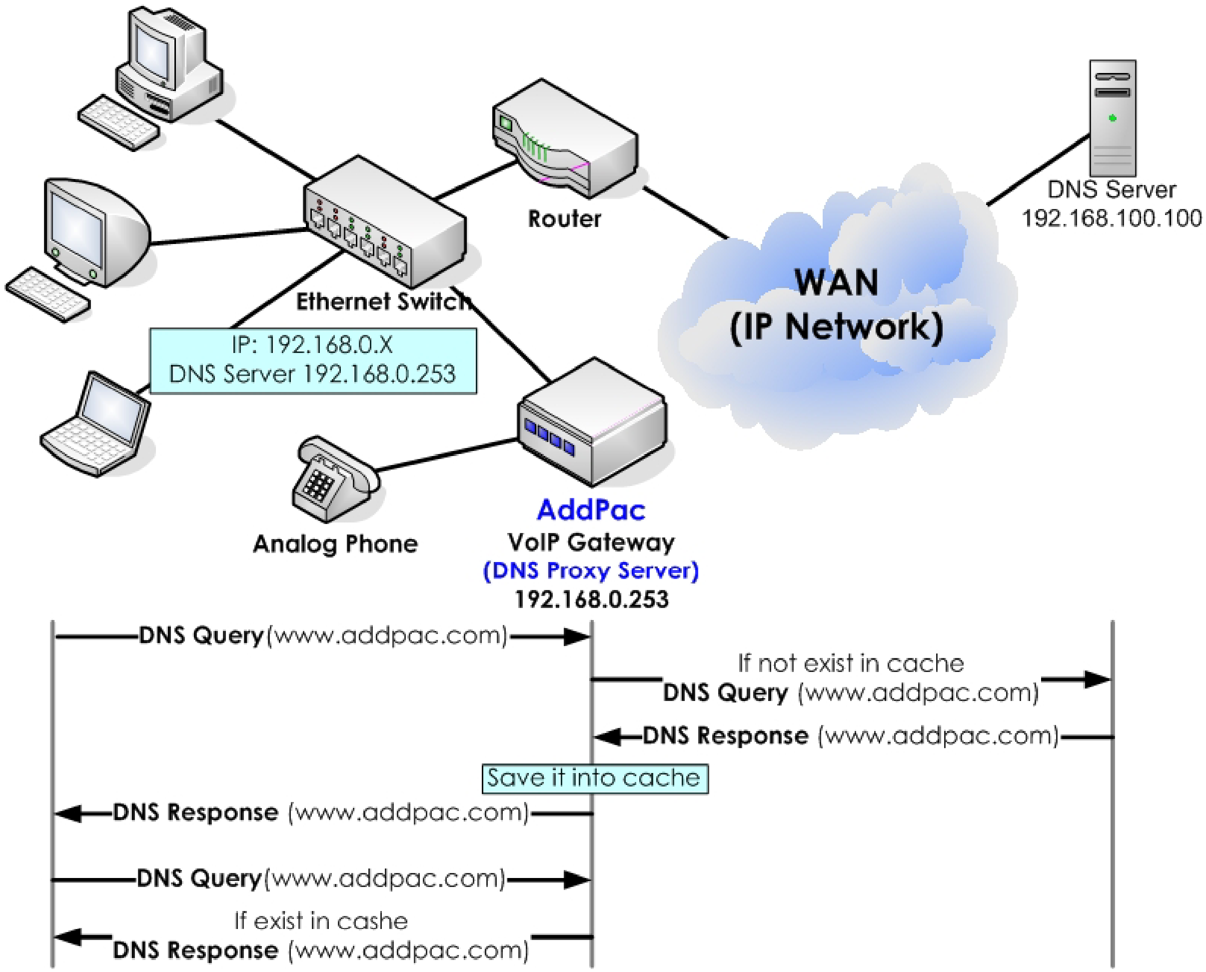
Contents

- What is DNSProxy?
- Network Service Diagram
- APOS Commands for DNS Proxy function

What is DNSProxy ?

- DNSProxy Server recognize the various local character set from Client, and encode the UTF-8(RACE support) format , and then send to DNS server.
- DNSProxy Server is existed between Local Client (PC) and DNS Server
- Local Client Domain Name Query to DNSProxy Server and If DNS Proxy Server don’t have a Enquired Domain Name (Cache missing), DNSProxy Server this Domain Name Query to DNS Server and Relay to Original Local Client.
- DNSProxy listen to Well-Known UDP Port(53) to receive DNS Query from Client.

Network Service Diagram



APOS Commands for DNSProxy

DNSProxy Function Enable

Step	Command	Explanation
1	(config)# **service dnsproxy**	DNSProxy Function Enable

DNSProxy Function Disable

Step	Command	Explanation
1	(config)# **no service dnsproxy**	DNSProxy Function Disable

Dual MAC Address Concept

Contents

- QoS Enabled VoIP Service
- Dual MAC Address Features
- Network Diagram

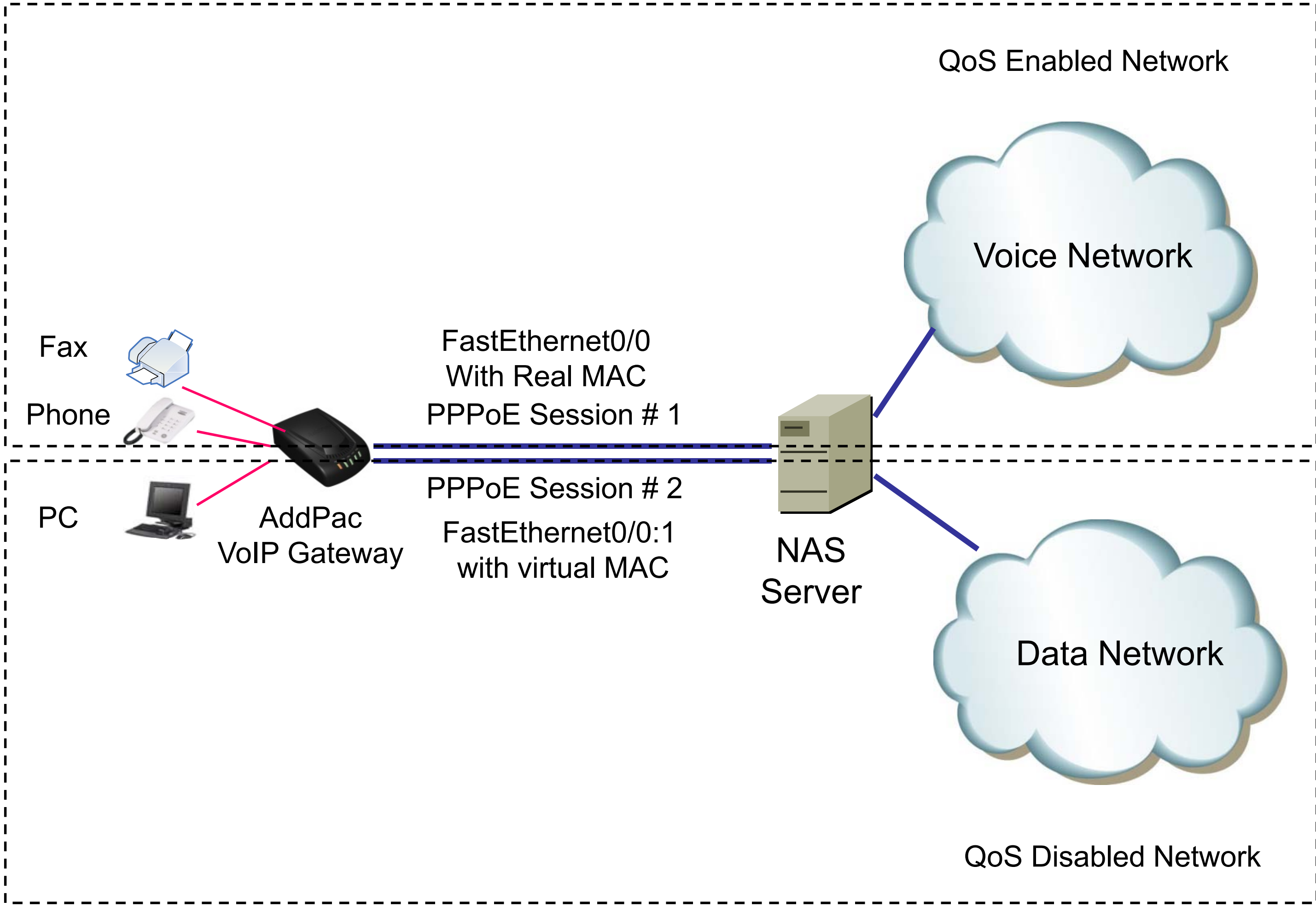
QoS Enabled VoIP Service

- AddPac VoIP Gateway supports Two(2) Ethernet Interface for LAN traffic such as Personal Computer.
- Some ISP want to provide the QoS Enable Network Service for High Quality VoIP Service.
- QoS Enabled Network Service for Real-Time Traffic such as Voice over IP traffic
- Best Effort Network Service for Normal Data Traffic such as Web, Email

Dual MAC Address Features

- Normally working at PPPoE Environment (DHCP also possible)
- PPPoE Server(NAS) has 2 service (voice & data)
- Gateway support 2 MAC Address
  - Real MAC Address
  - Virtual MAC Address
- The User set the virtual MAC address at Ethernet Sub-interface
- Gateway Get Public Address using PPPoE with different PPPoE Service Name

Network Diagram

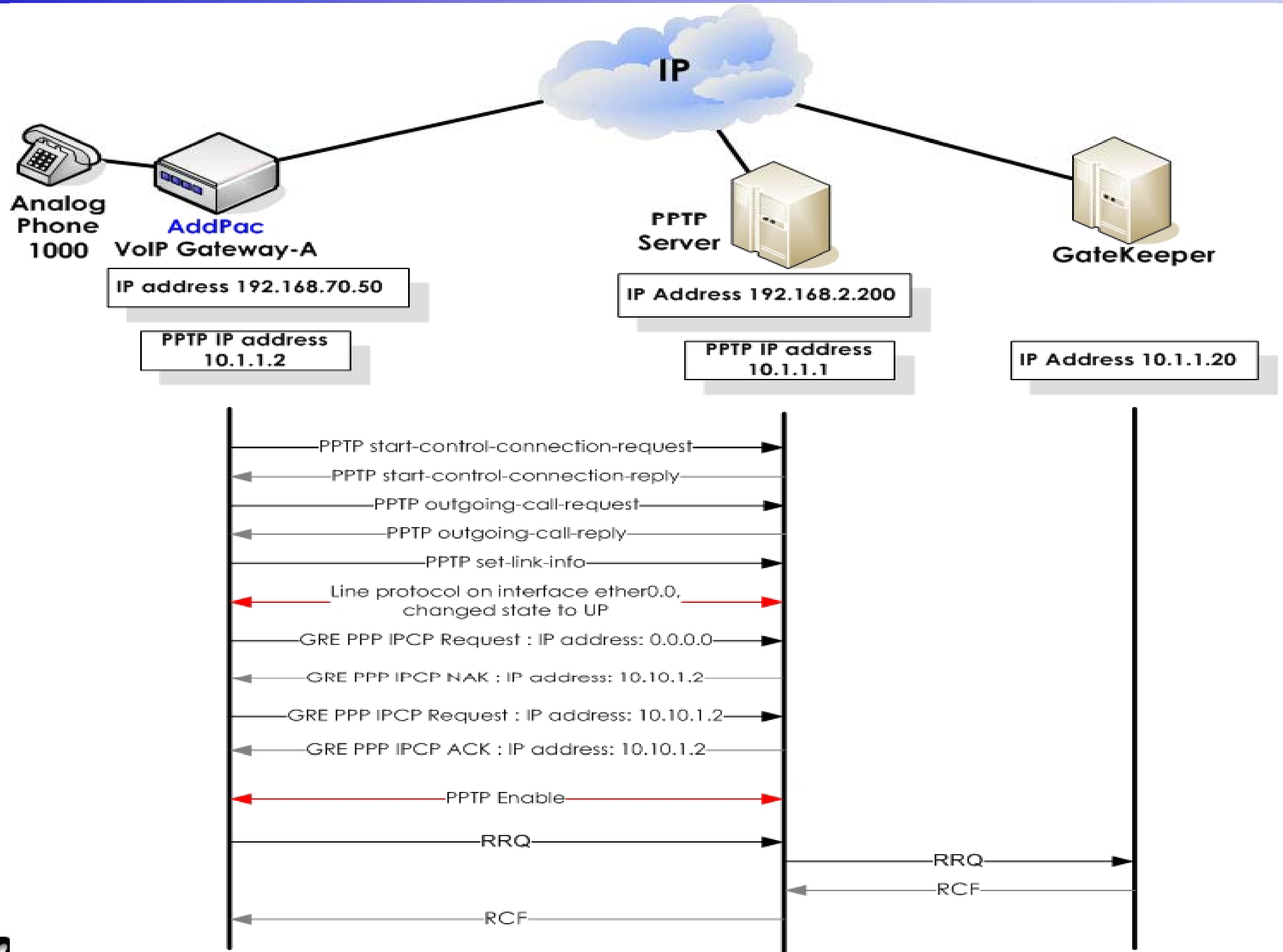


PPTP (Point-to-Point Tunneling Protocol) Features

Contents

- PPTP Network Service Diagram
- APOS Commands for STUN function
- Application Examples

Network Service Diagram



APOS Commands for PPTP

PPTP Function Enable

STEP	Command	Explanation
1	# **config**	Enter the APOS command Setting Mode
2	**(config)# interface eth 0.0**	Enter the interface setting mode
3	(config-ether0.0)# **no ip address**	IP address disable
4	(config-ether0.0)# **encapsulation ppp-pptp**	PPTP setting as Network Protocol (notice : interface pptp0 is created when encapsulation ppp-pptp is enable)
5	(config-ether0.0)# **pptp ip remote 192.168.2.200**	PPTP Server IP address setting
5	(config-ether0.0)# **pptp route data**	This command is used when a user want to send Data to PPTP interface (optional)
7	(config-ether0.0)# **ppp authentication chap callin**	Chap protocol setting as PPP authentication
8	(config-ether0.0)# **ppp chap hostname addpac**	Chap USER ID = "addpac"
9	(config-ether0.0)# **ppp chap password 1234**	Chap PASSWORD = "1234"
10	(config-ether0.0)# **no ppp ipcp ms-dns**	Disable the configuration setting that DNS IP address can be received from PPP server

APOS Commands for PPTP

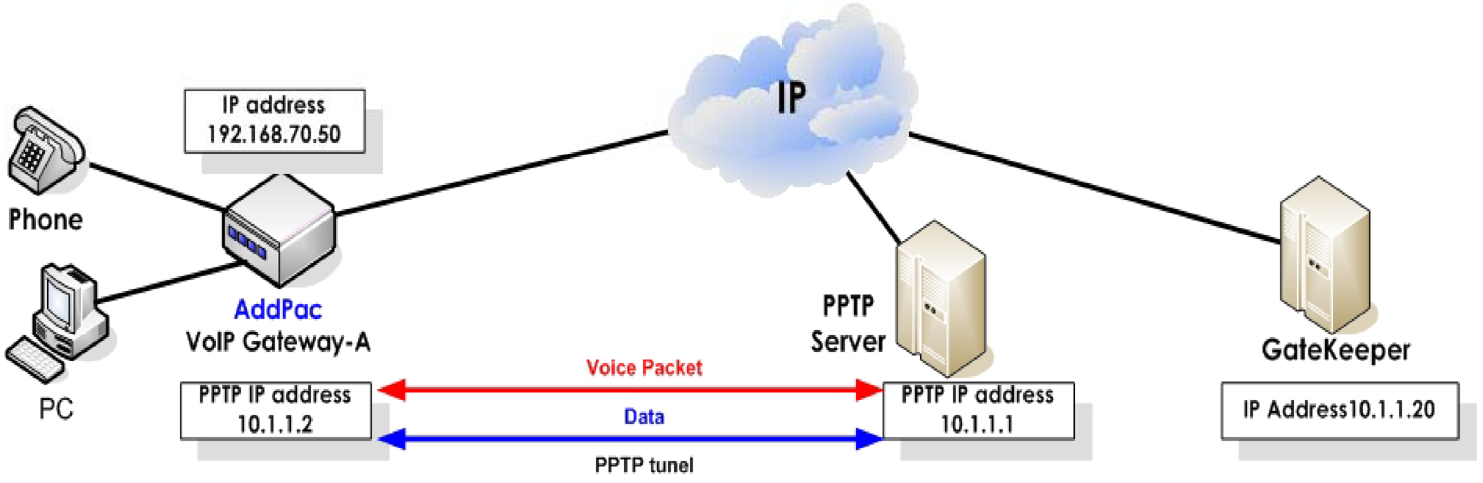
11	(config-ether0.0)# **no ppp ipcp default-route**	**Disable the configuration setting that Default router's IP address can be received from PPP Server. (important)**
12	(config-ether0.0)#**exit**	Exit from the interface setting mode
13	(config)# **interface pptp0**	Enter the interface pptp0 setting mode
14	(config-pptp0)# **ip address 192.168.70.50 255.255.255.0**	IP address setting (Please refer to Quick Operation Guide for DHCP, PPPoE configuration.)
15	(config-ether0.0)#**exit**	Exit from interface 0.0 setting mode
16	(config)#**route 0.0.0.0 0.0.0.0 192.168.70.1**	**Default router setting**
17	(config)#**route 20.1.1.0 255.255.255.0 10.1.1.1**	If a user want to send the traffic of 20.1.1.0 network to other network via 10.1.1.1 network, this static routing command is used. (optional)
18	(config)# **ip-policy ip host voip-interface any route-if ether0.0**	This configuration is used when a user want to send DATA traffic to Public network and VoIP traffic to Private Network (optional)
19	(config)#**exit**	Exit from setting mode

PPTP Function Disable

STEP	**Command**	**Explanation**
1	(config-ether0.0)#**no encapsulation ppp-pptp**	PPTP Configuration Disable

Application Example 1. (cont.)

Send all traffic(VoIP + Data) to PPTP Interface



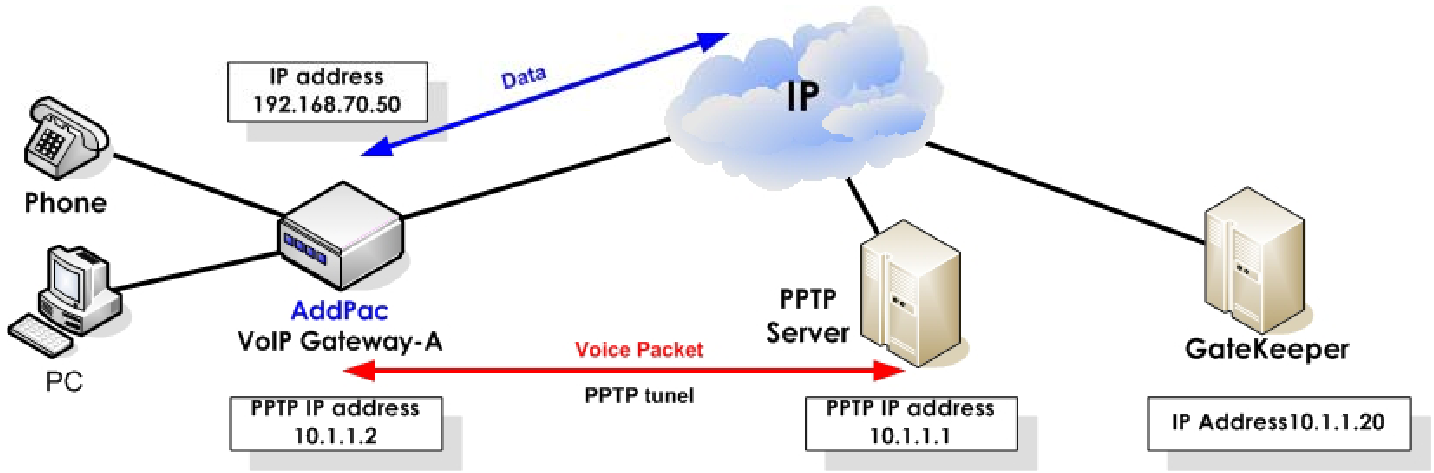

```
version 8.22p1
!
hostname AP100
!
dhcp-list 0 type server
dhcp-list 0 address server interface ether0.0
dhcp-list 0 option dhcp-lease-time 600
dhcp-list 0 option dns 168.126.63.1
dhcp-list 0 option router-option 216.55.248.129
```

Application Example 1.

```
!
dhcp-list 1 type server
dhcp-list 1 address server  10.1.1.2 10.1.1.126 255.255.255.128
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
!
interface ether0.0
 no ip address
 encapsulation ppp-pptp
 pptp ip remote 192.168.2.200
ppp authentication chap callin
 ppp chap hostname Addpac
 ppp chap password 1234
 no ppp ipcp ms-dns
 no ppp ipcp default-route
!
interface ether1.0
 no ip address
 ip dhcp-group 0
!
interface pptp0
 ip address 192.168.70.50 255.255.255.0
```

Application Example 2. (cont.)

