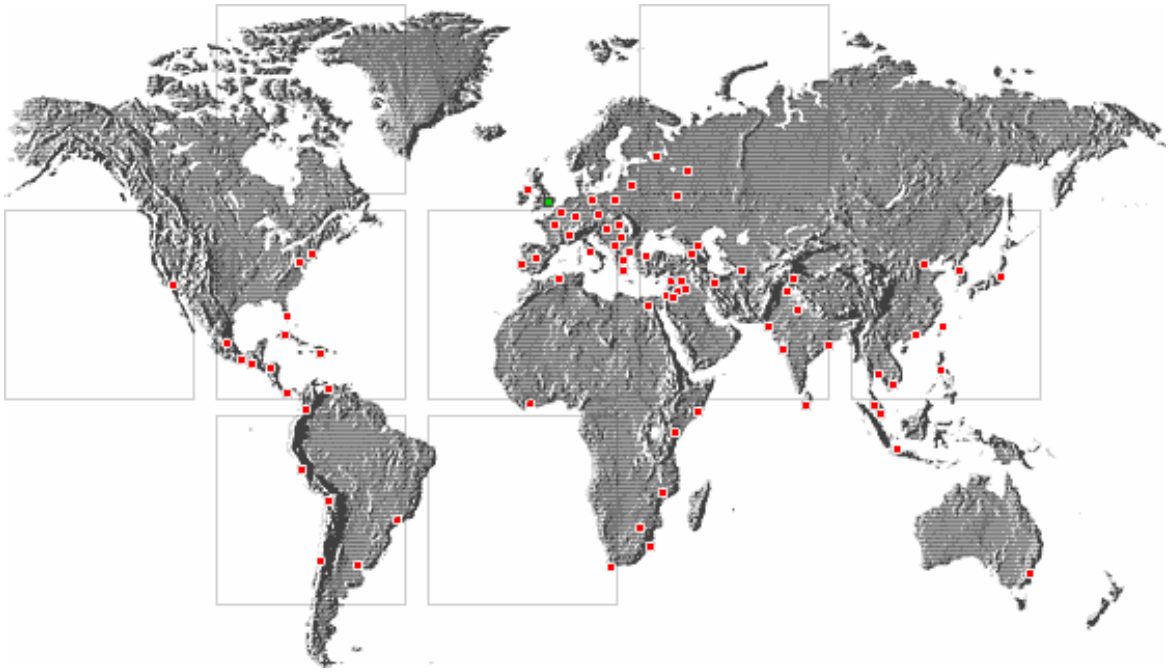
APOS Release Note

Release 8.10 June, 2004



June 2004

AddPac Technology Co., Ltd.
AddPac Technology R&D Center

Note!

This Release Note includes the commands and debugging information of APOS v7.01 and v8.00.

[Contents]

New Software Features

1 Numbering-type

This command configures the number type of calling and called party information included in the Q.931 setup message.
Usually, the numbering type is configured as “unknown” (as default). However, sometimes, a equipment or VoIP network requires to set the same numbering type for the related equipment. The numbering type can be applied to both POTS peer and VOIP peer.

Commands & Syntax

Configure numbering-type

Step	Command	Remark
1	(config)# **dial-peer voice X <pots | voip>**	X : Identifier.
2	(config)# **numbering-type ?** abbreviated international national network subscriber **unknown (default)**	

Disable numbering-type (default)

Step	Command	Remark
1	(config)# **no numbering-type <cr>**	Set Numbering Type as default(unknown).

Default : Unknown

2 Polarity-Inverse Detect / Generate

The FXO port of the gateway detects the polarity inverse signal generated by PBX. The same configuration is able to apply on the FXS port and, in this case, the FXS port generates the polarity inverse signal and transmits it to PBX.

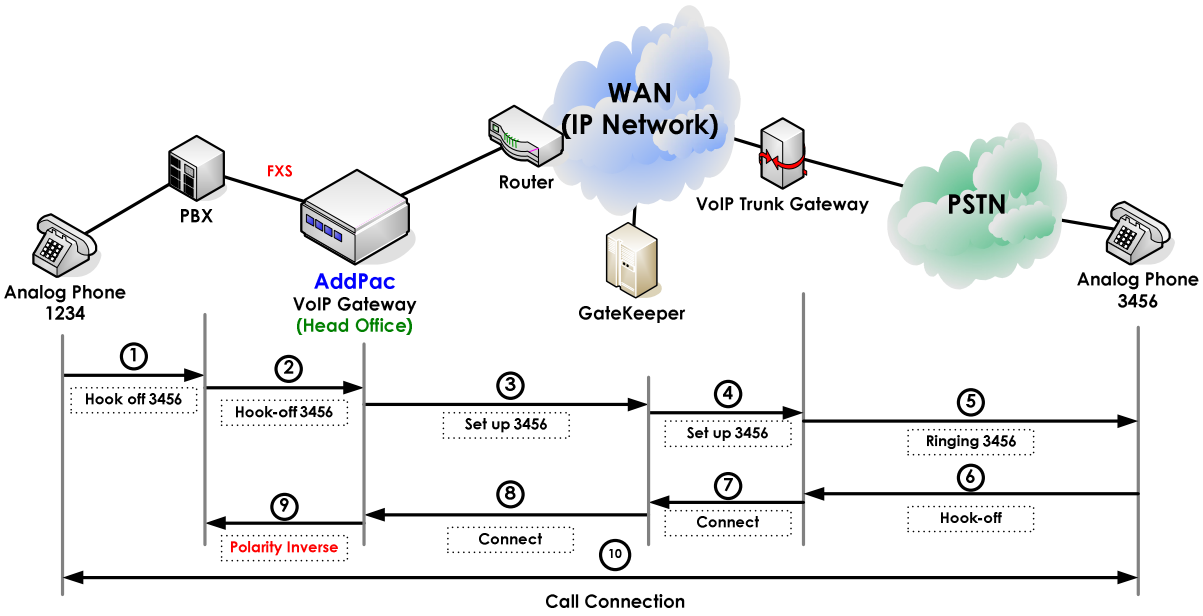
With an incoming VoIP call on the FXO port, the gateway sends Q.931 connect message after detecting the polarity inverse signal on the FXO port. With an outgoing VoIP call originated from the FXS port, the FXS port generates the polarity inverse signal when the called party's Q.931 connect messages is received.

The PSTN/PBX or the telephone connected to the FXS or FXO port are required to support Polarity inverse generation/detect features.

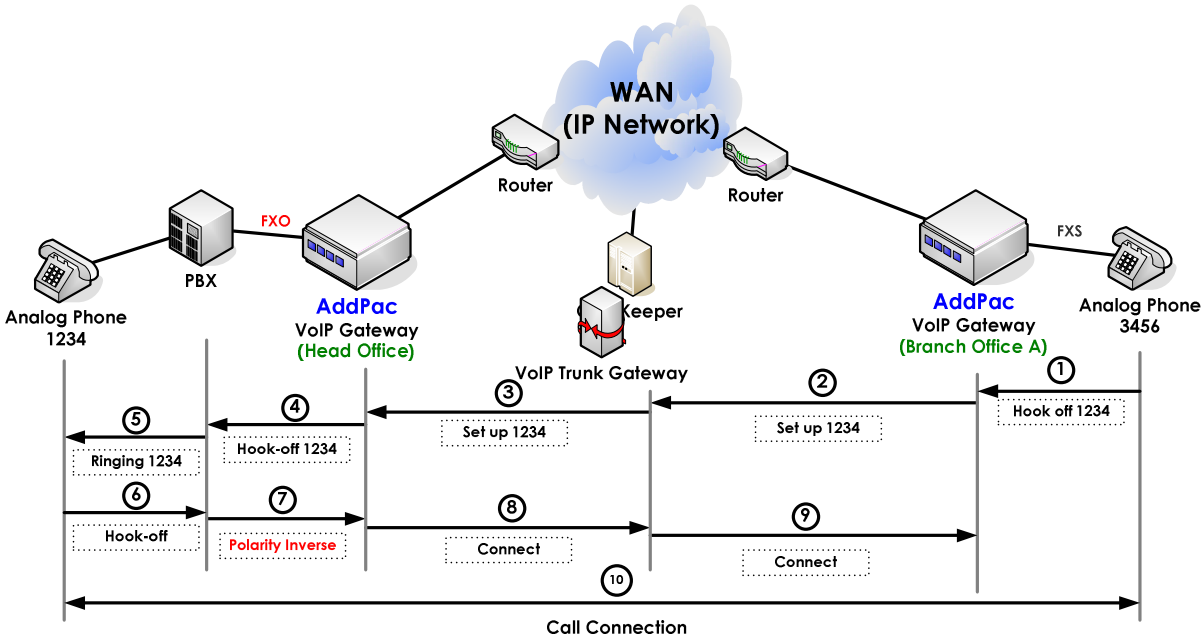
The below models do not support this feature.

AP200-B,C, AP1100, and the FXO modules (for AP2520, AP2830, AP2850, AP2120, AP2110, AP3100) without CID detect feature.

Network Diagram



[Figure 1] VoIP gateway Polarity-Inverse Generate(FXS)



[Figure 2] VoIP Gateway Polarity-Inverse Detect(FXO)

Commands & Syntax

Enable Polarity-inverse

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice-port 0/0**	Select the port to configure.
3	(config-voice-port-0/0)# (config-voice-port-0/0)# **polarity-inverse**	Enable Polarity-inverse feature.

Disable Polarity-inverse

Step	Command	Remark
1	(config-voice-port-0/0)# **no polarity-inverse**	Disable Polarity-inverse feature.

Default : disable

3 CID(Caller-ID) Detect / Generate

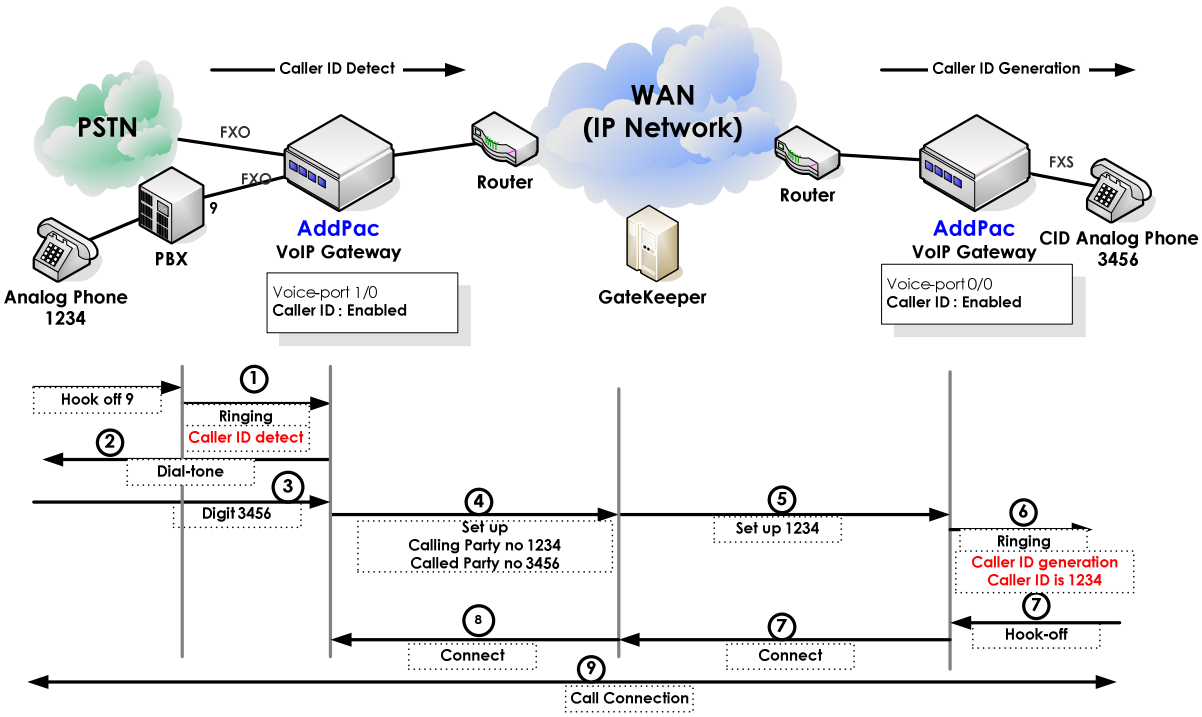
The FXO ports connected to PSTN or PBX are able to detect Caller-ID. Also, the FXS ports enable to send Caller-ID information to the telephones or the PBX.

With a VoIP call originated from the FXO port, the FXO port detects the caller-ID and uses the number as the VoIP calling party number. With an incoming VoIP call to the FXS port, the calling party number at the VoIP setup messages is used as the caller-ID and passed to the telephone or PBX.

The below models do not support this feature.

AP200-B,C, AP1100, and the FXO modules (for AP2520, AP2830, AP2850, AP2120, AP2110, AP3100) without CID detect feature.

Network Diagram



[Figure 3] VoIP gateway CID(Caller-ID) feature

Commands & Syntax

Enable CID(Caller-ID)

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice-port 0/0**	Select the right port.
3	(config-voice-port-0/0)# (config-voice-port-0/0)# **caller-id type {bellcore | etsi | etsi-dtmf | etsi-dtmf-prior-ring | ntt}**	Set the right CID Type according to the customer's network.
4	(config-voice-port-0/0)# **caller-id name {enable | disable}**	Enable/Disable CID name field display.
5	(config-voice-port-0/0)# **caller-id enable**	Enable CID feature.

Disable CID(Caller-ID)

Step	Command	Remark
1	(config-voice-port-0/0)# **no caller-id enable**	Disable CID feature.

Default : caller-id disable, caller-id name disable, caller-id type bellcore

4 E&M Optional Feature (wink-without-pulse)

"wink-without-pulse" is added as the E&M Signaling type option. When the E&M signaling is configured as "wink-start," the gateway terminates the call if there is no ACK signal from the PBX during the certain period. However, certain PBXs don't send the signal properly. In this case, the gateway should keep the call even though there is no ACK signal. Thus this feature is not required when the interfacing PBXs comply with the ACK signal standard.

