AddPac VoIP Gateway Series

Release Note

V7.01

AddPac Technology, Co. Ltd.

2/3 fl., Jeong-Am Building., 769-12 Yoksam-dong

Kangnam-ku Seoul, Korea 135-080

Phone: (82 2) 568-3848

Fax: (82 2) 568-3847

E-mail : info@addpac.com

http://www.addpac.com

[Table of Contents]

1. New Features

1.1 Numbering-type

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

Commands

(config)# dial-peer voice X <pots | voip>   → X : Identifier
(config-dialpeer-pots-0)# numbering-type ?
   abbreviated   Abbreviated representation of the complete number
   international   International numbering type
   national   National numbering type
   network   Administrative or service number
   subscriber   Subscriber number in a local network
   unknown   Unknown type

   default :   unknown

1.2 FXO port Polarity-Inverse detect

The FXO ports of the gateway detect the polarity inverse signal which is generated by PBX.   The same configuration is able to apply on FXS ports.   In this case, the FXS ports of the gateway generate the polarity inverse signal and the signal is transmitted to PBX.

When there is 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.

When there is 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.

Commands

(config)# voice-port <slot / port>
(config- voice-port-0/0)# polarity-inverse

default : disable

1.3 FXO port Caller-id detection feature

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 FXO port, the calling party number at the VoIP setup messages is used as the caller-ID and passed to the telephone or PBX.

Note that this feature is available when the PSTN/PBX or the telephone connected to FXO/FXS support the Caller-ID generation/detection.

The caller-ID information is detected on the FXO port between the first and the second ring.

Command

(config)# voice-port <slot / port>
(config- voice-port-0/0)# caller-id <enable | name | type>

enable: Enable the caller-id detection feature. (Default: disable)
Name: Detects the name field of the caller-id information. (Default: disable)
Type: Configure the Caller-ID type according to the specific country's standard.
(Default: bellcore [korea, usa])
    Bellcore | etsi | etsi-dtmf | etsi-dtmf-prior-ring | ntt

default : disable

1.4 E&M features

"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 while interfacing with the PBXs comply with the ACK signal standard.

Commands

(config)# voice-port <slot / port>
(config- voice-port-0/0)# signal wink-without-pulse

default : disable

1.5 VRRP (Virtual Router Redundancy Protocol)

VRRP allows several routers to utilize the same virtual IP address and assigns one of the routers acting as the Master. 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.   At least 2 routers should be on the same LAN.

This feature is only implemented on the models supporting the dynamic routing protocol such as AP2850, AP2830, AP2520.   At the next release, VRRP will be implemented by all the models.

Commands

(config)# interface Ethernet 0.0
(config-ether0.0)# VRRP ?
   <1-255>   the group-id of the virtual server (Assign an ID to the VRRP group.)
(config-ether0.0)# vrrp 1 ?
   authentication   Set the authentification type
   ip   The ip address(es) of the virtual server
   mac   Set Virtual Interface Mac Address
   preempt   Enable the preemption mode (Enabled by default)
   priority   Set the priority of this host(default:100)

timers   Set VRRP Timer variables

ip : Assign a virtual IP address to the VRRP group.

Mac: Set whether to send the virtual MAC address or physical MAC address at the ARP message. (Default: virtual)

Preempt: When a new router is included at the existing VRRP group and it has the higher priority than the active system, it can operate as the Master router. (Default: on)

Priority: Specifies the priority among the routers of the 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 high IP address has the higher priority. (Default priority: 100)

Timers: Sets the VRRP advertisement time.   It indicates the time interval for the Master router multicasting VRRP advertisement packets.   If there is no VRRP advertisement packet during the time, the backup routers send VRRP advertisement packets.   Then decides the priority with the received advertise packets and then the new Master router is decided.   The Timer value of the routers of one VRRP group should be identical. (Default: 1 sec)

Note: VRRP is only applied to Ethernet Interface. VRRP is a Multicast-Protocol and "**Line-ctrl multicast-all**" command should be implemented on the interface.   To check the VRRP status, use "**Show VRRP**" command.

