iPECS is an Ericsson-LG Brand

Unified SIP Features

(iPECS-SMB-TRA-01-030)

13 Oct, 2017

Ericsson-LG Enterprise

iPECS Your Communications Solution

REVISION HISTORY

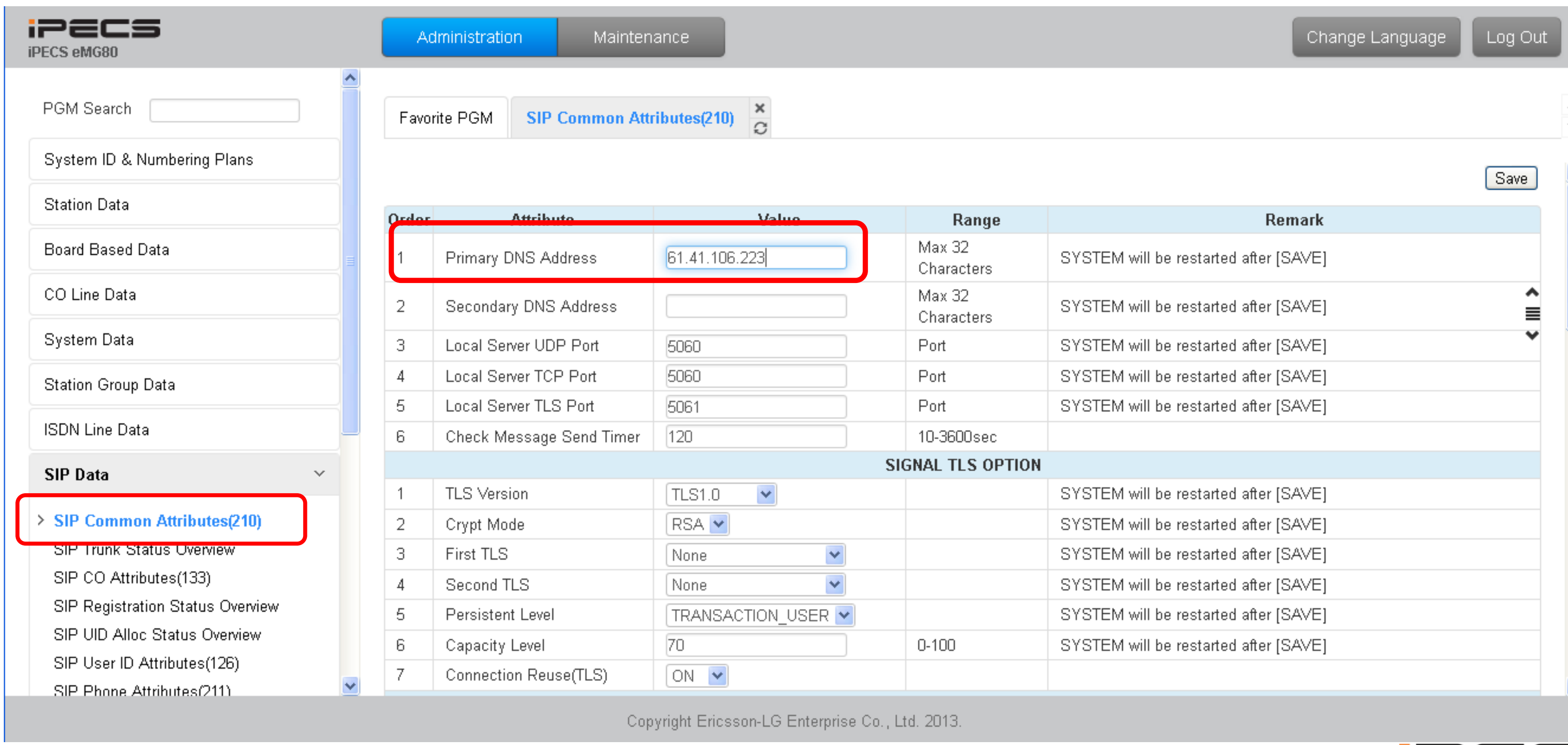
ISSUE	DATE	DESCRIPTION OF CHANGES
1.0	13-Oct-17	Preliminary release

Table of Contents

Basic Configuration

PGM 210

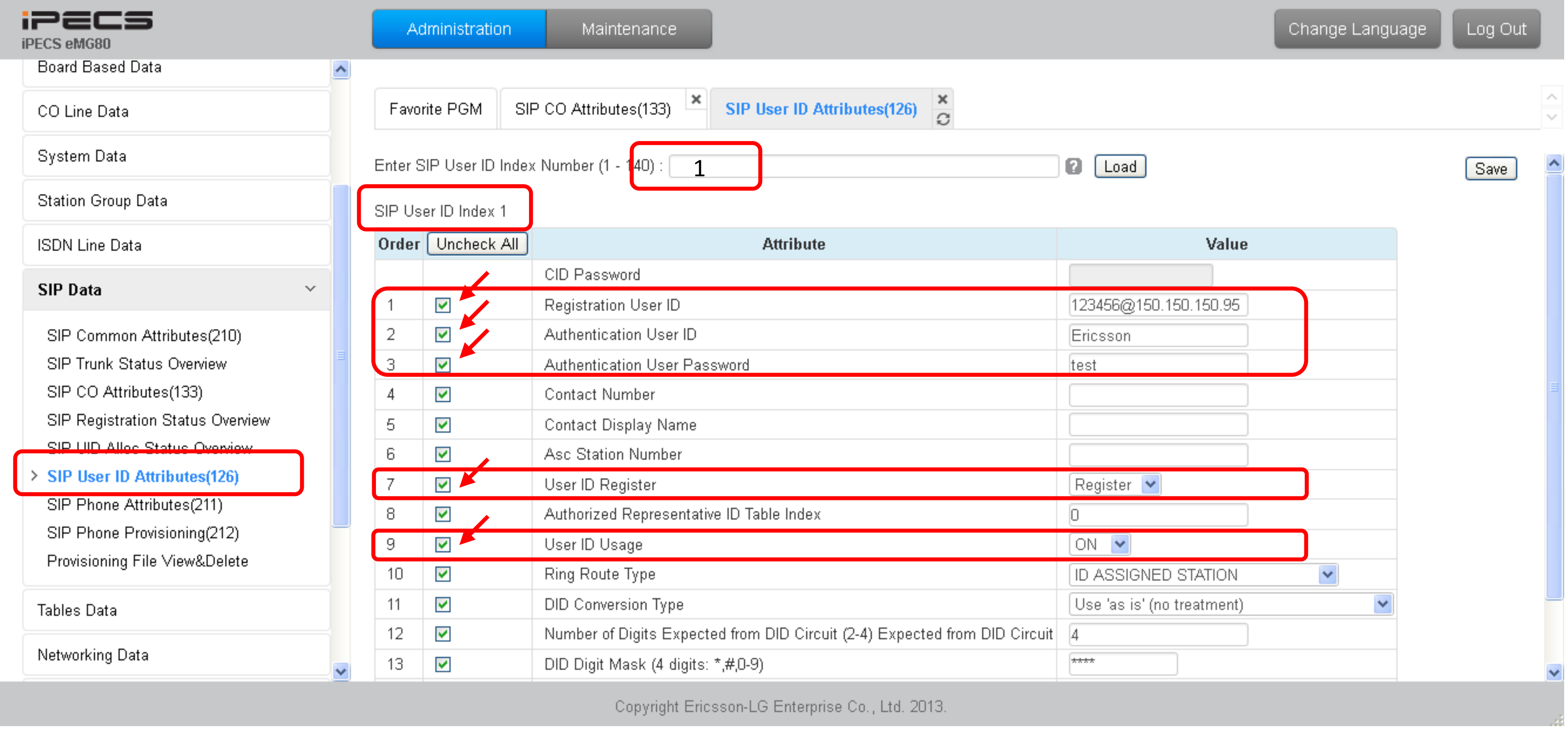
- Enter DNS Address
  - If Domain Name is used for SIP server, DNS Query will be sent to DNS Address.



Basic Configuration

PGM 126

- Enter Registration ID – check **[CheckBOX]** before saving data.
  - Enter index number and Click [Load] - index1 is used in capture.
  - Enter “Registration User ID” – ID@serveraddress.
  - Enter “Authentication User ID” and “Authentication User Password”.
  - Set “User ID Usage” – ON and set “User ID Register” – Register/Provision.

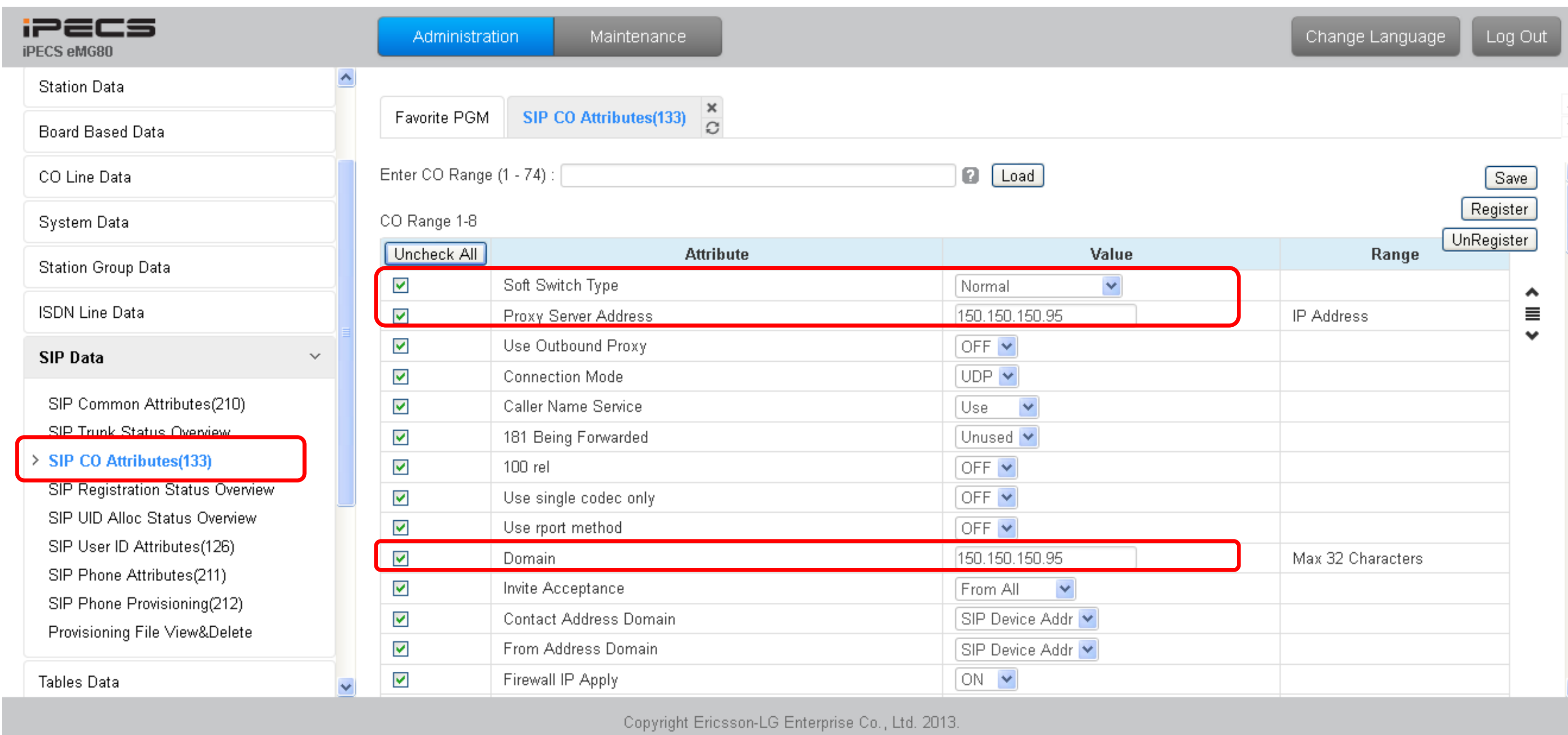


Your Communications Solution

Basic Configuration

PGM 133

- Soft Switch Type : It depends on the server type tested with LIK/eMG/UCP.
  - Default : Normal
- Proxy Server Address : SIP Server Address - IP Address or Domain.
- Domain : SIP Server Domain - IP Address or Domain.

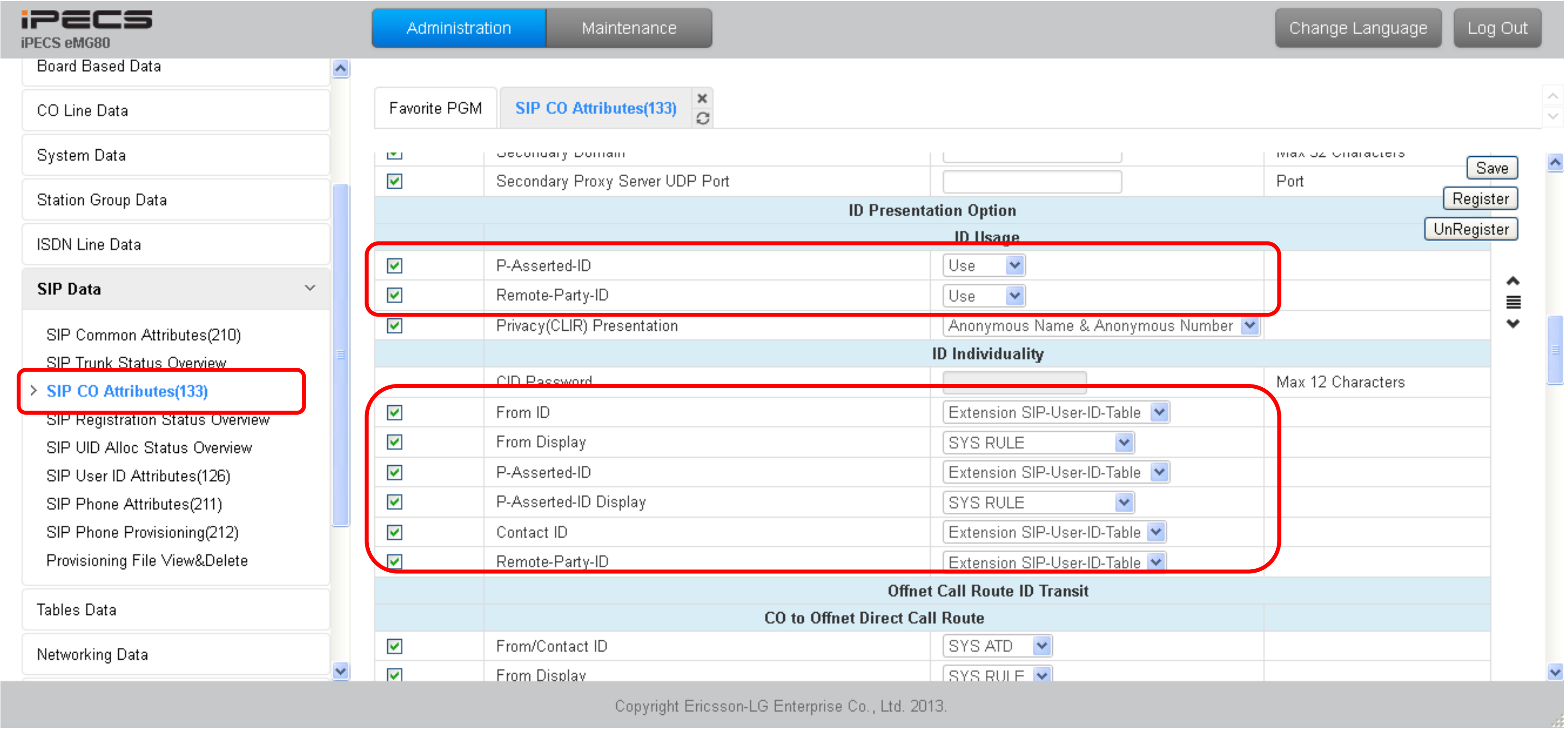


iPECS Your Communications Solution

Basic Configuration

PGM 133

- P-Asserted-ID, Remote-Party-ID :
  - Set Usage of P-Asserted-ID and Remote-Party-ID
- From ID, P-Asserted-ID, Contact, Remote-Party-ID
  - Select outgoing CLI rule.