Commands & Syntax

Enable wink-without-pulse

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice-port 0/0**	Select the right port.
3	(config-voice-port-0/0)# **signal wink-without-pulse**	Enable signal wink-without-pulse.

Disable wink-without-pulse

Step	Command	Remark
1	(config-voice-port-0/0)# **no signal wink-without-pulse**	Disable signal wink-without-pulse.

Default : disable

5 Gateway History

It displays the history information of the gateway along with basic event information such as booting, booting, in Service, voip-interface and etc.

Commands & Syntax

Step	Command	Remark
1	# **# show gateway history**	
	<5>Dec 9 13:09:40 booting Gateway is in service(172.19.1.200)	
	<4>Dec 9 13:09:35 interface VoIP Interface Up (172.19.1.200)	
	<3> Dec 9 13:09:35 interface VoIP Interface Down	

6 StartH245 option (calling-only)

A new option is included at the force-starth245 command. With “calling-only” option, only the calling party gateway sends the startH245 message.

Commands & Syntax

Enable calling-only

Step	Command	Remark
1	# # **config**	Enter APOS Command Mode.
2	(config)# **voice service voip**	Enter VOIP Global Configuration Mode.
3	(config-vservice-voip)# **force-starth245 calling-only**	Enable force-starth245 calling-only.

Disable calling-only

Step	Command	Remark
1	(config-vservice-voip)# **no force-starth245**	Disable force-starth245 calling-only.

Default : disable

7 OpenLogicalChannel negotiation Option

Among the forward/reverse OpenLogicalChannel information from the received Q.931 fast start element, the forward information is forcefully selected. With this command, the forward information is selected unconditionally, thus be careful using this command at the normal operation environment.

For example, there are an AddPac gateway (local) and a Cisco gateway (remote) under NAT environment. When the AddPac gateway originates a call, sometimes, the forward OLC information contains the public IP address of the remote side, and the reverse OLC information contains the private IP address of the remote side. In this case, the gateway utilizes the public IP information with this command. However, it is not a typical situation, so it is disabled as the default configuration.

Commands & Syntax

Enable ignore-reverse-channel-info

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice service voip**	Start VoIP Service configuration..
3	(config-vservice-voip)# **ignore-reverse-channel-info**	Enable ignore-reverse-channel-info.

Disable ignore-reverse-channel-info

Step	Command	Remark
1	(config-vservice-voip) # **no ignore-reverse-channel-info**	Disable ignore-reverse-channel-info.

Default : disable

8 Chinese Announcement Feature

The Chinese announcement is added.

Commands & Syntax

Enable Chinese announcement

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice service voip**	Start VoIP Service configuration..
3	(config-vservice-voip)# **announcement language chinese**	Enable announcement language chinese.

Disable Chinese announcement

Step	Command	Remark
1	(config-vservice-voip) # **no announcement**	

Default : disable

9 SIP Dial-peer Registration

A separate username and password can be assigned for the each dial-peer. If there is preconfigured sip-username and sip-password at sip-ua, the username and password assigned at the each dial-peer is not applicable. That is, the username and password at sip-ua has higher priority than those of dial-peer.

Commands & Syntax

Configure Dial-peer Registration

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **dial-peer voice 0 pots**	Enter Port Configuration Mode.
3	(config-dialpeer-pots-0)# **user-name <string>** (config-dialpeer-pots-0)# **user-password <string>**	

Disable Dial-peer Registration

Step	Command	Remark
1	(config-dialpeer-pots-0)# **no user-name <string>** (config-dialpeer-pots-0)# **no user-password <string>**	

Default : disable

Configuration Example

```
# show run
!
dial-peer voice 0 pots
 destination-pattern 1000
 port 0/0   0
 user-name addpac
 user-password addpac
!
#show sip

Proxyserver Registration Information
    proxyserver registration option = e164
    Proxyserver list :
        ------------------------------------------------------------
        Server address     Port      Priority      Status
        ------------------------------------------------------------
        192.168.100     5060     128    Registered(E.164)

    Proxyserver registration status :
        ------------------------------------------------
        UserName       Regist         Status
        ------------------------------------------------
        addpac          yes       Registered

SIP UA Timer counters
    retry counter = 10
SIP UA Timer values
    tretry (sip retry timer) = 500 msec.
    treg (sip register timer) = 60 sec.
    tregtry (sip register retry timer) = 20 sec.
```

Proxyserver list supports five (5) kinds of status information; “Not Registered”, “Trying”, “Failed”, “Registered (E.164)”, “Registered”. Proxyserver registration supports three (3) kinds of status information; “Not Registered”, “Fail”, “Registered”.

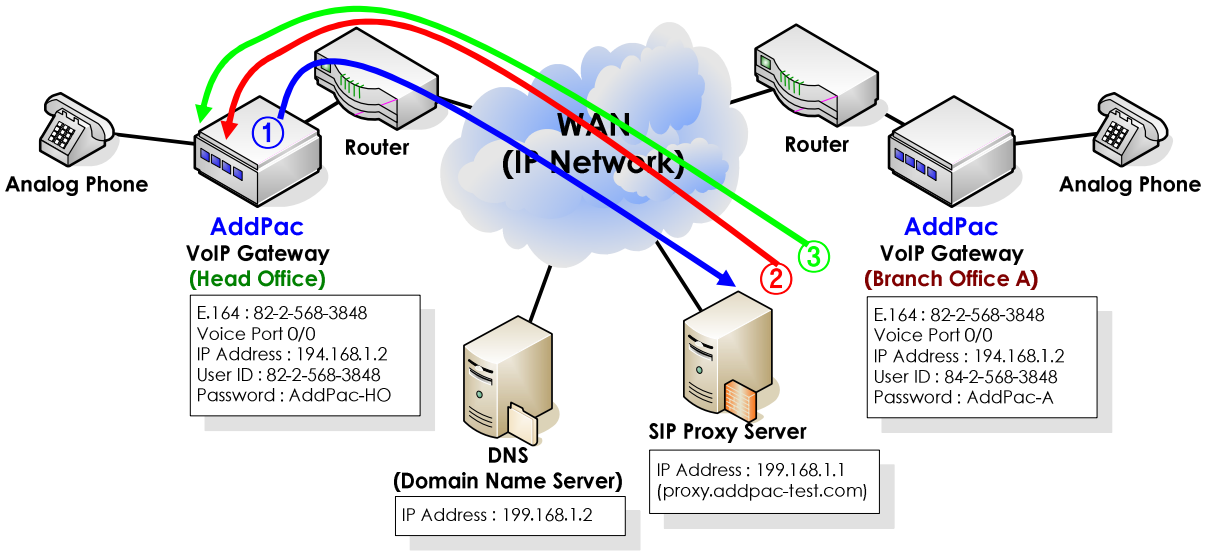
10 SIP BYE Authentication

When the Proxy server sends 401 unauthorized messages as a reply to the gateway's BYE message, the gateway retransmits the BYE message with username and password.

11 SIP Registration with User-name

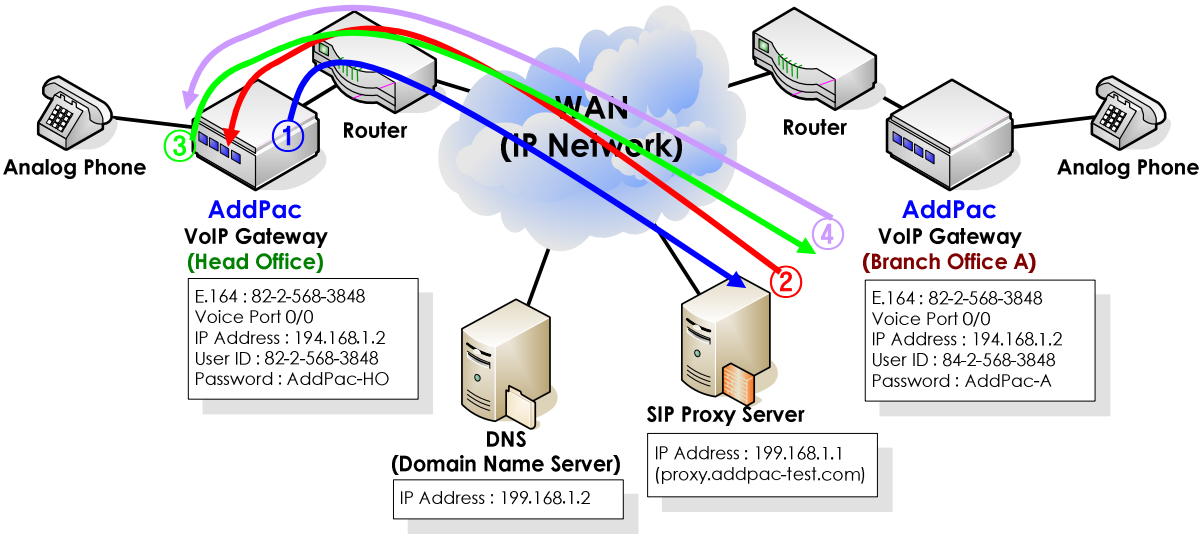
The user-name on the dial-peer is utilized for the registration, not the User-ID(E.164). The feature is applicable for origination-only gateway or for the certain proxy server's asking user-name for the registration.

SIP Registration without Authorization



① **AddPac Gateway transmits Register Message to the Proxy**
② **The proxy transmits 100 Trying Message to AddPac Gateway**
③ **The Proxy transmits 200 OK Message to AddPac Gateway (Registration without authentication)**

SIP Registration with Authorization



① AddPac Gateway transmits Register Message to the Proxy

② Proxy transmits 401 Unauthorized Message to AddPac Gateway (Authentication request)

③ AddPac Gateway transmits Register Authorization Message to (Authentication information transmit)

④ Proxy transmits 200 OK Message to AddPac Gateway (Authentication success- Registration finished)

- if the Proxy transmits 403 Forbidden Message instead of 200 OK message, reconfirm the user-name or password.

Registration using Dial-Peer Destination-pattern(E.164)

When transmitting REGISTER message, use the destination-pattern of the dial dial-peer voice X pots as the USER-ID. Refer to the below configuration example (Head office).

```
 !
dial-peer voice 0 pots
  destination-pattern 8225683848
  port 0/0
!
sip-ua
 sip-server 199.168.1.1
 register e164
!
```

SIP Register Message

```
        Sending SIP PDU to (199.168.1.1:5060) from 5060
REGISTER sip:199.168.1.1 SIP/2.0
CSeq: 1 REGISTER
From: sip:8225683848@199.168.1.1;tag=773f9b21a4
To: sip: 8225683848@199.168.1.1
Contact: sip: 8225683848@194.168.1.1
Expires: 60
```

Registration using Dial-Peer User-name

When transmitting REGISTER message, use user-name <string> as the user ID instead of the destination-pattern of theal dial-peer voice X pots.

```
dial-peer voice 0 pots
 destination-pattern 8224583848
 port 0/0
 user-name AddPac-HO
 user-password AddPac-HO
!
sip-ua
   user-register
   sip-server 199.168.1.1
   register e164
!
```

SIP Register Message

```
        Sending SIP PDU to ( 199.168.1.1:5060 ) from 5060
REGISTER sip:199.168.1.1 SIP/2.0
CSeq: 1 REGISTER
From: sip:AddPac-HO@199.168.1.1;tag=773f9b21a4
To: sip: AddPac-HO@199.168.1.1
Contact: sip: AddPac-HO@194.168.1.1
Expires: 60
```

Registration using Dial-Peer User-name with Authorization

When Proxy transmits 401 Unauthorized Message, retry the authentication with the username/ password of the dial-peer.

```
!
dial-peer voice 0 pots
 destination-pattern 8224583848
 port 0/0
 user-name AddPac-HO
 user-password AddPac-HO
!
sip-ua
 sip-server 199.168.1.1
 register e164
!
```

Registration using Sip-Username with Authorization

When the gateway receives 401 Unauthorized Message from the Proxy, it tries authentication with the sip-username/ sip-password of sip-ua.

```
!
dial-peer voice 0 pots
 destination-pattern 8224583848
 port 0/0
!
sip-ua
 sip-server 199.168.1.1
 sip-username AddPac-HO
 sip-password AddPac-HO
 register e164
!
```

12 SIP Registration Retry counter

Registration Retry counter indicates the length of time the gateway waits before retrying gatekeeper registration after a failed registration attempt.