Send VoIP traffic only to PPTP Interface (IP Share Environment)



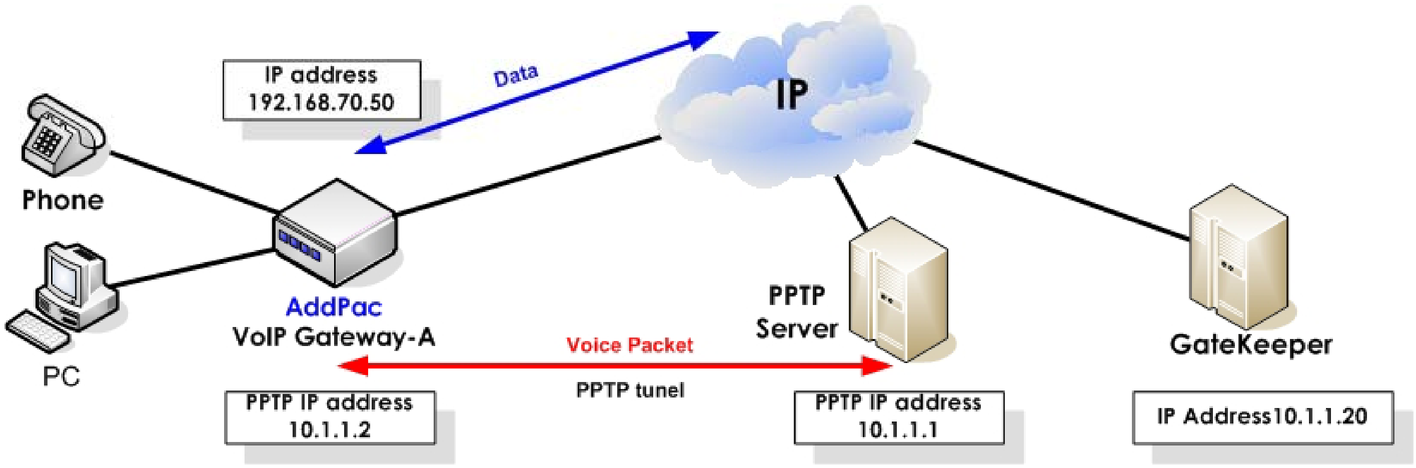

```
version 8.22p1
!
hostname AP100
!
dhcp-list 0 type server
dhcp-list 0 address server interface pptp0
dhcp-list 0 option dhcp-lease-time 600
dhcp-list 0 option dns 168.126.63.1
dhcp-list 0 option router-option 216.55.248.129
```

Application Example 2.

```
!
dhcp-list 1 type server
dhcp-list 1 address server  10.1.1.2 10.1.1.126 255.255.255.128
!
ip-share enable
ip-share interface net-side pptp0
ip-share interface local-side ether1.0
!
interface ether0.0
 no ip address
 encapsulation ppp-pptp
 pptp ip remote 192.168.2.200
 pptp route data
 ppp authentication chap callin
 ppp chap hostname Addpac
 ppp chap password 1234
 no ppp ipcp ms-dns
 no ppp ipcp default-route
!
interface ether1.0
 no ip address
 ip dhcp-group 0
!
interface pptp0
 ip address 192.168.70.50 255.255.255.0
!
ip-policy ip    host  voip-interface any  route-if ether0.0
```

Application Example 3. (cont.)

Send VoIP traffic only to PPTP Interface (PAT Environment)




```
version 8.234
!
hostname AP100
!
dhcp-list 0 type server
dhcp-list 0 address server  10.1.1.2 10.1.1.254 255.255.255.0
dhcp-list 0 option dns 168.126.63.1
dhcp-list 0 option router-option 10.1.1.1
!
nat-list 1 pat static-entry tcp 1720  local
```

Application Example 3.(cont.)

```
nat-list 1 pat static-entry udp 5060  local
nat-list 1 pat static-entry tcp 1723  local
nat-list 1 pat group-static-entry udp 22000 22001 local
nat-list 1 pat group-static-entry udp 23000 24999 local
nat-list 1 pat group-static-entry tcp 10000 10999 local
nat-list 1 pat group-static-entry tcp 14000 14999 local
nat-list 1 pat group-static-entry tcp 18000 18999 local
nat-list 1 pat static-entry tcp 23  local
nat-list 1 pat group-static-entry tcp 20 21 local
nat-list 1 pat group-static-entry udp 67 68 local
nat-list 1 pat static-entry icmp ping  local
!
no ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
!
interface ether0.0
 no ip address
 encapsulation ppp-pptp
 pptp ip remote 192.168.2.200
 pptp route data
 ppp authentication chap callin
 ppp chap hostname addpac
```

Application Example 3.

```
ppp chap password addpac
no ppp ipcp ms-dns
no ppp ipcp default-route  ← This command is used when a used doesn't
want to get the default routing information from PPTP server
!
interface ether1.0
 ip address 10.1.1.1 255.255.255.0
 ip nat-group 1 pat pptp0  ← pptp0 interface ip (public  IP) translate ,
 ip dhcp-group 0
!
interface pptp0
 no ip address
 encapsulation pppoe
 ppp authentication pap callin
```

Tunneling Service Features

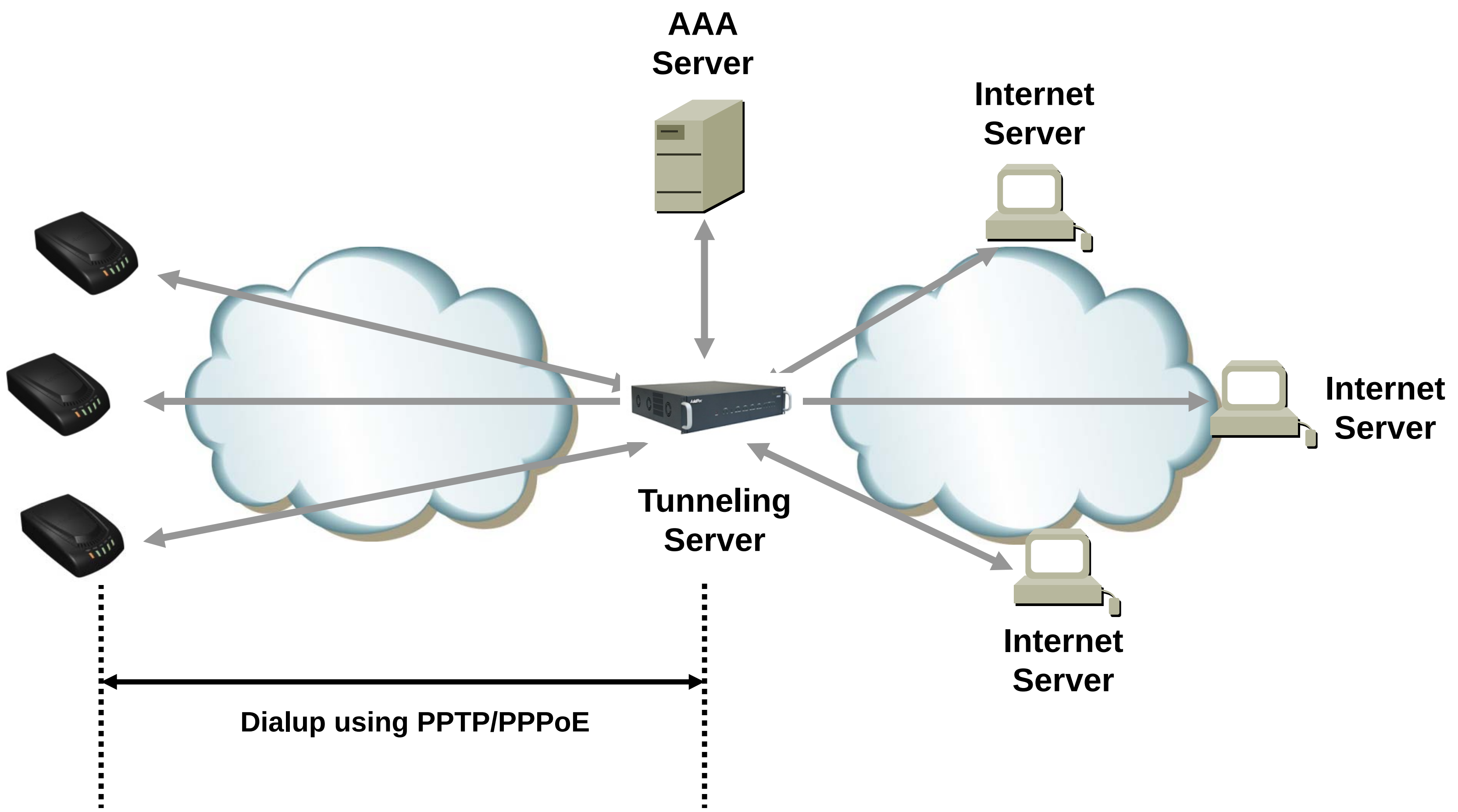
Contents

- Tunneling Server Feature
- Dialup Tunneling Protocol
- IP Tunneling Protocol at NAT/PAT
- Tunneling Service at NAT/PAT
- Tunneling Service at VPN

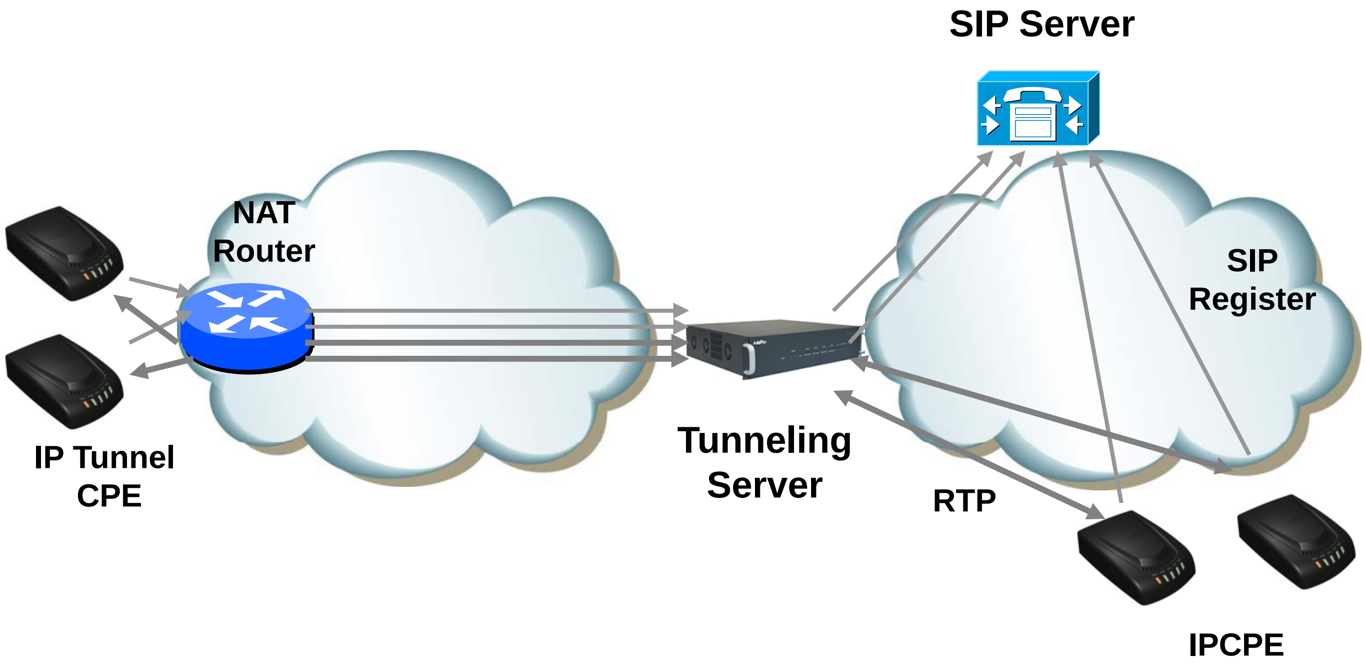
Tunneling Service Feature

- RADIUS Interface (AAA)
- Dialup Tunneling Protocol
  - PPTP
  - PPPoE
- IP Tunneling Protocols
  - IPIP
- PPP Authentication
  - PAP
  - CHAP