Basic Configuration

PGM 133

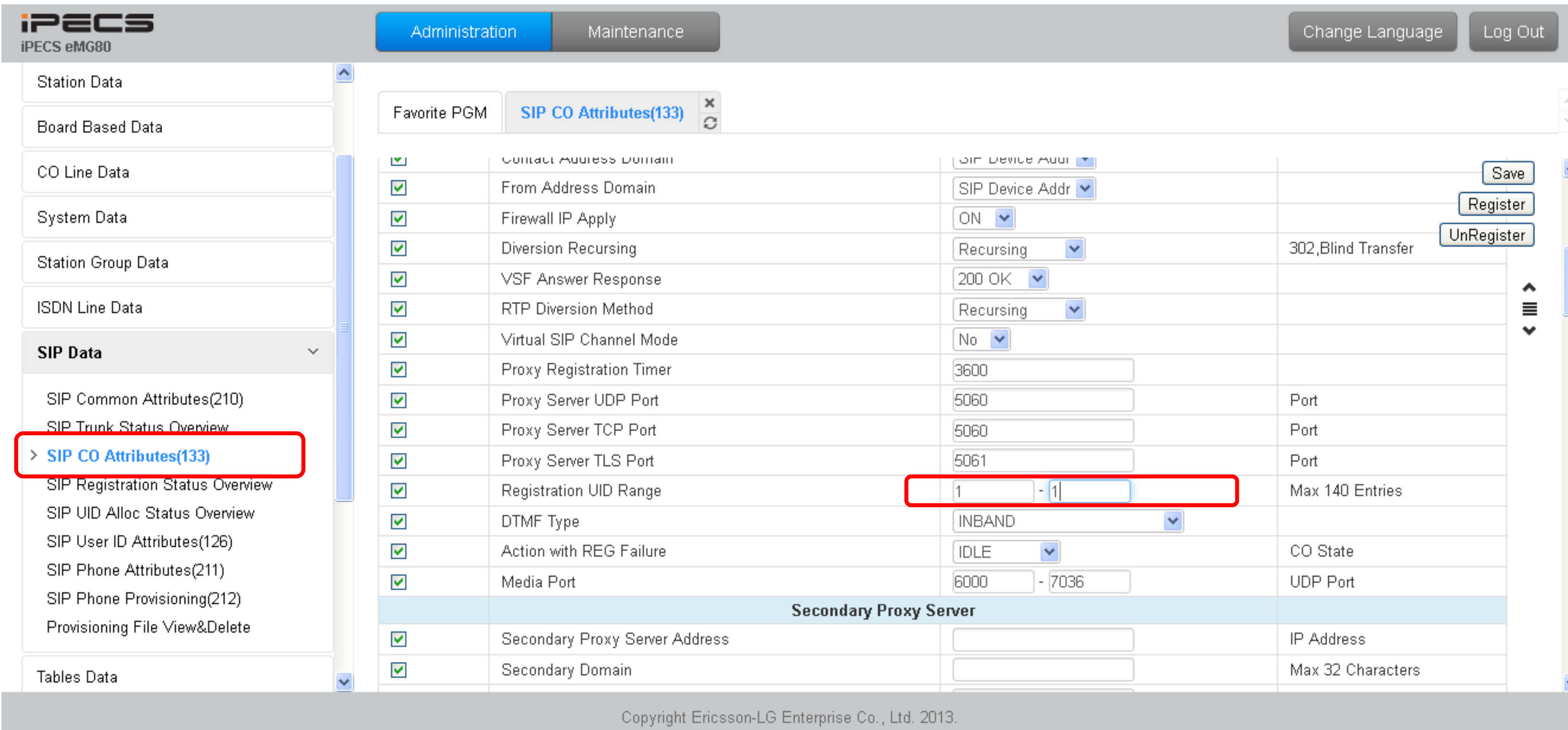
ID Settings	Description
Extension SIP-User-ID Table	• Follow PGM111 - SIP USER TABLE INDEX number. • SIP USER TABLE INDEX number must be set PGM126-index.
Extension Outgoing CLI	• Follow ISDN Outgoing CLI rule. • PGM113, PGM151, PGM201 ..
Authorized Representative ID	• Follow PGM126 - Authorized Representative ID Table Index
Fixed Table	• Follow PGM133 - SIP User ID Fixed Table Index • Normally main ID will be used.
Original CLI	• Use CLI of incoming Trunk. – Call Forward, Call Transfer case.
Extension	• Follow PGM133 - ID Individuality- From ID.

Display Settings	Description
SYS RULE	• Use Station Name of related station. - Normal outgoing call : name of outgoing station. - Call forward : name of forwarding station - Co-Co Call forward : name of attendant station.
Original	• Use name received from incoming Trunk. If there is no name, CLI will be used as diaplay.

Basic Configuration

PGM 133

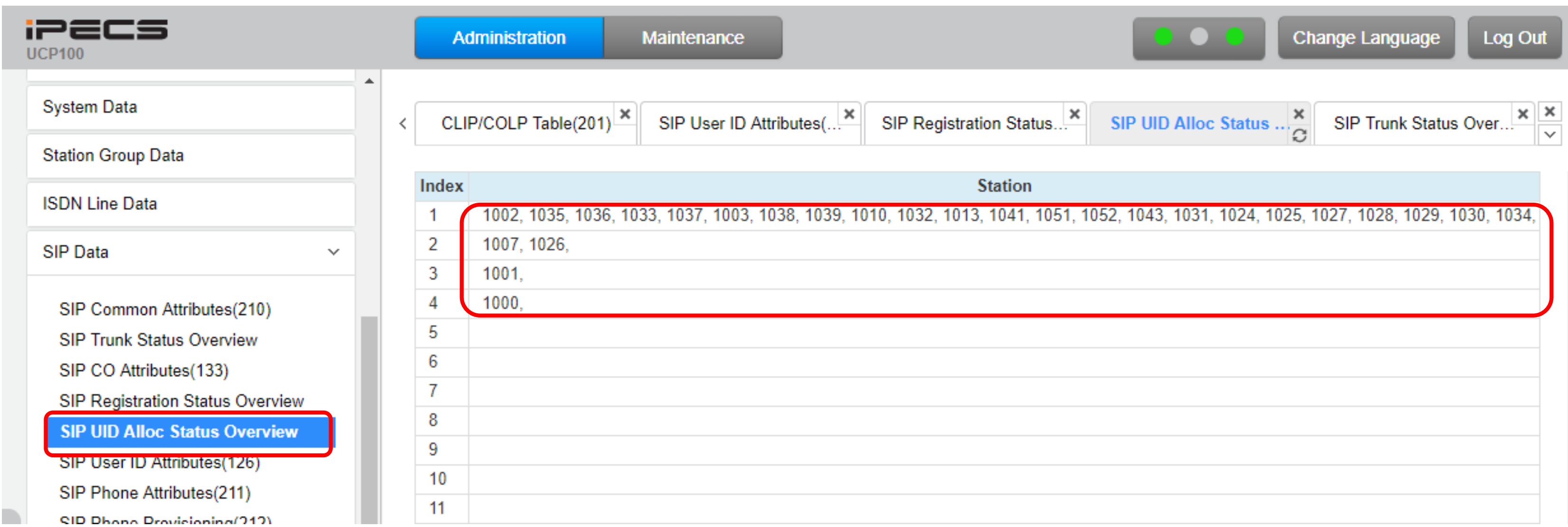
- Registration UID Range: Enter index number of PGM126 related with Registration ID



Basic Configuration

SIP UID Alloc Status

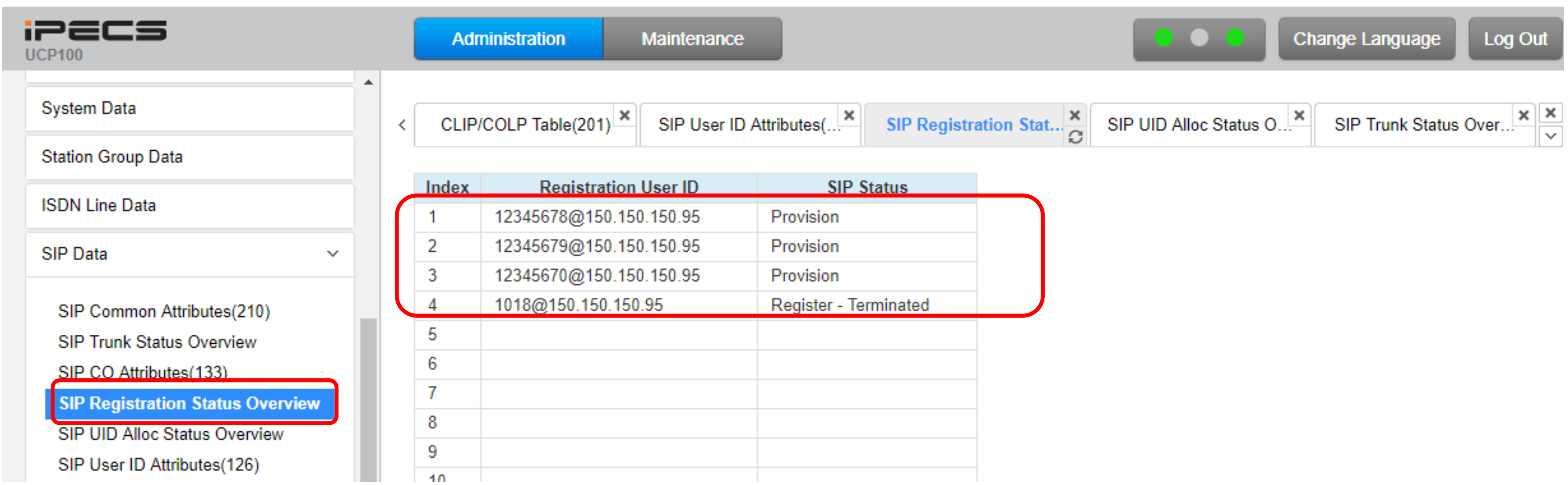
- User can see the ID allocation status.



Basic Configuration

SIP Registration Status

- User can see the Registration status.
  - Register/Provision
  - Registration Status in case of Register

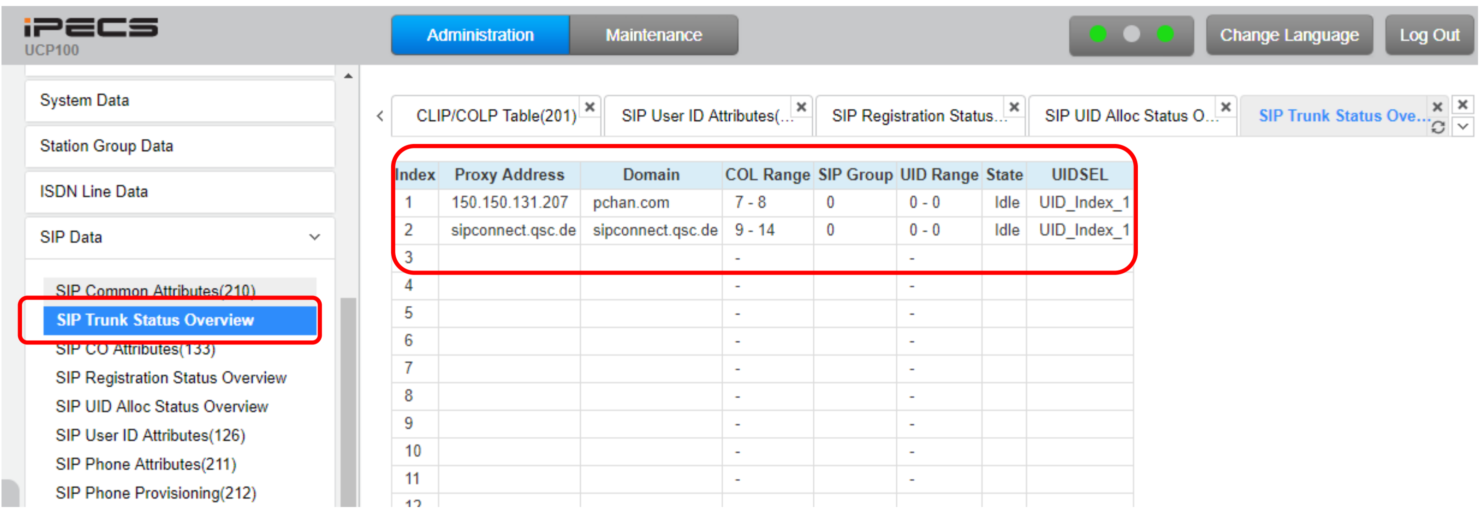


iPECS
Your Communications Solution

Basic Configuration

SIP Trunk Status

- User can see the Admin Status for Trunk
  - 150.150.131.207 for Trunk 7-8.
  - sipconnect.qsc.de for Trunk 9-14.