Commands & Syntax

Configure Registration Retry counter

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **sip-ua**	Enter SIP Global Configuration Mode.
3	(config-dialpeer-pots-0)# **retry-counter <3-10>**	

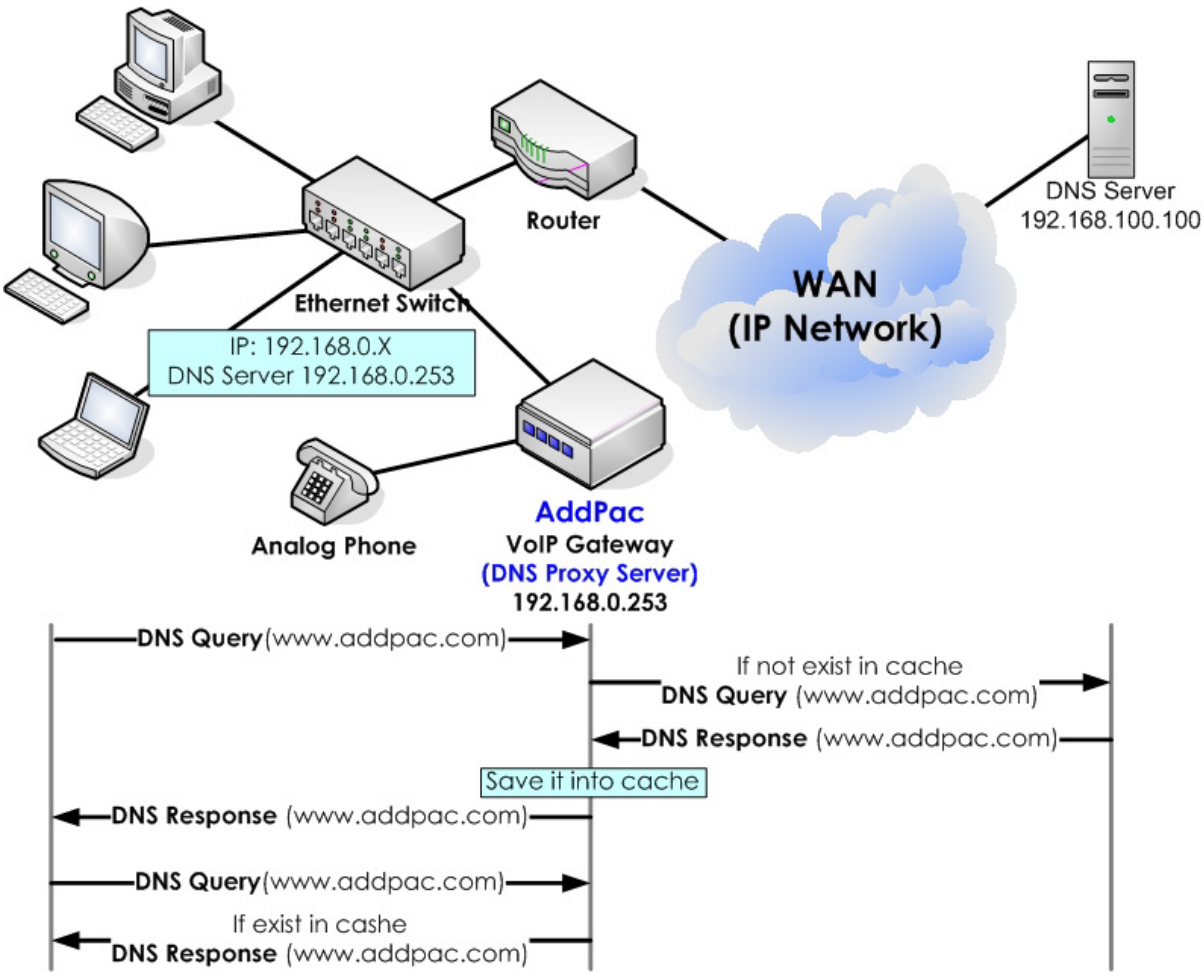
Default: 10 times

13 DNSProxy Supported

It identifies various local character sets, encodes them into UTF-8 (RACE supported) and forwards it to the real DNS server. It listens with the IP address and the port no. (35) of DNS server. When receiving packets, it encodes the information of the configuration file and sends the encoded data to DNS server.

AddPac's all VoIP products supports the feature and it can be enabled/disabled by configuration.

Network Diagram



[Figure 4] VoIP Gateway DNSProxy Feature

Commands & Syntax

Enable DNSProxy

Step	Command	Remark
1	(config)# **service dnsproxy**	Enable DNSProxy feature.

Disable DNSProxy

Step	Command	Remark
1	(config)# **no service dnsproxy**	Disable DNSProxy feature.

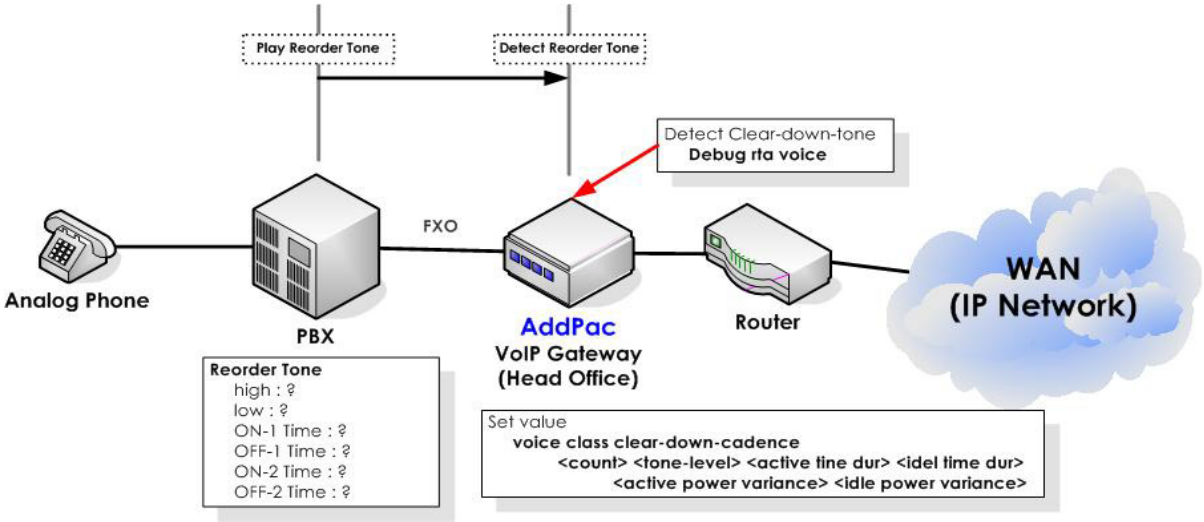
Default : Disable

14 voice class clear-down-cadence

When a FXO interface is used between the local PABX and VoIP gateway as shown in Figure 5 and a call is disconnected from local PABX, the FXO interface detects the re-order-tone or clear-down-tone to disconnect the VoIP call. However, if the FXO interface is not able to detect the tone properly, it cannot tranmit the release signal to the remote gateway. That is, the FXO port is busy even though the local user is on-hook. In this case, the clear-down-toen frequency and cardence value of the local PABX should be configured at the gateway. If this setting cannot solve this issue, apply voice class clear-down-cadence command.

This command detects the ON/Off time (cadence) of the clear-down-tone and the enegery level drift, then it forefully clears the port. The ON/OFF points of the tone and voice codec greatly affect the energy level drift, so carefully review this document before using this command.

Network Diagram



[Figure 5] Voice class clear-down-cadence

Example of analyzing Clear-down-tone cadence and energy level

(Example (In case of codec = g7231))

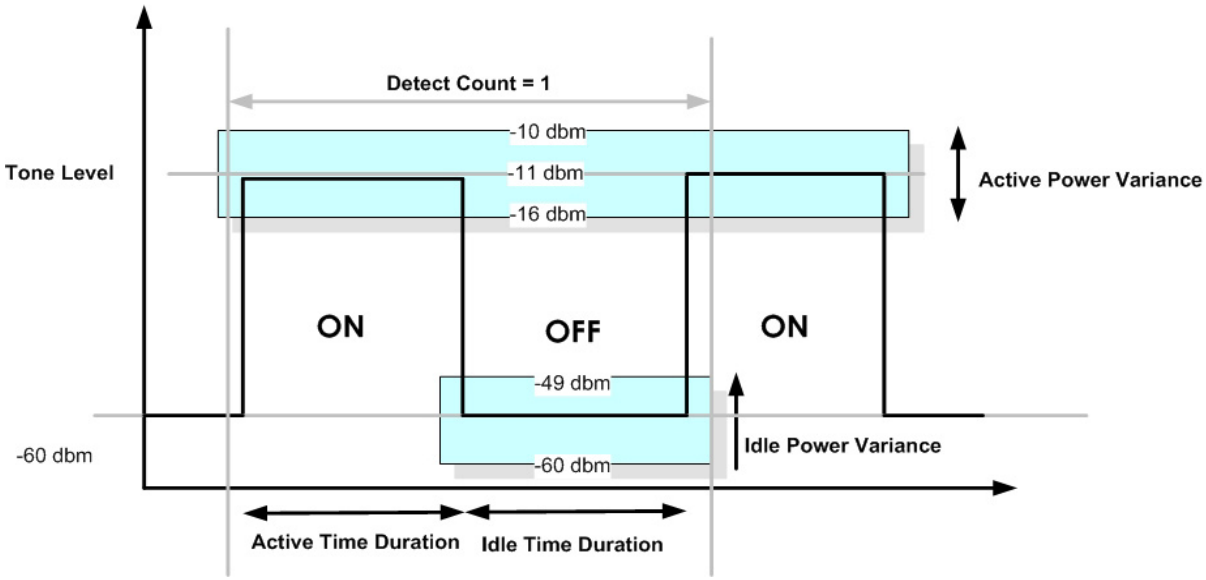
Codec=G711,G729 (10msec * count), G7231 (30msec * count)

debug rta voice
Make PABX play clear-down-tone by hook-on the phone which connected extension line.

8 18 18 17 17 17 17 17 17 18 18 18 18 18 18 14 10 12 11 11 12 10 12 11 11 12 10 12 11 11 12 10 12 11 11 12 10 12 11 11 16 49 58 56 57 54 58 56 53 56 57 56 56 55 57 56 57 55 56 55 57 55 57 55 57 55 15 10 12 11 11 12 10 12 11 11 12 10 12 11 11 12 10 12 11 11 12 10 12 11 11 16 50 57 55 57 57 57 56 57 56 57 57 57 55 56 56 56 54 57 55 58 56 57 55 58 15 10 12 11 11 12 10 12 11 11 12 10 12 11 11 12 10 12 11 11 12 10 12 11 11 16 50 56 55 56 56 57 56 57 56 57 56 58 56 57 56 57 54 57 55 57 56 57 54 58 15 10 12 11 11 12 10 12 11 11 12 10 12 11 11 12 10 12 11 11 12 10 12 11 11

Calculation

- count of Tone Level (-10 ~ -16dbm) = 25
- Active Time Duration (25 * 30ms) = 750ms, if codec is g711 or g729, it will be codec 250ms (25 * 10ms)
- count of Idle level (-49 ~ -60dbm) = 25
- Idle Time Duration (25 * 30ms) = 750ms, if codec is g711 or g729, it will be codec 250ms (25 * 10ms)
- Tone Level = -11
- Active Power Variance = 5 (-6 ~ 16dbm)
- Idle Power Variance = 11 (-49 ~ -60)
  - Idle Tone Level is set as -60 dbm internally, so it was calculated as (11 = (-60(Min)) - (49(Max))).



[Figure 6] Clear-down-tone parameter Detection

Commands & Syntax

Configuring voice class clear-down-cadence

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice class clear-down-cadence 1 -11 750 750 5 11**	Detect Count = 1 Tone Level = -11 ActiveTimeDuration=750ms Idle Time Duration =750ms Active Power Variance = 5 Idle Power Variance = 11.

Disable voice class clear-down-cadence

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# no voice class clear-down-cadence	Disable voice class clear-down-cadence.

Verify voice class clear-down-cadence parameters

```
# show clear-down-cadence
 count   level   actvTime   idleTime   actvMargin   idleMargin
-----------------------------------------------------------------
  1      -11       750        750         5            11
```

Default : Disable

15 FXO port forced-clear-down

The gateway detecs silence and forcefully clears the FXO port. If the energy level of the FXO port is below the certain energy level, the FXO port is disconnected after a preset priod. Use this commnad when there is a period of silence after the hook-on on the user side.

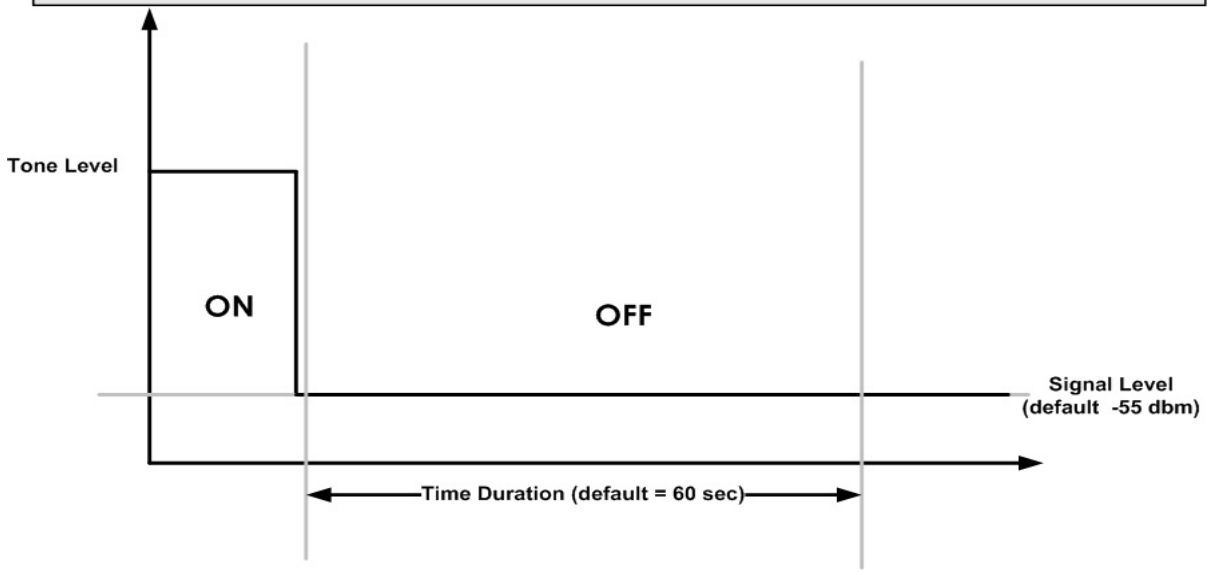
All AddPac VoIP garteway models support this feature and it can be either enabled or disabled.

(Example (In case of codec = g7231))

Codec=G711,G729 (10msec * count), G7231 (30msec * count)

debug rta voice
Make PABX play clear-down-tone by hook-on the phone which connected extension line.
18 18 18 17 17 17 17 17 17 18 18 18 18 18 18 14 *49 58 56 57 54 58 56 53 56 57 56 56 55 57 56 57 55 56 55 57 55 57 55 57 55 49 58 56 57 54 58 56 53 56 57 56 56 55 57 56 57 55 56 55 57 55 57 55 57 55 57 55 49 58 56 57 54 58 56 53 56 57 56 56 55 57 56 57 55 56 55 57 55 57 55 57 55 49 58 56 57 54 58 56 53 56 57 56 56 55 57 56 57 55 56 55 57 55 57 55 57 55 49 58 56 57 54 58 56 53 56 57 56 56 55 57 56 57 55 56 55 57 55 57 55 57 55 49 58 56 57 54 58 56 53 56 57 56 56 55 57 56 57 55 56 55 57 55 57 55 57 55*

Calculation
Tone Level = -14 ~ -18 dbm
Time Duration = 30 sec
Signal Level = - 49 dbm



[Figure 7] Clear-down-tone parameter Detection

Commands & Syntax

Configure FXO port Forced-Clear-Down

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice-port 2/0**	Enter Voice Port Configuration Mode.
3	(config-voice-port-2/0)# (config-voice-port-2/0)# **forced-clear-down <dBm> <sec>**	Enable Forced clear down. dBm: The energy level to detected as silence sec: detecting time

Disable FXO port Forced-Clear-Down

Step	Command	Remark
1	(config-voice-port-2/0)# **no forced-clear-down**	Disable Forced clear down.