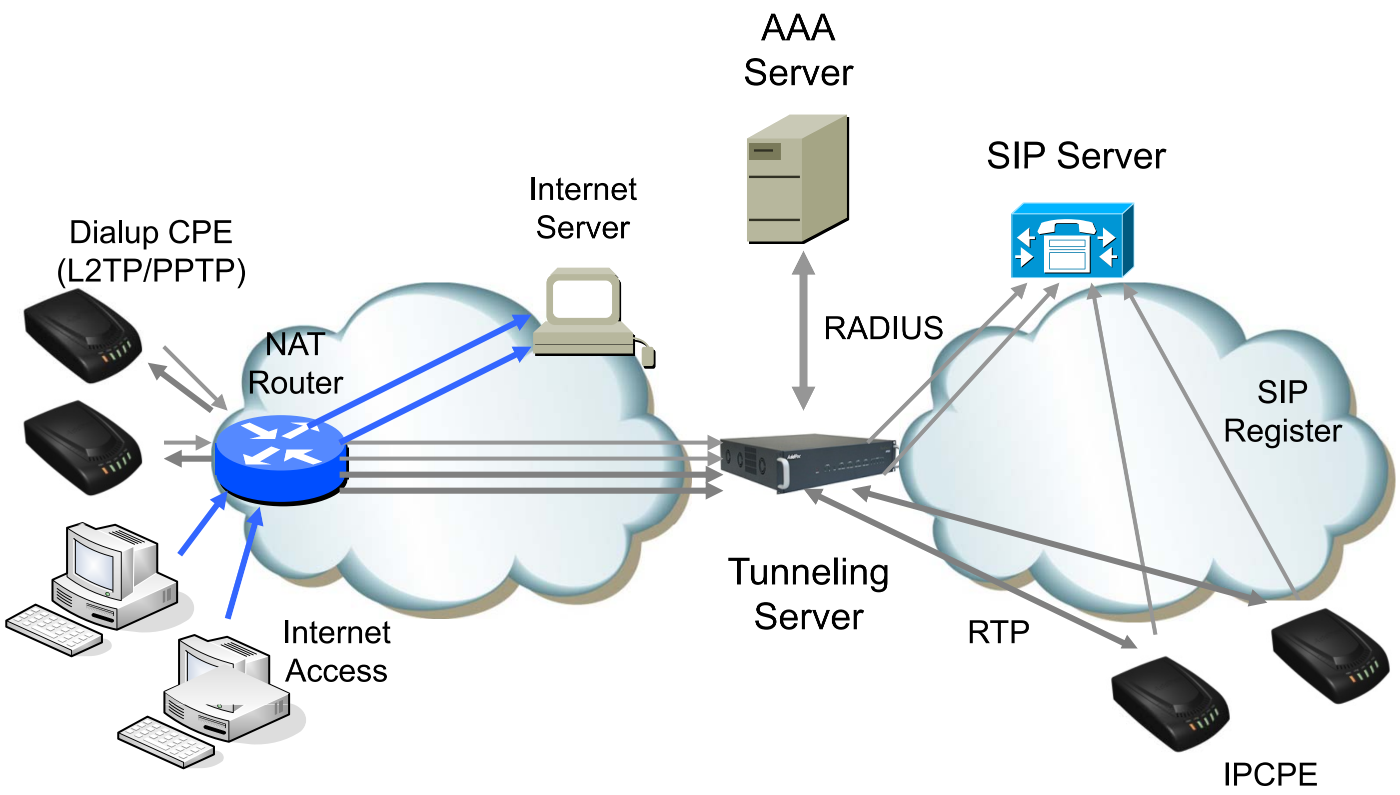
Dialup Tunneling Protocol



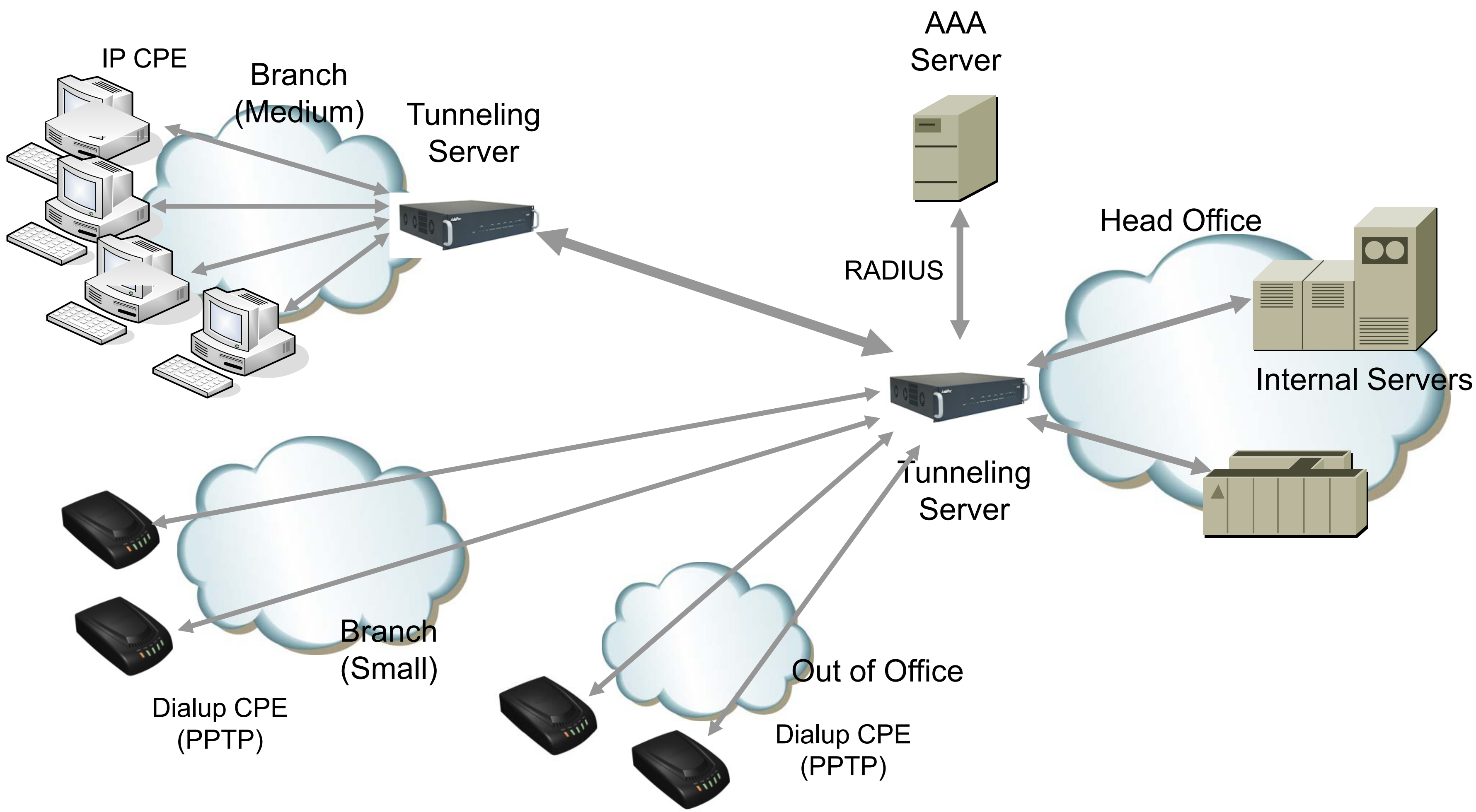
IP Tunneling Protocol at NAT/PAT



Tunneling Service at NAT/PAT



Tunneling Service at VPN

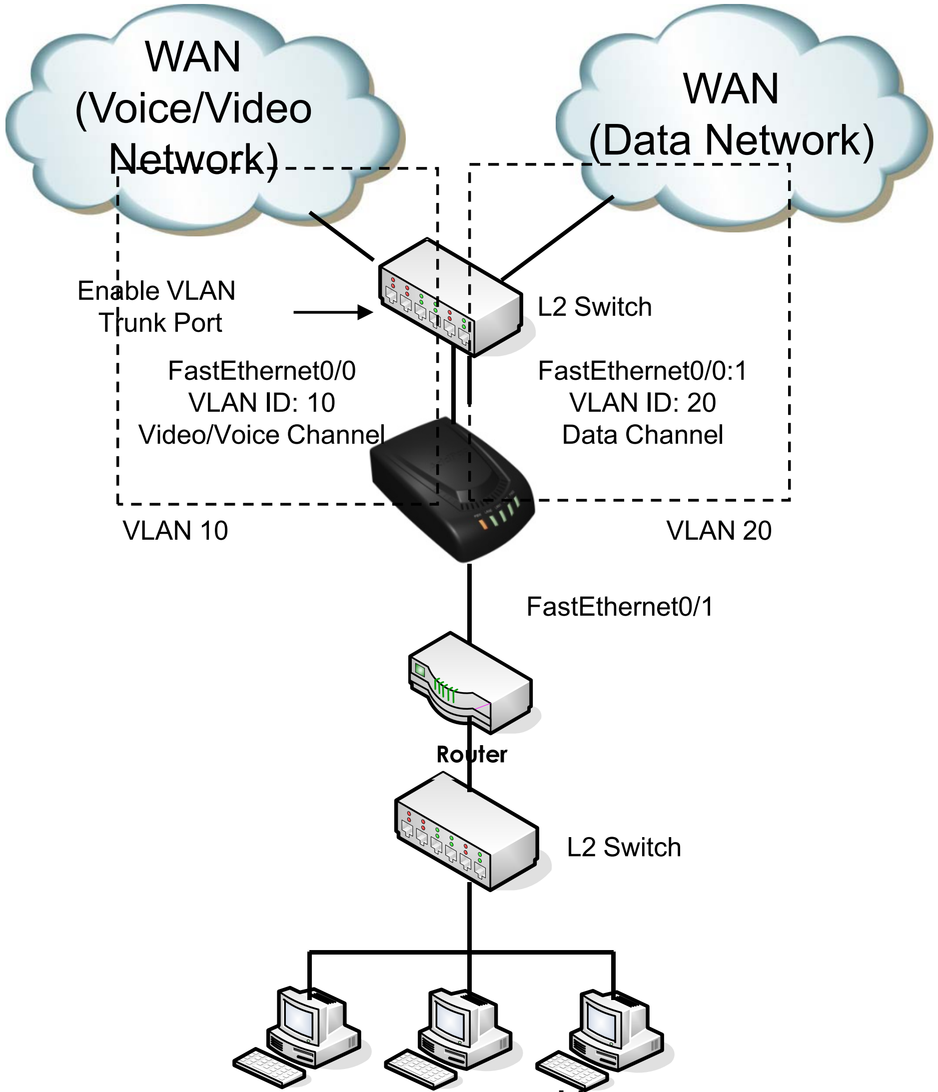


802.1Q + 802.1P + Bridge VLAN

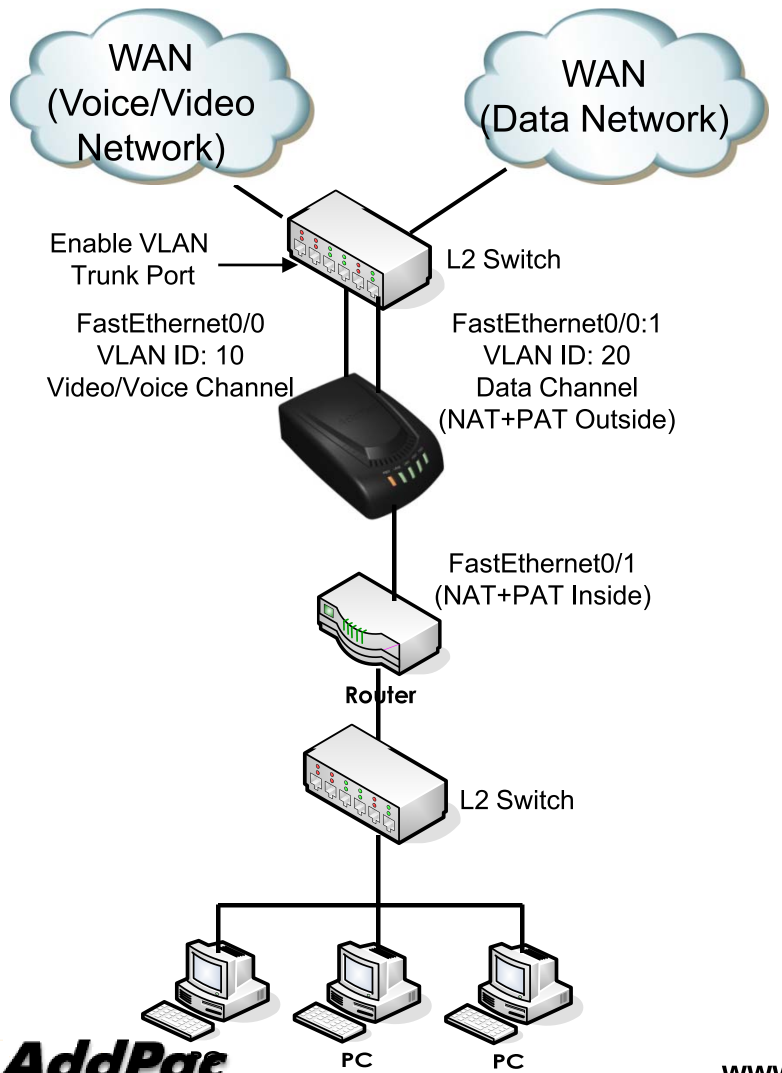
Contents

- 802.1Q VLAN Encapsulation
- 802.1P VLAN Priority
- VLAN Bridge

802.1Q VLAN +NAT/PAT

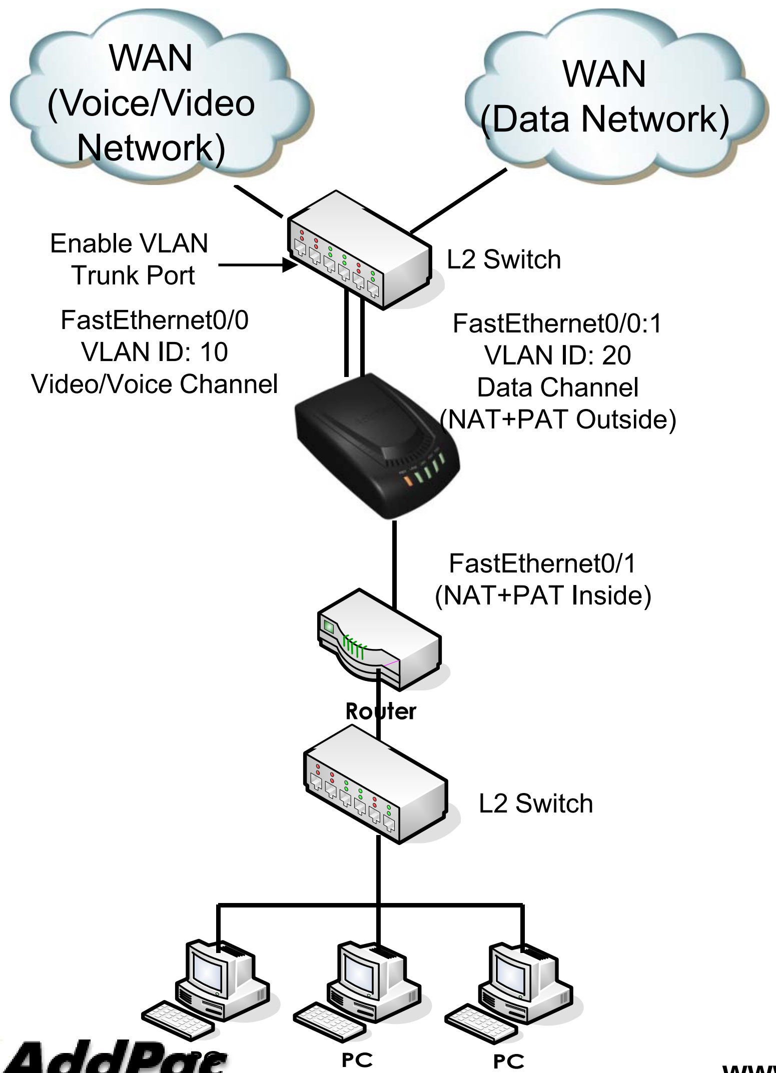


Public IP (Static IP) + NAT/PAT



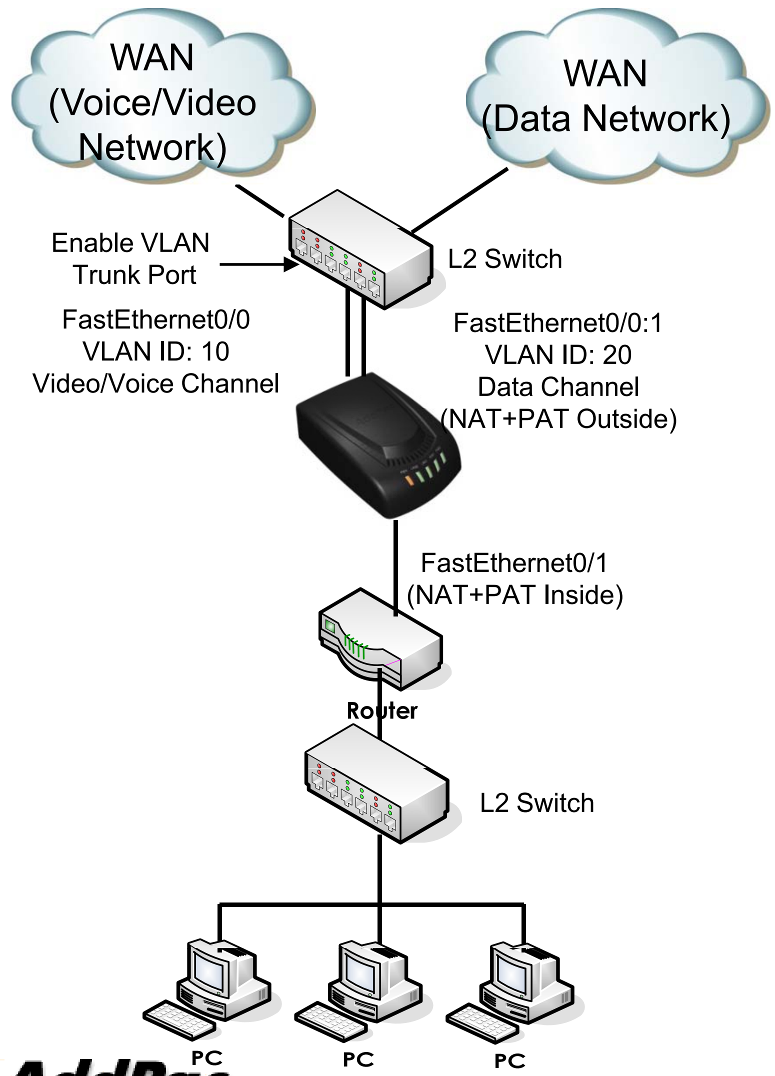

```
!
interface Loopback0
 ip address 127.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 ip address 200.212.149.130 255.255.255.0
 encapsulation dot1Q 10
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 speed auto
!
interface FastEthernet0/0:1
 ip address 61.33.161.130 255.255.255.0
 encapsulation dot1Q 20
 ip nat outside
!
ip route 0.0.0.0 0.0.0.0 61.33.161.1
ip route 0.0.0.0 0.0.0.0 200.212.149.1
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
ip nat inside source list 1 interface FastEthernet0/0:1 overload
!
```

Public IP (DHCP) + NAT/PAT



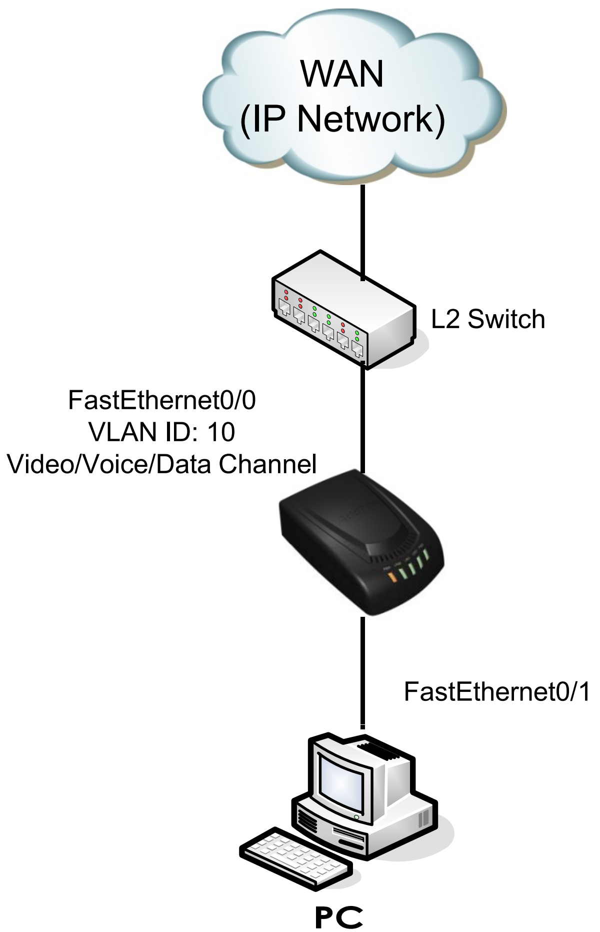

```
interface Loopback0
 ip address 127.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 ip address dhcp
 encapsulation dot1Q 10
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 speed auto
!
interface FastEthernet0/0:1
 ip address dhcp
 encapsulation dot1Q 20
 ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
ip nat inside source list 1 interface FastEthernet0/0:1 overload
```

Public IP (PPPoE) + NAT/PAT

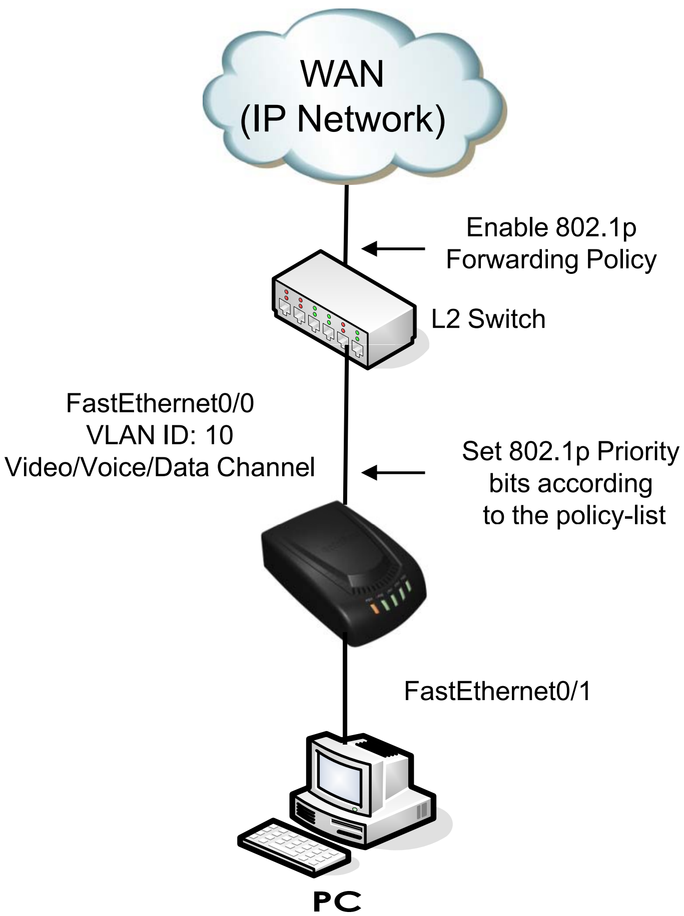



```
interface FastEthernet0/0
 no ip address
 encapsulation dot1Q 10
 pppoe enable
 encapsulation ppp
 pppoe-client local-interface
 ppp authentication pap callin
 ppp pap sent-username test password test
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 speed auto
!
interface FastEthernet0/0:1
 no ip address
 encapsulation dot1Q 20
 pppoe enable
 encapsulation ppp
 pppoe-client local-interface
 ppp authentication pap callin
 ppp pap sent-username test password test
 ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
ip nat inside source list 1 interface FastEthernet0/0:1 overload
```

802.1Q VLAN +802.1P CoS

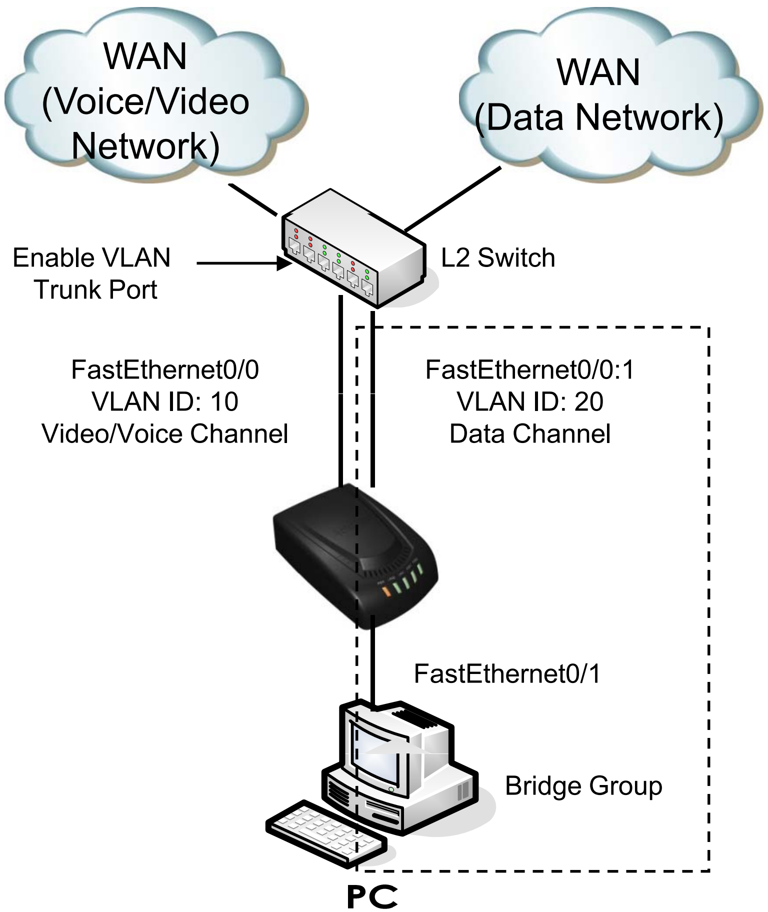


VLAN + CoS

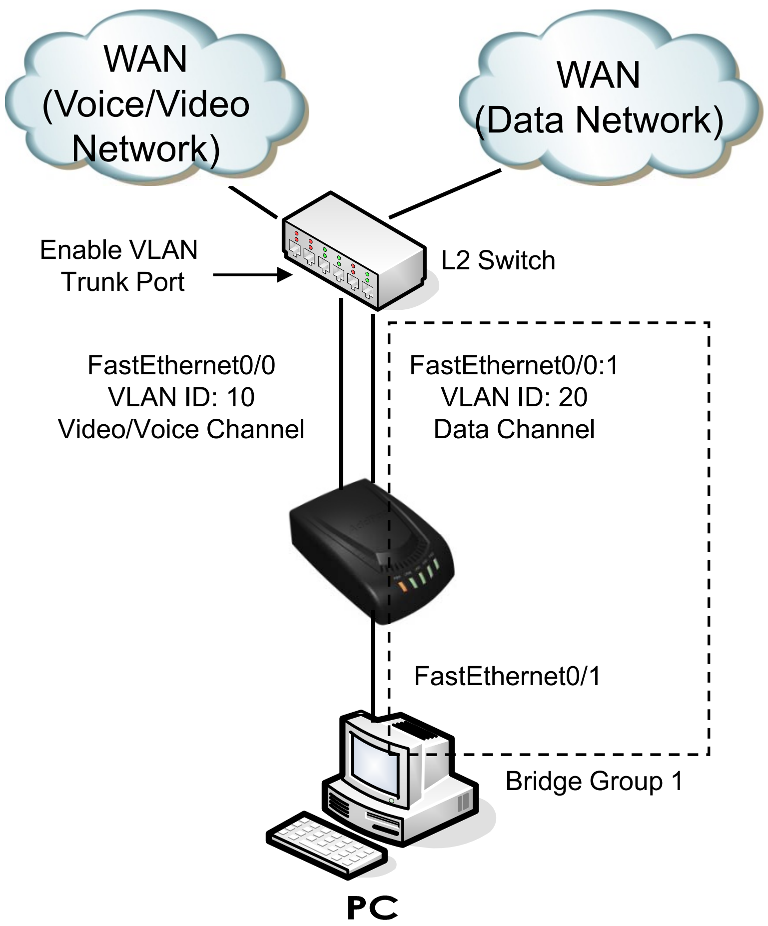



```
!
interface Loopback0
 ip address 127.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 ip address 200.212.149.130 255.255.255.0
 encapsulation dot1Q 10
 ip nat outside
 ip policy-group 1
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 speed auto
!
ip route 0.0.0.0 0.0.0.0 200.212.149.1
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
ip policy-list 1 local signaling cos 7
ip policy-list 1 local rtp cos 7
ip policy-list 1 default cos 0
!
ip nat inside source list 1 interface FastEthernet0/0 overload
!
```

802.1Q VLAN +Bridge

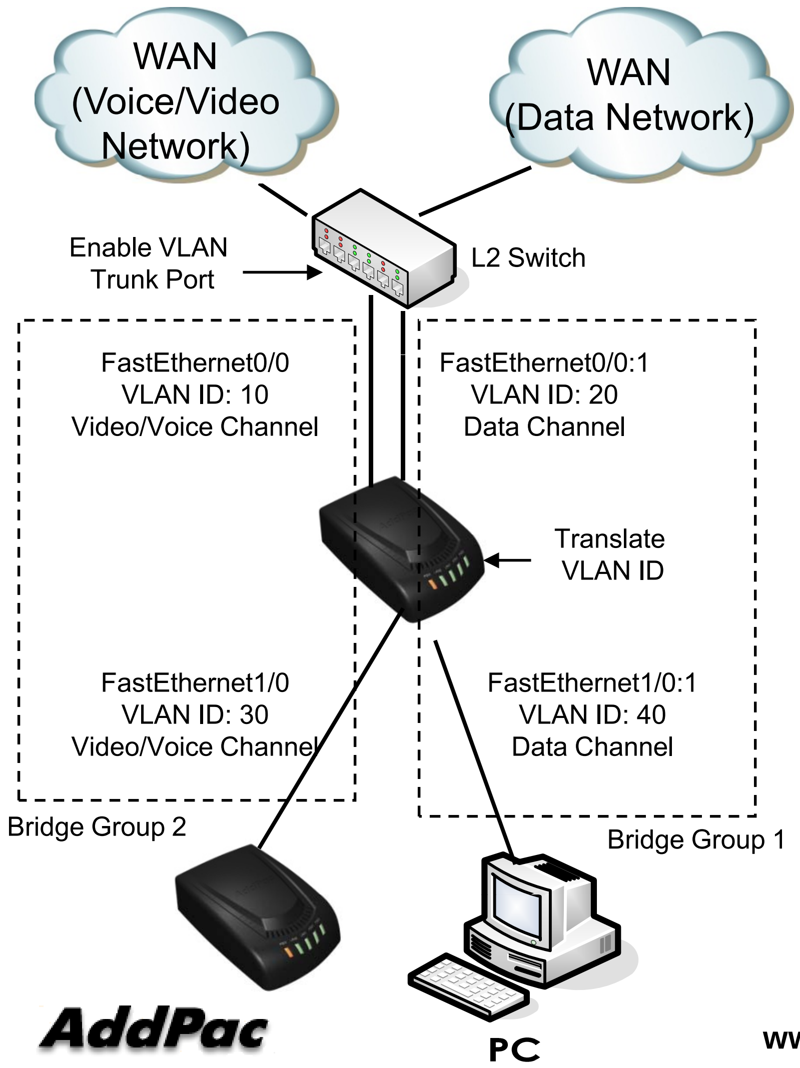


VLAN + Single Bridge Group




```
!
interface Loopback0
 ip address 127.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 ip address 200.212.149.130 255.255.255.0
 encapsulation dot1Q 10
 speed auto
!
interface FastEthernet0/1
 no ip address
 bridge-group 1
 speed auto
!
interface FastEthernet0/0:1
 no ip address
 encapsulation dot1Q 20
  bridge-group 1
!
no ip routing
!
ip route 0.0.0.0 0.0.0.0 200.212.149.1
!
!
!
```

VLAN + Double Bridge Group




```
!
interface FastEthernet0/0
 ip address 200.212.149.130 255.255.255.0
 encapsulation dot1Q 10
 bridge-group 2
 speed auto
!
interface FastEthernet0/1
 no ip address
 encapsulation dot1Q 30
 bridge-group 2
 speed auto
!
interface FastEthernet0/0:1
 no ip address
 encapsulation dot1Q 20
 bridge-group 1
!
interface FastEthernet1/0:1
 no ip address
 encapsulation dot1Q 40
 bridge-group 1
!
no ip routing
!
ip route 0.0.0.0 0.0.0.0 200.212.149.1
!
```