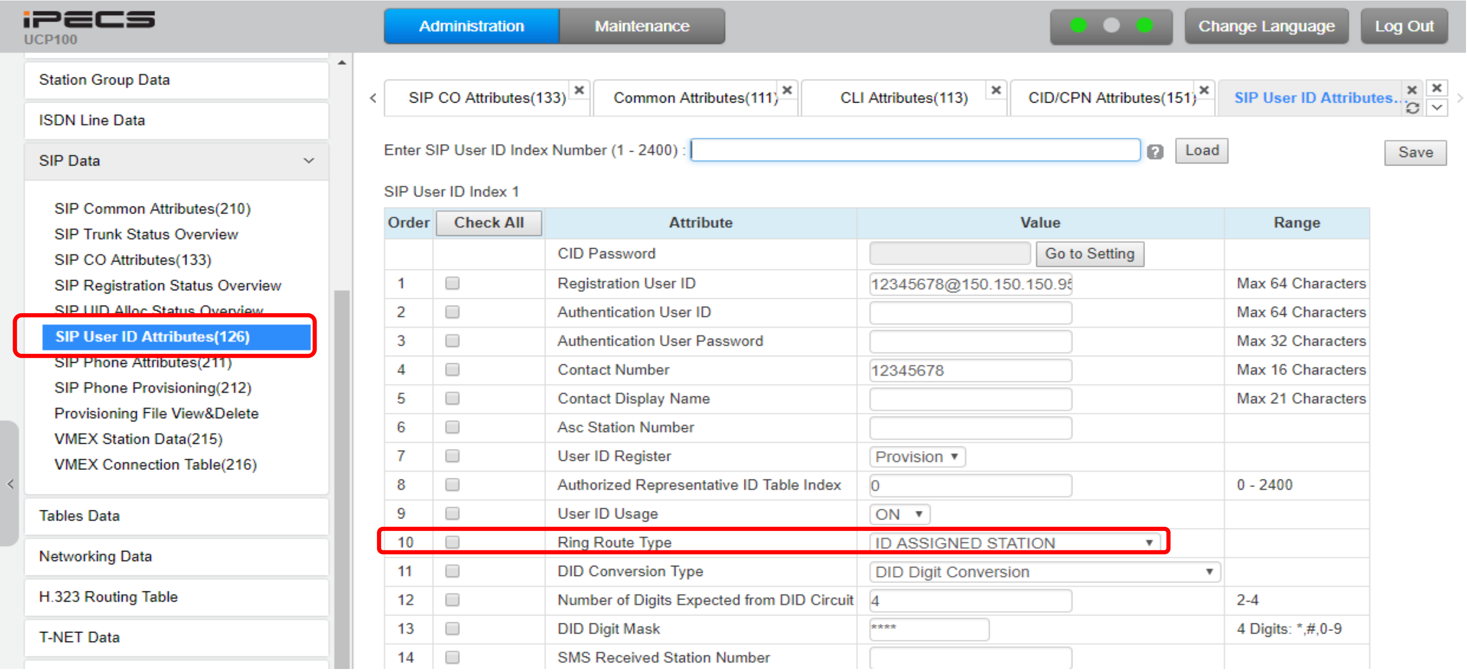
Index	Proxy Address	Domain	COL Range	SIP Group	UID Range	State	UIDSEL
1	150.150.131.207	pchan.com	7 - 8	0	0 - 0	Idle	UID_Index_1
2	sipconnect.qsc.de	sipconnect.qsc.de	9 - 14	0	0 - 0	Idle	UID_Index_1
3			-		-		
4			-		-		
5			-		-		
6			-		-		
7			-		-		
8			-		-		
9			-		-		
10			-		-		
11			-		-		
12							

Basic Configuration

Incoming call

- Incoming CLI is matched with PGM126 – index .
  - Follow PGM 126 - Ring Route Type.

  (ID Assigned station, Ring assignment, DID conversion, MSN-DID conversion)
- Incoming CLI is not matched with PGM126 – index .
  - Follow ISDN rule. ->PGM145, PGM151.



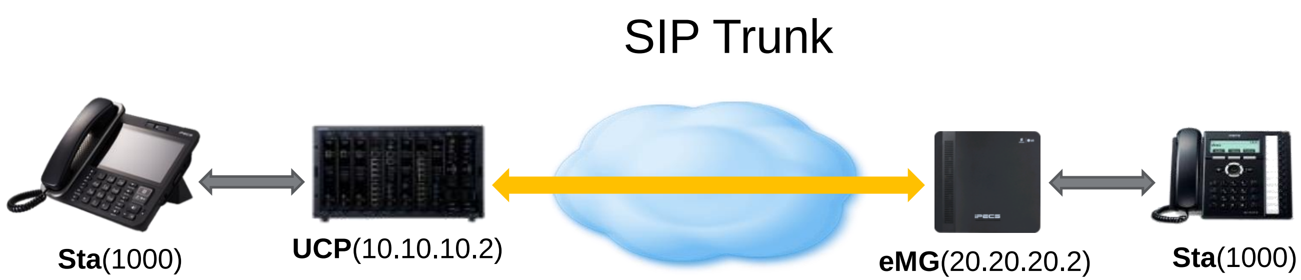
Your Communications Solution

Basic Configuration

Trunk configuration

- Configure Basic SIP configuration between UCP and eMG80.

Practice



Tel : 12341000

Tel : 56781000

Basic Configuration

Trunk configuration

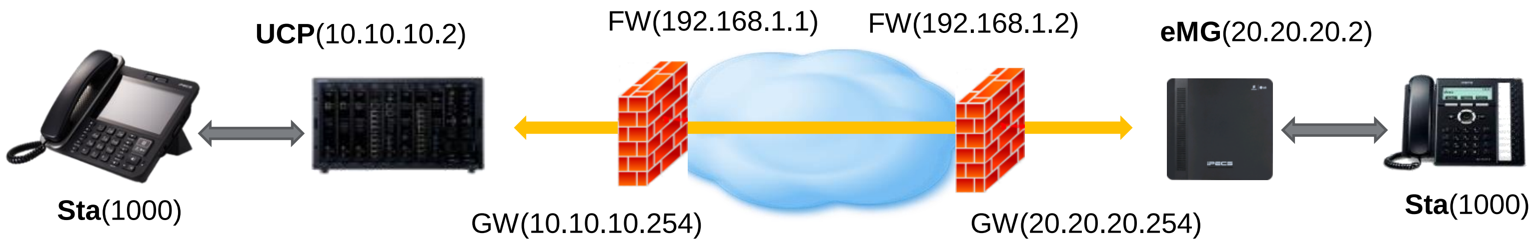
- Configure Basic SIP configuration with F/W device.
  - Set Port Forwarding in each F/W – SIP port and RTP ports
  - Set F/W IP in PGM102 - Firewall IP Address and PGM132 - Firewall IP Address.

UCP:

-. Slot number of VOIM (2402)

eMG80:

-. Slot number of VOIB (14)



Tel : 12341000

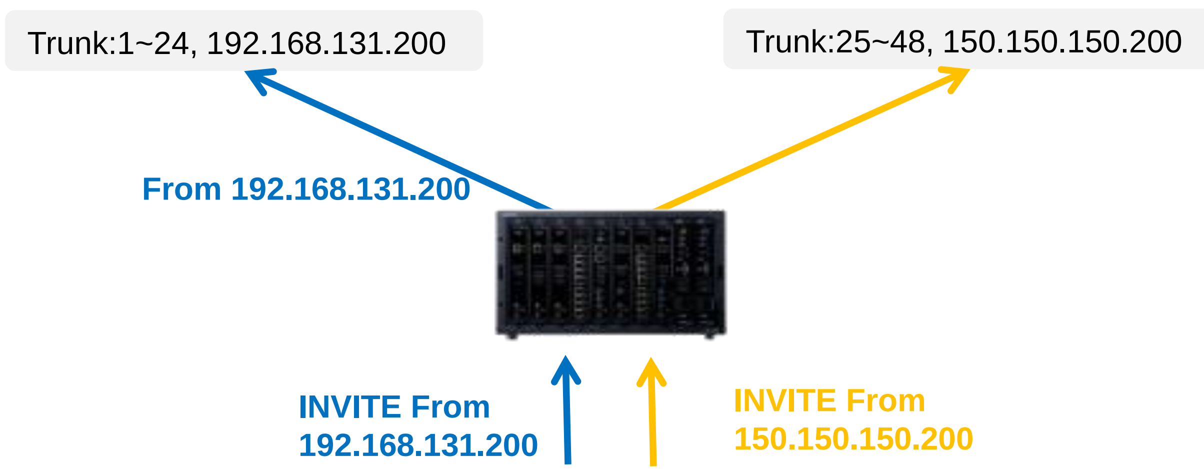
Tel : 56781000

Specific settings for SIP Service

SIP Group for SIP Trunk Control

All SIP Trunk will be grouped based on PGM133 – Proxy Server Address.

- For Co 1~24, Proxy Server Address is 192.168.131.200.
- For Co25~48, Proxy Server Address is 150.150.150.200.
- Then two SIP trunk Group will be stored. → Co range must be sequential.



Incoming SIP Call will be distributed
based on Server Address

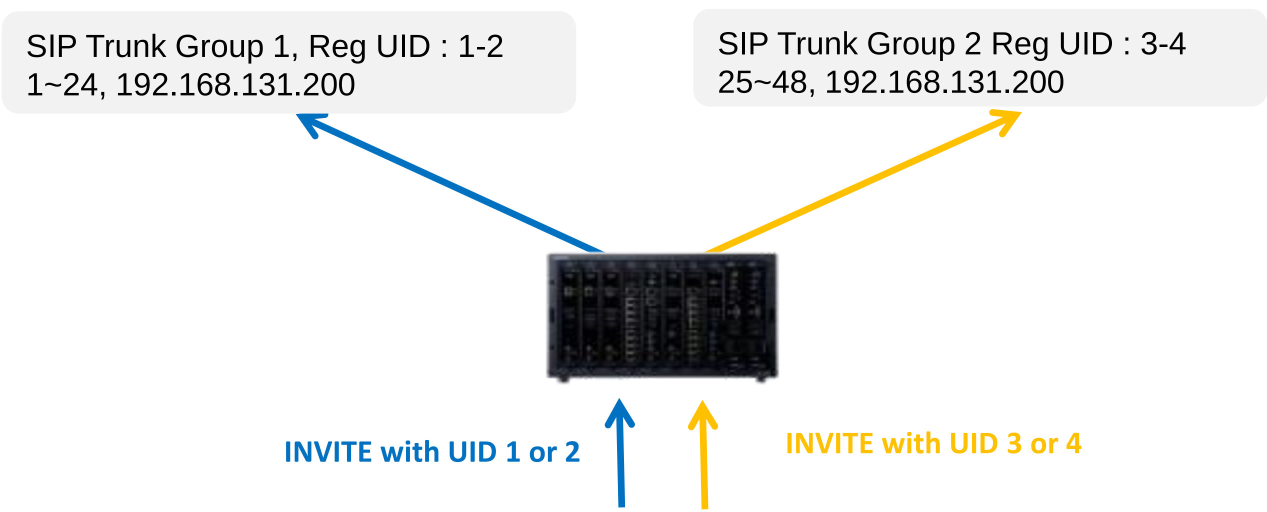
Specific settings for SIP Service

PGM133 - SIP Trunk Group

It is independent with PGM140 – CO/IP Group.

- SIP Trunk Group setting is just used in SIP Trunk.

With different PGM133-SIP Trunk Group value, it will be treated as different SIP Group even though PGM133-Proxy Server Address is same.



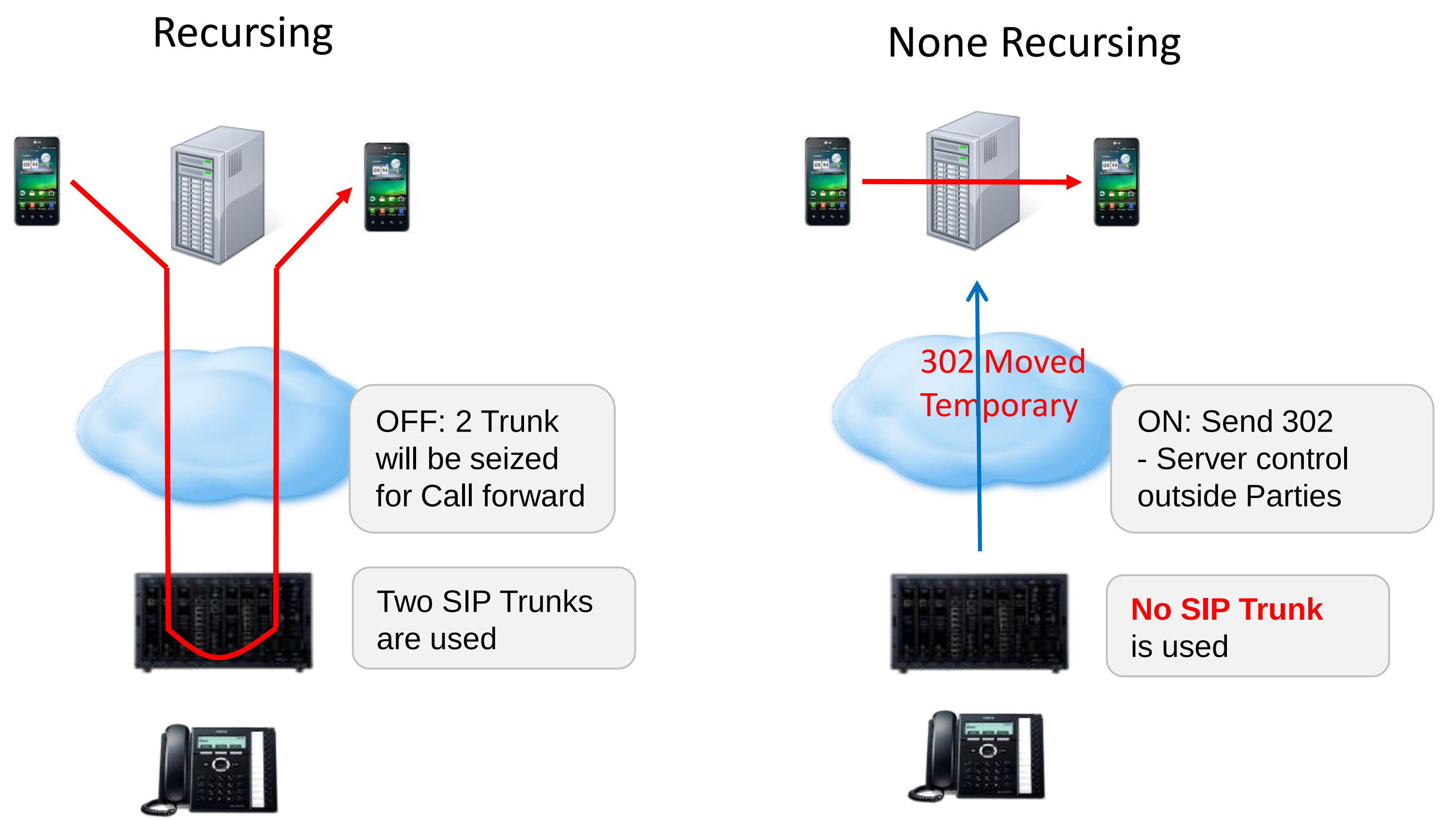
Incoming SIP Call will be distributed **based on Server Address & Reg UID in PGM126**

iPECS Your Communications Solution

Specific settings for SIP Service

PGM133 –Diversion Recursing

Some Proxy Server supports 302 response for Call Forward.