1.6 Gateway history

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

Command

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

1.7 StartH245 feature

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

Command

(config)# voice service voip
(config-vservice-voip)# force-starth245 ?
 <cr>
 calling-only   Only the calling party send starth245

default : disable

1.8 OpenLogicalChannel negotiation feature

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.

Command

(config)# voice service voip
(config-vservice-voip)# ignore-reverse-channel-info

default : disable

1.9 Chinese announcement feature

The Chinese announcement is added.

Command

(config)# voice service voip

(config-vservice-voip)# announcement ?

element   enable each element

language   set language

<cr>   enable all elements

(config-vservice-voip)# announcement language ?

chinese   Chinese

dutch   Dutch

english   English

korean   Korean

Default: Korean

1.10 Modified or newly added SIP features

1. 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.

Command

(config)# dial-peer voice 0 pots

(config-dialpeer-pots-0)# ?

    user-name   set username of dial peer

    user-password   set password of dial peer

(config-dialpeer-pots-0)# user-name <string>

(config-dialpeer-pots-0)# user-password <string>

When the User-name and password of the dial-peer are not configured, the destination-pattern number is utilized for the user name and the password of sip-ua is utilized as the user-password.

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"**.

2. BYE Authentication feature

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.

3. 183 Session Progress message transmission feature

When a call is received on E1, T1 (R2 DTMF), E&M, FXO interface, the gateway transmits SDP and **183 Session Progress** message.

At the previous release, **180 Ringing** message is transmitted.
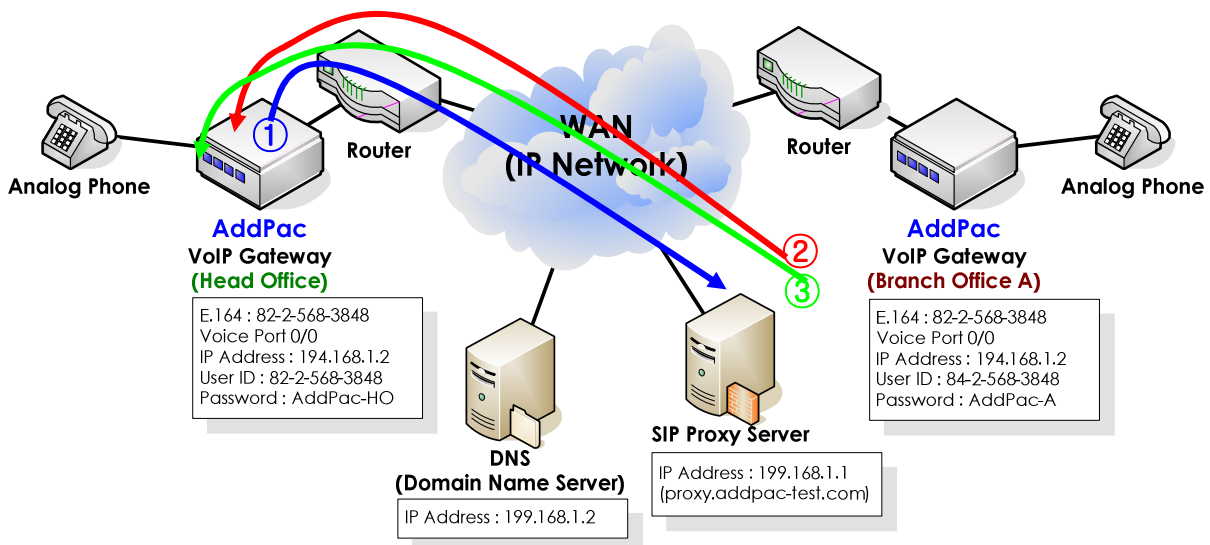
4. Registration with User-name