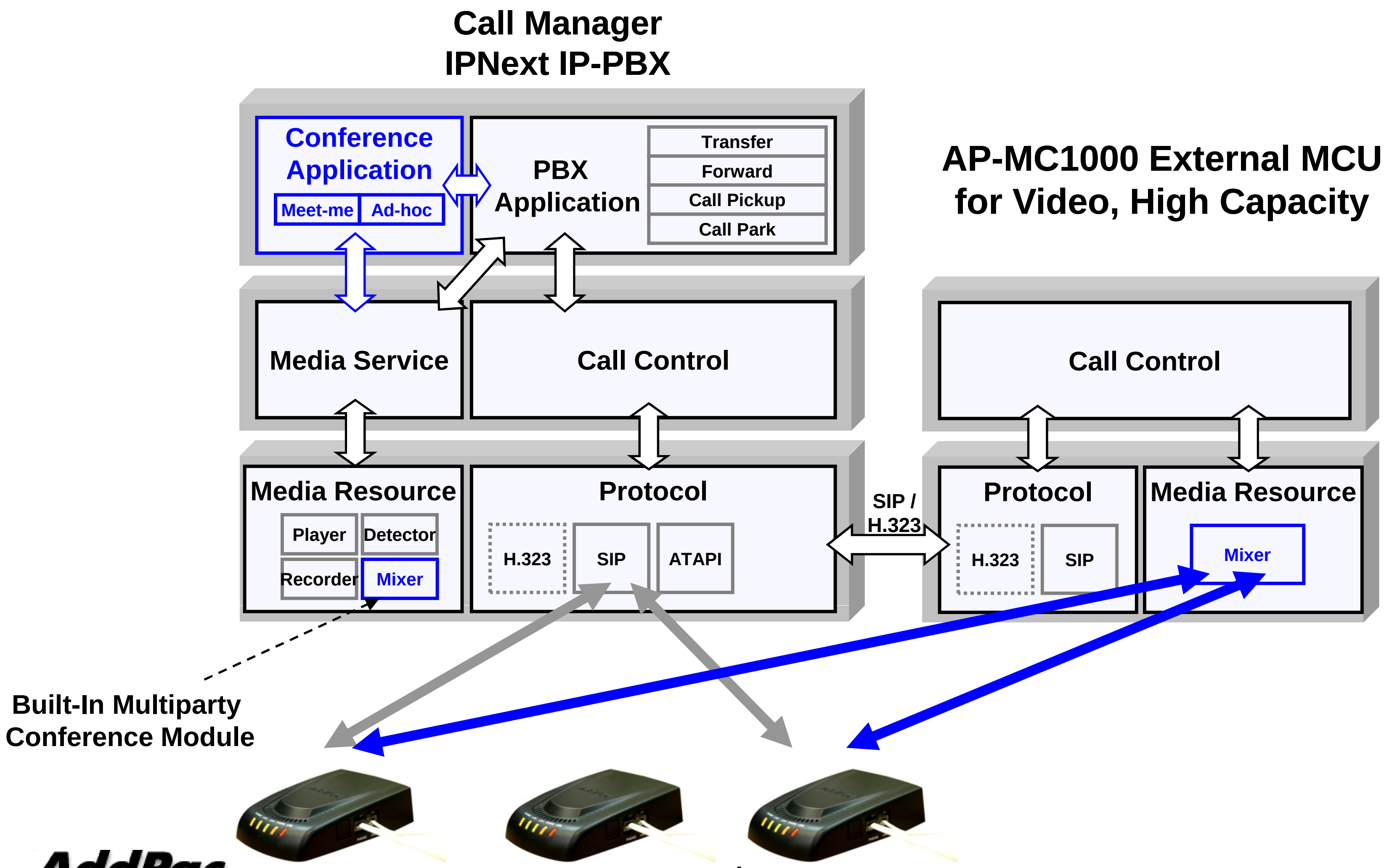
Standalone 3-Party Call Conference (AP100 1-Port FXS Gateway)

Contents

- Multiparty Conference Model (External MCU)
- Standalone AP100 3-Party Conference Model
- Network Diagram
- Signal Flow Diagram

Multiparty Conference Model

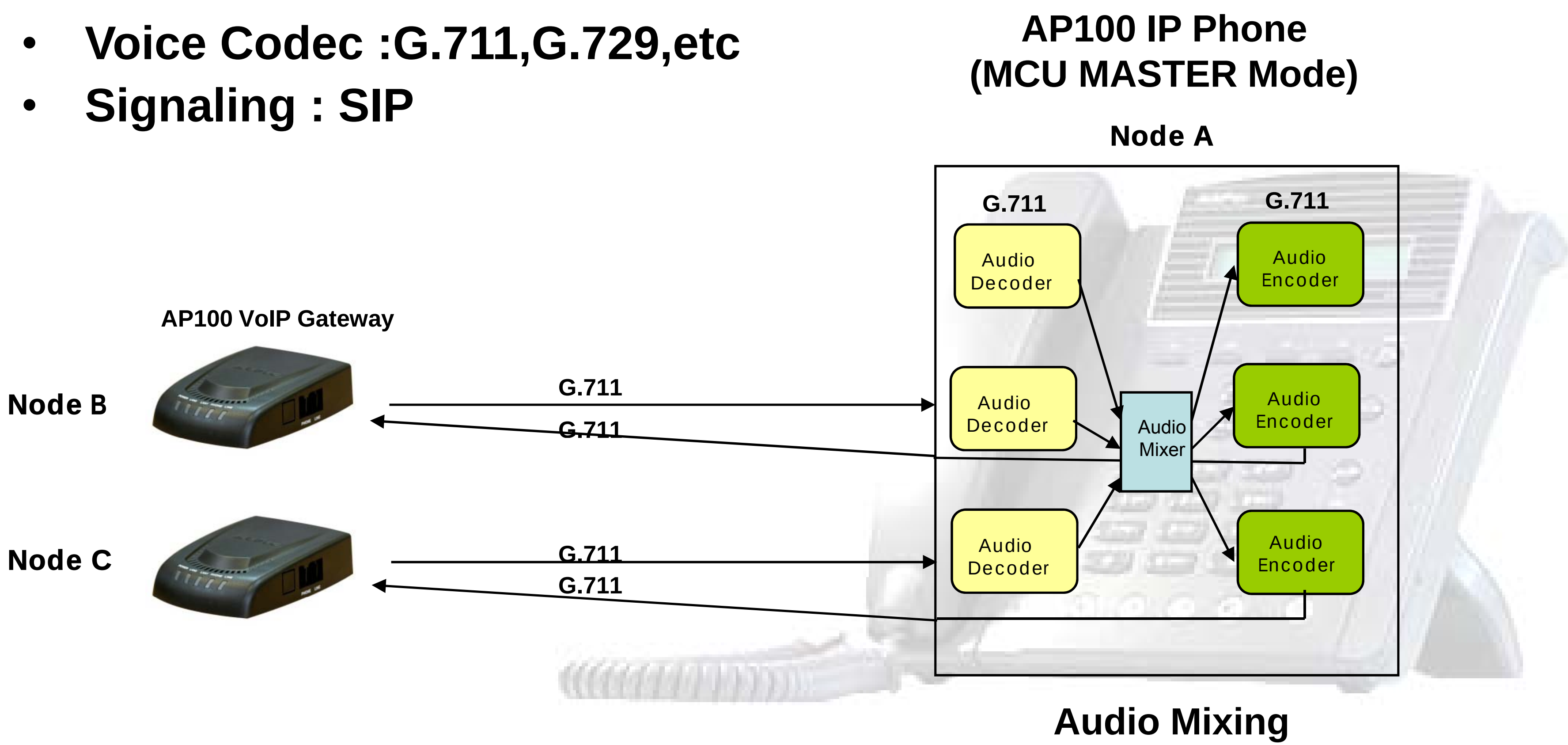
External MCU Model



Standalone 3-Party Conference Model

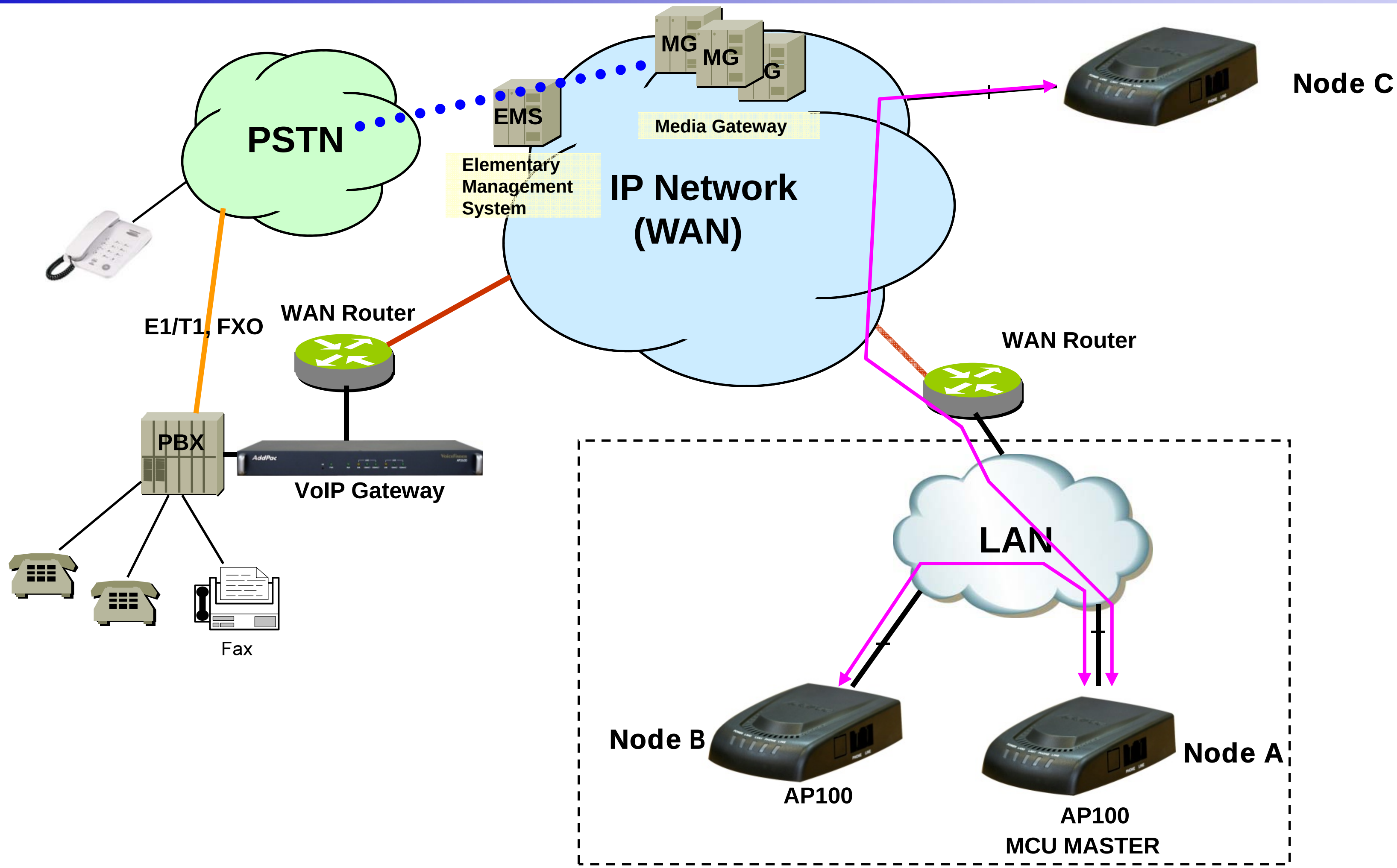
AP100 Built-In 3-Party Conference

- **Voice Codec :G.711,G.729,etc**
- **Signaling : SIP**



Network Service Diagram

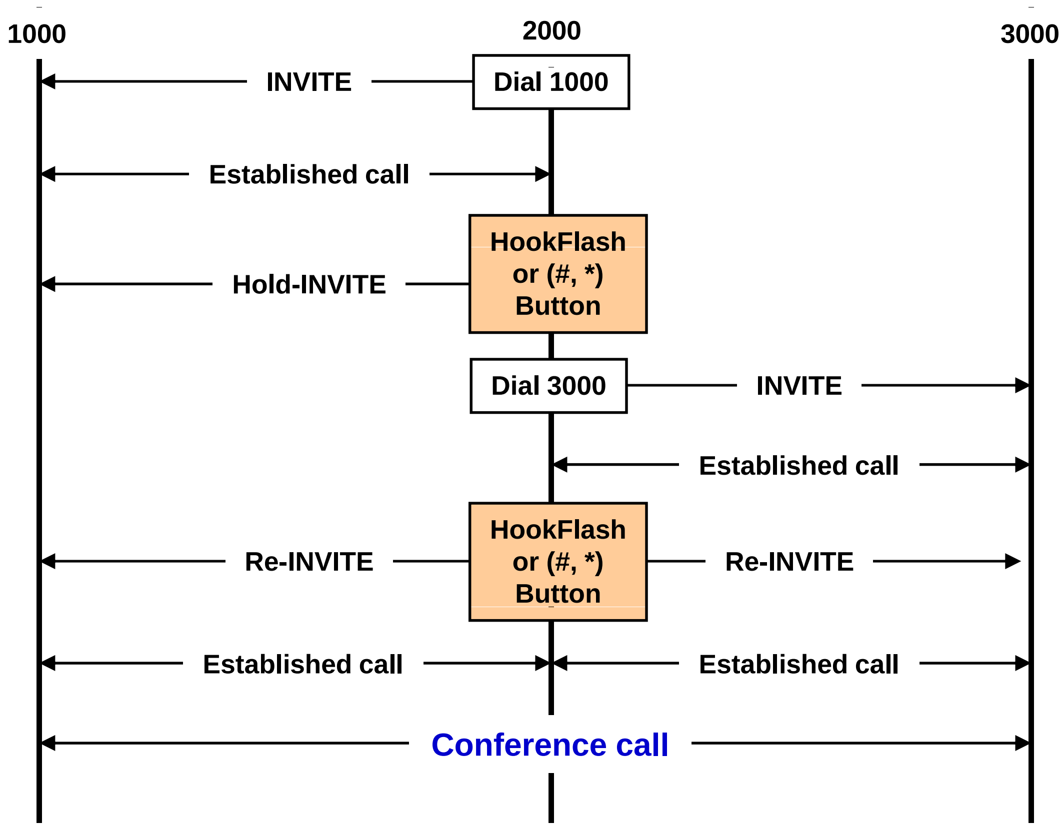
AP100 1-Port VoIP Gateway



Conference Call Network

Signal Flow Diagram

Conference Call Flow



VoIP Gateway/IP-PBX Interworking with Skype

IPNext50
IP-PBX

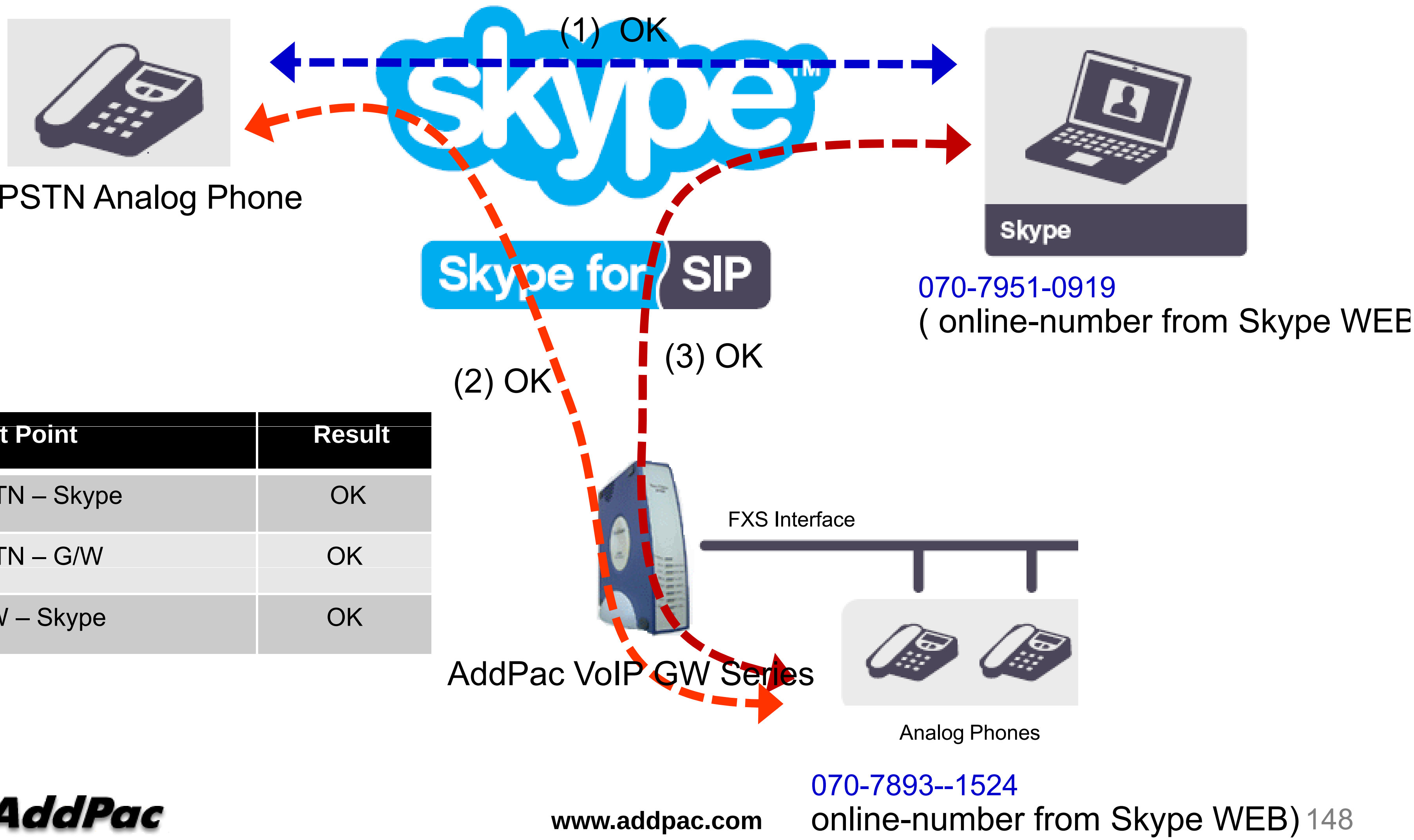
IPNext20
IP-PBX

AP100B
VoIP Gateway

Contents

Skype Interworking Test
(GW – Skype :using online-number)

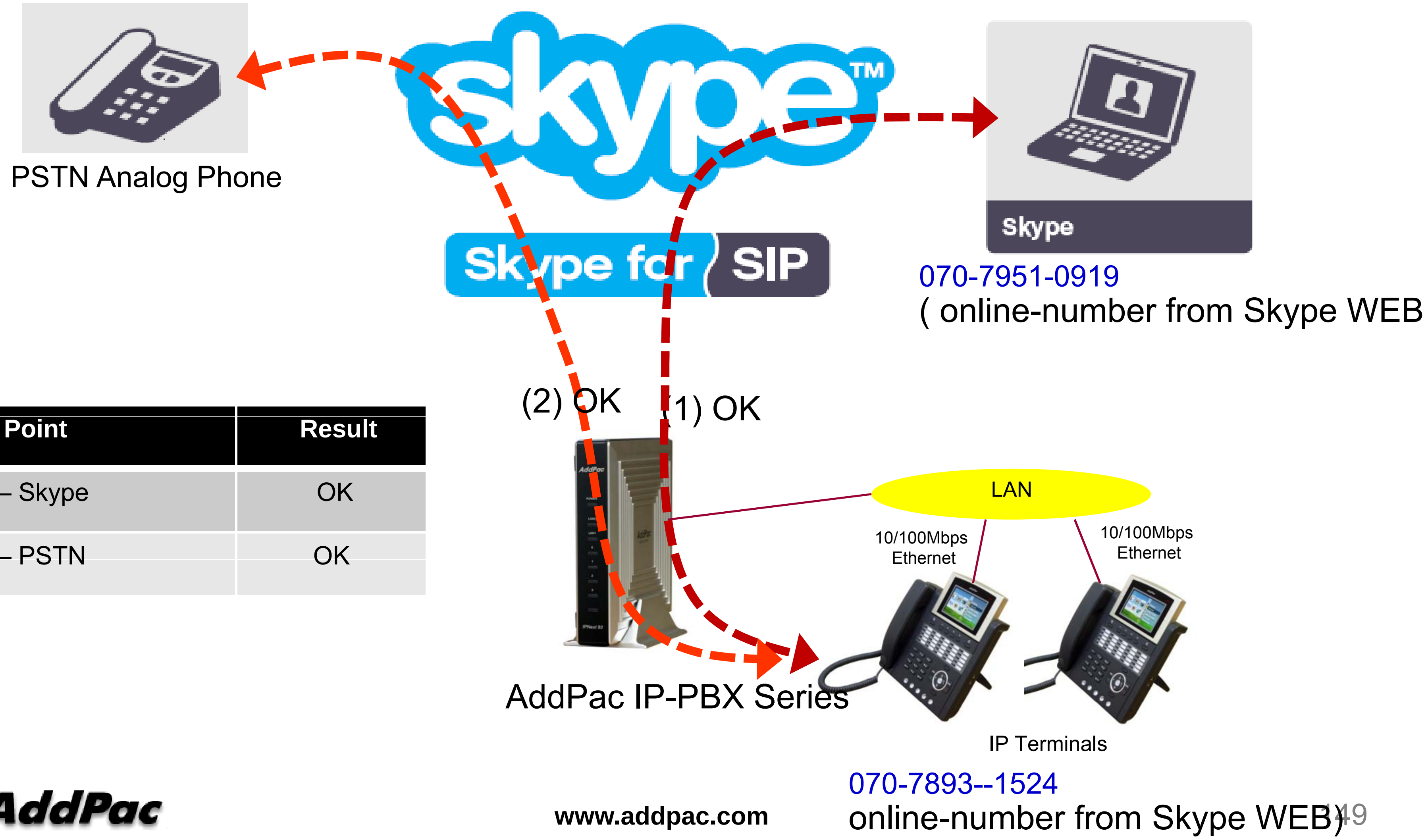
Test System Diagram (GW – Skype)



Test Point	Result
PSTN – Skype	OK
PSTN – G/W	OK
G/W – Skype	OK

Skype Interworking Test
(IP-PBX– Skype :using online-number)

Test System Diagram (IP-PBX – Skype)