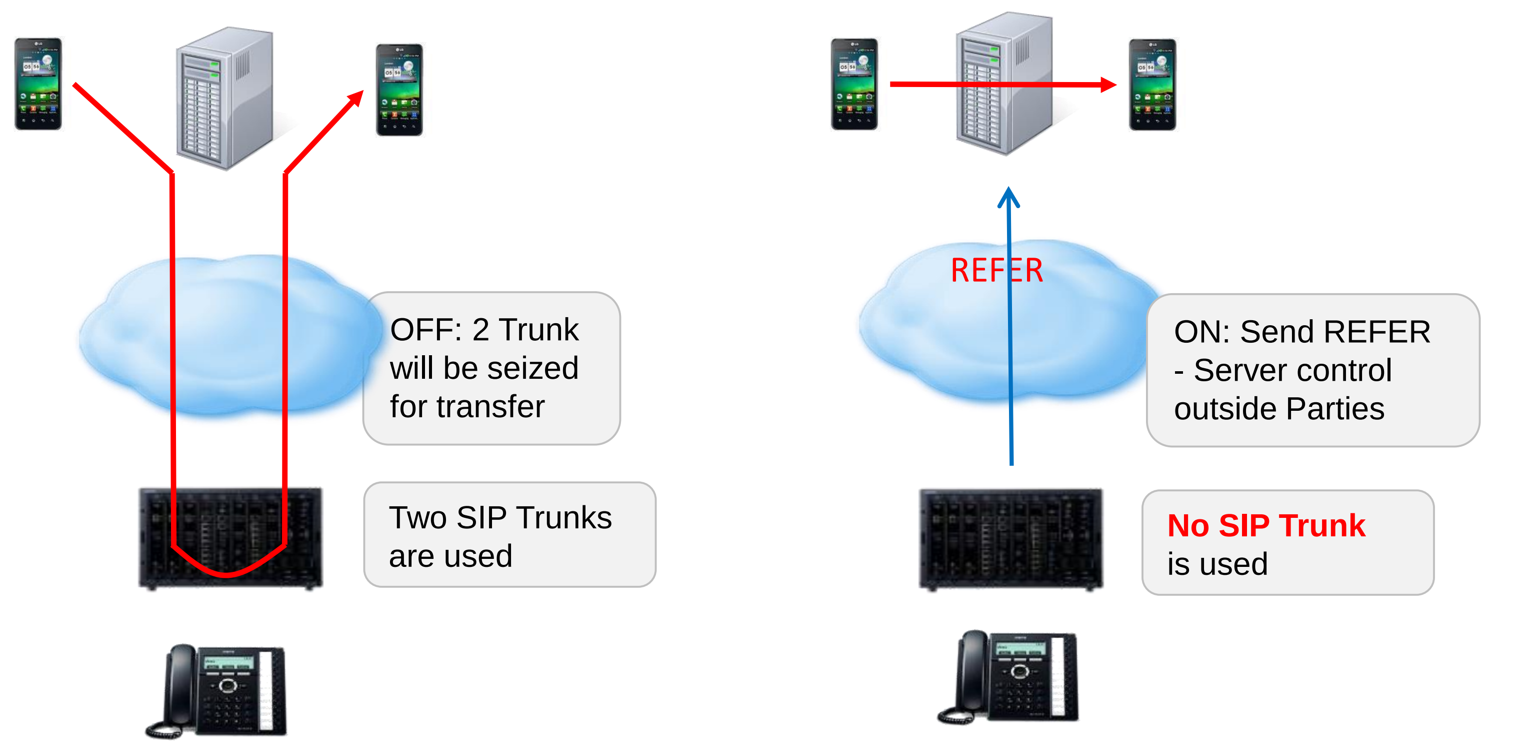


Specific settings for SIP Service

PGM133 – Send REFER for Transfer

Some Proxy Server supports REFER message for Transfer.

P133, “Send Refer for Transfer”



iPECS Your Communications Solution

Specific settings for SIP Service

PGM133 – SIP User ID SELECTION

PGM111- SIP USER TABLE INDEX, SIP USER TABLE INDEX2, SIP USER TABLE INDEX3 are used for different service provider.

PGM111

SIP USER TABLE INDEX	1
SIP USER TABLE INDEX 2	2
SIP USER TABLE INDEX 3	3

PGM126

SIP User ID Index 1

Order	Check All	Attribute	Value	Range
		CID Password	Go to Setting	
1	☐	Registration User ID	11111111@1.1.1.1	Max 64 Characters

SIP User ID Index 2

Order	Check All	Attribute	Value	Range
		CID Password	Go to Setting	
1	☐	Registration User ID	22222222@2.2.2.2	Max 64 Characters

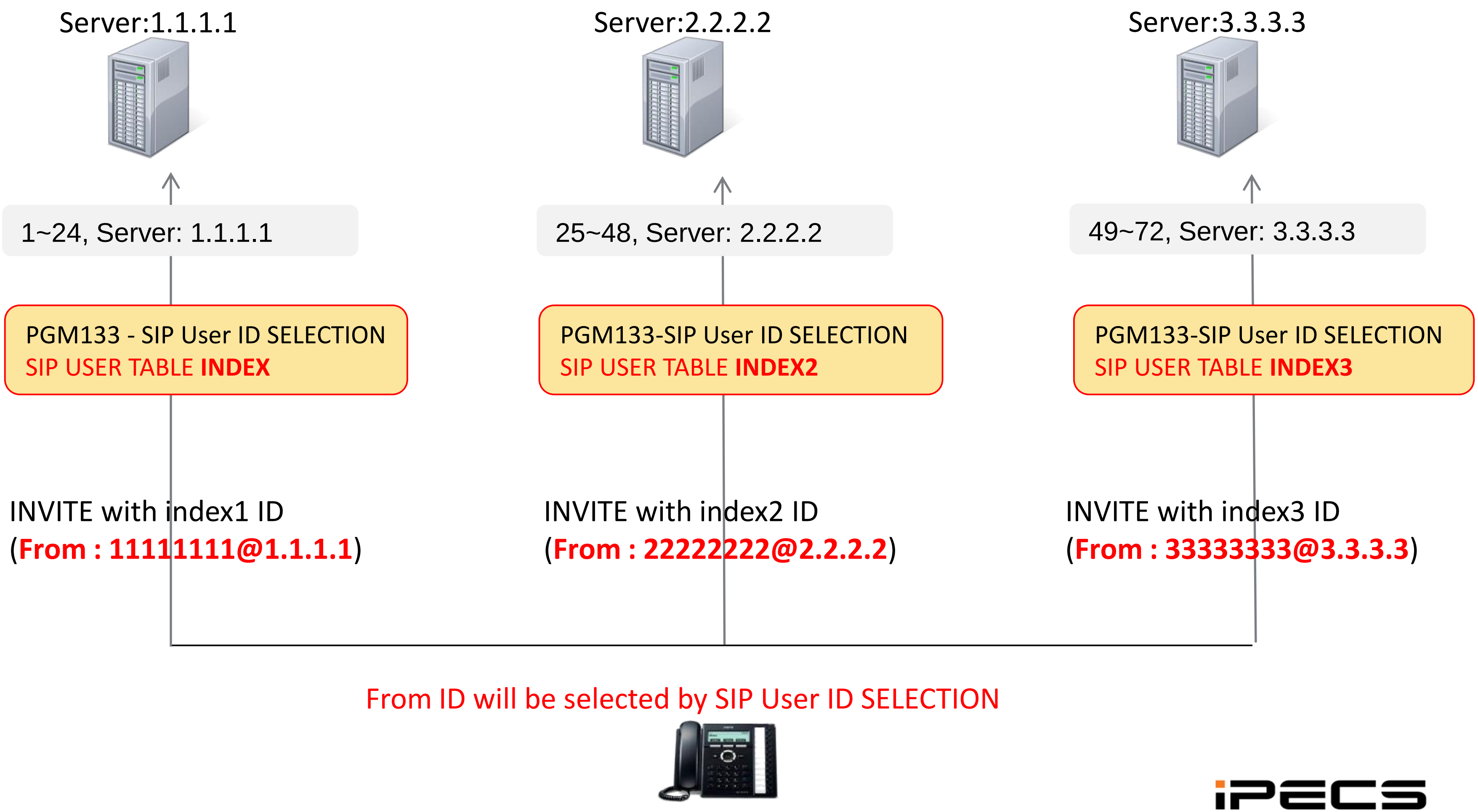
SIP User ID Index 3

Order	Check All	Attribute	Value	Range
		CID Password	Go to Setting	
1	☐	Registration User ID	33333333@3.3.3.3	Max 64 Characters

iPECS Your Communications Solution

Specific settings for SIP Service

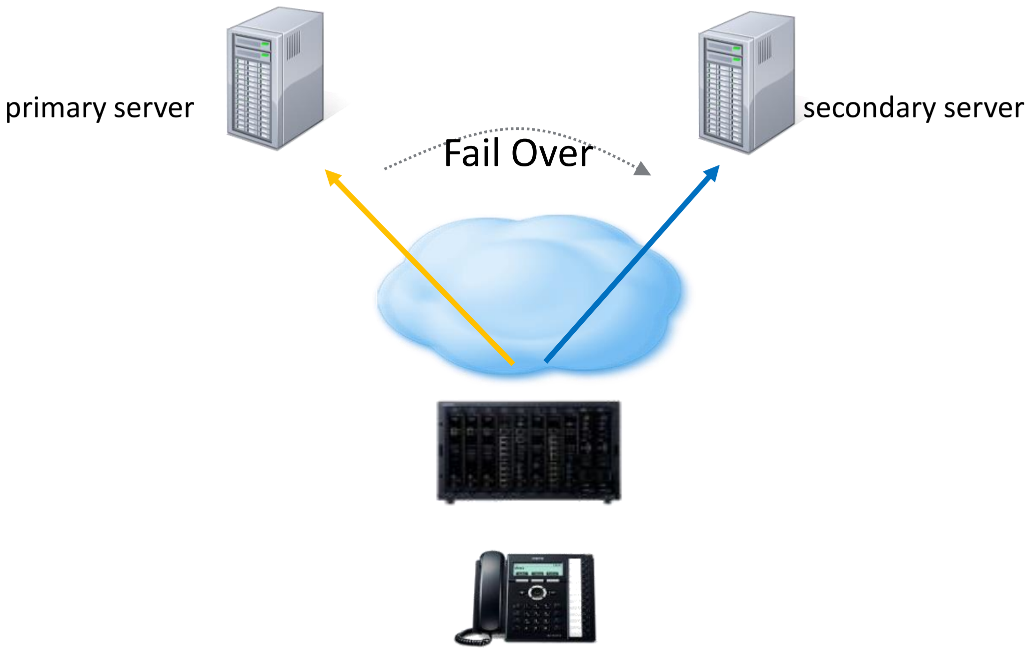
PGM133 – SIP User ID SELECTION



Specific settings for SIP Service

PGM133 – Secondary Proxy Server

- PGM133-Soft Switch Type : KT, KT Centrex.
  - Follow specific redundancy flow.
- PGM133-Soft Switch Type : Normal
  - PGM133-Redundancy Usage : Fail Over – If there is no response from Proxy Server.
  - PGM133-Redundancy Usage : Load Balancing – Use Proxy Server and Secondary Proxy Server evenly.