- Note:
  - DTMF Tone dBm : Higher then -25dBm
  - General Voice dBm : Between -25 ~ -55 dBm
  - Silence dBm : Lower then -55dBm

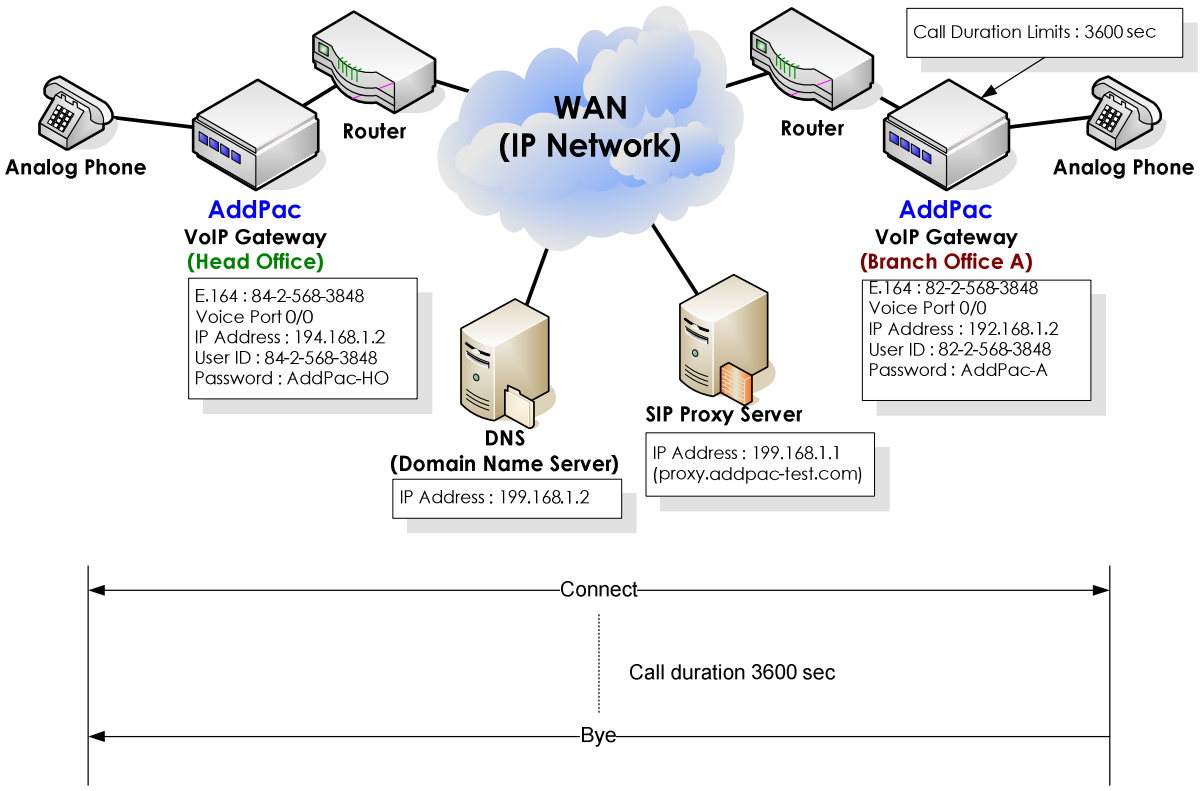
Default : Disable

16 Limited Call Duration

It places a limit on call duration time. A call is forcefully terminated by the gateway in preconfigured call duration time after a call is originated/ received.

AddPac's all VoIP products supports the feature and it can be enabled/disabled by configuration.

Network Diagram



[Figure 8] Limited Call Duration

Commands & Syntax

Set Call Duration Time

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice service voip**	Enter Voice Service Configuration Mode.
3	(config-vservice-voip)# (config-vservice-voip)# **timeout : 10 ~ 86400 tterm**	Set the call duration time.

Remove The Call Duration Time (default)

Step	Command	Remark
1	(config)# (config)# **no timeout tterm**	Disable call duration time setting.

Default : Disable

17 PPPoE Bridge Feature

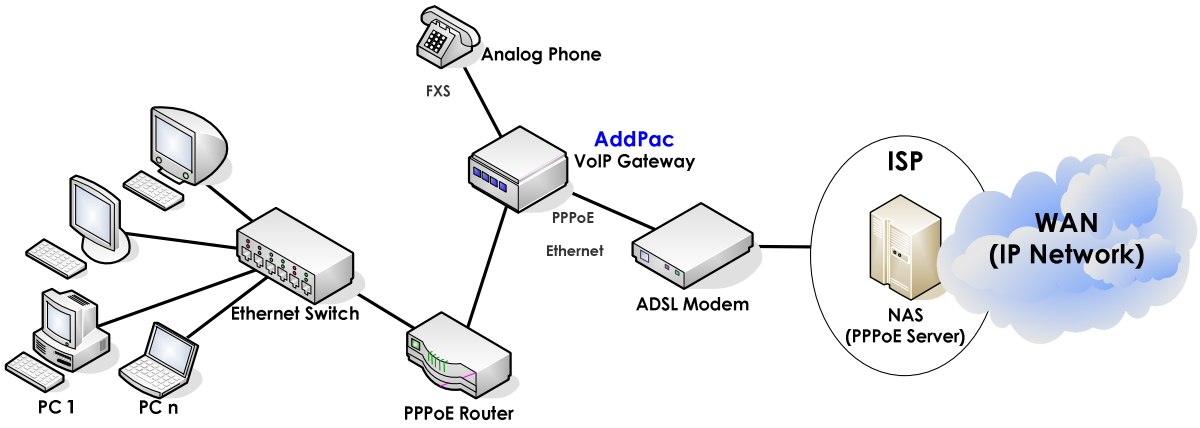
It supports Transparent Bridge mode for PPPoE.

As shown below figure, the VoIP gateway is a transmission path for the PPPoE client PCs or a PPPoE router behind the LAN switch. These clients establish independant PPPoE session with NAS server via WAN interface of the gateway. Also, the gateway establishes a separate PPPoE session with NAS.

By applying QoS on the WAN interface, the gateway controls priority and bandwidth for the traffic coming from its LAN interfce to the WAN interface.

AddPac's all VoIP products supports the feature and it can be enabled/disabled by configuration.

Network Diagram



[Figure 9] PPPoE Bridge Feature

APOS Command Script

```
!
no ip routing
!
no bridge spanning-tree
!
!
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 pppoe
 ppp authentication pap callin
 ppp pap sent-username <username> password <password>
 ppp echo interval 60
 ppp ipcp ms-dns
 ppp ipcp default-route
 qos-control
 line-ctrl promiscuous
 bridge
!
interface ether1.0
 no ip address
 line-ctrl promiscuous
 bridge
!
```

Commands & Syntax

Configure below parameters to connect Internet via ISP(Internet Service Provider).

- ID: "**AddPac"**
- Password: "**1234**"
- get DNS IP (option)
- get default-router IP (option)

Step	Command	Remark
1	# # **config** Enter configuration commands, one per line. End with CNTL/Z	Enter APOS Configuration Mode.
2	(config)# **no ip routing**	Disable IP routing.
3	(config)# **no bridge spanning-tree**	Disable BPDU exchange.
4	(config-ether0.0)# **interface ether0.0** (config-ether0.0)#	Enter Ethernet Interface Configuration Mode.
5	(config-ether0.0)# **encapsulation pppoe**	Set PPPoE.
6	(config-ether0.0)# **ppp authentication pap callin**	Set PAP authentication.
7	(config-ether0.0)# **ppp pap sent-username addpac password 1234**	Set the ID and Password for PAP authentication.
8	(config-ether0.0)# **ppp ipcp ms-dns**	Receive the DNS IP address from PPP server.
9	(config-ether0.0)# **ppp ipcp default-route**	Receive the default router's IP address from PPP server.
10	(config-ether0.0)# **qos-control**	Set QoS.
11	(config-ether0.0)# **bridge**	Enable Bridge mode.
12	(config-ether0.0)# **interface ether1.0** (config-ether1.0)#	Enter Ethernet Interface (1.0) Configuration Mode.
13	(config-ether1.0)# **no ip address**	Disable IP routing.
14	(config-ether1.0)# **bridge**	Enable bridge mode.
15	(config-ether1.0)# **exit** (config)#	Exit from Ethernet Interface (1.0) Configuration Mode.

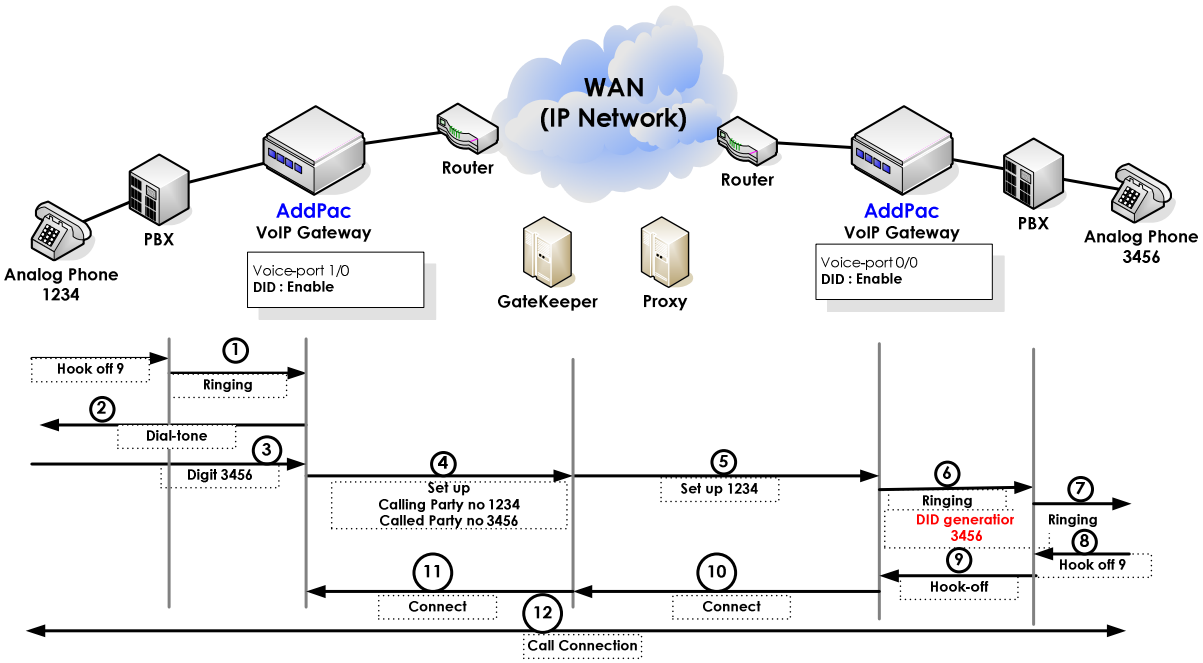
18 DID(Direct Inward Dialing) Modem/PB Type

The gateway supports DTMF, Modem and PB(Push/Button Dial Signal) types for tone genearation. It is applied to the FXS 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



[Figure 10] DID(Direct Inward Dialing) Feature

Commands & Syntax

Enable DID(Direct Inward Dialing)

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice-port 0/0**	Select the port.
3	(config-voice-port-0/0)# (config-voice-port-0/0)# **did {none| normal| ntt-modem| ntt-pb}**	Configure the preferred DID type. None : Disable DID feature Normal : DTMF type Ntt-modem : FSK Modem type Ntt-pb : PB type

- Note :
  - forward-digit, prefix
  - The digit forward type to the PBX's extension/trunk line connected to the Voice-Port is deceided by DID.

Default : did-normal

19 Cascade Function Utilizing IP Sharing

Cascade function is support as one of the supplementary service of IP-share feature. With one public IP, number of AddPac gateways can be stacked and meets the port augmentation requirments.

In IP sharing application, the public IP address of VoIP gateway is shared with the devices of local network such as personal computers. It is different from NAT (network Address Translation)/PAT (Port Address Translation) converting the public IP address to private ones.

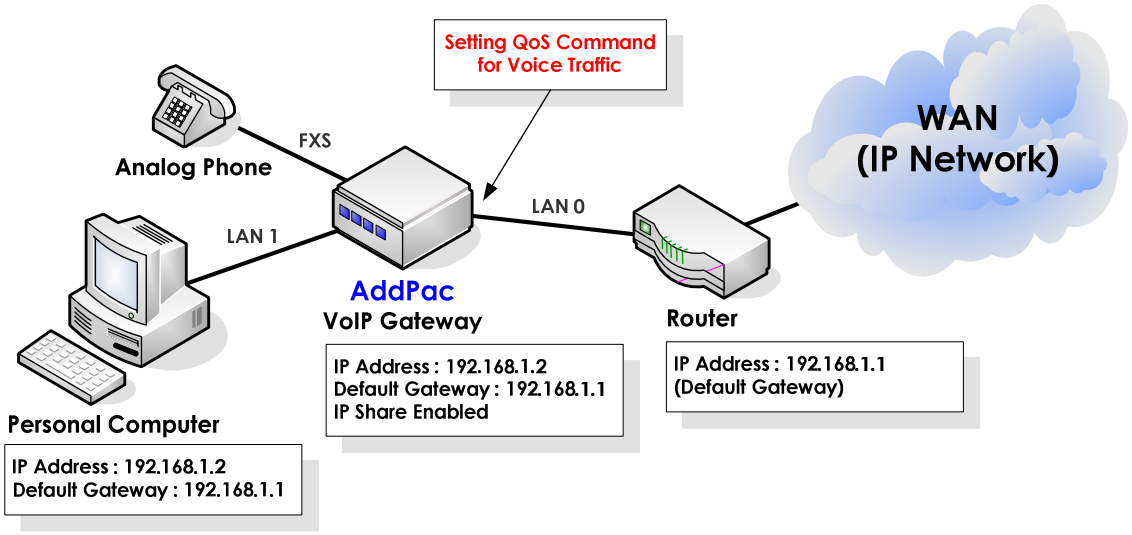
Currently, ordinary houses or SOHO users use dynamic or fixed IP for broadband Internet access. In case of dynamic IP address, a new IP address is assigned every time connecting Internet via ADSL Modem or Cable Modem. On the other hands, for the fixed IP Internet access, ADSL modem or dedicated line is assigned with fixed IP from ISP.