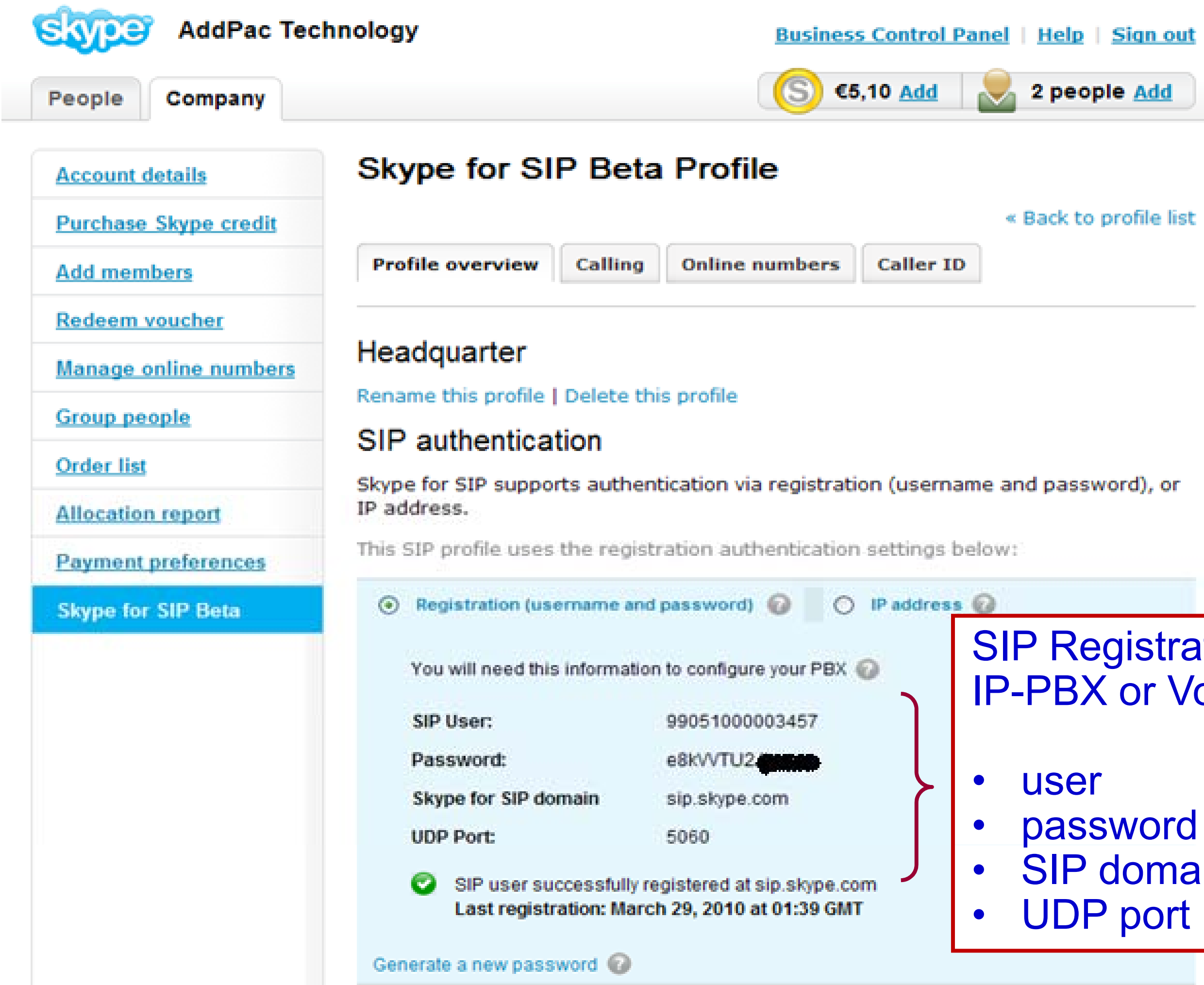
Test Point	Result
PBX– Skype	OK
PBX– PSTN	OK

Skype Interworking Test
(IP-PBX– Skype :using **Skype-name**)

Test System Diagram (IP-PBX – Skype)

Skype Configuration for IP-PBX or G/W (1/3)

Skype for SIP Beta

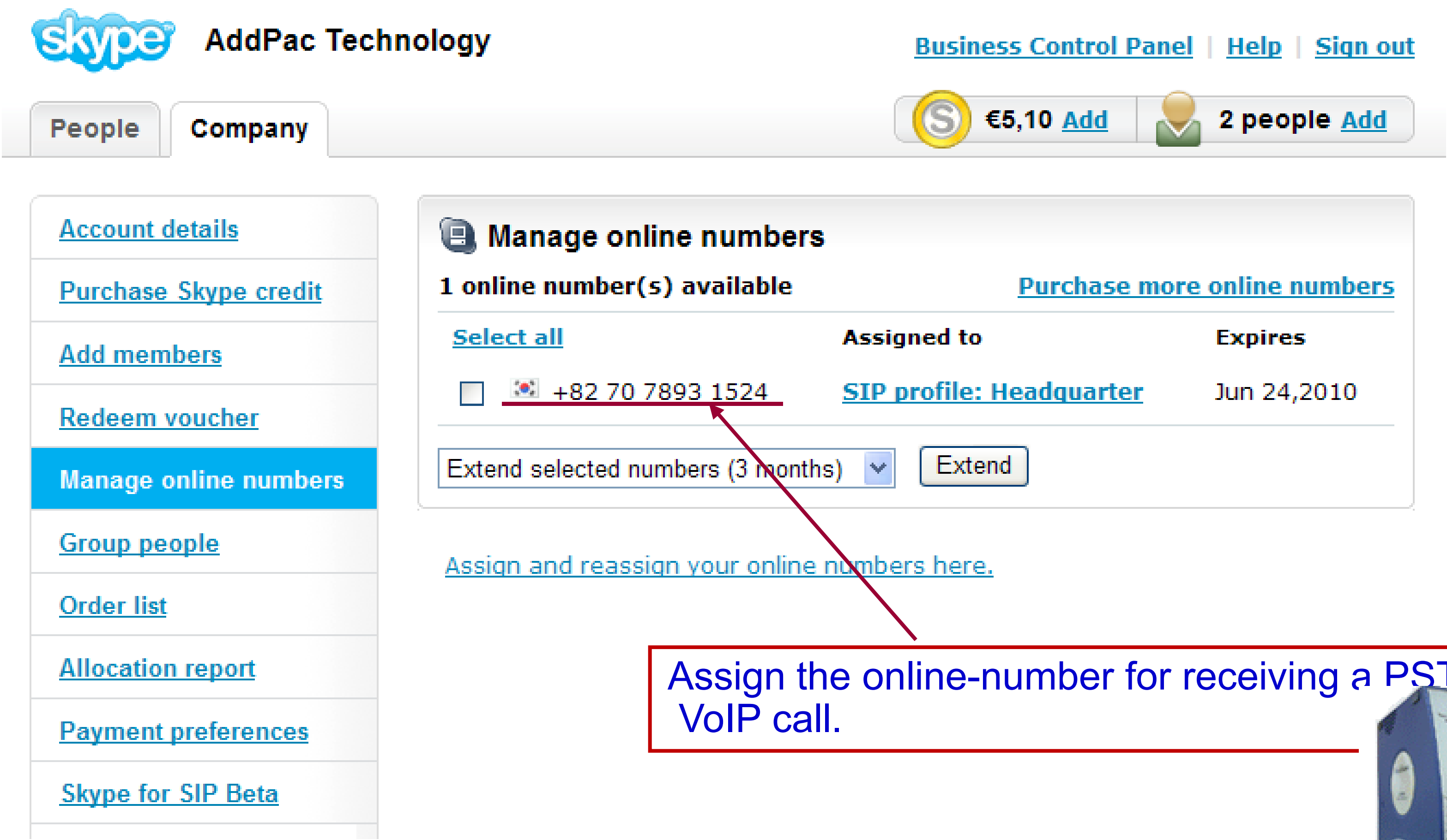


SIP Registration Information for IP-PBX or VoIP Gateway

- user
- password
- SIP domain
- UDP port

Skype Configuration for IP-PBX or G/W (2/3)

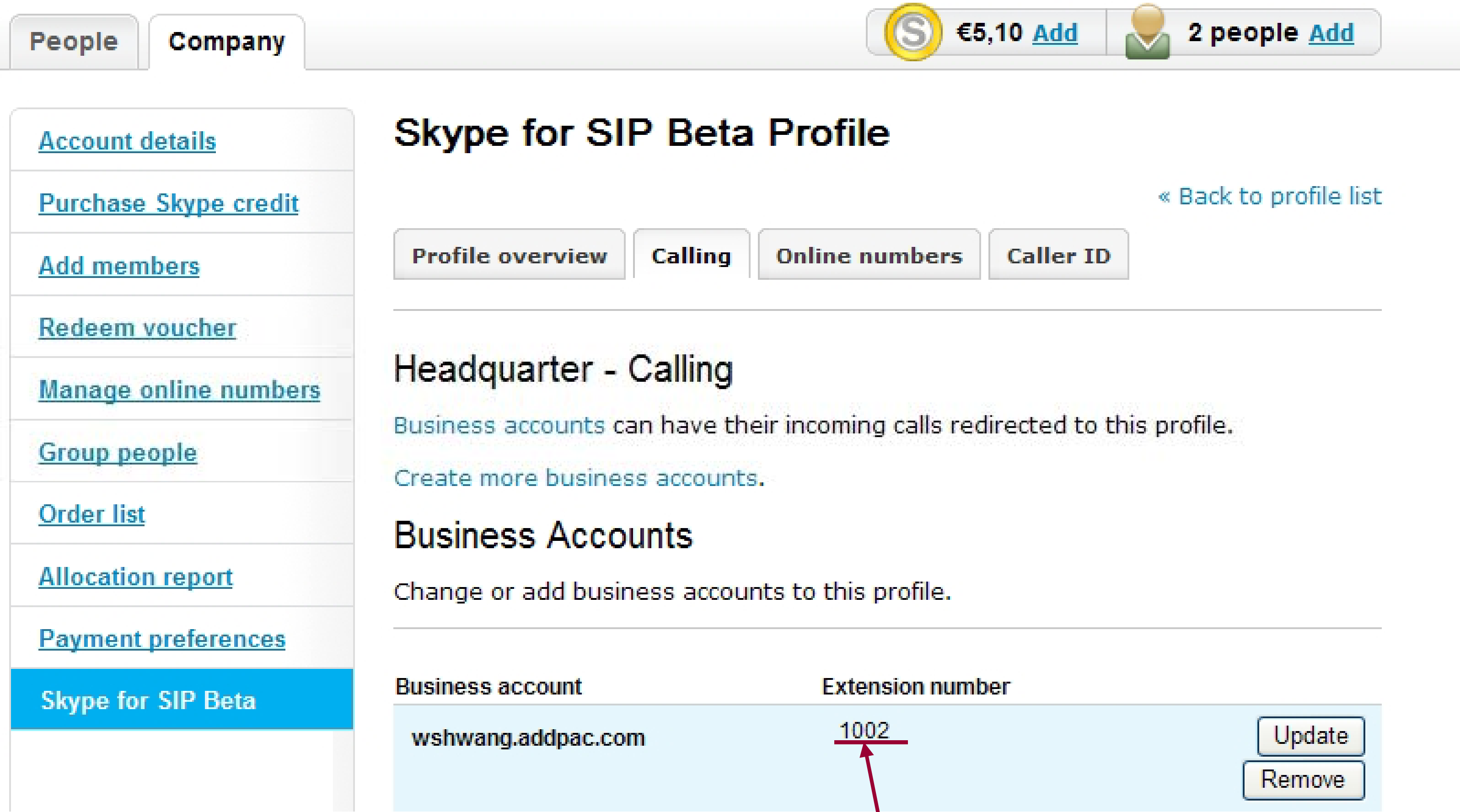
Manage online numbers



Assign the online-number for receiving a PSTN or VoIP call.

Skype Configuration for IP-PBX or G/W (3/3)

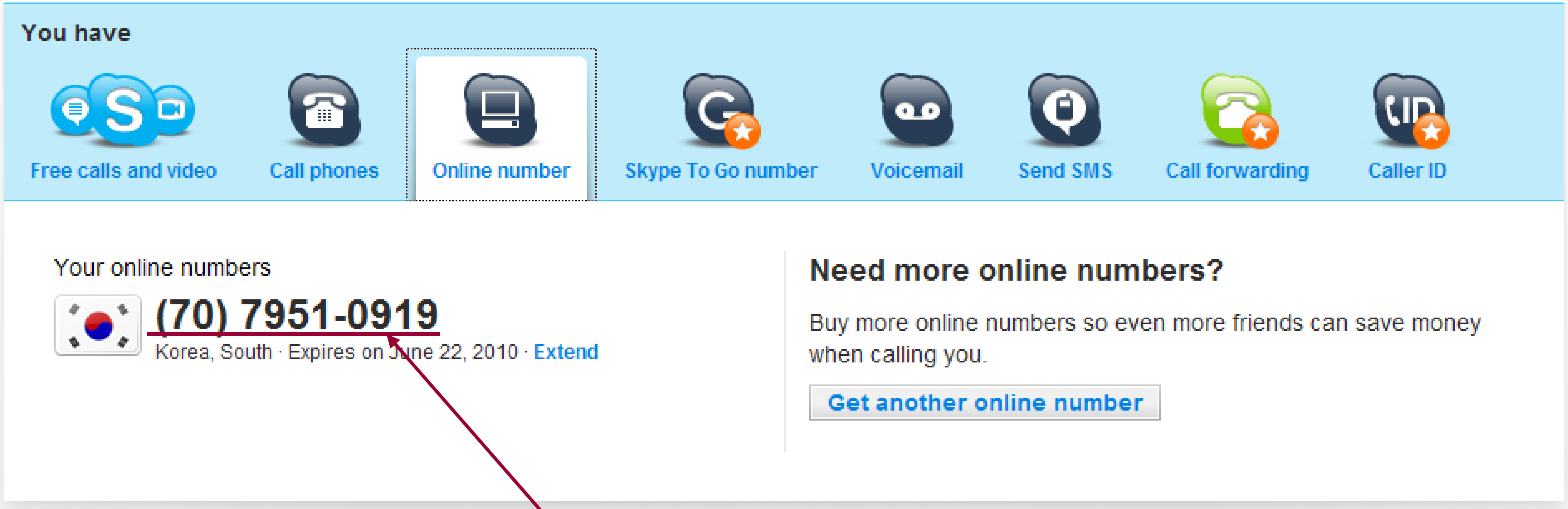
Configure Extension Line



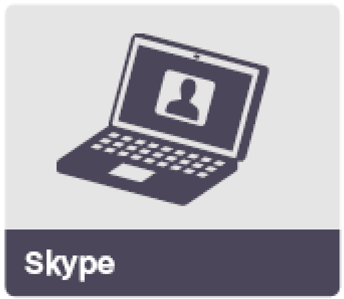
Assign the extension line number for receiving a PSTN or VoIP call.

Configuration for Skype Application

Online number for Skype Application



Assign the online-number for receiving a PSTN or VoIP call.



AddPac VoIP Gateway Configuration

AddPac G/W configuration

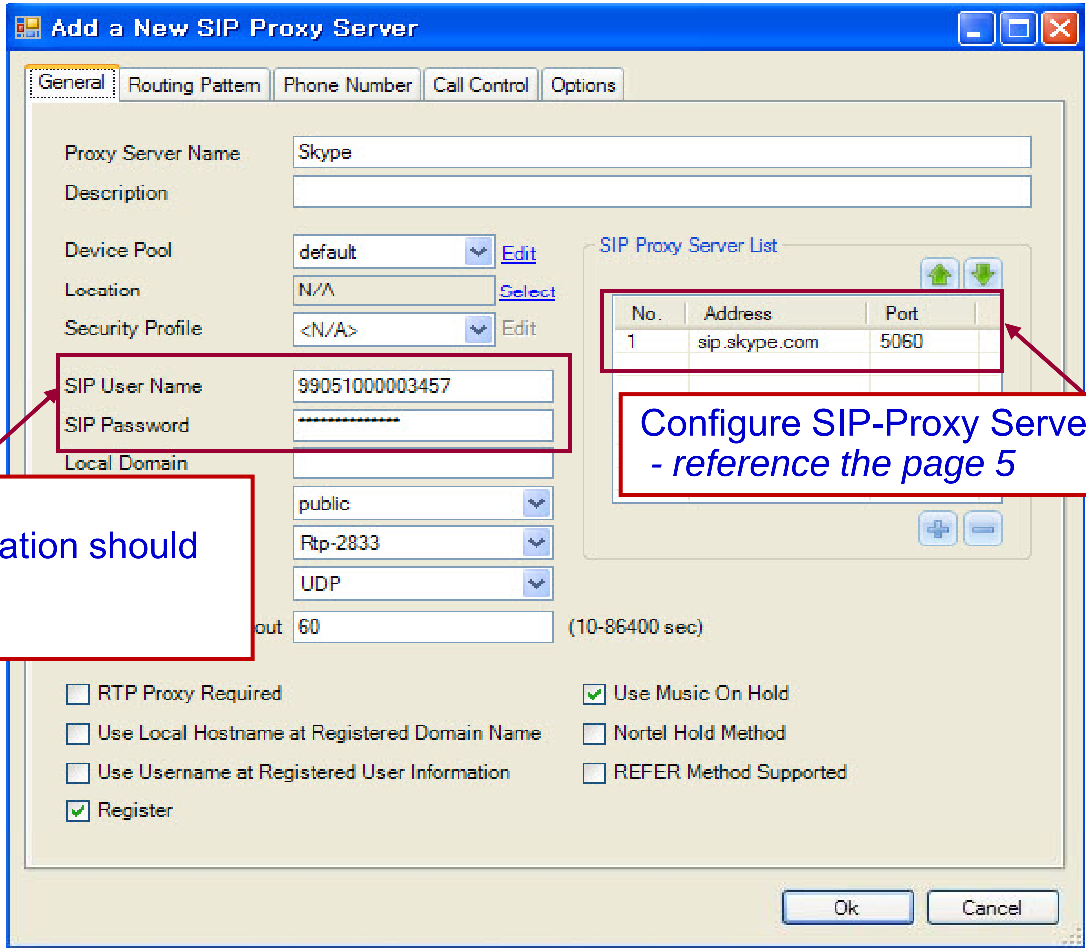
```
dial-peer voice 0 pots
 destination-pattern 827078931524
 port 0/0
 no register e164
 user-name 99051000003457
 user-password e8kVVTU2Jxxxxx
!
dial-peer voice 1 pots
 destination-pattern 99051000003457
 port 0/0
 user-password e8kVVTU2Jxxxxx

sip-ua
 sip-server sip.skype.com
 called-party-number to-field
```

Configure online-number for receiving a call.
Also, The authentication information should be configured.
- reference page 4-5

The authentication information should be configured for REGISTRATION.
- reference page 5

Configure SIP-Proxy Server information.
The option(called-party-number) should be configured for extracting called-number from 'To filed'.
- reference page 5

Skype Proxy Server Configuration



Configure SIP-Proxy Server information.
- *reference the page 5*

The authentication information should be configured.
- *reference the page 4*

AddPac IP-PBX Configuration(2/4)

Translation Rule Configuration

Number Translation Rule

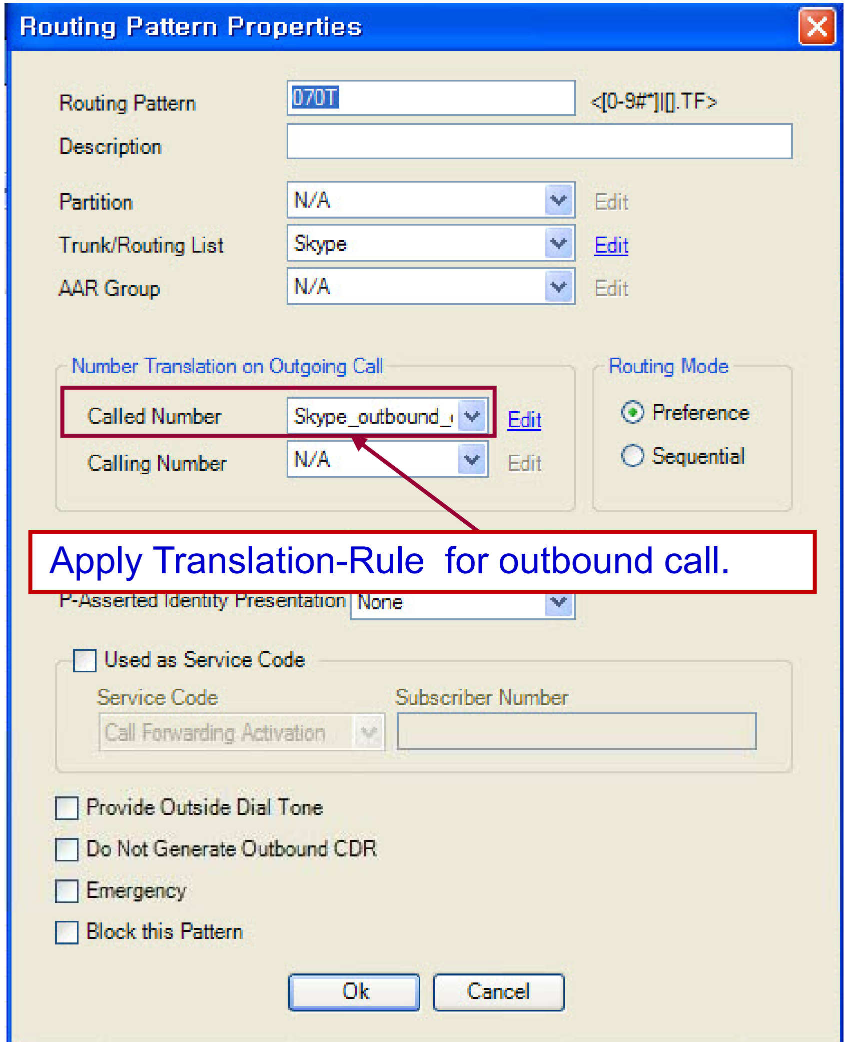
No	Number Translation Rul	Input Matched Pattern	Substituted Pattern	Description
1	외부발신_called	9T 8T 53T 54T 55T 56T 57T	%02%99 %02%99 %03%99 %03%99 %03%99 %03%99 %03%99	
2	Skype_outbound_called	070T	82%02%99	
3	Skype_inbound_called	8270T	0%03%99	

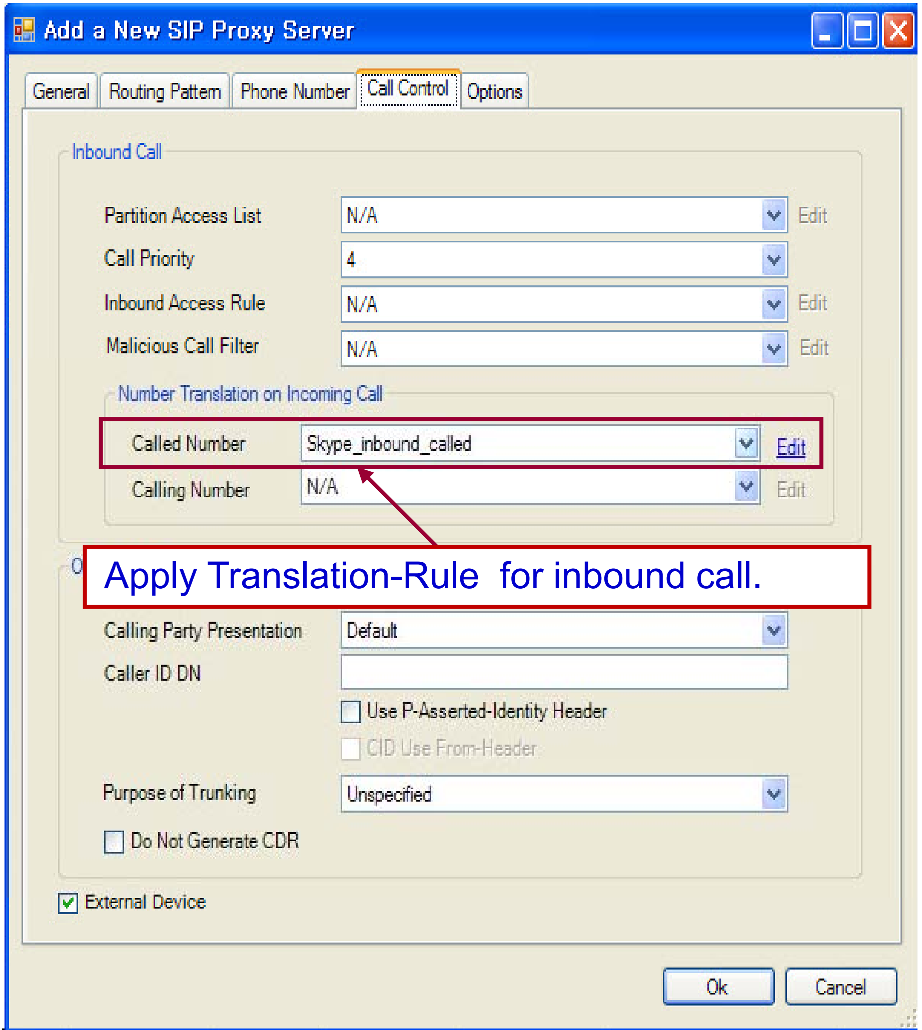
Configure Translation-Rules for inbound and outbound call.