Specific settings for SIP Service

PGM133 – Soft Switch Type(DNS REDUN), PGM210 - DNS SRV Usage

- DNS Service Query is performed to get IP address.
- System sends INVITE to all IP addresses evenly.
- System accepts INVITE from all IP addresses.
- Example : Server Domain : sipconnect.qsc.de

59642320-[Sipm_SipTimerCallBack] DNS Redun, now!!!(Provider:2)
59642320-Sipm_GetDnsQueryResult Start: sipconnect.qsc.de
59642331-Sipm_SipResolverReportDataEv : mode=TRANSPORT BY NAPTR, nextmode=TRANSPORT BY 3WAY SRV, query=sipconnect.qsc.de
59642339-Sipm_SipResolverReportDataEv : mode=TRANSPORT BY 3WAY SRV, nextmode=IP BY HOST, query=sipconnect.qsc.de
59642339-Sipm_SipResolverReportDataEv Srv:1, Host:2, IP:0
59642339-Sipm_SipResolverReportDataEv : srv=_sip._udp.sipconnect.qsc.de (SIP service query)
59642339-Sipm_SipResolverReportDataEv : host=duro01.sipconnect.qsc.de, priority:10, weight:10, port:5060, proto:0
59642346-Sipm_SipResolverReportDataEv IP_BY_HOST: 213.148.136.222(providerIndex:2, NumHost:1)
59642346-Sipm_SipResolverReportDataEv IP_BY_HOST(mode:NAPTR): 1-st Server:**213.148.136.222**
59642346-Sipm_SipResolverReportDataEv : mode=IP BY HOST, nextmode=IP BY HOST, query=duro01.sipconnect.qsc.de
59642346-Sipm_SipResolverReportDataEv Srv:0, Host:1, IP:0
59642346-Sipm_SipResolverReportDataEv : host=duro02.sipconnect.qsc.de, priority:20, weight:10, port:5060, proto:0
59642354-Sipm_SipResolverReportDataEv IP_BY_HOST: 213.148.136.190(providerIndex:2, NumHost:0)
59642354-Sipm_SipResolverReportDataEv IP_BY_HOST(mode:NAPTR): 0-st Server:**213.148.136.190**
59642354-Sipm_SipResolverReportDataEv : mode=IP BY HOST, nextmode=Undefined, query=duro02.sipconnect.qsc.de

Protocol	Length	Info
DNS	77	Standard query 0x924f NAPTR sipconnect.qsc.de
DNS	116	Standard query response 0x924f NAPTR sipconnect.qsc.de NAPTR 100 50 s
DNS	87	Standard query 0x9250 SRV _sip._udp.sipconnect.qsc.de
DNS	207	Standard query response 0x9250 SRV _sip._udp.sipconnect.qsc.de SRV 20 10 5060 duro02.sipconnect.qsc.de SRV 10 10 5060 duro01.sipconnect.qsc.de A 213.148.136.190 A 213.148.136.222
DNS	84	Standard query 0x9251 A duro01.sipconnect.qsc.de
DNS	100	Standard query response 0x9251 A duro01.sipconnect.qsc.de A 213.148.136.222
DNS	84	Standard query 0x9252 A duro02.sipconnect.qsc.de
SIP	870	Request: REGISTER sip:150.150.150.95 (1 binding) |
SIP	753	Status: 200 OK (1 binding) |
DNS	100	Standard query response 0x9252 A duro02.sipconnect.qsc.de A 213.148.136.190

iPECS
Your Communications Solution

Specific settings for SIP Service

PGM133 – Soft Switch Type(DNS REDUN), PGM210 - DNS SRV Usage

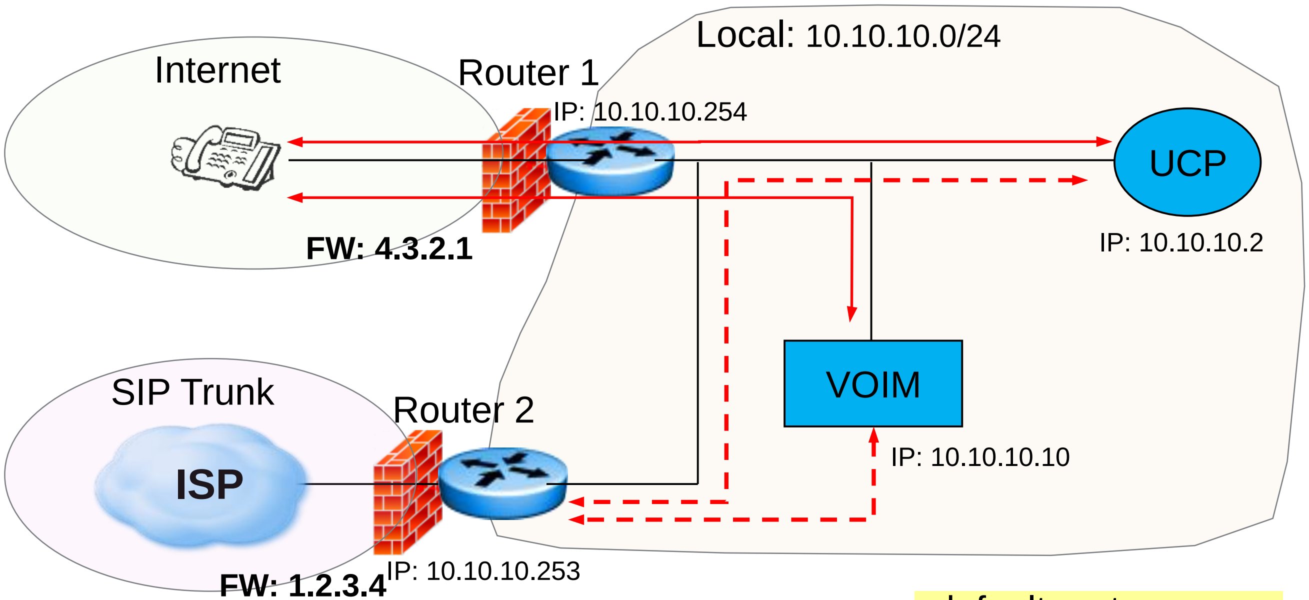
- List of service provider using DNS REDUN.
  - (1)sip-corporate.tele2.se, (2)nexvortex.com, (3)sipconnect.qsc.de

- Set PGM210 – Primary DNS Address.
- Set PGM210 – DNS SRV Usage.
- Set PGM133 – Soft Switch Type : DNS REDUN.
- Set PGM133 – Proxy Server Address : nexvortex.com.
- Set PGM133 – Domain : nexvortex.com.
- Press PGM133 – [REGISTER] button.
- Check IP Addresses resolved in system trace or ethereal trace.

Specific Configurations

Dual Broadband

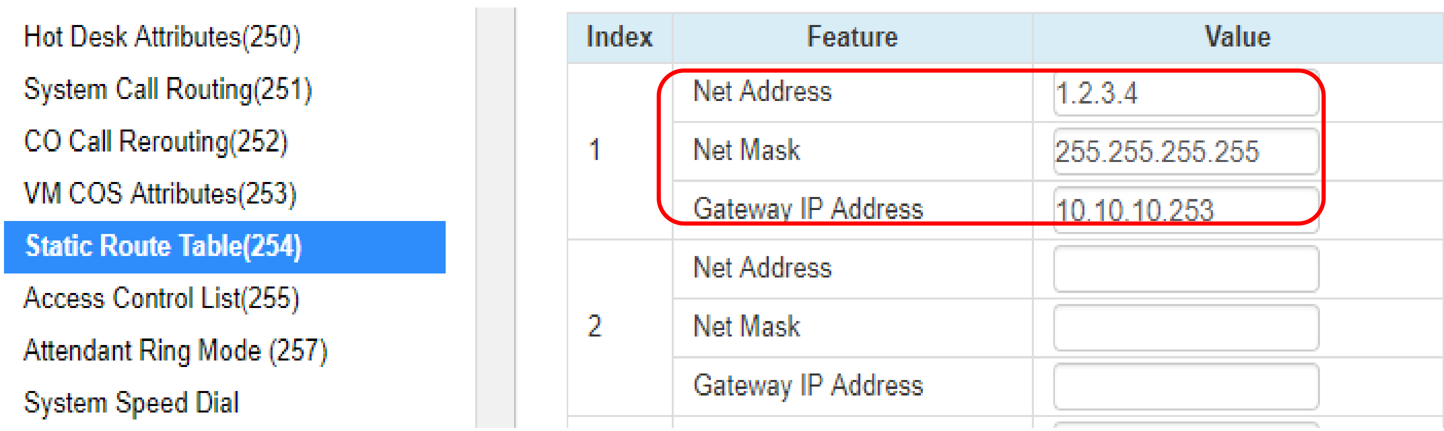
- SIP trunk is provided by an Internet Service provider (ISP) and its network is divided from default network (internet) by using second router device.



Specific Configurations

Dual Broadband

- The static routes feature can be used to communicate with second broadband network. So you need to know the **network address of SIP and media servers from ISP.**

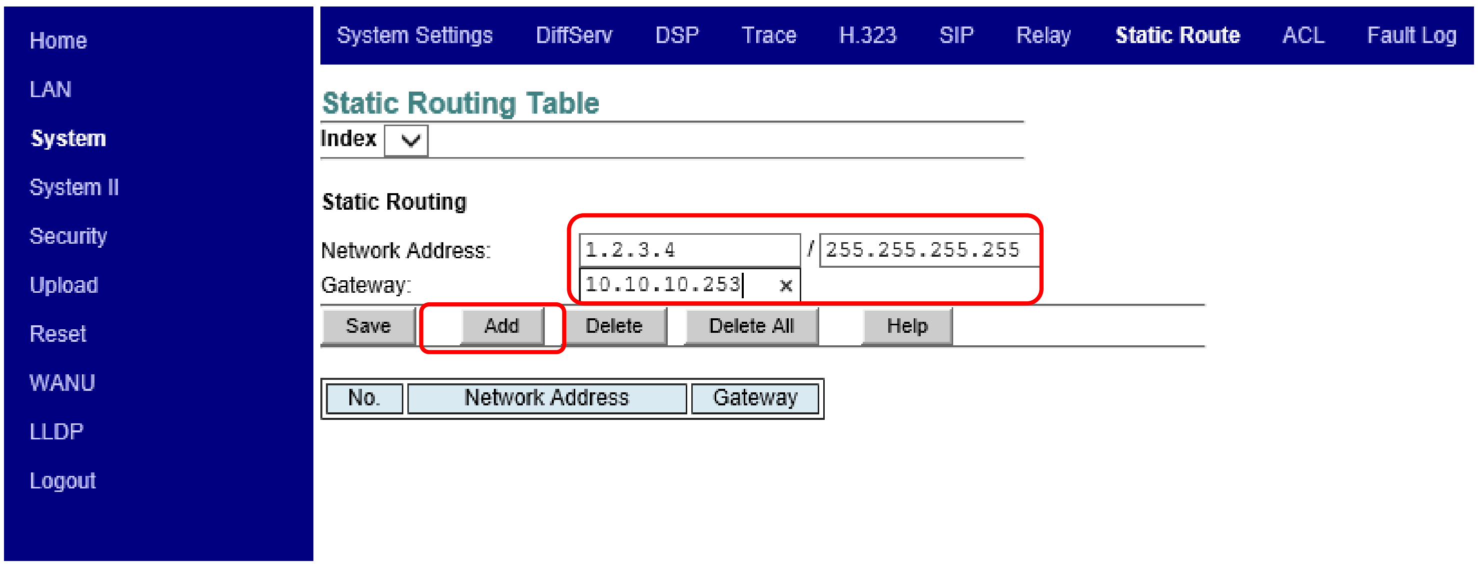


iPECS
Your Communications Solution

Specific Configurations

Dual Broadband

- Static Route, VOIM/VCIM/VVMU/VOIB8-24



Specific Configurations

Dual Broadband

- SIP Signaling

  1) UCP sends SIP packets to **router 2** by static route.

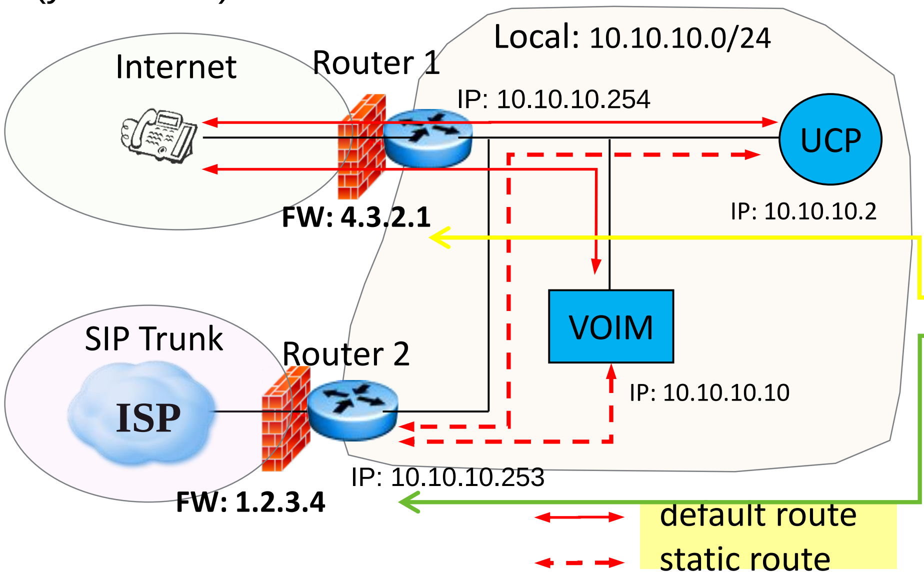
  2) Configure the firewall IP address of **router 2** and enable 'USE Board IP for SIP' field for the dedicated SIP trunk. (green line)

- Media Exchange Between VOIM and SIP Media Server

  VOIM sends RTP packets to SIP media server by static router.

- Media Exchange Between VOIM and Remote Device

  Configure the firewall IP address of **router 1** at 'RTP Packet Relay Firewall IP Address' field. (yellow line)



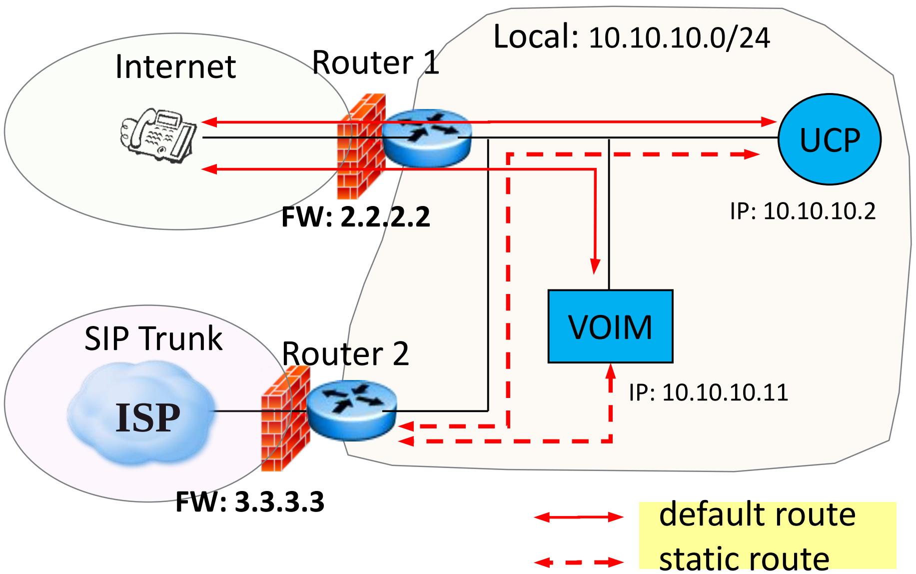
Attribute	Value
Router IP Address	10.10.10.254
Device Codec Type	System Codec
Firewall IP Address	1.2.3.4
RTP Packet Relay Firewall IP Address	4.3.2.1
RTP Security	
T-NET Enable	OFF
T38 Enable	OFF
USE Board IP for SIP	ON

Specific Configurations

Example

- Configure Dual Broadband case.