For dynamic IP access, VoIP Gateway is assigned with a dynamic & public IP address with PPPoE and DHCP application. Then the public IP is shared with the local network users. For fixed IP access, the fixed IP assigned by network service providers or ISPs is shared by the VoIP Gateway and the PC s of the local network. It is similar with transparent bridge in terms of bypassing all the packets except directed itself. However, it is not assigned with a separate IP address. Also, It is similar to NAT/PAT in terms of not having a separate IP address. However, it does not form a private network.

With dynamic IP access, assign the dynamic IP to Ethernet 0.0 (LAN 0) and configure Ethernet 1.0 (LAN 1) as DHCP Server without assigning IP address. With fixed IP address, assign the IP to the Ethernet 0.0 (LAN 0) and do not assign IP address to Ethernet 1.0 (LAN 1).

For IP sharing function, at least two(2) Ethernet Interfaces (LAN0, LAN1) are required.

Network Diagram



[Figure 11] VoIP network on IP-share Environment

At the view of packet transmission path, IP sharing is same as that of Bridge mode. QoS configuration of Ethernet 0.0 Interface (LAN 0) is required to allow higher priority for the voice traffic. With the QoS configuration, the VoIP Gateway can offer priority and bandwidth control for all the data coming through Ethernet 1.0 (LAN 1) and VoIP traffic as well, which realizes optimized voice quality.

Basically, changing existing user environment is not recommendable. So if the up-link port is PPPoE Client, assign the local interface as PPP Server. If up-link port is DHCP Client, assign the local interface as DHCP Server. Also, if up-link interface is assigned with Static IP, configure the local interface as static.

VoIP gateway up-link interface configuration

Up-link Interface (LAN 0)	Local Interface (LAN 1)	Configurability
DHCP	DHCP	O
	PPP	O
	Static	X
PPP	DHCP	O
	PPP	O
	Static	X
Static	DHCP	O
	PPP	O
	Static	O

Commands & Syntax

The below parameters should be configured at the VoIP Gateway for the above application.

- IP address configuration of LAN 0 & LAN 1 interface: PPPoE, DHCP, Static
- IP address of default router: Optional
- Traffic QoS configuration for LAN 0 interface: Optional
- IP sharing configuration

DHCP environment with public IP address assigned

DHCP environment application is for the users of broadband network using cable modems.

APOS command script

```
!
dhcp-list 0 type server
dhcp-list 0 address server interface ether0.0
dhcp-list 0 option dhcp-lease-time 600
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
!
interface ether0.0
   ip address dhcp
   mac-address 00:02:a5:00:00:00
   qos 200 150
!
```

```
interface ether1.0
  no ip address
  ip dhcp-group 0
!
```

Step	Command	Remark
1	# # **config** Enter configuration commands, one per line. End with CNTL/Z (config)#	Enter APOS Configuration mode.
2	(config)# **dhcp-list 0 type server**	configure the VoIP gateway as DHCP server.
3	(config)# **dhcp-list 0 address server interface ether0.0**	Assign the IP address of the interface as the IP address of DHCP server.
4	(config)# **dhcp-list 0 option dhcp-lease-time 600**	The public IP address from Cable network is refreshed periodically. The internal PCs check for the IP address at every 300 seconds (600/2). It is recommend to configure “dhcp-lease-time” as “10 min”.
5	(config)# **ip-share enable**	Enable IP sharing
6	(config)# **ip-share interface net-side ether0.0**	Assign the public IP address to the Ethernet interface 0.0.
7	(config)# **ip-share interface local-side ether1.0**	Connect Internal PCs or other devices to the Ethernet Interface 1.0.
8	(config)# **interface ether0.0**	Enter the interface configuration mode.
9	(config-ether0.0)# **ip address dhcp**	Assign the IP address with DHCP.
10	(config-ether0.0)# **mac-address 00:02:a5:00:00:00**	Change the MAC address of the Ethernet 0 as “00:02:a5:00:00:00.” Some cable modems ask for the MAC address of the internal PC for the authentication. Use the MAC address of the internal PC for the Ethernet interface 0.0. (The MAC address of the VoIP gateway is changed temporary and the original address is recovered when the command is removed.) Use this command only when it is necessary.
11	(config-ether0.0)# **qos 200 150**	Configure QoS.
12	(config-ether0.0)# **interface ether1.0**	Enter the interface configuration mode.

13	(config-ether1.0)# **no ip address**	Do not assign an IP address to the interface.
14	(config-ether1.0)# **ip dhcp-grou 0**	To share a dynamically allocated IP address, configure the interface as DHCP Server interface.
15	(config-ether1.0)# **exit** (config)#	Exit from the interface configuration mode.
16	(config)# **exit** #	Exit from APOS Configuration mode.

PPPoE environment with public IP assigned

PPPoE environment application is for the users of broadband network using ADSL modems.

APOS command script

```
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
!
interface ether0.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   qos 200 150
!
interface ether1.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   ppp role server
!
```

Step	Command	Remark
1	# # **config** Enter configuration commands, one per line. End with CNTL/Z (config)#	Enter APOS Configuration Mode.

2	(config)# **ip-share enable**	Enable IP sharing.
3	(config)# **ip-share interface net-side ether0.0**	Configure IP sharing features on the Ethernet interface 0.0, the interface for external access.
4	(config)# **ip-share interface local-side ether1.0**	Configure IP sharing features on the Ethernet interface 1.0, the interface for internal access.
5	(config)# **interface ether0.0** (config-ether0.0)#	Enter the interface configuration mode.
6	(config-ether0.0)# **no ip address**	Do not assign an IP address to the interface.
7	(config-ether0.0)# **encapsulation pppoe**	Configure encapsulation type.
8	(config-ether0.0)# **ppp authentication pap callin**	Configure PPP authentication as PAP.
9	(config-ether0.0)# **ppp pap sent-username addpac password test**	Configure the PAP User ID as “addpac” and the password as “1234”.
10	(config-ether0.0)# **ppp echo interval 20**	
11	(config-ether0.0)# **ppp ipcp ms-dns**	Configure to get default router IP from PPP Server.
12	(config-ether0.0)# **ppp ipcp default-route**	Configure to get DNS IP from PPP Server.
13	(config-ether0.0)# **qos 200 150**	
14	(config-ether0.0)# **interface ether1.0** (config-ether1.0)#	Enter the interface configuration mode.
15	(config-ether1.0)# **no ip address**	Do not assign an IP address to the interface.
16	(config-ether1.0)# **encapsulation pppoe**	Configure encapsulation type.
17	(config-ether1.0)# **ppp authentication pap callin**	Configure PPP authentication as PAP.
18	(config-ether0.0)# **ppp pap sent-username addpac password test**	Configure the PAP User ID as “addpac” and the password as “1234”.
19	(config-ether1.0)# **ppp echo interval 20**	
20	(config-ether1.0)# **ppp ipcp ms-dns**	Configure to get default router IP from PPP Server.
21	(config-ether1.0)# **ppp ipcp default-route**	Configure to get DNS IP from PPP Server.
22	(config-ether1.0)# **ppp role server** Set to PPPoE Server	
23	(config-ether1.0)# **exit** (config)#	Exit the interface configuration mode.
24	(config)# **exit** #	Exit from APOS Configuration Mode..

Fixed IP environment with public IP assigned

Fixed IP environment with a public IP address is for the users of broadband network using a WAN router (PPP, HDLC, Frame-Relay, ATM and etc.).

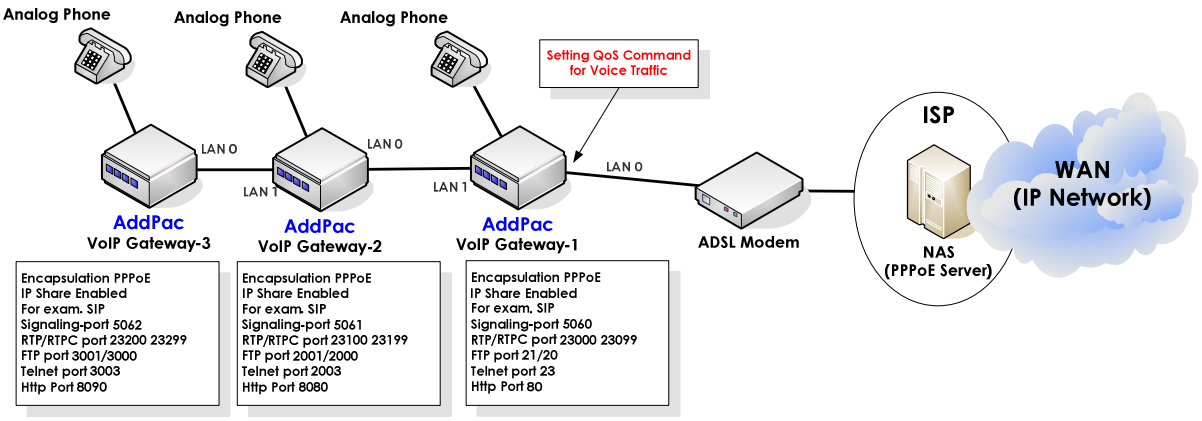
Configurations (static)

```
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
!
interface ether0.0
 ip address 192.168.1.2 255.255.255.0
!
interface ether1.0
 no ip address
!
route 0.0.0.0 0.0.0.0 192.168.1.1
!
```

Step	Command	Remark
1	# **config** Enter configuration commands, one per line. End with CNTL/Z (config)#	Enter APOS Configuration Mode.
2	(config)# **ip-share enable**	Enable IP sharing feature.
3	(config)# **ip-share interface net-side ether0.0**	Configure IP sharing features on the Ethernet interface 0.0, the interface for external access.
4	(config)# **ip-share interface local-side ether1.0**	Configure IP sharing features on the Ethernet interface 1.0, the interface for internal access.
5	(config)# **interface ether0.0** (config-ether0.0)#	Enter the interface configuration mode.
6	(config-ether0.0)# **ip address 192.168.1.2 255.255.255.0**	Assign the IP address to the interface.
7	(config-ether0.0)# **interface ether1.0** (config-ether1.0)#	Enter the interface configuration mode.
8	(config-ether1.0)# **no ip address**	
9	(config-ether1.0)# **route 0.0.0.0 0.0.0.0 192.168.1.1**	Assign the default router.
10	(config-ether1.0)# **exit** (config)#	Exits from the interface configuration mode.
11	(config)# **exit** #	Exits from APOS configuration mode.

Cascade on PPPoE Environment 1

Network Diagram



[Figure 12] Cascade on PPPoE Environment 1

APOS Command Script : AddPac Gateway-1

```
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
ip-share cascade
ip-share sending group-static-entry udp 5061 5062 local-side
ip-share sending group-static-entry udp 23100 23299 local-side
ip-share sending group-static-entry tcp 2000 2003 local-side
ip-share sending group-static-entry tcp 3000 3003 local-side
ip-share sending group-static-entry tcp 8080 8090 local-side
!
interface ether0.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   qos-control
!
interface ether1.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   ppp role server
!
```

```
voice service voip
!
minimize-voip-port service rtp-udp-listen 23000 23099
!
```

APOS Command Script : AddPac Gateway-2

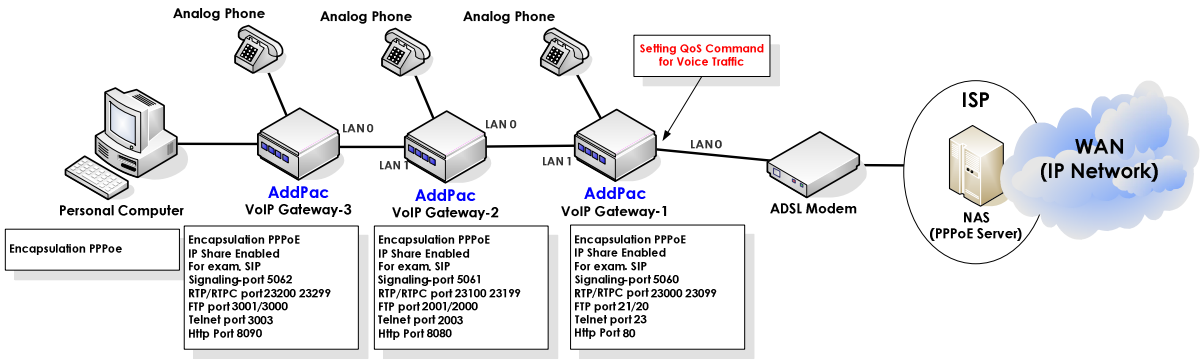
```
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
ip-share cascade
ip-share sending static udp 5062 local-side
ip-share sending group-static-entry udp 23200 23299 local-side
ip-share sending group-static-entry tcp 3000 3003 local-side
ip-share sending static tcp 8090 local-side
ip-share sending static udp 5060 net-side
ip-share sending group-static-entry udp 23000 23099 net-side
ip-share sending group-static-entry tcp 20 23 net-side
ip-share sending static tcp 80 net-side

!
interface ether0.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   qos-control
!
interface ether1.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   ppp role server
!
service-port ftpd 2001 2000
service-port telnetd 2003
service-port httpd 8080
!
voice service voip
!
minimize-voip-port service rtp-udp-listen 23100 23199
!
sip-ua
!
   signaling-port 5061
```

APOS Command Script: AddPac Gateway-3

```
!
no ip-share enable
!
interface ether0.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   qos-control
!
interface ether1.0
   no ip address
!
service-port ftpd 3001 3000
service-port telnetd 3003
service-port httpd 8090
!
voice service voip
!
minimize-voip-port service rtp-udp-listen 23200 23299
!
sip-ua
!
   signaling-port 5062
```