For the outbound call starting with '070', Eliminate one digit, and then insert '82' digits.
(ex: called-number 070-8888-9999 → 8270-8888-9999)
For the inbound call starting with '8270', Eliminate two digits, and then insert '0' digit.
(ex: called-number 8270-8888-9999 → 070-8888-9999)

AddPac IP-PBX Configuration(3/4)

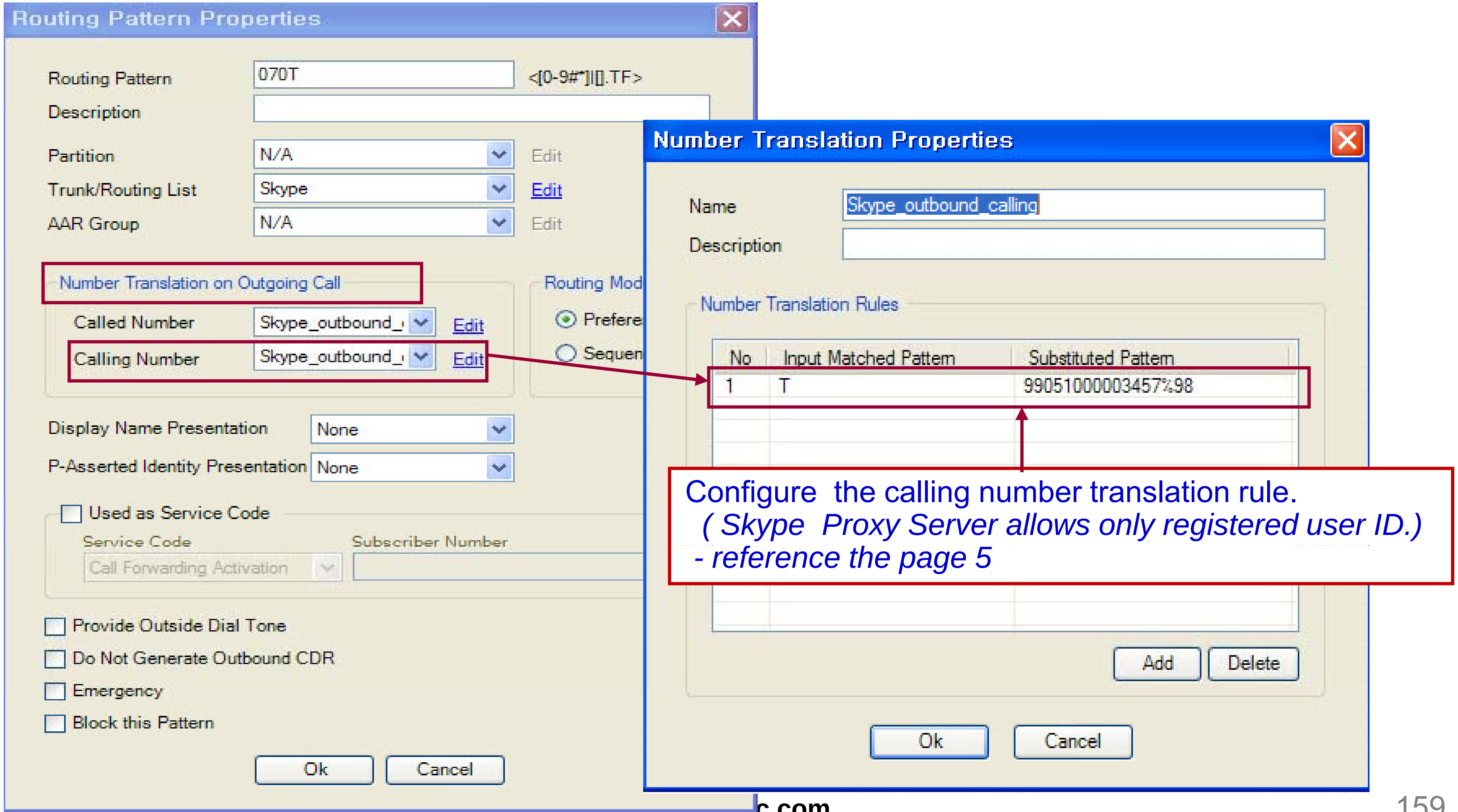
Apply Translation Rule



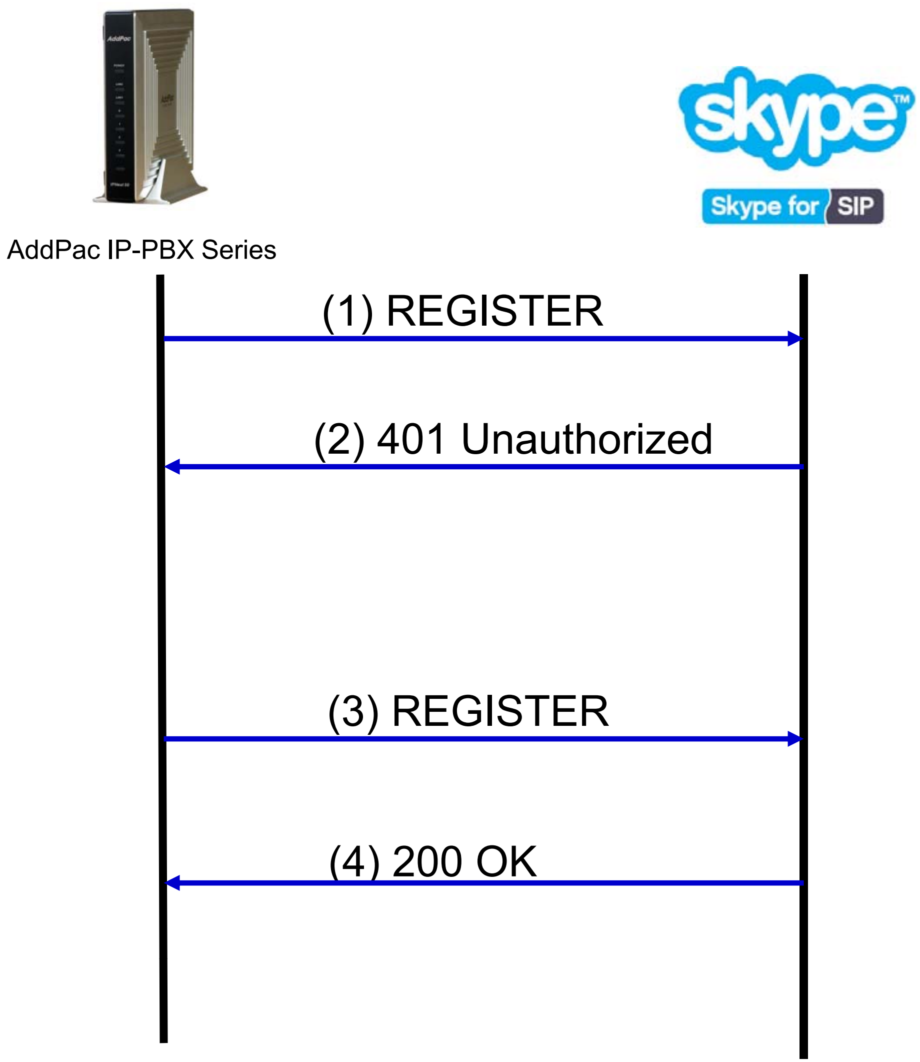


AddPac IP-PBX Configuration(4/4)

Configure Routing Pattern



SIP REGISTER (1/3)



SIP REGISTER (2/3)

(1) REGISTER

```
⊟ Request-Line: REGISTER sip:sip.skype.com SIP/2.0
    Method: REGISTER
    [Resent Packet: False]
⊟ Message Header
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK494b7346a41
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=494b7346a4
  ⊞ To: sip:99051000003457@sip.skype.com
    Call-ID: 495fb04b-9947-7314-8046-0002a4ff4869@60.196.6.77
    CSeq: 1 REGISTER
    Date: Mon, 29 Mar 2010 17:05:29 GMT
    User-Agent: AddPac SIP Gateway
  ⊞ Contact: <sip:99051000003457@60.196.6.77>;expires=60
    Expires: 60
    Content-Length: 0
    Max-Forwards: 70
```

SIP user is inserted to From-Field.
- reference the page 5

(2) 401 Unauthorized

```
⊟ Status-Line: SIP/2.0 401 Unauthorized
    Status-Code: 401
    [Resent Packet: False]
⊟ Message Header
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=494b7346a4
  ⊞ To: <sip:99051000003457@sip.skype.com>;tag=05aed4eb43523e287156e2da6464d890.fe30
    Call-ID: 495fb04b-9947-7314-8046-0002a4ff4869@60.196.6.77
    CSeq: 1 REGISTER
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK494b7346a41
    WWW-Authenticate: Digest realm="sip.skype.com", nonce="4bb05f6b000128eb7223ee8f101719a27202e08df27d98d7", algorithm=MD5
    Server: OpenSIPS
    Content-Length: 0
```

SIP REGISTER (3/3)

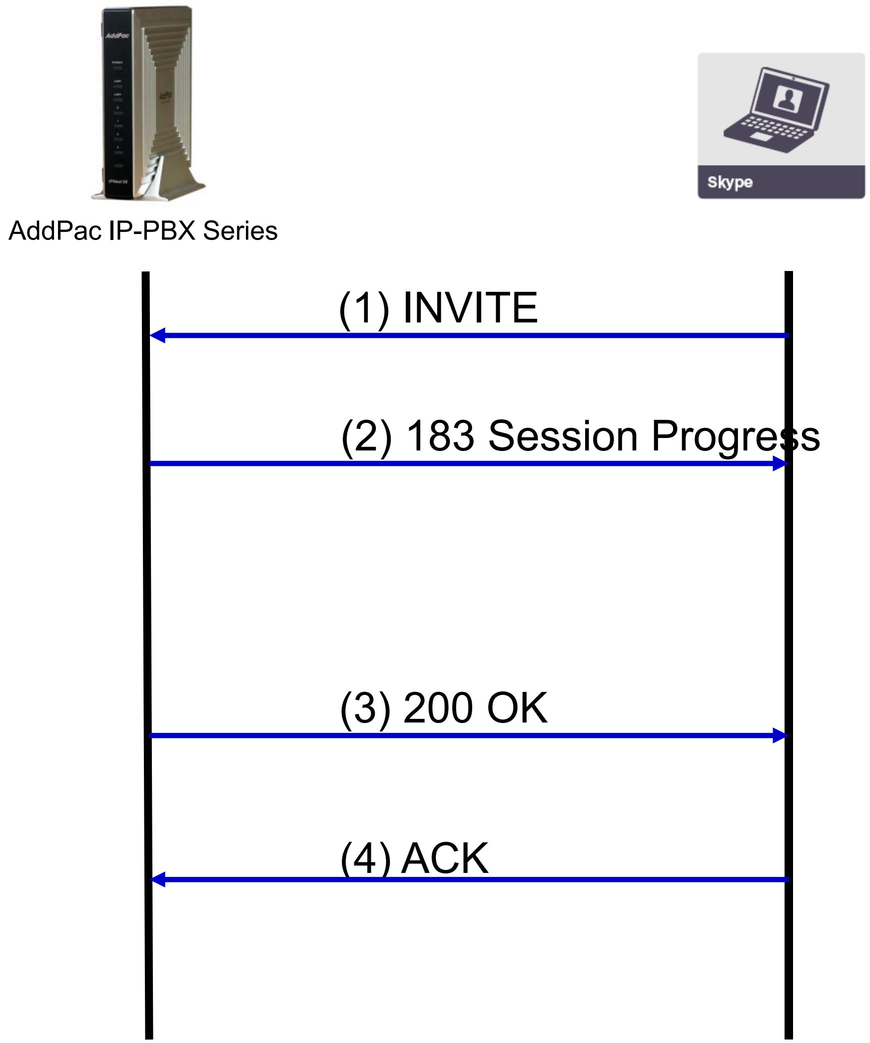
(3) REGISTER

```
⊟ Request-Line: REGISTER sip:sip.skype.com SIP/2.0
    Method: REGISTER
    [Resent Packet: False]
⊟ Message Header
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK494b7346a42
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=494b7346a4
  ⊞ To: sip:99051000003457@sip.skype.com
    Call-ID: 495fb04b-9947-7314-8046-0002a4ff4869@60.196.6.77
    CSeq: 2 REGISTER
    Date: Mon, 29 Mar 2010 17:05:29 GMT
    User-Agent: AddPac SIP Gateway
    Authorization: Digest username="99051000003457", realm="sip.skype.com", nonce="4bb05f6b000128eb7223ee8f101719a27202e08df27d98d7", uri="sip:sip.skype.com", response="9e7434a787cdef395518b
  ⊞ Contact: <sip:99051000003457@60.196.6.77>;expires=60
    Expires: 60
    Content-Length: 0
    Max-Forwards: 70
```

(4) 200 OK

```
⊟ Status-Line: SIP/2.0 200 OK
    Status-Code: 200
    [Resent Packet: False]
⊟ Message Header
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=494b7346a4
  ⊞ To: <sip:99051000003457@sip.skype.com>;tag=05aed4eb43523e287156e2da6464d890.d621
    Call-ID: 495fb04b-9947-7314-8046-0002a4ff4869@60.196.6.77
    CSeq: 2 REGISTER
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK494b7346a42
  ⊞ Contact: <sip:99051000003457@60.196.6.77>;expires=60
    Server: OpenSIPS
    Expires: 60
    Content-Length: 0
```

Inbound Call from Skype (1/5)



Inbound Call from Skype (2/5)

(1) INVITE

```
⊞ Request-Line: INVITE sip:99051000003457@60.196.6.77 SIP/2.0
⊟ Message Header
  ⊞ From: <sip:Anonymous@sip.skype.com>;tag=a4a109cc-13c4-4bb0601c-2729e3f7-36880b6f
  ⊞ To: <sip:827078931524@sip.skype.com>
    Call-ID: CXC-59-6942a370-a4a109cc-13c4-4bb0601c-2729e3f7-2afee549
    CSeq: 1 INVITE
    Via: SIP/2.0/UDP 204.9.161.164:5060;branch=z9hG4bK-287ea-4bb0601c-2729e3f7-3242e07c
    Max-Forwards: 12
    User-Agent: sipgw-1.0
    Privacy: id
    P-Asserted-Identity: <sip:Anonymous@sip.skype.com>
    Remote-Party-ID: <sip:Anonymous@sip.skype.com>;party=calling;screen=yes;privacy=full
    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE
  ⊞ Contact: <sip:Anonymous@204.9.161.164:5060;transport=udp>
    Content-Type: application/sdp
    Content-Length: 263
⊟ Message body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): Anonymous 1269850140 1269850140 IN IP4 204.9.161.164
      Session Name (s): Skype call
    ⊞ Connection Information (c): IN IP4 204.9.161.164
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 28924 RTP/AVP 18 0 8 101
    ⊞ Media Attribute (a): rtpmap:18 G729/8000
    ⊞ Media Attribute (a): rtpmap:0 PCMU/8000
    ⊞ Media Attribute (a): rtpmap:8 PCMA/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:18 annexb=no
```

Inbound Call from Skype (3/5)

(2) 183 Session Progress

```
⊞ Status-Line: SIP/2.0 183 Session Progress
⊟ Message Header
    Via: SIP/2.0/UDP 204.9.161.164:5060;branch=z9hG4bK-287ea-4bb0601c-2729e3f7-3242e07c
  ⊞ From: <sip:Anonymous@sip.skype.com>;tag=a4a109cc-13c4-4bb0601c-2729e3f7-36880b6f
  ⊞ To: <sip:827078931524@sip.skype.com>;tag=194b5b49a4
    Call-ID: CXC-59-6942a370-a4a109cc-13c4-4bb0601c-2729e3f7-2afee549
    CSeq: 1 INVITE
    User-Agent: AddPac SIP Gateway
  ⊞ Contact: <sip:99051000003457@60.196.6.77>
    Content-Type: application/sdp
    Content-Length: 177
⊟ Message body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): addpac 1269850137 1269850137 IN IP4 60.196.6.77
      Session Name (s): AddPac Gateway SDP
    ⊞ Connection Information (c): IN IP4 60.196.6.77
    ⊞ Time Description, active time (t): 1269850137 0
      Session Attribute (a): sendonly
    ⊞ Media Description, name and address (m): audio 26128 RTP/AVP 18
    ⊞ Media Attribute (a): rtpmap:18 G729/8000
```

Inbound Call from Skype (4/5)

(3) 200 OK

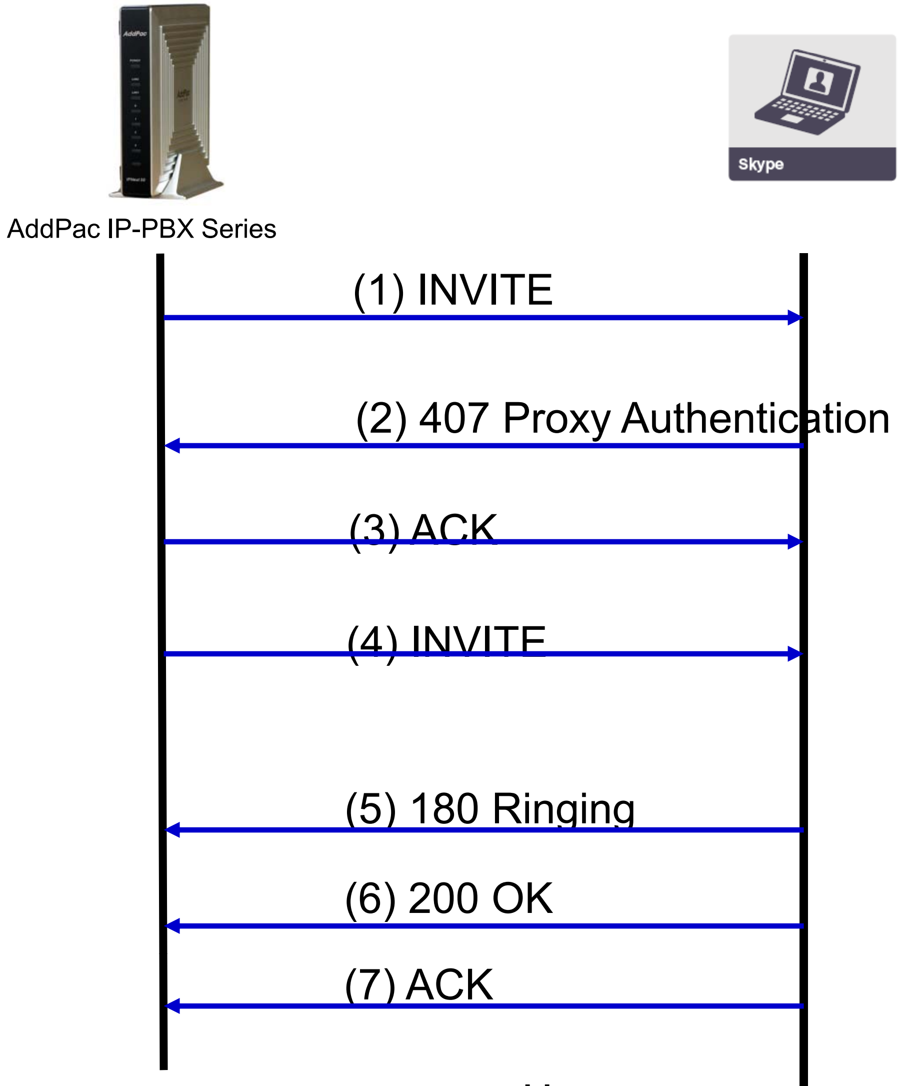
```
⊞ Status-Line: SIP/2.0 200 OK
⊟ Message Header
    Via: SIP/2.0/UDP 204.9.161.164:5060;branch=z9hG4bK-287ea-4bb0601c-2729e3f7-3242e07c
  ⊞ From: <sip:Anonymous@sip.skype.com>;tag=a4a109cc-13c4-4bb0601c-2729e3f7-36880b6f
  ⊞ To: <sip:827078931524@sip.skype.com>;tag=194b5b49a4
    Call-ID: CXC-59-6942a370-a4a109cc-13c4-4bb0601c-2729e3f7-2afee549
    CSeq: 1 INVITE
    User-Agent: AddPac SIP Gateway
  ⊞ Contact: <sip:99051000003457@60.196.6.77>
    Content-Type: application/sdp
    Content-Length: 248
⊟ Message body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): 07078931524 1269882543 1269882543 IN IP4 172.17.111.211
      Session Name (s): AddPac Gateway SDP
    ⊞ Connection Information (c): IN IP4 172.17.111.211
    ⊞ Time Description, active time (t): 1269882543 0
    ⊞ Media Description, name and address (m): audio 23106 RTP/AVP 18 101
    ⊞ Media Attribute (a): ptime:20
    ⊞ Media Attribute (a): rtpmap:18 G729/8000/1
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000/1
    ⊞ Media Attribute (a): fmtp:101 0-15
```

Inbound Call from Skype (5/5)