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.
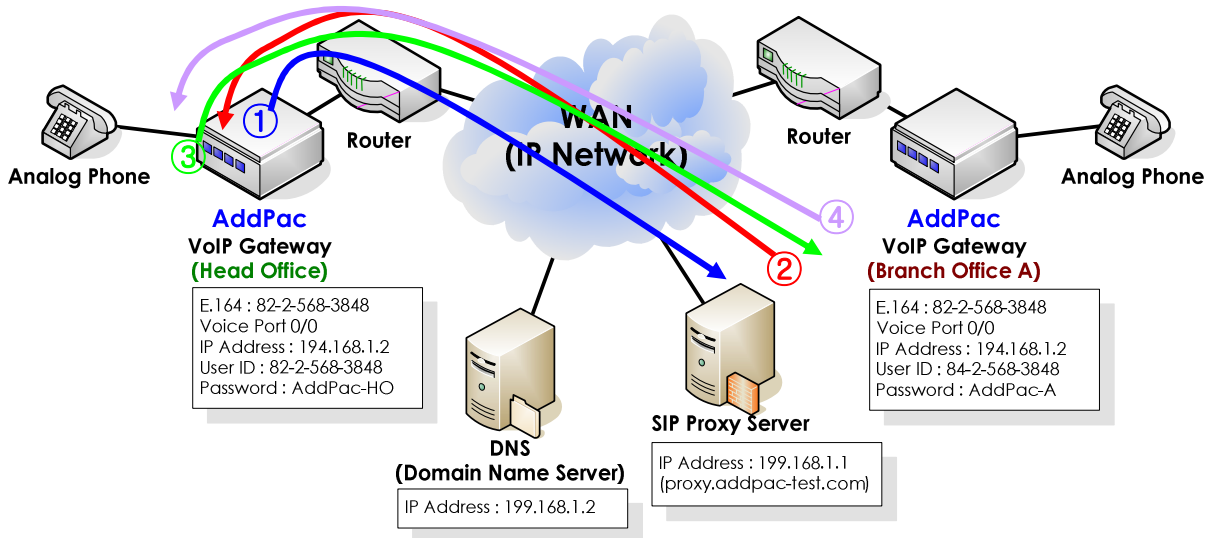
Example:

➢   1. SIP Registration without Authorization

Network Diagram

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)**

> 2. SIP Registration with Authorization

Network Diagram

① **AddPac Gateway transmits the register message to the Proxy**

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

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

④ **Proxy transmits 200 OK 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.

① **SIP supports Dial-Peer Destination-pattern (E.164) Registration**

When transmitting REGISTER message, use the destination-pattern of the dial dial-peer voice X pots as the USER-ID.   The gateway 1 transmits Registration message to the Proxy server.

!

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

② **SIP supports Dial-Peer User-name Registration**

When transmitting REGISTER message, use user-name <string> as the user ID instead of the destination-pattern of the dial dial-peer voice X pots.   The gateway 1 transmits Registration message to the Proxy server.

!

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

③ **SIP supports Dial-Peer User-name 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
!
```

④ **SIP supports Sip-Username 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
!
```

⑤ **(Example)**

Tries to register with User-ID(E.164) and authenticates with Global user-name/ user-password.

The below is the sample configuration when the gateway is registered with the E.146 number of each dial-peer and authenticated with one global user-name and password.