Cascade on PPPoE Environment 2



[Figure 13] Cascade on PPPoE Environment 2

APOS Command Script : AddPac Gateway-1

```
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
ip-share cascade
ip-share sending group-static-entry udp 5061 5062 local-side
ip-share sending group-static-entry udp 23100 23299 local-side
ip-share sending group-static-entry tcp 2000 2003 local-side
ip-share sending group-static-entry tcp 3000 3003 local-side
ip-share sending group-static-entry tcp 8080 8090 local-side
!
interface ether0.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   qos-control
!
interface ether1.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   ppp role server
!
voice service voip
!
minimize-voip-port service rtp-udp-listen 23000 23099
!
```

APOS Command Script: AddPac Gateway-2

```
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
ip-share cascade
ip-share sending static udp 5062 local-side
ip-share sending group-static-entry udp 23200 23299 local-side
ip-share sending group-static-entry tcp 3000 3003 local-side
ip-share sending static tcp 8090 local-side
ip-share sending static udp 5060 net-side
ip-share sending group-static-entry udp 23000 23099 net-side
ip-share sending group-static-entry tcp 20 23 net-side
ip-share sending static tcp 80 net-side

!
interface ether0.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   qos-control
!
interface ether1.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   ppp role server
!
service-port ftpd 2001 2000
service-port telnetd 2003
service-port httpd 8080
!
voice service voip
!
minimize-voip-port service rtp-udp-listen 23100 23199
!
sip-ua
!
   signaling-port 5061
```

APOS Command Script: AddPac Gateway-3

```
!
ip-share enable
ip-share interface net-side ether0.0
ip-share interface local-side ether1.0
ip-share sending group-static-entry udp 5060 5061 net-side
ip-share sending group-static-entry udp 23000 23199 net-side
ip-share sending group-static-entry tcp 2001 2003 net-side
ip-share sending group-static-entry tcp 20 23 net-side
ip-share sending static tcp 8080 net-side
ip-share sending static tcp 80 net-side
!
interface ether0.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   qos-control
!
interface ether1.0
   no ip address
   encapsulation pppoe
   ppp authentication pap callin
   ppp pap sent-username addpac password test
   ppp echo interval 20
   ppp ipcp ms-dns
   ppp ipcp default-route
   ppp role server
!
service-port ftpd 3001 3000
service-port telnetd 3003
service-port httpd 8090
!
voice service voip
!
minimize-voip-port service rtp-udp-listen 23200 23299
!
sip-ua
!
   signaling-port 5062
```

20 VRRP(Virtual Router Redundancy Protocol)

This protocol ties a number of routers as a group and assigns one virtual IP Address to the group. When a failure occurs in the master router, one of backup routers takes over the master's role, so that it can provides stable routing service.

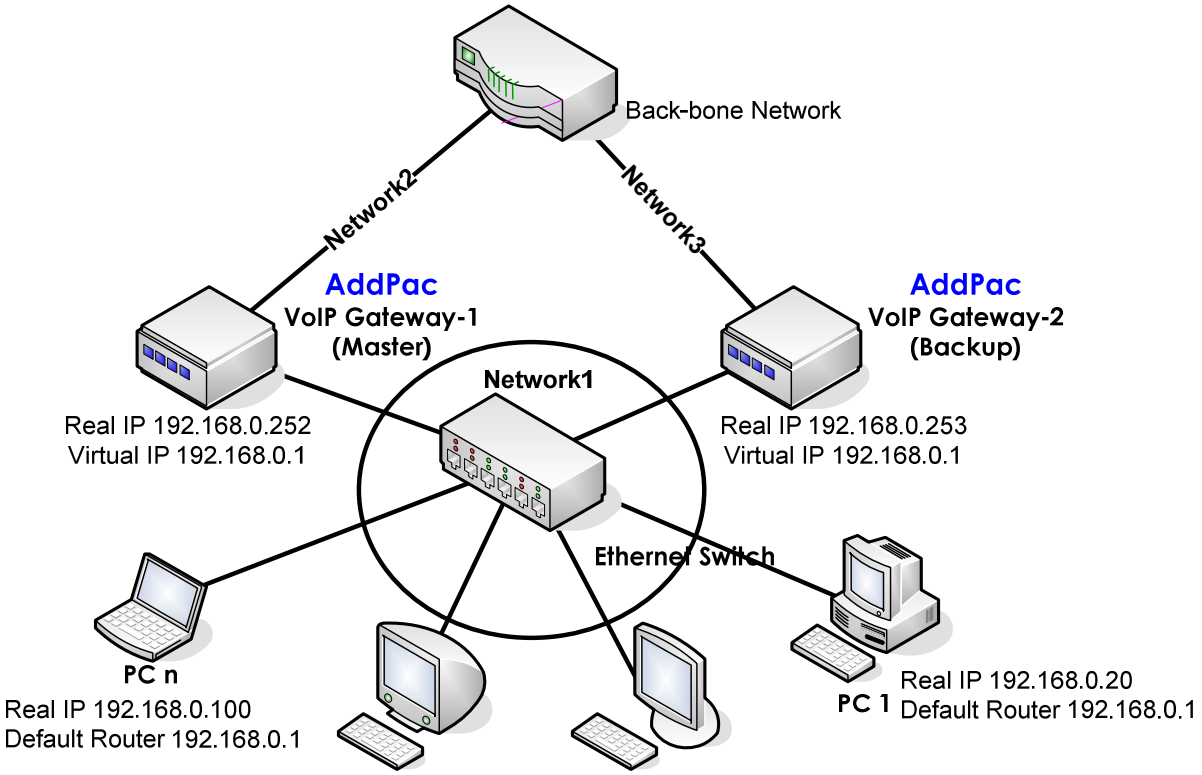
The client end-users in general network environment access to the exterior network using the routing service of a default router. However, in case the default router has a disorder, users are disconnected from the outer network and only the local networking is available. Usually it takes from minutes to hours for its recovery. VRRP is a protocol, developed to prevent this kind of incident. It assigns two or more routers as one VRRP group, and then creates a virtual IP address and informs it to clients as IP address of default router.

VRRP uses the concept of Master/Backup. In a VRRP setup, one router is elected as the master router with the other routers acting as backups in case of the failure of the master. Master router provides routing service, and at the same time, transmits VRRP advertisement packets at the stated periods to the network to inform its status to backup routers. If there is no VRRP advertisement packet during the time, the backup routers send VRRP advertisement packets. Then they decide the priorities according to the received advertise packets and then the new Master router is decided. Thus they proceed on normal routing service.

In the network embodied by VRRP, the clients do not need to know the real master router and the status of the router. Clients only utilize the VRRP virtual IP address as the default router address.

This feature is not supported with AP160, AP200 series and AP1000 series.

Network Diagram



[Figure 14] VRRP Network

In the above figure, router1 and router2 form a VRRP group, and provide routing service to clients. The concept of Master/Backup is applied in VRRP, and the routers belonging to the same VRRP group decide Master/Backup operation of each one by the priority. VRRP is the protocol based on multicast, and available at Ethernet Interface.

APOS Command Script : AddPac Gateway-1

```
!
Interface ether0.0
  Ip address 192.1680.252 255.255.255.0
  Line-ctrl multicast-all
vrrp 1 priority 100
  vrrp 1 preempt
  vrrp 1 timers advertise 1
  vrrp 1 ip 192.168.0.1
```

APOS Command Script: AddPac Gateway-2

```
!
Interface ether0.0
  Ip address 192.1680.253 255.255.255.0
  Line-ctrl multicast-all
vrrp 1 priority 100
  vrrp 1 preempt
  vrrp 1 timers advertise 1
  vrrp 1 ip 192.168.0.1
```

Commands & Syntax

VRRP ID : Assigns VRRP group. The routers, which operate as master/backup, should have the same ID. Also, one Ethernet Interface belongs to multiple VRRP groups by adding VRRP IDs. The corresponding options of VRRP can be added/changed only after ID has been assigned, the usable range of ID is 1~255.

VRRP IP Address : indicates VRRP virtual IP address. Routers in a VRRP group must have the same virtual IP address like VRRP ID. Virtual IP address must belong to the same address range as the real IP address of interface.

VRRP MAC Address : Basically, when VRRP function is activated, the router creates virtual MAC address corresponding to virtual IP address. However, this option is used when “Physical MAC address “is demanded by the users. In case “Physical MAC Address” is selected, the master router makes clients change the MAC address of default router by using ARP packet. Available options are “Virtual/Physical,” and the default value is “Virtual.”

VRRP Preempt : determines whether, only in case the router currently operating as backup has higher priority over the router operating as master, it will take the authority of master or not. The “delay” option determines the delay time before taking the master’s authority. The default value is “On.”

VRRP Priority : determines priority in a VRRP group. The priority value range is 1~255 and the 255 is the highest priority. If several routers have the same priority, the router with higher IP address has the higher priority. The usable range is “1~255”, and the default value is “100”.

VRRP Timers : determines the transmission interval of VRRP advertisement packet. The router operating as a master transmits VRRP advertisement packets at stated

periods. This packet includes information such as master router's priority, and backup routers check this packet periodically according to their VRRP Timers value. If VRRP advertisement packet is not transmitted to backup routers at the stated time, backup routers consider it as a disorder occurred in the master router. Then they transmit VRRP advertisement packets, and a new master router is selected by comparing the exchanged packets. Therefore, routers in a VRRP group should have the same VRRP Timers value. The usable range is 1~255, and the default value is "1". (Unit: seconds)

Line-ctrl multicast-all : VRRP is the protocol based on multicast. Therefore, configuration for transmission-reception of the multicast packet in the Ethernet interface is required.

show vrrp : displays the VRRP option currently configured at the router and the master/backup operation status of the router.

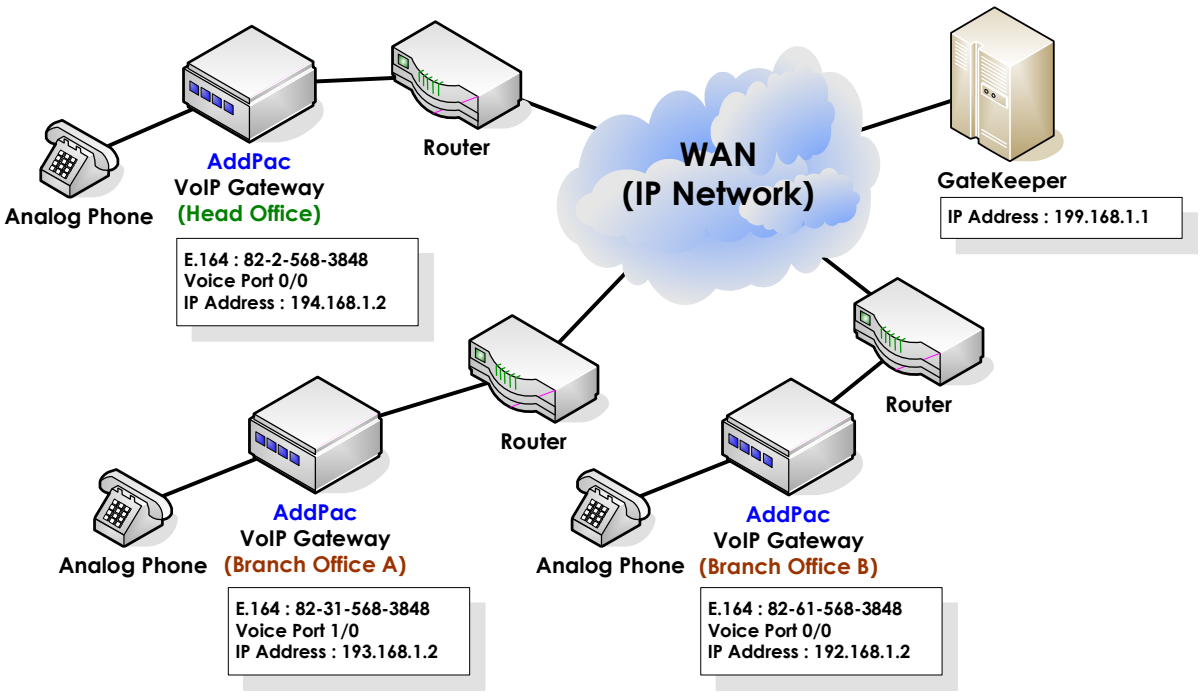
21 ACF-DEST-INFO

With H.323 signalling protocol, the gateway accepts/ignores Destination information field that is returned in the ACF(Admission Confirm) message.

According to the figure below, the gateway at Head Office dials “82315683848” and it is included at the destination filed of ARQ message. The gatekeeper modifies the destination filed as “0315683848” that is returned in the ACF message. The caling gateway overwrites the Called Party Number with the destination filed in ACF.

Disable this feature to use the original destination number as Called Party Number in setup message.

Network Diagram



[Figure 15] ACF-DEST-INFO Feature

Commands & Syntax

Enable ACF-DEST-INFO

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **gateway**	
3	(config-gateway)# (config-gateway)# **acf-dest-info**	Enable ACF-DEST-INFO feature.

Disable ACF-DEST-INFO

Step	Command	Remark
1	(config-gateway)# **no acf-dest-info**	Disable ACF-DEST-INFO feature.