(4) ACK

```
⊞ Request-Line: ACK sip:99051000003457@60.196.6.77 SIP/2.0
⊟ Message Header
  ⊞ From: <sip:Anonymous@sip.skype.com>;tag=a4a109cc-13c4-4bb0601c-2729e3f7-36880b6f
  ⊞ To: <sip:827078931524@sip.skype.com>;tag=194b5b49a4
    Call-ID: CXC-59-6942a370-a4a109cc-13c4-4bb0601c-2729e3f7-2afee549
    CSeq: 1 ACK
    Via: SIP/2.0/UDP 204.9.161.164:5060;branch=z9hG4bK-287eb-4bb0601f-2729ee10-66a221b2
    Max-Forwards: 70
    P-Asserted-Identity: <sip:Anonymous@sip.skype.com>
  ⊞ Contact: <sip:Anonymous@204.9.161.164:5060;transport=udp>
    Content-Length: 0
```

Outbound Call from IP-PBX (1/7)



Outbound Call from IP-PBX (2/7)

(1) INVITE

```
⊞ Request-Line: INVITE sip:827079510919@sip.skype.com SIP/2.0
⊟ Message Header
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK964b554ca484
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=964b554ca4
  ⊞ To: <sip:827079510919@sip.skype.com>
    Call-ID: 9666b04b-146c-556e-804c-0002a4ff4869@60.196.6.77
    CSeq: 84 INVITE
    Supported: timer, 100rel
    Min-SE: 1800
    Date: Mon, 29 Mar 2010 17:36:38 GMT
    Session-Expires: 1800
    User-Agent: AddPac IP-PBX
  ⊞ Contact: <sip:99051000003457@60.196.6.77>
    Accept: application/sdp
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE, PRACK, REFER, NOTIFY, INFO
    Content-Type: application/sdp
    Content-Length: 449
    Max-Forwards: 69
⊟ Message body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): 99051000003457 1269884196 1269884196 IN IP4 172.17.101.240
      Session Name (s): AddPac Gateway SDP
    ⊞ Connection Information (c): IN IP4 172.17.101.240
    ⊞ Time Description, active time (t): 1269884196 0
    ⊞ Media Description, name and address (m): audio 23394 RTP/SAVP 18 101
    ⊞ Media Attribute (a): ptime:20
    ⊞ Media Attribute (a): crypto:1 AES_CM_128_HMAC_SHA1_80 inline:WzF4/tpRiWLdXEzcioXzodDOOffSwJXMzmE7wrAX
    ⊞ Media Attribute (a): rtpmap:18 G729/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:101 0-15
    ⊞ Media Description, name and address (m): audio 23394 RTP/AVP 18 101
    ⊞ Media Attribute (a): ptime:20
    ⊞ Media Attribute (a): rtpmap:18 G729/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:101 0-15
```

Outbound Call from IP-PBX (3/7)

(2) 407 Proxy Authentication

```
⊞ Status-Line: SIP/2.0 407 Proxy Authentication Required
⊟ Message Header
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=964b554ca4
  ⊞ To: <sip:827079510919@sip.skype.com>;tag=a4a109cc-13c4-4bb0669a-27433f01-4d79c76
    Call-ID: 9666b04b-146c-556e-804c-0002a4ff4869@60.196.6.77
    CSeq: 84 INVITE
    Proxy-Authenticate: Digest realm="sip.skype.com", nonce="4bb066b80001781bc891b9609d299d2022c6c16fb79e8c19", algorithm=MD5
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK964b554ca484
    Content-Length: 0
```

Outbound Call from IP-PBX (4/7)

(3) ACK

```
⊞ Request-Line: ACK sip:827079510919@sip.skype.com SIP/2.0
⊟ Message Header
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK964b554ca484
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=964b554ca4
  ⊞ To: <sip:827079510919@sip.skype.com>;tag=a4a109cc-13c4-4bb0669a-27433f01-4d79c76
    Call-ID: 9666b04b-146c-556e-804c-0002a4ff4869@60.196.6.77
    CSeq: 84 ACK
    Content-Length: 0
    Max-Forwards: 70
```

Outbound Call from IP-PBX (5/7)

(4) INVITE

```
⊞ Request-Line: INVITE sip:827079510919@sip.skype.com;transport=udp;maddr=204.9.161.164 SIP/2.0
⊟ Message Header
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK964b554ca485
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=964b554ca4
  ⊞ To: <sip:827079510919@sip.skype.com>
    Call-ID: 9666b04b-146c-556e-804c-0002a4ff4869@60.196.6.77
    CSeq: 85 INVITE
    Supported: replaces, timer, 100rel, early-session
    Min-SE: 1800
    Date: Mon, 29 Mar 2010 17:36:38 GMT
    Session-Expires: 1800
    User-Agent: AddPac SIP Gateway
  ⊞ Contact: <sip:99051000003457@60.196.6.77>
    Accept: application/sdp
    Proxy-Authorization: Digest username="99051000003457", realm="sip.skype.com", nonce="4bb066b80001781bc891b9609d299d2022c6c16fb79e8c19",
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, UPDATE, PRACK, REFER, NOTIFY, INFO
    Content-Type: application/sdp
    Content-Length: 449
    Max-Forwards: 70
⊟ Message body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): 99051000003457 1269884196 1269884196 IN IP4 172.17.101.240
      Session Name (s): AddPac Gateway SDP
    ⊞ Connection Information (c): IN IP4 172.17.101.240
    ⊞ Time Description, active time (t): 1269884196 0
    ⊞ Media Description, name and address (m): audio 23394 RTP/SAVP 18 101
    ⊞ Media Attribute (a): ptime:20
    ⊞ Media Attribute (a): crypto:1 AES_CM_128_HMAC_SHA1_80 inline:WzF4/tpRiWLdXEzcioXzodDOOffSwJXMzmE7wrAX
    ⊞ Media Attribute (a): rtpmap:18 G729/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:101 0-15
    ⊞ Media Description, name and address (m): audio 23394 RTP/AVP 18 101
    ⊞ Media Attribute (a): ptime:20
    ⊞ Media Attribute (a): rtpmap:18 G729/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:101 0-15
```

Outbound Call from IP-PBX (6/7)

(5) 180 Ringing

```
⊞ Status-Line: SIP/2.0 180 Ringing
⊟ Message Header
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=964b554ca4
  ⊞ To: <sip:827079510919@sip.skype.com>;tag=a4a109cc-13c4-4bb0669a-27433f01-4d79c76
    Call-ID: 9666b04b-146c-556e-804c-0002a4ff4869@60.196.6.77
    CSeq: 85 INVITE
    User-Agent: sipgw-1.0
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK964b554ca485
  ⊞ Contact: <sip:827079510919@sip.skype.com:5060;maddr=204.9.161.164;transport=udp>
    Content-Length: 0
```

Outbound Call from IP-PBX (7/7)

(6) 200 OK

```
⊞ Status-Line: SIP/2.0 200 OK
⊟ Message Header
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=964b554ca4
  ⊞ To: <sip:827079510919@sip.skype.com>;tag=a4a109cc-13c4-4bb0669a-27433f01-4d79c76
    Call-ID: 9666b04b-146c-556e-804c-0002a4ff4869@60.196.6.77
    CSeq: 85 INVITE
    Allow: INVITE,ACK,CANCEL,OPTIONS,BYE
    User-Agent: sipgw-1.0
    Via: SIP/2.0/UDP 60.196.6.77:5060;branch=z9hG4bK964b554ca485
  ⊞ Contact: <sip:827079510919@sip.skype.com:5060;maddr=204.9.161.164;transport=udp>
    Content-Type: application/sdp
    Content-Length: 220
⊟ Message body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): 99051000003457 1269884196 1269884196 IN IP4 204.9.161.164
      Session Name (s): Skype call
    ⊞ Connection Information (c): IN IP4 204.9.161.164
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 24068 RTP/AVP 18 101
    ⊞ Media Attribute (a): rtpmap:18 G729/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:18 annexb=no
```

(7) ACK

```
⊞ Request-Line: ACK sip:827079510919@sip.skype.com;transport=udp;maddr=204.9.161.164 SIP/2.0
⊟ Message Header
    Via: SIP/2.0/UDP 60.196.6.77;branch=z9hG4bK964b554ca485
  ⊞ From: <sip:99051000003457@sip.skype.com>;tag=964b554ca4
  ⊞ To: <sip:827079510919@sip.skype.com>;tag=a4a109cc-13c4-4bb0669a-27433f01-4d79c76
    Call-ID: 9666b04b-146c-556e-804c-0002a4ff4869@60.196.6.77
    CSeq: 85 ACK
    Content-Length: 0
    Max-Forwards: 70
```

Unwanted Call Blocking Service Features
(Hacking Call, Illegal Call, etc)

Contents

- Overview
- Unwanted Call Blocking Service for VoIP Gateway, IP-PBX
  - Blocking of Call Generated from unregistered IP address
  - Unregistered Calling Number's PSTN Routing Blocking
  - PSTN Routing Blocking by using Called Number digit pattern.
- DDoS Attack Blocking
- ACL(access-list) Function

Overview

- AddPac VoIP Gateway/IP-PBX anti-hacking function, blocking of illegal call, DDoS attack blocking, etc

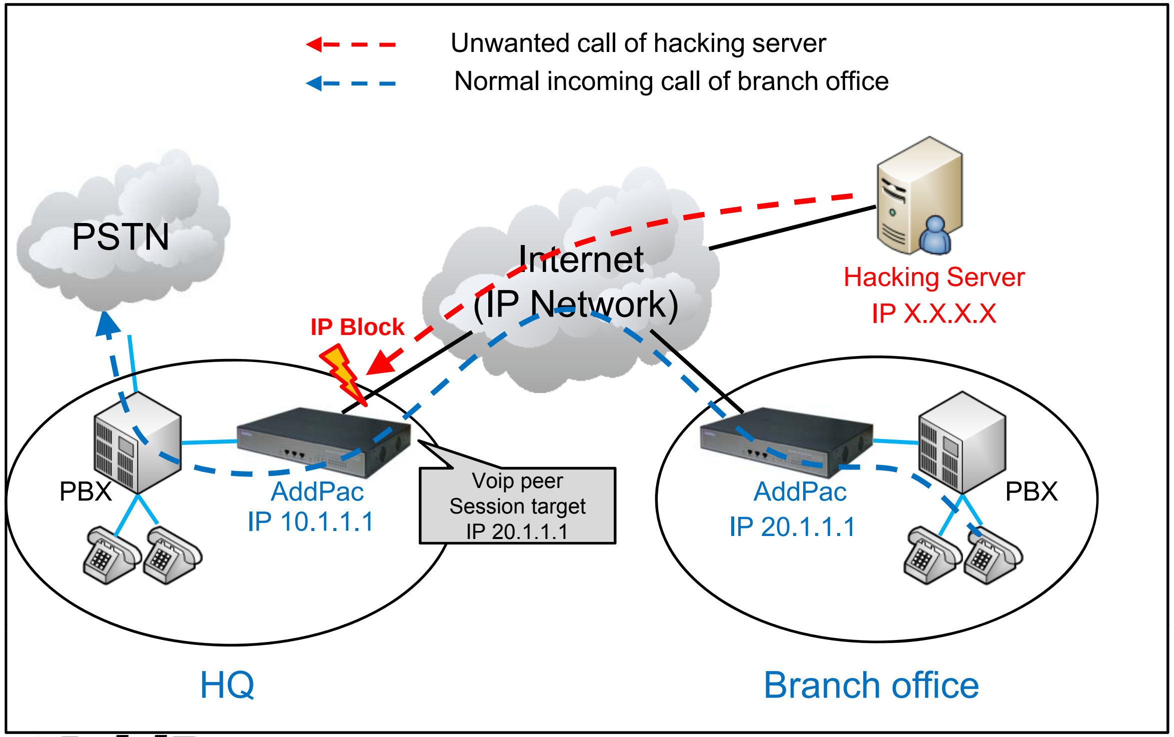
  — Blocking of call generated from unregistered IP address
  — Unregistered Calling Number's PSTN Routing Blocking
  — Unwanted PSTN Routing Call Blocking by using called number digit pattern.
  — DDoS attack blocking by ethernet packet analysis when DDoS attack is occurred.
  This ensures service continuity by blocking related IP for a certain time after continuous DDoS attack and pattern analysis when sending data.
  — Blocking of unwanted packet by setting ACL (access-list)
  Standard & Extended IP Access List

Unwanted Call Blocking Service

- Blocking of call generated from unregistered IP address in VoIP gateway

  -This function does not response when call is incoming, except pre-registered H.323 GateKeeper, SIP server, Head and Branch office IP address.

  - When illegal hacking server try to port scanning, this function prevent VoIP gateway from hacking server by no response SIP or H.323 message, and blocking incoming call from unwanted outside VoIP gateway.



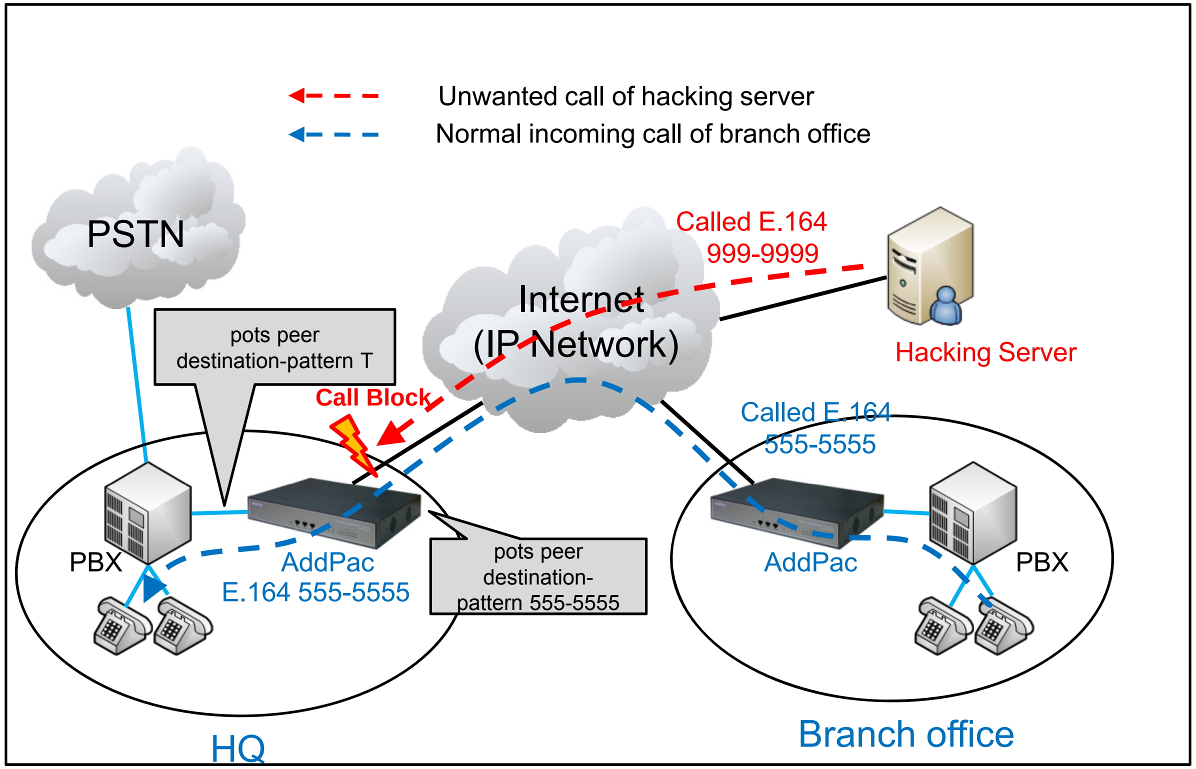
When unregistered IP address blocking scheme is enabled, following operation is occurred.

- Blocking incoming call by discarding H.323 and SIP message except branch office IP registered in HQ VoIP Gateway
- Registered GK and SIP proxy server IP address in VoIP gateway is processed as normal call even if it is not registered IP in Branch office.
- Server address registered by DNS is automatically processed as normal call.

Unwanted Call Blocking Service

- Unregistered calling number's PSTN routing call blocking

  - This function block the incoming call except E.164 registered in VoIP gateway.
    (Block PSTN routing call by ignoring configuration of destination-pattern T)
  - Regardless of E.164 address , incoming call from GK or SIP proxy server is considered normal call.

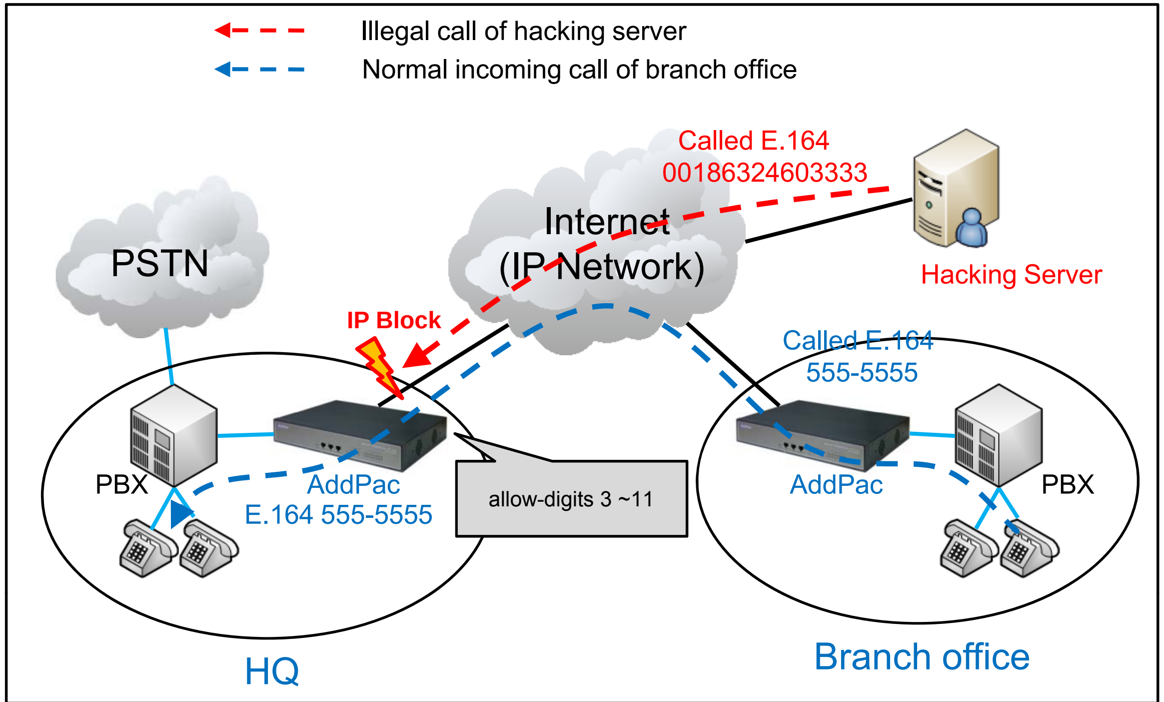


Block of unwanted call by configuring PSTN back-up

- When PSTN line is connected for back-up line in VoIP network design, unwanted hacking call via PSTN line can be occurred.
- Only permit incoming call from phone number registered PBX'S port connected to VoIP gateway.

Unwanted Call Blocking Service

- Unwanted PSTN Routing Call Blocking by using called number digit pattern
  - This function block the call by using E.164 called number digit pattern.
  - For example, international call or long distance call use the E.164 prefix number for numbering plan.
  - By using call routing pattern-match, international or long distance outbound call from VoIP gateway via hacking can be blocked or controlled.



Incoming call blocking by using incoming call E.164 address digit-pattern

- Permit VoIP gateway's incoming call E.164 digit number only from 3 digits to 11digits, and if digit number is under 2 digits or upper 12 digits, this call is blocked.

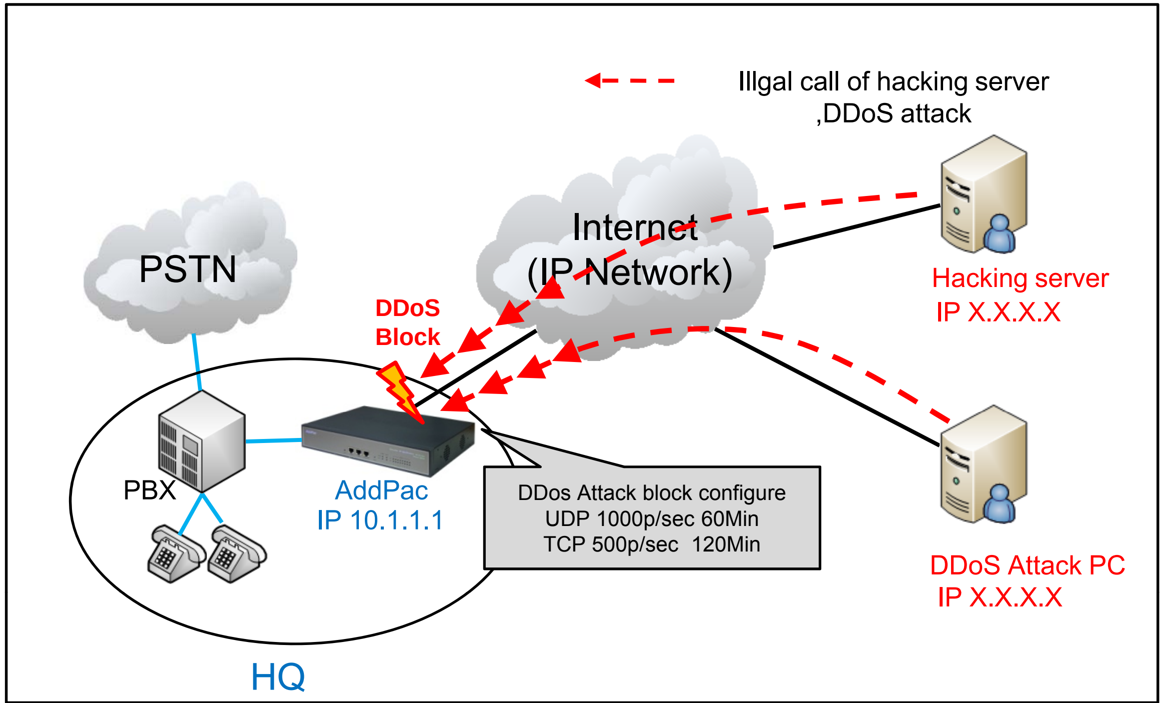
VoIP gateway DDoS Attack Blocking

- DDoS attack blocking function

- If traffic level coming from a unspecific IP address is over threshold, ethernet packet from this IP address is all blocked.