(Sample config)
```
!
dial-peer voice 0 pots
   destination-pattern 8225683848
   port 0/0
!
sip-ua
 sip-server 199.168.1.1
 sip-username AddPac-HO
 sip-password AddPac-password
 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

Received SIP PDU from (199.168.1.1:5060)

SIP/2.0 **401 Unauthorized**

Via: SIP/2.0/UDP 194.168.1.1:5060;branch=z9hG4bK773f9b21a4139

To: <sip:8225683848@199.168.1.1>;tag=77bf2010

From: <sip:8225683848@199.168.1.1>;tag=773f9b21a4

Call-ID: 77cfc03f-a778-9bee-8021-0002a400380b@194.168.1.1

CSeq: 1 REGISTER

WWW-Authenticate: Digest

algorithm=MD5,nonce="1070376732",realm="127.0.0.1"

      Content-Length: 0

Sending SIP PDU to (199.168.1.1:5060) from 5060

REGISTER sip:199.168.1.1 SIP/2.0

Date: Wed, 26 Nov 2003 18:15:15 GMT

CSeq: 2 REGISTER

Via: SIP/2.0/UDP 194.168.1.1:5060;branch=z9hG4bK773f9b21a4140

User-Agent: AddPac SIP Gateway

Authorization: Digest   username="AddPac-HO",   realm="127.0.0.1",
nonce="1070376732", uri="sip:199.168.1.1", response="df522680b903ed
e5e7dce05612b8fa51", algorithm=MD5

From: sip:8225683848@199.168.1.1;tag=773f9b21a4

Call-ID: 77cfc03f-a778-9bee-8021-0002a400380b@194.168.1.1

To: sip:8225683848@199.168.1.1

Contact: sip:8225683848@194.168.1.1

Expires: 60

Content-Length: 0

Max-Forwards: 70

Received SIP PDU from (199.168.1.1:5060)

SIP/**2.0 200 OK**

Via: SIP/2.0/UDP 194.168.1.1:5060;branch=z9hG4bK773f9b21a4140

To: <sip:8225683848@199.168.1.1>;tag=1100e157

From: <sip:8225683848@199.168.1.1>;tag=773f9b21a4

Call-ID: 77cfc03f-a778-9bee-8021-0002a400380b@194.168.1.1

CSeq: 2 REGISTER

Expires: 60

Contact: <sip:8224583848@194.168.1.1>

Content-Length: 0

5. Registration Retry counter

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

Command

(config-sip-ua)# ?

  no   set to default configuration

register   try registration to sip registrar

retry-counter   set retry timer counter value

signaling-port   set SIP signaling port (default 5060)

sip-server   set a SIP Server Interface

sip-username   Set Username of SIP User Agent

sip-password   Set Password of SIP User Agent

timeout   Set timeout value

user-register   Set registration with username

end   Go to Top menu

exit   Exit from the EXEC

AP2520-B(config-sip-ua)# retry-counter ?

<3 - 10>   retry counter

Default: 10 times

2. Removed features

2.1 Announcement

The below models do not support the announcement feature.

Model: AP200D, AP200E, AP1002, AP1005

2.2 Gatekeeper

The below models do not support the built-in H.323 Gatekeeper feature.

Model: AP160, Ap200 series, Ap10XX series, AP1100 series, AP1005

2.3 Web-base management

The below models do not support the Web-based management feature.

Model: AP200D, AP200E

2.4 CLI Ez-Setup

AddPac's all models do not support CLI ez-setup command.

Please download the Easy-setup (GUI) for www.addpac.com for easy configuration.

3. Bug fix

3.1 Dynamic IP problem

On the ADSL dynamic IP environment, the gateway's IP address changes without terminating PPP session.   In this case, the VoIP listening-port's IP address is not changed properly, thus affects the VoIP call.

3.2 Ease-Setup (GUI)

With AP160 model, after changing the configuration with the Easy-Setup (GUI), the new configuration is not saved properly.

4. Known Bug

4.1 "no ems server" command error

When disabling ems server feature, the gateway might reboot in 3~4 seconds after executing "no ems server" command. In this case, the gateway reboots before saving the configuration and turns to the default setting. Thus follow the below configuration update method.

Configuration update via FTP

Access to the gateway via FTP and download the configuration file (config.cfg) to the PC. Open this file with text editor program, and remove the configuration related to EMS-Server. Save the changed configuration file and upload it to the gateway. After restarting the gateway, the new configuration is applied. Refer to FAQ on our website (http://www.addpac.com/english/faq_1.html#1) for the information on the configuration download and upload via FTP.

Command
no ems server

Bug Fix
Next release.

4.2 Call Pick-up function error

The bug was found for "Call Pick-up" function at version 7.01 only. Do not use call pick-up function with version 7.01. Any other version (except for version 7.01) should be used if call pick-up function is needed.

4.3 call history information error under NTP

The bug was found which call history problem regarding time information if users setup NTP. Any other version (except for version 7.01) should be used if call history information is needed under NTP environment.