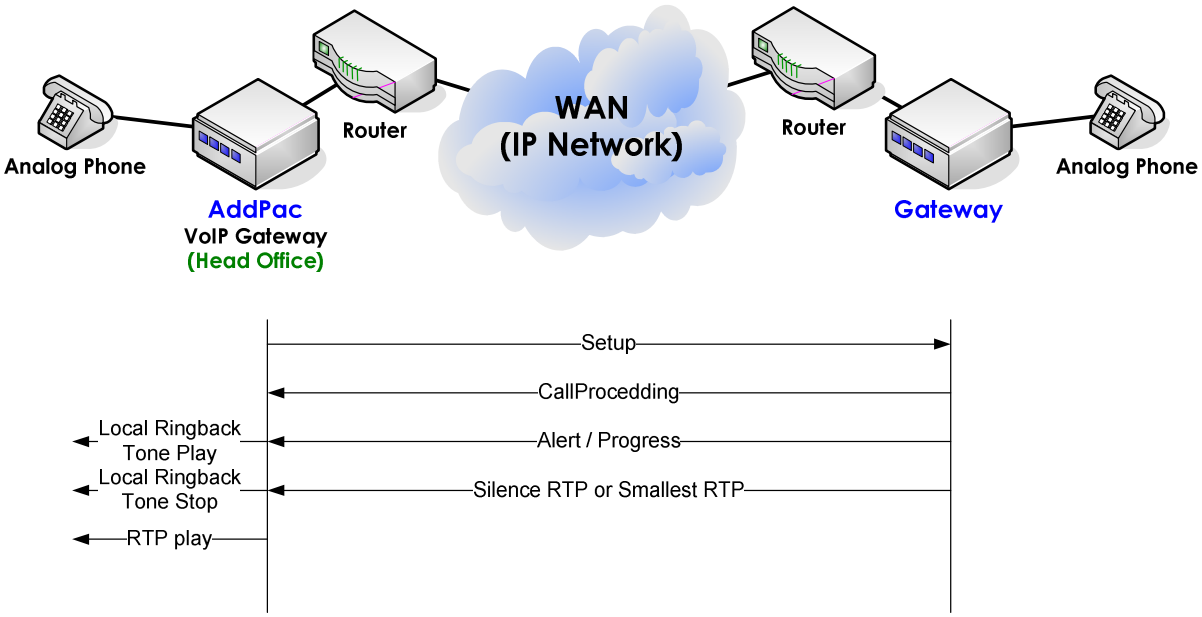
Default : Enable

22 Accept-FSE-at-Connet

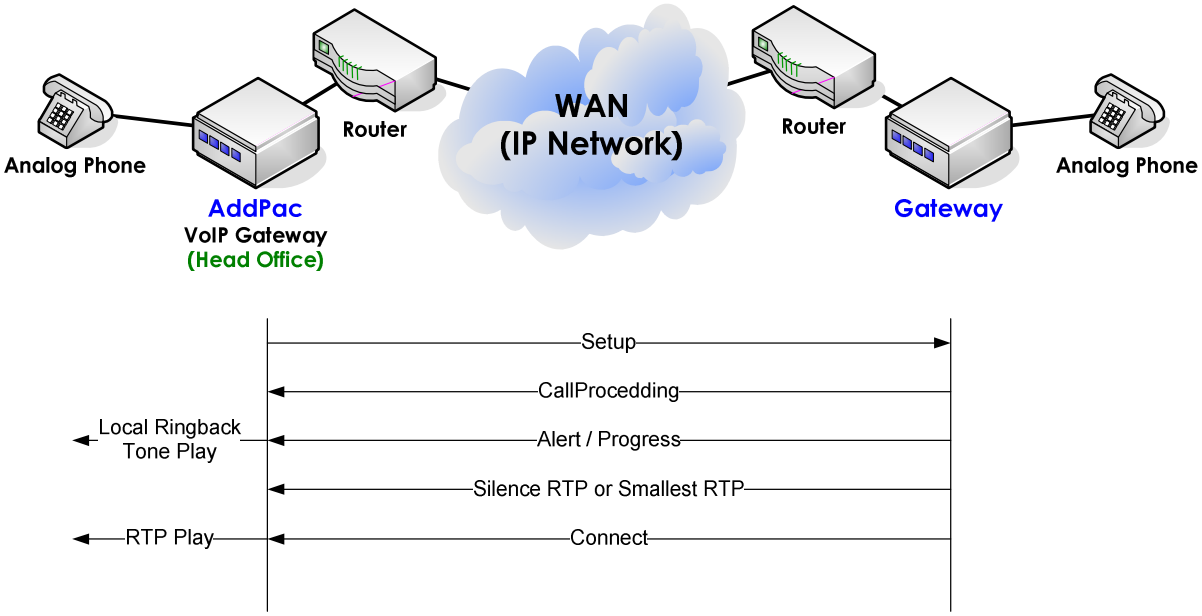
In case of H.323 call origination, the gateway plays Ring-Back-Tone regardless of receiving the alarting message from the called party.

The OLC channel is not opened so that it does not receive Ring-Back-Tone as Inband (RTP) before establish the connection.

Network Diagram



[Figure 16] Without Accept-FSE-at-Connect Setting



[Figure 17] With Accept-FSE-at-Connect Setting

Commands & Syntax

Enable Accept-FSE-at-Connect

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice service voip**	Enter VoIP Service Configuration Mode.
3	(config-vservice-voip)# (config-vservice-voip)# **accept-fse-at-connect**	Enable Accept-FSE-at-Connect feature.

Disable Accept-FSE-at-Connect

Step	Command	Remark
1	(config-vservice-voip)# **no accept-fse-at-connect**	Disable Accept-FSE-at-Connect feature.

Default : disable

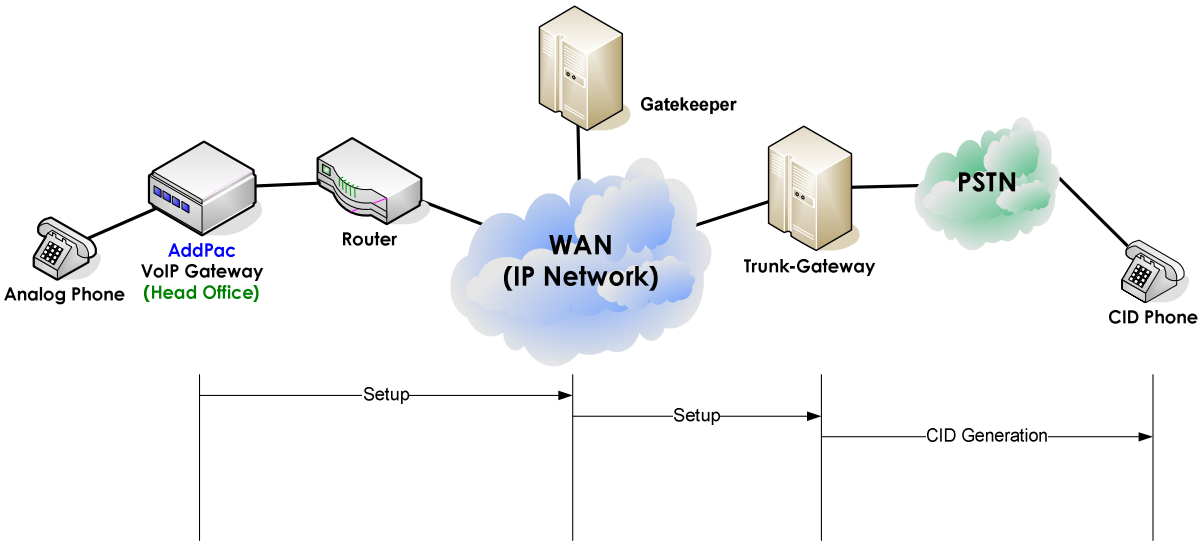
23 CLID(Calling Line Indetification)

For H.323 signaling, AddPac gateway supports Presentation indicator and screening indicator filed within Q.931 Calling party number information element.

Generally, when the number type of Q.931 Setup message is “unknown,” the gateway only sends calling party number without Presentation indicator and screening indicator field. In this case, the trunk gateway adds specific digits or prefix. Configure Presentation indicator and screening indicator field in setup message to foward the calling party number or restrict the number.

Reference: ITU-T Recommendation Q.931 Calling party number.

Network Diagram



[Figure 18] CLID Feature

Commands & Syntax

Configure CLID

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **dial-peer voice XXXX voip**	Enter VoIP Peer Configuration Mode.
3	(config-dialpeer-voip-XXXX)# (config-dialpeer-voip-XXXX)# **clid {network-number| restrict| strip}**	Configure CLID. Refer to the below table.

Disable CLID

Step	Command	Remark
1	(config-dialpeer-voip-XXXX)# **no clid**	Disable CLID.

- Note: Message filed in CLID

	Presentation Indicator	Screening Indicator	Calling party number
CLID disable	X	X	O
CLID network-number	Presentation allowed	Network provided	O
CLID restrict	Presentation restricted	User-provided, verified and failed	O
CLID strip	X	X	X

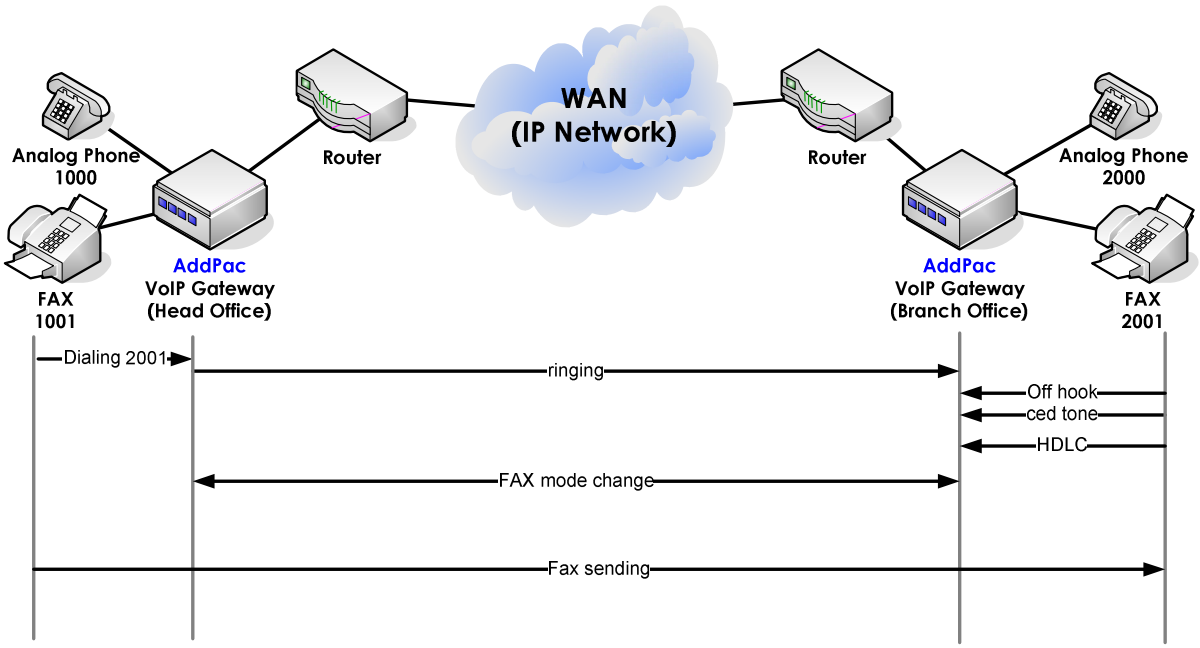
Default : disable

24 FAX-Early-Detect

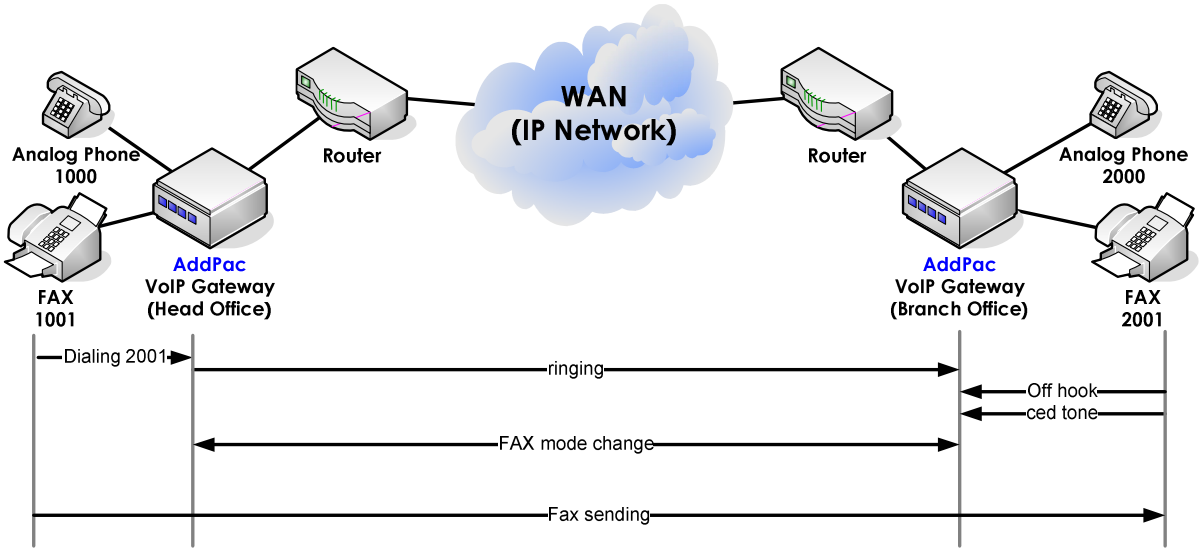
To prevent the gateway from entering FAX mode by the side tone (CED tone) of the neighboring gateway, the gateway does not enter FAX mode without receiving HDLC flag as defult. However, some FAX machines do not support the feature of resending the HDLC data. When the HDLC data is sent before the VoIP call setup, the gateway cannot detect the HDLC and it is not able to enter the FAX mode. Fax-rearly-detect makes the gateway enter FAX mode by detecing CED tone even though HDLC flage is not received.

With fax-early-detect, the gateway might enter the FAX mode by the side-tone of neighboring gateways. So it is not generally recommanded.

Network Diagram



[Figure 19] Normal FAX Service Network



[Figure 20] FAX Service with FAX-Early-Detect

Commands & Syntax

Enable FAX-Early-Detect

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **voice-port 0/0**	Select the voice port.
3	(config-voice-port-0/0)# **fax-early-detect**	Enable FAX-Early-Detect.

Disable FAX-Early-Detect

Step	Command	Remark
1	(config-voice-port-0/0)# **no fax-early-detect**	Disable FAX-Early-Detect.