- Providing function of browsing/deleting blocked IP address index in supervisor admin mode.

- Seamless service is possible because this function provides the automatic IP address unblock service in DDoS attack IP address black list after certain time is pass



Detection of DDoS of unspecific IP

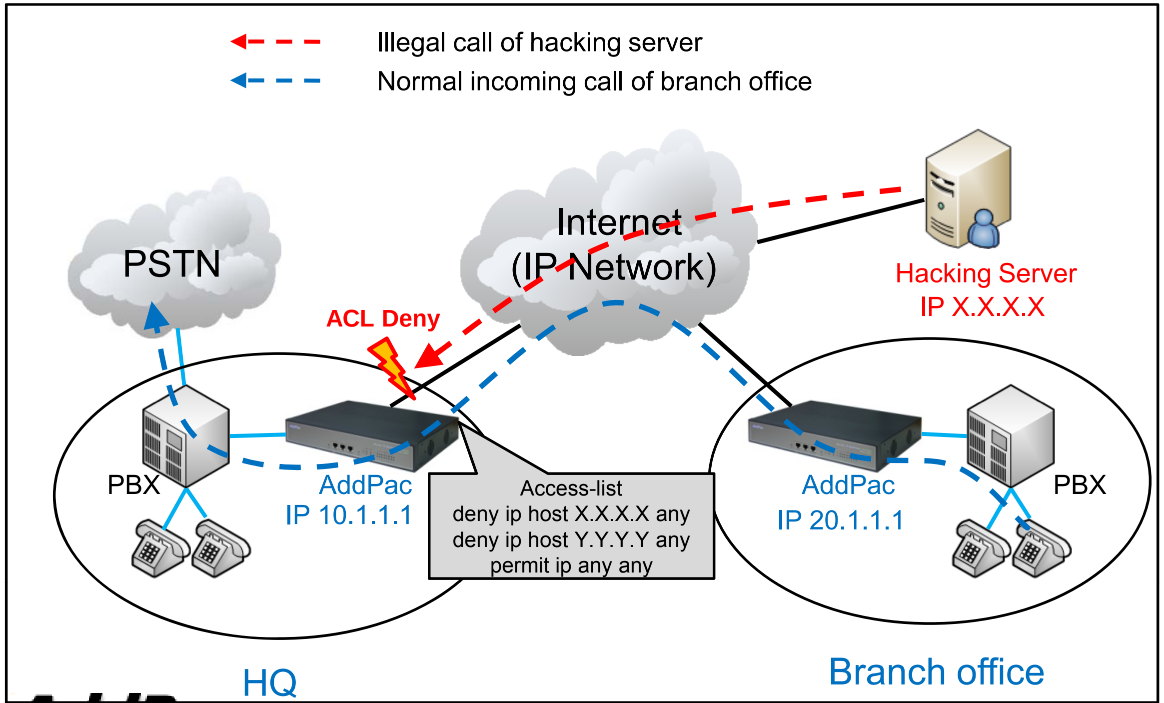
- Monitoring number of packet per time by setting threshold of network protocol(TCP, UDP, ICMP etc.)
- Blocking packet about related IP address when threshold is exceeded.
- This service is only applicable in DDoS attack outside network interface like as internet

Administrating of index of DDoS block

- Configuring each protocol. (configuration of administer)
- Providing automatic IP address unblock service after some time duration by setting block time about blocked IP address list.
- Decreasing device overload using real time DDoS attack monitoring, This help to increase the VoIP gateway performance.

ACL (access-list) Function

- Unwanted call blocking using Access List
  - Preventing VoIP gateway from hacking attack via ethenet packet block/unblock by ACL function.
  - Providing effective call block function by black list in case of specific pattern or consistent IP attack, or by white list in case of complicate packet pattern and unspecific attack.
  - Providing two method s of ALC like Standard Access, Extended Access



Effective call block service using standard, extended ACL

- Standard ACL searches only source IP address, and then block it if source IP address is unregistered.
- Extended ACL searches registered Source, Destination IP and then block it if unregistered.

Digital VoIP Gateway Active-Standby Backup Service using VRRP Protocol

AddPac

Contents

- What is VRRP Protocol?
- VRRP Protocol in VoIP Gateway Service
- Network Diagram
- Sample Configuration using Command Line Interface (CLI)

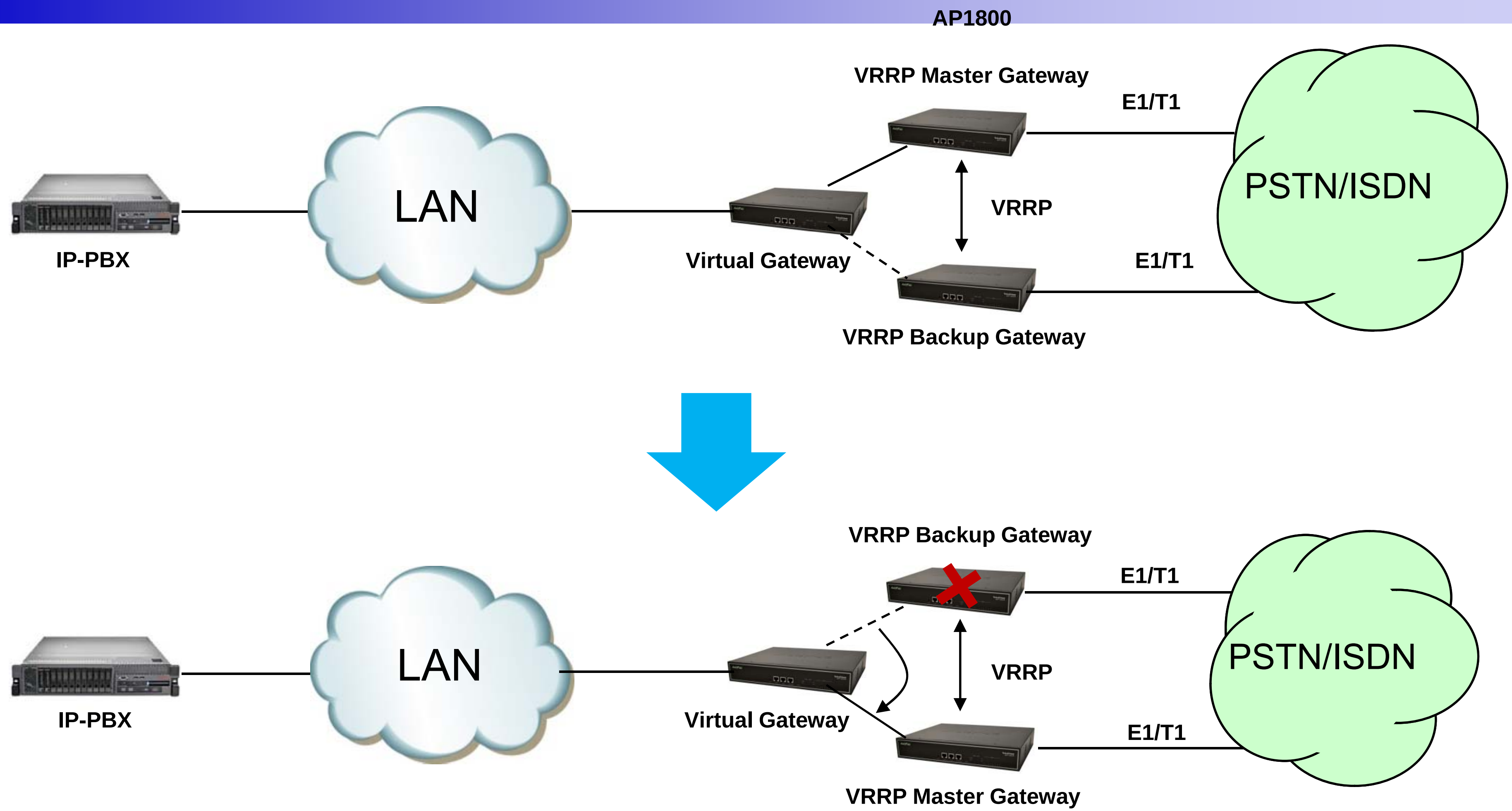
What is VRRP Protocol?

- Virtual Router Redundancy Protocol
- Originally Developed for Router System
- Described in RFC 2338
- Two types of routers; master and backup routers.
- Configure up to 255 virtual routers in a group.
- Master routers have a priority of 255 and backup routers have a priority of 1-254.

VRRP Protocol in VoIP Gateway Service

- High-Availability Solutions for VoIP Service
- Enables a pair of redundant (1+1) gateways on a LAN to negotiate ownership of a virtual IP address. One device is elected to be active and the other to be standby.
- If the active fails, the backup server takes over.

Network Diagram for VRRP



Sample Configuration (CLI)

Master Gateway

```
interface FastEthernet0/0
 ip address 172.16.8.49 255.255.0.0
 speed auto
 vrrp 1 ip 172.16.8.1
```

Backup Gateway

```
interface FastEthernet0/0
 ip address 172.16.8.48 255.255.0.0
 speed auto
 vrrp 1 ip 172.16.8.1
```

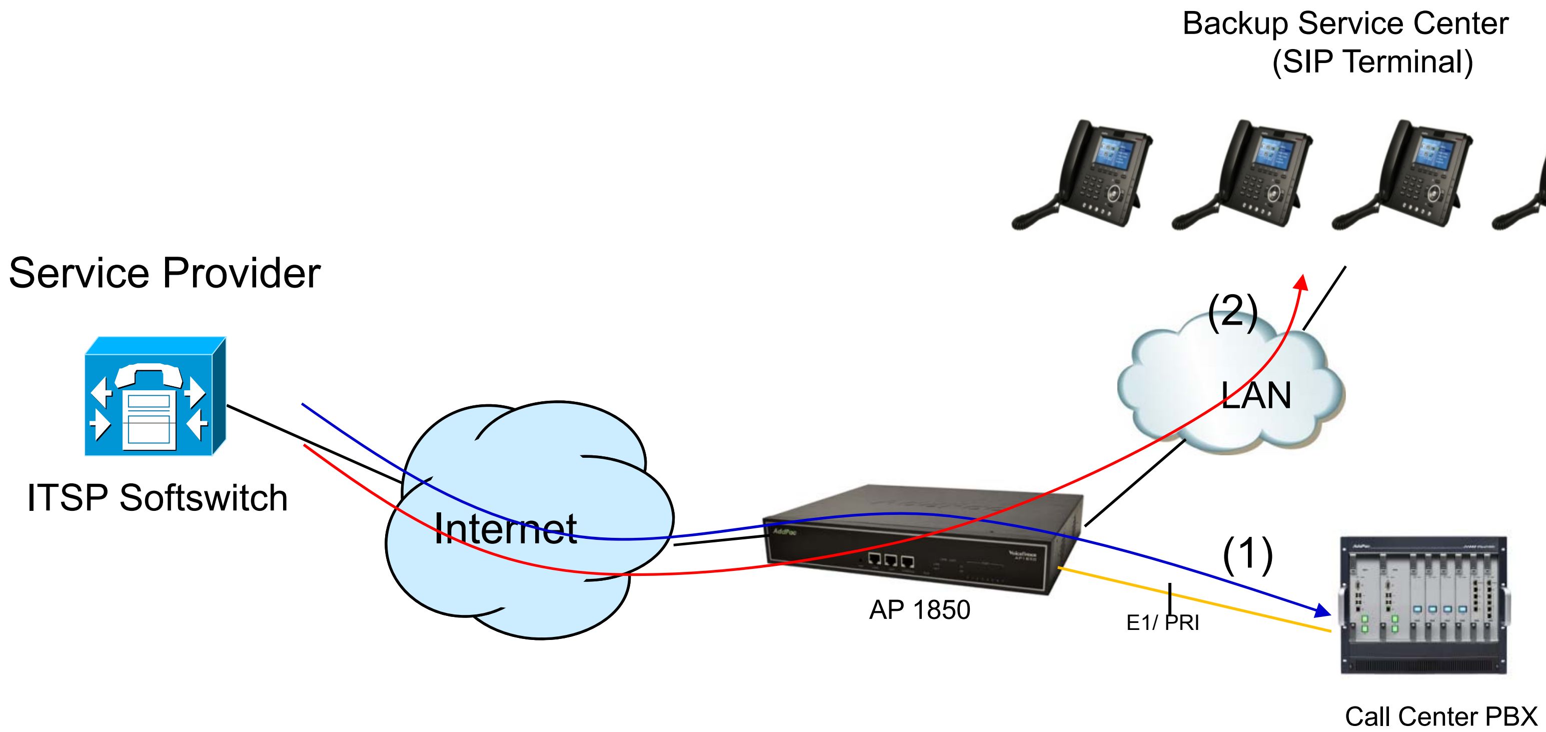
```
Router# show vrrp
FastEthernet0/0 vrid 1 state is Master
    Advertisement Interval: 1 second(s)
    Auth Type: No Authentication (0)
    Priority: 100 (default backup priority)
    Preempt is enabled
    MAC address: use virtual address (0000.5e00.0101)
    IP Address: 172.16.8.1
Router#
```

SIP-to-SIP Call Diversion Service for Digital Link Backup

Contents

- SIP-to-SIP Call Diversion Service Diagram for Digital Link Backup
- Signal Call Flow
- Smart Web Configuration

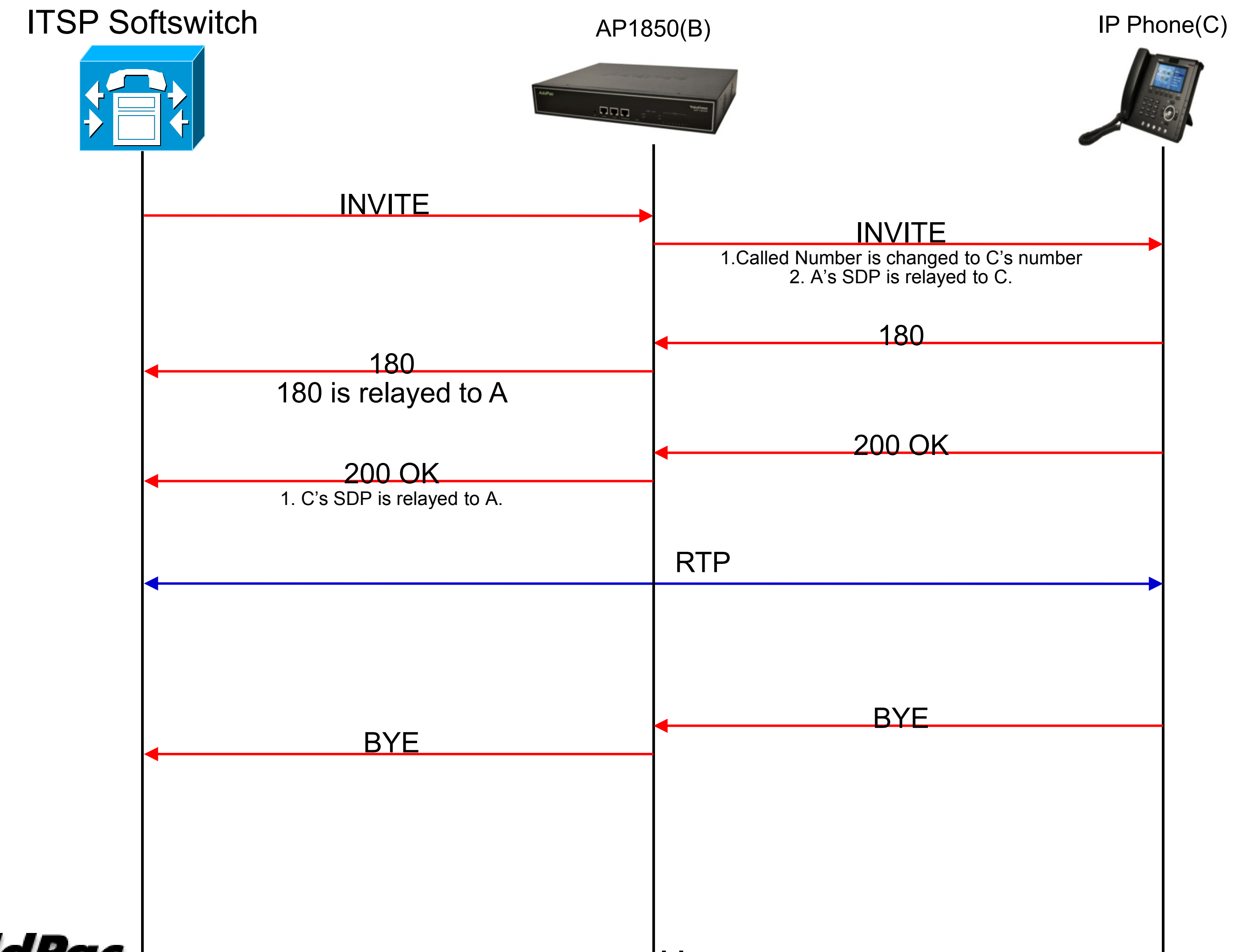
SIP-to-SIP Call Diversion Service for Digital Link Backup



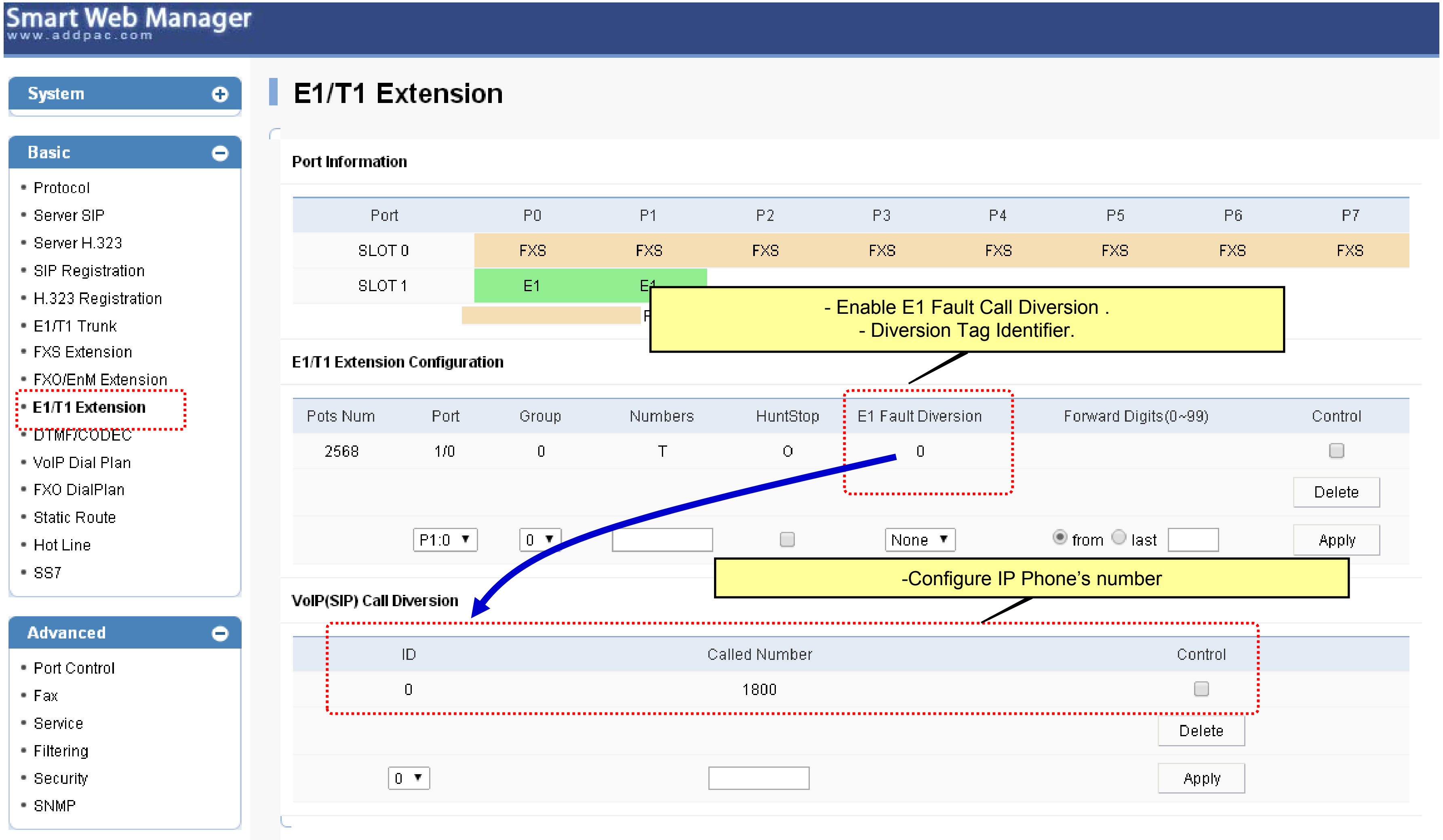
(1) SIP Calls are routed to Call Center PBX via digital line when E1/PRI link is normal state.
(2) SIP Calls are routed to SIP terminal based Backup Service Center when E1/PRI link is down

** All Phones have same numbers and different IP address in Backup service Center.*
** Calls for Backup Service Center are routed by the algorithm(least selected number).*

Signal Call Flow



VoIP(SIP) Call Diversion Configuration(1/2)



VoIP(SIP) Call Diversion Configuration(2/2)

Smart Web Manager
www.addpac.com

- System
- Basic
  - Protocol
  - Server SIP
  - Server H.323
  - SIP Registration
  - H.323 Registration
  - E1/T1 Trunk
  - FXS Extension
  - FXO/EnM Extension
  - E1/T1 Extension
  - DTMF/CODEC
  - VoIP Dial Plan
  - FXO DialPlan
  - **Static Route**
  - Hot Line
  - SS7

Static Route

- IP Phones are configured in 'static route' with same phone number.

Set Remote Site Call(5-digit number is set to begin '2->'2...)

VoIP Num	Remote Site IP	Signaling Port	Prefix	Digits to Insert	Digits to Delete	Name of Remote Site	Answer Addr	Control
10100	172.16.9.10	5060	1800		0	Backup Center	T	
10101	172.16.9.11	5060	1800		0	Backup Center	T	
10102	172.16.9.12	5060	1800		0	Backup Center	T	
10103	172.16.9.13	5060	1800		0	Backup Center	T	
								Delete
*								Apply

* Static Route - Assigned Voip Tag Number : 10100 - 10199
* Static Route - Assigned Translation-Rule Tag Number : 10100 - 10199

Thank you!

AddPac Technology Co., Ltd.

Sales and Marketing

Phone +82.2.568.3848 (KOREA)
FAX +82.2.568.3847 (KOREA)
E-mail sales@addpac.com