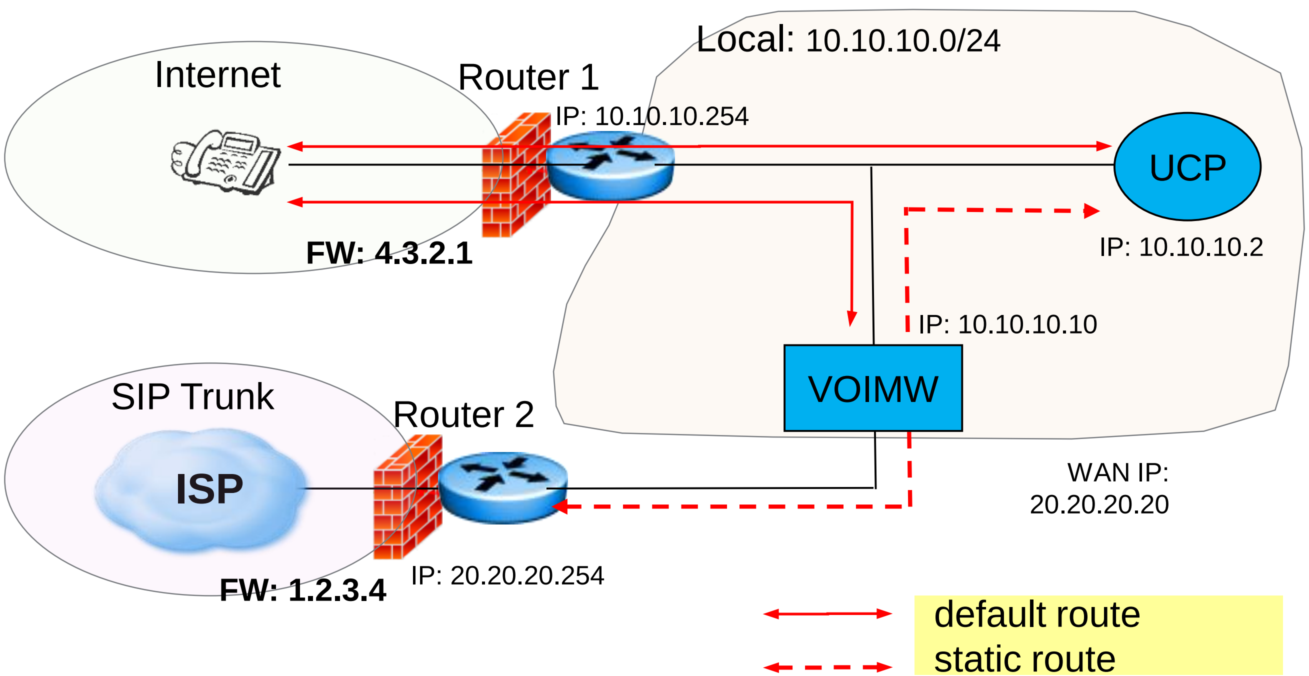
Condition:



Specific Configurations

Dual Broadband with WANU

- Router1 and Router2 are separated network.
- WANU must control SIP and RTP packets to relay Local and WAN network.
  - Refer WANU_Overview.ppt for WANU setting.



Specific Configurations

Dual Broadband with WANU

- Router IP address of UCP will be WANU local IP.

UCP IP Address	10.10.10.2
UCP MAC Address	B40EDC281BCA
UCP Subnet Mask	255.255.255.0
Router IP Address	10.10.10.10

Specific Configurations

Dual Broadband with WANU

- Router IP address of VOIM will be WANU local IP.
- Set Firewall IP and Relay Firewall IP.
- Set USE Board IP for SIP

1	☐	Router IP Address	10.10.10.10	IP Address
2	☐	Device Codec Type	System Codec ▼	
3	☐	Firewall IP Address	1.2.3.4	IP Address
4	☐	RTP Packet Relay Firewall IP Address	4.3.2.1	IP Address
5	☐	RTP Security	ON ▼	
6	☐	T-NET Enable	OFF ▼	
7	☐	T38 Enable	OFF ▼	
8	☐	USE Board IP for SIP	ON ▼	

iPECS
Your Communications Solution

Specific Configurations

Dual Broadband with WANU

- Wanu Config

Config | WAN | MFIM | VOIP | VSF | PC | Port

WANU Configuration

Run 'Update' submenu to apply changed configurations.

WANU Control

WANU : (•) Enabled ( ) Disabled

Accepting WAN Side Access

ICMP (ping) : (•) On ( ) Off

Web : (•) On ( ) Off

Maintenance : (•) On ( ) Off

Accepting LAN Side Access

ICMP (ping) : (•) On ( ) off

Voim Function

VOIM Gateway : (•) Enabled ( ) Disabled

ALG Function

SIP : (•) On ( ) Off

SIP Seize : ( ) First (•) Round

SIP poll : 10 seconds, (default 10)

H.323 : (•) On ( ) Off

H.323 Seize : ( ) First (•) Round

H.323 GK : ( ) On (•) Off

H.323 poll : 0 seconds, (default 10)

Save WANU Settings

WAN Network Configuration

Run 'Update' submenu to apply changed configurations.

WAN Configurtion

IP Address:	20.20.20.20
Netmask:	255.255.255.0
Gateway:	20.20.20.254
Firewall:	1.2.3.4

Save WAN Settings

MFIM Configuration

Run 'Update' submenu to apply changed configurations.

MFIM Configurtion

IP Address: 10.10.10.2

	[Public Port]		[Private Port]
IPKTS Protocol Port (default UDP 5588):	5588		5588
IPKTS Protocol Port (default TCP 5588):	5588		5588
TCP maintenance Port (default TCP 5003):	5003		5003
Web Server Port (default TCP 80):	80		80
Web TLS Server Port (default TCP 443):	443		443
TFTP Server Port (default UDP 69):	69		69
FTP Control Server Port (default TCP 21):	21		21
FTP Data Server Port (default TCP 9700..9709):	9700	- 9709	9700
SMTP Server Port (default TCP 25):	25		25
SNMP Server Port (default UDP 161):	161		161
NTP Server Port (default UDP 123):	123		123
UC Web Port (default TCP 8899):	8899		8899
UC XML Port (default TCP 7878):	7878		7878
UCP Telnet Port (default TCP 23):	23		23
UCP SSH Port (default TCP 22):	22		22
UCP Rsync Port (default TCP/UDP 873):	873		873

Save MFIM Settings

iPECS Your Communications Solution

Specific Configurations

Dual Broadband with WANU

- WANU Configuration

Index	0	1
VOIP IP Address	10.10.10.2	10.10.10.10
SIP Proxy Address	255.255.255.255	255.255.255.255
SIP Proxy(2nd. or Subnet)	255.255.255.255	255.255.255.255
SIP Server Port	5060	0
SIP Server TCP Port	5060	0
SIP Server TLS Port	5061	0
H.323 Proxy IP Address	255.255.255.255	255.255.255.255
H.323 Server Port	0	1720
Q.931 Signal Ports	0 - 0	2048 - 2559
H.245 Signal Ports	0 - 0	2560 - 3071
RAS Signal Port	0 - 0	2048 - 3071
Remote Maint Port	5003	5004
Web Server Port	80	8000
Data Sharing Ports	0 - 0	0 - 0
RTP P1 Ports	0 - 0	10000 - 10083
RTP P2 Ports	0 - 0	10084 - 10167
RTP Signal Ports	0 - 0	10168 - 10251
RTP T.38 Ports	0 - 0	10252 - 10335
ALG Total Channels	120	24
ALG Max SIP Channels	120	0
ALG Max H.323 Channels	0	24
ALG SIP Order	-1	-1
ALG SIP Call Direction	TxRx	TxRx
ALG H.323 order	-1	-1
ALG H.323 Call Direction	TxRx	TxRx
ALG H.323 Gatekeeper	No	No

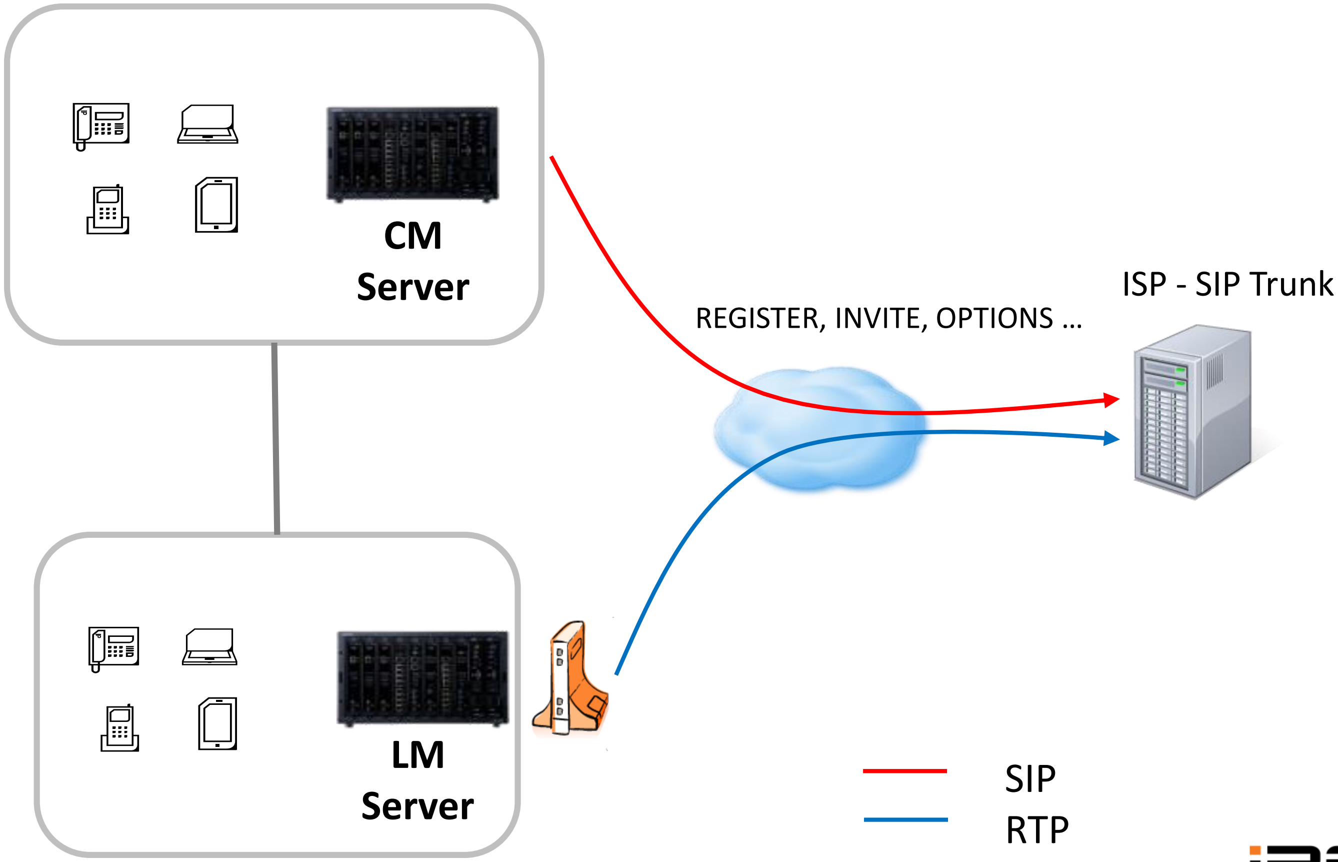
SIP ports are forwarded to UCP. All SIP related ports are assigned to UCP to forward SIP packets to UCP.

RTP packets should be handled in VOIP gateway.

Specific Configurations

SIP Service in T-NET

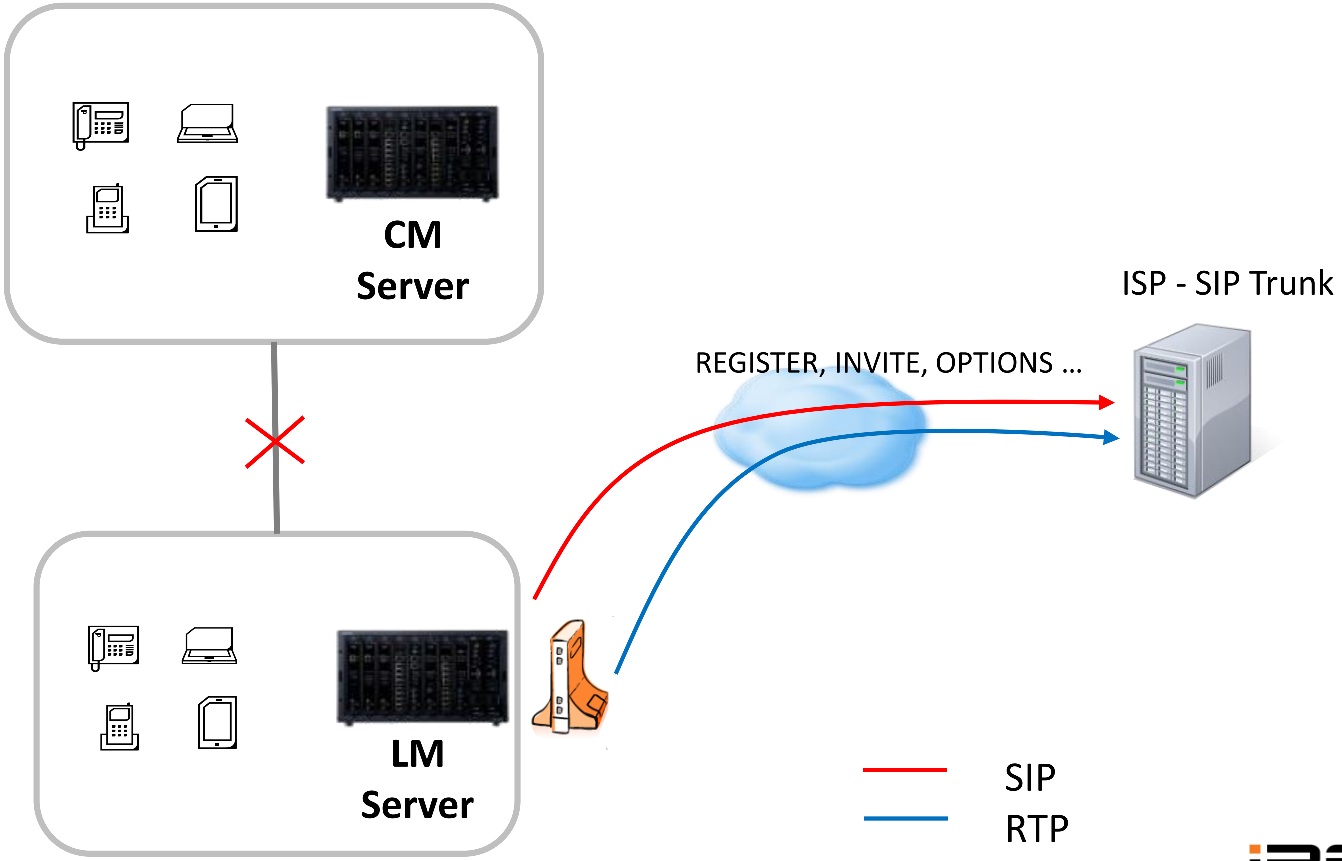
- SIP Trunk is used in T-NET configuration.
  - LM VOIU/VOIM is controlled by CM Server.
  - After connection, REGISTER will be sent to server by CM server.