Default : disable

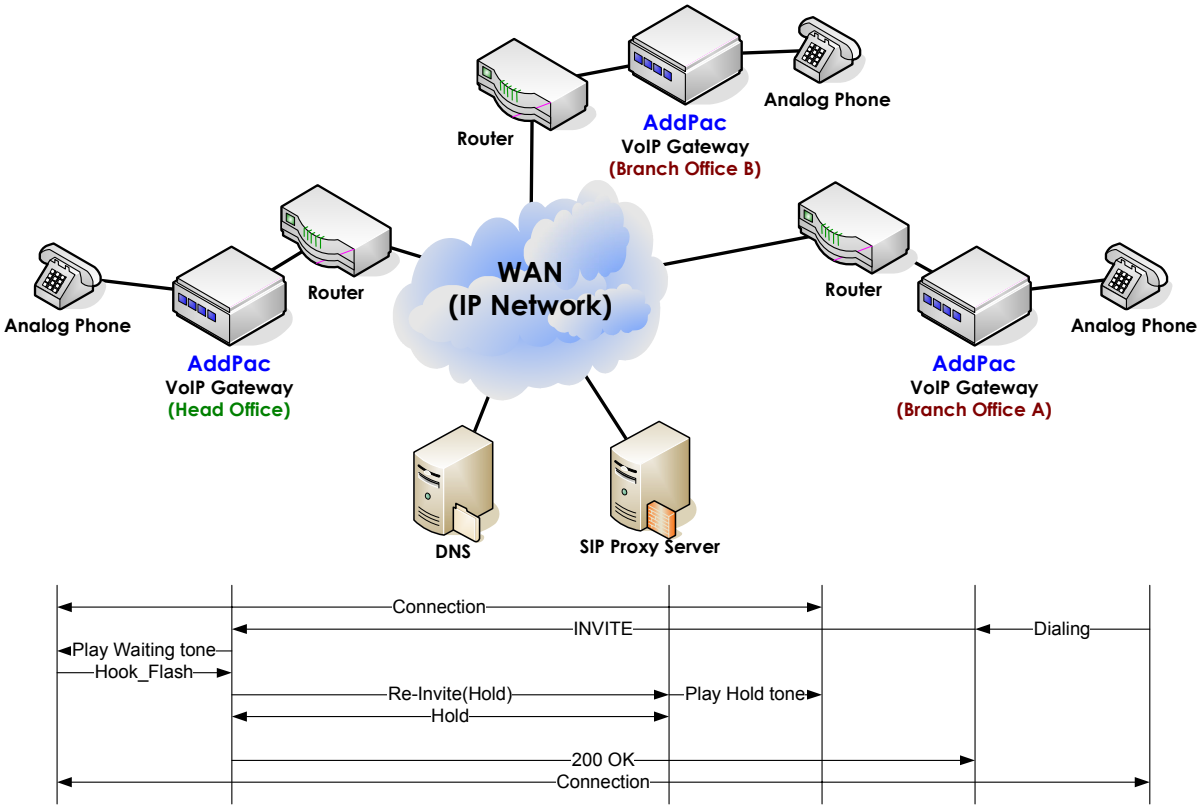
25 SIP Call-Waiting (call hold)

Call-waiting is implemented with SIP signaling protocol.

When on a call, if a new call comes in, the user hears an audible tone and can switch over to the new user with the Hook-flash button. The first call is put into hold and the second incoming clall is received. To retrieve the first calll, press Hook-Flash Button again.

For the gateway with PSTN back-up ports such as AP200, AP1000 and AP160, diable “switch-to-pstn-on-call” and “switch-to-voip-on-call.”

Network Diagram



[Figure 21] VoIP Gateway Call-Waiting Feature

Commands & Syntax

Set Call-Waiting

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **dial-peer voice 0 pots**	Select the pots peer.
3	(config-dialpeer-pots-0)# **call-waiting**	Enable Call-Waiting.

Disable Call-Waiting

Step	Command	Remark
1	(config-voice-port-0/0)# **no call-waiting**	Disable Call-Waiting.

Default : disable

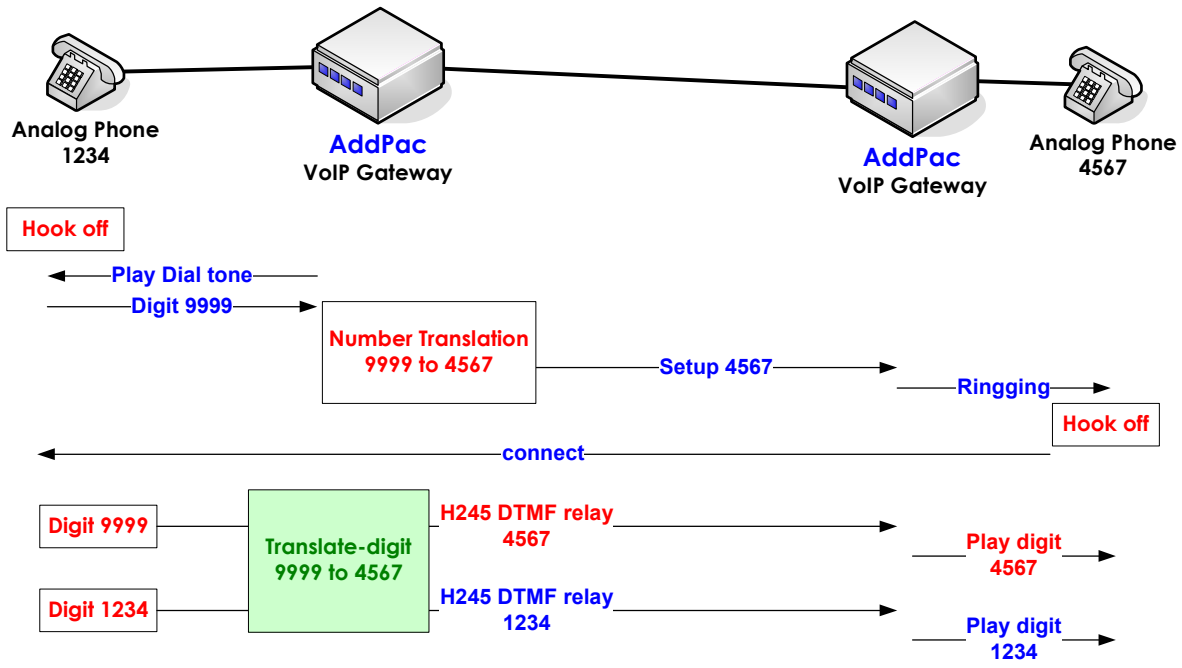
26 H323 Translation-Digit-In-Call

It translates the relayed digits (DTMF digits) after a call setup to preconfigured numbers. This featue is not same as the number translation which translates the calling party number or called party number during the call setup.

The below figure illustrates the differnece between number translation (translation-rule) and translation-digit commands. When the rule translating the dialed number (“9999”) to “4567” is applied to the called-party number (destination number), it affects the called-party number used for call setup.

In case of transtion-digit, it translats the digits transfered by DTMF relay during a call. So it is not relateed to the e.164 number for call setup.

Network Diagram



[Figure 22] Translation-Digit-In-Call Feature

APOS Command Script: Number Translation

```
!
dial-peer voice 1000 voip
 destination-pattern T
 session target 61.33.161.47
 dtmf-relay h245-alphanumeric
 translate-outgoing called-number 0
!
translation-rule 0
 rule 0   9999    4567
```

APOS Command Script : Translation-Digit-In-Call

```
!
dial-peer voice 1000 voip
 destination-pattern T
 session target 61.33.161.47
 dtmf-relay h245-alphanumeric
translate-outgoing digits-in-call 0
!
translation-rule 0
                    rule 0   9999    4567
```

27 Resource threshold (RAI)

It limits the number of concurrent calls to prevent the faluts caused by the overload of the equpment or network. When the port utilization exceeds the high-threshold, a RAI message with the “OutOfResource” field “TRUE” is sent to the gatekeeper indicating the gateway cannot accept any more calls. When the port utilization reaches the low-threshold, it sends a RAI message with “OutOfResouce” filed “FALSE” to the gatekeeper. So that it can receive calls from gatekeeper again.

Commands & Syntax

Configure Resource threshold

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **gateway**	Move to Gateway configuration mode.
3	(config-gateway)# **resource threshold** **{ high threshold | low threshold |<cr> }**	Set Resource threshold parameters. Default: high threshold: 90%, low threshold : 70%

Disable Resource threshold

Step	Command	Remark
1	(config-gateway)# **no resource threshold**	Disable Resource threshold.

Default : disable

28 E1 PRI Channel ID Information (Called Party Gateway)

When a gateway with E1 PRI interface gets a call from PABX, it receives Channel ID information in Q931 Setup message normally. However, sometimes, this is not the case and the call is not established. With version 8.10, the called gateway sends Channel ID in Call Proceding message if there is an available channel.

Commands & Syntax

None

29 Out-barred-group in Pots (voip)-peer

When a call is initiated via a Voip or Pots peer and its called party numbner is listed in a pattern-group, the call is restricted.

APOS Command Script:
Restrict the called party number starting with 0001, 0002 and 10

```
!
! Voip peer configuration.
!
dial-peer voice 1000 voip
  destination-pattern T
  session target ras
  dtmf-relay h245-alphanumeric
  out-barred-group 0
!
!
!
!
!
!
gatekeeper
!
!
! Gateway configuration.
!
gateway
  h323-id AddPac-GW
  gkip 192.168.0.10 1719 128
  register
!
!
! Dial Pattern Group configuration.
!
dialpattern-group 0
  pattern 0         0001
  pattern 1         0002
  pattern 2         10T
!
```

Commands & Syntax

Configure Out-barred-group

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **dialpattern-group <tag>**	Create Out-barred-group.
3	(config-dialpattern-group#0)# **pattern** **{ <tag> | dial pattern }**	Set the numbers to bar.
4	(config-dialpeer-voip-xxx)# **out-barred-group <tag>**	Apply the group to a voip or pots peer.

Disable Out-barred-group

Step	Command	Remark
1	(config-dialpeer-voip-xxx)# **no out-barred-group**	Disable out-barred-group on a voip or pots peer.
2	(config)# **no dialpattern-group <tag>**	Disable Out-barred-group.

Default : disable

30 AP160 IDLE Timer

In Keep Active mode, AP160 automatically terminates the Internet connection if there is no VoIP call attemps for a certain period. AP160 trys the connection again with a VoIP call attemp. In this case, there should be no local network behind the gateway. So this feature is not able to utitlize together with IP share or NAT/PAT function.

Commands & Syntax

Configure IDLE timer

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **dial-peer pstn-switch** **{ # | * |hook | none }**	Set PSTN Switching.

Disable IDLE timer

Step	Command	Remark
1	(config)# **dial-peer pstn-switch none**	Disable PSTN Switching.

Default : disable

31 AP160 PSTN Switching

The user can make PSTN direct call via AP160. When the line is hook-off, press the preconfigured key (#, * or hook-flash), then the gateway tries a PSTN call, not modem connection. So the user can hear PSTN dial-tone.

To use this feature, diable keep active mode.

Commands & Syntax

Configure PSTN Switching

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **dial-peer pstn-switch** **{ # | * | hook | none }**	Enable PSTN Switching.

Disable PSTN Switching

Step	Command	Remark
1	(config)# dial-peer pstn-switch none	Disable PSTN Switching.

Default : disable

32 SIP 183 Session Progress

When a call is received on E1, T1 (R2 DTMF), E&M and FXO voice interface, it transmitts SDP and 183 Session Progress message.

With previous version, it only transmits 180 Ringing message.

33 Improved Performance

The VoIP call processing capacity of all AddPac gateways improved 10% with the version 8.10.

Modifited Software Features

34 FTP data port chnage

With previous software, ftp port change command only changed the signal port, but not the data port. With APOS version 8.10 both the signal port and the data port are changable.

Commands & Syntax

FTP port change

Step	Command	Remark
1	# # **config**	Enter APOS Configuration Mode.
2	(config)# **service-port ftpd 64X 65X**	Set the signal and data port.

Disable FTP port change

Step	Command	Remark
1	(config-voice-port-0/0)# **no service-port ftpd**	Set as defult ports.

Default : signal port (TCP 21) / data port (TCP 20)

Removed Software Features

35 Announcement

The below models do not support announcement feature.

Model: AP200D, AP200E, AP1002, AP1005

36 Gatekeeper

The below models do not support gatekeeper feature.

Model: AP160, AP200 series, AP1005

37 Web-base management

The below models do not support Web-based management.

Model: AP200D, AP200E

38 CLI Ez-Setup

AddPac VoIP gateways do not support CLI ez-setup commands.

Fixed Bugs

39 “no ems server”

When ems is disabled (no ems sever), it reboots in 3~4 seconds.

40 SIP record routing field

Without refering to “Record-Route" field, it sends Response message(ex; ACK, BYE...) with the address in FROM field, so the messages send to the calling gateway directly when interoperating with SIP Proxy severs. With this version, the Response message is sent to the adddress in “Record-Route" field.

41 Call-Pickup

With version 7.01, call-pickup is not working properly.

42 Voice Confirmed Connection

When Voice Confirmed Connect is configuration, FAX is not working properly.

43 Ease-Setup (GUI)

Easy-Setup (GUI) configration is not saved . (AP160)

44 Call History Time Information with NTP

The call history information is not displayed properly with NTP. (Duration is marke as ‘0’ or “–‘).

45 RADIUS Messages

- Acct-Session-Time field
  The field value is marked as “-“.
- Two Stop Radius Messages with polarity Inverse function

When polarity inverse is enabled, it sends Radius stop message twice, once with polarity inverse and twice with the call disconnection. With this version, it only sends the message once with the call disconnection.

- Acct-Delay-Time filed
  When RADIUS message is retransmitted, the Acct-Delay-Time of 2nd or 3rd retry message is not correct.
- NTP sinycronization problem with the RADIUS STOP message
  With NTP, the call stop time in RADIUS STOP message is not matched with the real time.

Known Bugs

46 Changing Static IP to PPPoE (ADSL)

When static IP address is changed to PPPoE, the gateway is not able to get the new IP address. Restart the gateway after savinng the PPPoE setting.

47 PPTP Error

Routing service is not working proplery when the IP address of PPTP interface and the IP address assigned by PPTP Server are on the same network.