Specific Configurations

SIP Service in T-NET

- SIP Trunk is used in T-NET configuration.
  - LM VOIU/VOIM is controlled by LM Server by disconnection.
  - After disconnection, REGISTER will be sent to server by LM server.



SIP Service in T-NET

Practice

- Configure T-NET case

Trace related with SIP

SIP Raw Level Trace

- Print SIP message before sending to network and receiving from network.
  - Trace is same as Wireshark trace.
  - Mon>t s fsipm → Full SIP Message

```
[ 25/09/17 10:07:51 ]+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Sent 1085 Bytes to 150.150.131.207:5060 by UDP (SendEv)
------------------------------------------------------------------------------
INVITE sip:1000@150.150.131.207 SIP/2.0
From: "1018"<sip:1018@150.150.150.95>;tag=4e705130-5f969696-13c4-65014-257cf-333808ef-257cf
To: <sip:1000@150.150.131.207>
Call-ID: 4e93ccb8-5f969696-13c4-65014-257cf-3073a139-257cf
CSeq: 1 INVITE
Via: SIP/2.0/UDP 150.150.150.95:5060;rport;branch=z9hG4bK-257cf-9270161-3b35064c-4e413638
Max-Forwards: 70
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,REGISTER,REFER,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PRACK,UPDATE
Supported: replaces,UPDATE,INFO
P-Asserted-Identity: "1018"<sip:1018@150.150.150.95>
Remote-Party-ID: <sip:1018@150.150.150.95>; party=calling; privacy=off; screen=yes
Privacy: none
User-Agent: Ericsson-LG Enterprise iPECS-
Contact: "1018"<sip:1018@150.150.150.95:
Content-Type: application/sdp
Content-Length: 277
```

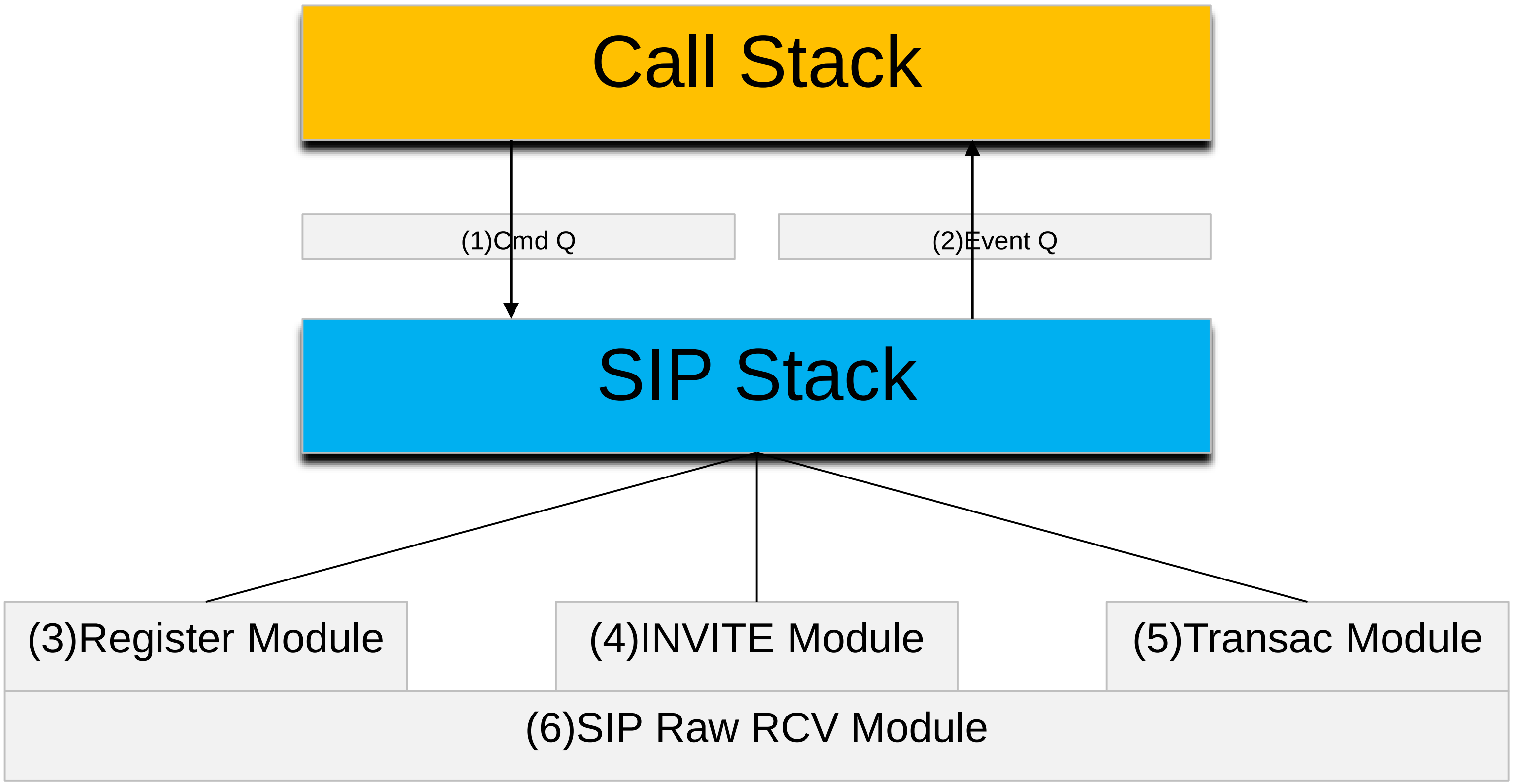
Same Call-ID

	Time	Source	Destination	Protocol	Length	Info
298	2017-09-25 10:16:36.257898	150.150.150.95	150.150.131.207	SIP/SDP	1127	Request: INVITE sip:1000@150.150.131.207 |
315	2017-09-25 10:16:36.371366	150.150.131.207	150.150.150.95	SIP	571	Status: 100 Trying |
348	2017-09-25 10:16:36.472330	150.150.131.207	150.150.150.95	SIP/SDP	914	Status: 183 Session Progress |

```
User Datagram Protocol, Src Port: 5060, Dst Port: 5060
Session Initiation Protocol (INVITE)
 > Request-Line: INVITE sip:1000@150.150.131.207 SIP/2.0
 v Message Header
   > From: "1018"<sip:1018@150.150.150.95>;tag=4e705130-5f969696-13c4-65014-257cf-333808ef-257cf
   > To: <sip:1000@150.150.131.207>
     Call-ID: 4e93ccb8-5f969696-13c4-65014-257cf-3073a139-257cf
   > CSeq: 1 INVITE
   > Via: SIP/2.0/UDP 150.150.150.95:5060;rport;branch=z9hG4bK-257cf-9270161-3b35064c-4e413638
     Max-Forwards: 70
     Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,REGISTER,REFER,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PRACK,UPDATE
     Supported: replaces,UPDATE,INFO
   > P-Asserted-Identity: "1018"<sip:1018@150.150.150.95>
   > Remote-Party-ID: <sip:1018@150.150.150.95>; party=calling; privacy=off; screen=yes
     Privacy: none
     User-Agent: Ericsson-LG Enterprise iPECS-UCP UCP100 2.2.24
   > Contact: "1018"<sip:1018@150.150.150.95:5060;transport=UDP>
     Content-Type: application/sdp
     Content-Length: 277
```

Trace related with SIP

Structure of SIP Call Flow



Mon>t s sip → Trace related with SIP handling

Your Communications Solution

Trace related with SIP

Structure of SIP Call Flow

(1) Command from Call Stack
- [Sipm_CallMsgHandler] CALL ---> SIPM (…….)

(2) Event to Call Stack
- <SIPM Msg> : MSG(SIP_INVITE_MSG) :Request
- <SIPM Msg> : MSG(SIP_RESPONSE_MSG) :Response

(3) Register Call Back Function
- [Sipm_SipEvRegState] : Status control
- [Sipm_SipEvRegMsgReceive] : Hooking for receiving
- [Sipm_SipEvRegMsgSend] : Hooking for sending

(4) Invite Call Back Function
- [Sipm_SipEvCallState] : Status control
- [Sipm_SipEvCallMsgReceive] : Hooking for receiving
- [Sipm_SipEvCallMsgSend] : Hooking for sending

(5) Transc Call Back Function
- [Sipm_SipEvTransState] : Status control
- [Sipm_SipEvTransMsgReceive] : Hooking for receiving
- [Sipm_SipEvTransMsgSend] : Hooking for sending

(6) Raw level Hooking for receiving
- [Sipm_SipTransportMsgReceivedExt] : Hooking Used for PGM210-IP Auth

Trace related with SIP

Structure of SIP Call Flow – Outgoing INVITE

- Check [Callidx:8] for one call.

(1) [CallIdx:8][**Sipm_CallMsgHandler**] CALL ---> SIPM (INVITE)
(2) [CallIdx:8][**Sipm_SipEvCallMsgSend**] SIPM ---> INVITE
→ INVITE
(3) [CallIdx:8][**Sipm_SipEvCallState(s:01)**)] OUTGOING - Inviting(reason:LOCAL_INVITING)
←100_TRYING
(4) [CallIdx:8][**Sipm_SipEvCallMsgReceive**] SIPM <--- 100(Method:INVITE(0), reason:Trying)
(5) <**SIPM Msg**> : MSG(SIP_RESPONSE_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(7)
(6) [CallIdx:8][**Sipm_SipEvCallState(s:13)**)] OUTGOING - Proceeding(reason:NOTHING_ALL)
←407_AUTHEN
(7) [CallIdx:8][**Sipm_SipEvCallMsgReceive**] SIPM <--- 407(Method:INVITE(0), reason:Proxy Authentication Required)
(8) [CallIdx:8][**Sipm_SipEvCallMsgSend**] SIPM ---> ACK
→ ACK
(9) [CallIdx:8][**Sipm_SipEvCallState(s:03)**)] OUTGOING - Unauthenticated(reason:AUTH_NEEDED)
(10) [CallIdx:8][**Sipm_SipEvCallMsgSend**] SIPM ---> INVITE
→ INVITE
(11) [CallIdx:8][**Sipm_SipEvCallState(s:01)**)] OUTGOING - Inviting(reason:LOCAL_INVITING)
←100_TRYING
(12) [CallIdx:8][**Sipm_SipEvCallMsgReceive**] SIPM <--- 100(Method:INVITE(0), reason:Trying)
(13) [CallIdx:8][**Sipm_SipEvCallState(s:13)**)] OUTGOING - Proceeing(reason:NOTHING_ALL)
(14) <**SIPM Msg**> : MSG(SIP_RESPONSE_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(7)
←180_RINGING
(15) [CallIdx:8][**Sipm_SipEvCallMsgReceive**] SIPM <--- 180(Method:INVITE(0), reason:Ringing)
(16) **<SIPM Msg>** : MSG(SIP_RESPONSE_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(7)
← 200_OK
(17) [CallIdx:8][**Sipm_SipEvCallMsgReceive**] SIPM <--- 200(Method:INVITE(0), reason:OK)
(18) [CallIdx:8][**Sipm_SipEvCallState(s:10)**)] OUTGOING - RemoteAccepted(reason:REMOTE_ACCEPTED)
(19) [CallIdx:8][**Sipm_SipEvCallMsgSend**] SIPM ---> ACK
→ ACK
(20) [CallIdx:8][**Sipm_SipEvCallState(s:06)**)] OUTGOING - Connected(reason:ACK_SENT)
(21) <**SIPM Msg**> : MSG(SIP_RESPONSE_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(7)

Trace related with SIP

Structure of SIP Call Flow – Outgoing INVITE Failure

- Check [Callidx:11] for one call.

(1) [CallIdx:11][**Sipm_CallMsgHandler**] CALL ---> SIPM (INVITE)
(2) [CallIdx:11][**Sipm_SipEvCallMsgSend**] SIPM ---> INVITE
→ INVITE
(3) [CallIdx:11][**Sipm_SipEvCallState(s:01)**] OUTGOING - Inviting(reason:LOCAL_INVITING)
←100_TRYING
(4) [CallIdx:11][**Sipm_SipEvCallMsgReceive**] SIPM <--- 100(Method:INVITE(0), reason:Trying)
(5) <**SIPM Msg**> : MSG(SIP_RESPONSE_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(11)
(6) [CallIdx:11][**Sipm_SipEvCallState(s:13)**] OUTGOING - Proceeding(reason:NOTHING_ALL)
←407_AUTHEN
(7) [CallIdx:11][**Sipm_SipEvCallMsgReceive**] SIPM <--- 407(Method:INVITE(0), reason:Proxy Authentication Required)
(8) [CallIdx:11][**Sipm_SipEvCallMsgSend**] SIPM ---> ACK
→ ACK
(9) [CallIdx:11][**Sipm_SipEvCallState(s:03)**] OUTGOING - Unauthenticated(reason:AUTH_NEEDED)
(10) [CallIdx:11][**Sipm_SipEvCallMsgSend**] SIPM ---> INVITE
→ INVITE
(11) [CallIdx:11][**Sipm_SipEvCallState(s:01)**] OUTGOING - Inviting(reason:LOCAL_INVITING)
←100_TRYING
(12) [CallIdx:11][**Sipm_SipEvCallMsgReceive**] SIPM <--- 100(Method:INVITE(0), reason:Trying)
(13) [CallIdx:1][**Sipm_SipEvCallState(s:13)**] OUTGOING - Proceeding(reason:NOTHING_ALL)
(14) <**SIPM Msg**> : MSG(SIP_RESPONSE_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(11)
←404_NOT_FOUND
(15) [CallIdx:11][**Sipm_SipEvCallMsgReceive**] SIPM <--- 404(Method:INVITE(0), reason:Not Found)
(16) [CallIdx:11][**Sipm_SipEvCallMsgSend**] SIPM ---> ACK
→ACK
(17) **<SIPM Msg>** : MSG(SIP_RESPONSE_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(11)
(18) [CallIdx:11][**Sipm_SipEvCallState(s:07)**] OUTGOING - Disconnected(reason:REQUEST_FAILURE)
(19) [[CallIdx:11][**Sipm_SipEvCallState(s:09)**] OUTGOING - Terminated(reason:CALL_TERMINATED)
(20) **<SIPM Msg>** : MSG(SIP_BYE_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(11)
(21) **<SIPM Msg>** : MSG(SIP_RLS_OK_MSG), Evt type(SIPTRUNK) type(SIPTRUNK) GWnum(13) phy_num(11)

Your Communications Solution

Trace related with SIP

Structure of SIP Call Flow – REGISTER

- Check [RegIdx:1] for one register.

(1) [RegIdx:1][**Sipm_SipEvRegMsgSend**] SIPM ---> REGISTER

→REGISTER

(2) [RegIdx:1][**Sipm_SipEvRegState**] (s:2) - Registering (reason:USER_REQUEST)

← 401 Unauth

(3) [RegIdx:1][**Sipm_SipEvRegMsgReceive**] SIPM <--- 401(Unauthorized)

(4) [RegIdx:1][**Sipm_SipEvRegState**] (s:4) - Unauthenticated (reason:RESPONSE_UNAUTHENTICATED_RECVD)

(5) [RegIdx:1][**Sipm_SipEvRegMsgSend**] SIPM ---> REGISTER

→ REGISTER

(6) RegIdx:1][**Sipm_SipEvRegState**] (s:2) - Registering (reason:USER_REQUEST)

←200 OK

(7) [RegIdx:1][**Sipm_SipEvRegMsgReceive**] SIPM <--- 200(OK)

(8) [RegIdx:1][**Sipm_SipEvRegState**] (s:5) - Registered (reason:RESPONSE_SUCCESSFUL_RECVD)

Trace related with SIP

Get the trace for each cases.

Practice

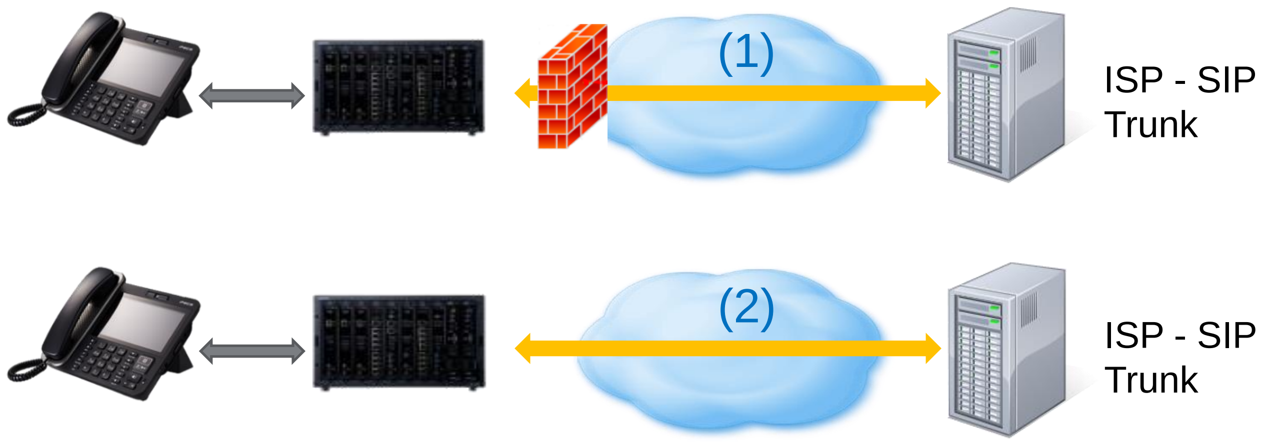
- Send SIP REGISTER and get the trace.
- Send SIP INVITE and get the trace.

iPECS
Your Communications Solution

Trouble Shooting

Network Configuration

- Check if F/W device is installed and where F/W device is located.
  - (1) Server is located outside of F/W - F/W IP must be used or SIP ALG feature is needed in F/W .
  - (2) Server is located inside of F/W or connected using public IP – Local IP must be used.

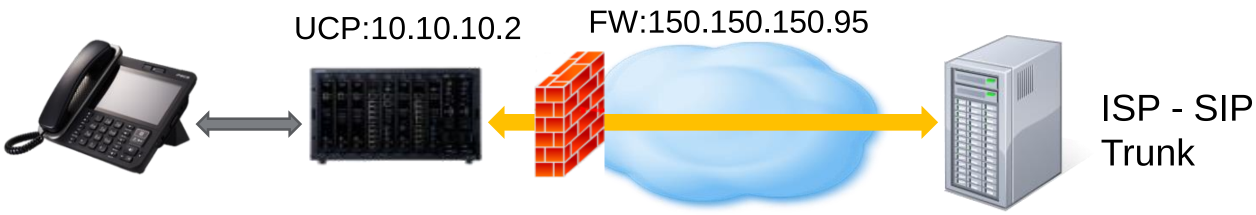


iPECS
Your Communications Solution

Trouble Shooting

Network Configuration

- Server is located outside of F/W
  - Is SIP ALG feature used in F/W device?
    - If SIP ALG feature malfunctions, mute problem happens.
  - SIP ALG must change ip address in SIP message – contact, via, media ip address.
  - SIP ALG must relay SIP message and RTP packets.

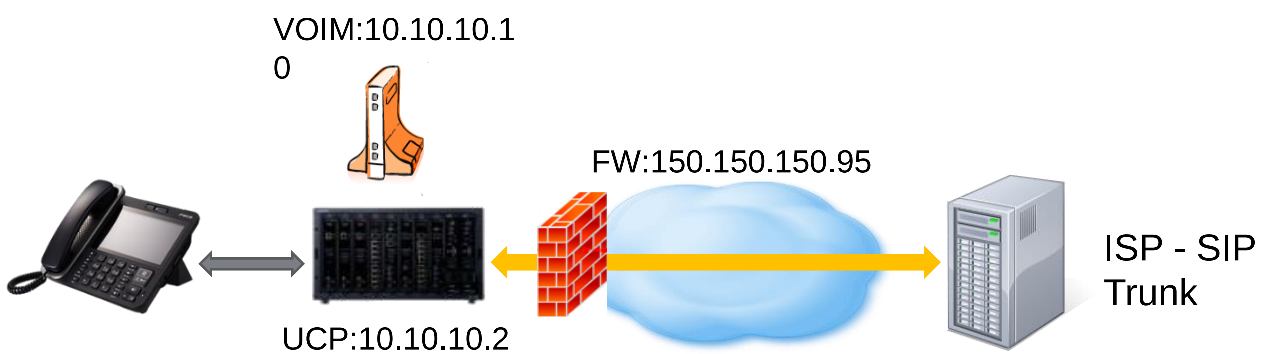


SIP ALG has own Table to forward packet and change IP address

Trouble Shooting

Network Configuration

- Server is located outside of F/W
  - Is it possible to disable SIP ALG feature?
    - Some F/W can not disable SIP ALG feature.
  - Is it possible to set Port Forwarding?



Local IP:port	Public IP:port	
10.10.10.2:5060	150.150.150.95:5060	SIP signaling port
10.10.10.10:10000 ~10048	150.150.150.95:10000 ~10048	RTP port

Port forwarding Table

Trouble Shooting

SIP Registration Log

- Maintenance – Trace – SIP RegUnreg Log View.
  - SENDFAIL(6) : No Response from server for REGISTER message.
    - Check network problem or server side.
  - FAIL(6) – 404 : “404 Not Found” from server for REGISTER message.
    - Check ID and password with server.
  - REG(5)   : “200OK” from server for REGISTER message.
    - System is successfully registered.

System Information | SIP RegUnreg Log View

SIP RegUnreg Log
18 Sep 2017 11:22:10 IP:150.150.131.207 ID:1018@150.150.150.95 SENDFAIL(6)
18 Sep 2017 11:22:36 IP:150.150.131.207 ID:1018@150.150.150.95 SENDFAIL(6)
18 Sep 2017 11:26:14 IP:sipconnect.qsc.de ID:1018@150.150.150.95 SENDFAIL(6)
22 Sep 2017 16:09:03 IP:150.150.131.207 ID:12345678@150.150.150.95 FAIL(6)-404
22 Sep 2017 16:14:44 IP:150.150.131.207 ID:1018@150.150.150.95 REG(5)

Trouble Shooting

SIP Registration Log

- If you see the below case, we can say that network or server is unstable in that time.
  - SENDFAIL(7)
  - FAIL(7)
  - REG(5)
  …

System Information | SIP RegUnreg Log View

SIP RegUnreg Log
22 Sep 2017 16:25:27 IP:150.150.131.207 ID:1018@150.150.150.95 REG(5)
22 Sep 2017 16:26:26 IP:150.150.131.207 ID:1018@150.150.150.95 SENDFAIL(7)
22 Sep 2017 16:26:26 IP:150.150.131.207 ID:1018@150.150.150.95 FAIL(7)
22 Sep 2017 16:27:17 IP:150.150.131.207 ID:1018@150.150.150.95 REG(5)
22 Sep 2017 16:28:16 IP:150.150.131.207 ID:1018@150.150.150.95 SENDFAIL(7)
22 Sep 2017 16:28:16 IP:150.150.131.207 ID:1018@150.150.150.95 FAIL(7)
22 Sep 2017 16:29:07 IP:150.150.131.207 ID:1018@150.150.150.95 REG(5)

Reg
Reg Fail
Reg
Reg Fail
Reg

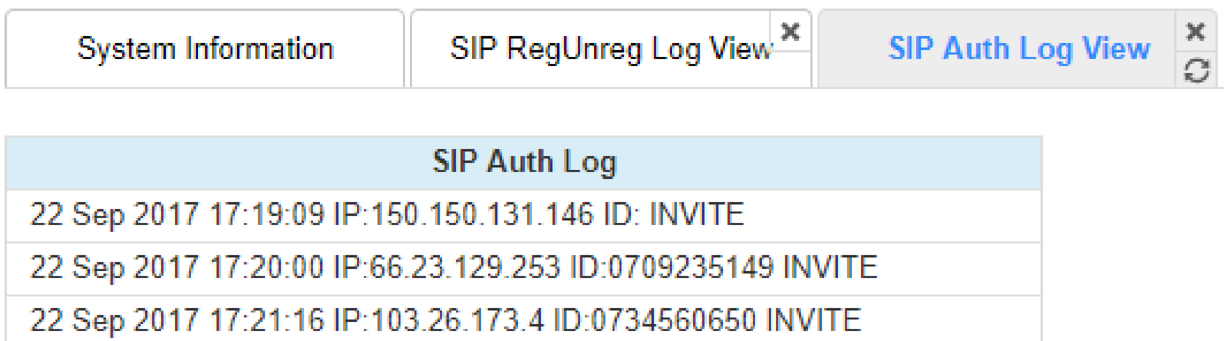
1: TERMINATED
2: REGISTERING
3: REDIRECTED
4: UNAUTHENTICATED
5: REGISTERED
6: FAILED
7: SEND_FAILURE

iPECS Your Communications Solution

Trouble Shooting

SIP Authentication Log

- Maintenance – Trace – SIP Auth Log View.
  - Data Time IP ID SIP_Method
  - 22 Sep 2017 17:20:00 IP:66.23.129.253 ID:0709235149 INVITE
  - 22 Sep 2017 17:21:16 IP:103.26.173.4 ID:0734560650 INVITE
- If there are many logs from unknown Ips, consider **hacking trial**.
  - For more information for security, refer security session.



Trouble Shooting

SIP call disconnection after 30 seconds

- SIP stack will disconnect incoming call if final ACK is not received.
  - This kind of problem is related with Contact IP address in 200OK contact header.
- Check which ip address must be used in your configuration.

Contact Header Rule

	PGM132-USE Board IP for SIP	PGM132-Firewall IP Address(VOIM)	PGM133-Firewall IP Apply	PGM102-Firewall IP Address	Contact IP Address
Dual Broadband case	O	O	O	Don't care	VOIM Firewall IP
	O	Other Cases			VOIM Local IP
Normal firewall case	X	Don't care	O	O	UCP Firewall IP
	X	Other Cases			UCP Local IP

Your Communications Solution

Trouble Shooting

SIP call disconnection after 30 seconds

- UCP IP is 10.180.240.220 and VOIM IP is 10.180.240.228.
- Customer set PGM132 – USE Board IP for SIP for VOIM (Turn off USE Board IP)
- Contact IP has VOIM Local IP.

No.	Time	Source	Destination	Protocol	Length	Info
259	2017-08-18 23:16:25.176433	10.4.254.14	10.180.240.220	SIP/SDP	1347	Request: INVITE sip:8773@10.180.240.220;user=phone;transport=tcp |
265	2017-08-18 23:16:25.235577	10.180.240.220	10.4.254.14	SIP	521	Status: 100 Trying |
266	2017-08-18 23:16:25.235732	10.180.240.220	10.4.254.14	SIP	697	Status: 180 Ringing |
338	2017-08-18 23:16:35.856782	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
343	2017-08-18 23:16:36.357518	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
345	2017-08-18 23:16:37.357836	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
349	2017-08-18 23:16:39.358197	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
367	2017-08-18 23:16:43.358437	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
401	2017-08-18 23:16:47.358732	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
425	2017-08-18 23:16:51.359043	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
434	2017-08-18 23:16:55.359360	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
462	2017-08-18 23:16:59.359702	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
489	2017-08-18 23:17:03.360008	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
512	2017-08-18 23:17:07.360310	10.180.240.220	10.4.254.14	SIP/SDP	878	Status: 200 OK |
516	2017-08-18 23:17:07.857244	10.180.240.220	10.4.254.14	SIP	590	[TCP Previous segment not captured] Request: BYE sip:5731@10.4.254.1
518	2017-08-18 23:17:07.888729	10.4.254.14	10.180.240.220	SIP	501	Status: 200 OK |

```
Session Initiation Protocol (200)
  Status-Line: SIP/2.0 200 OK
  Message Header
    From: <sip:5731@lim1.MX-ONE;user=phone>;tag=9051800c
    To: <sip:8773@10.180.240.220;user=phone>;tag=4e835dc8-dcf0b40a-13c4-65014-a9167-66e17340-a9167
    Call-ID: 4FJF46BrfuEhnmvKuAFnTQ..
    CSeq: 1 INVITE
    Via: SIP/2.0/TCP 10.4.254.14:5060;rport=59771;branch=z9hG4bK-524287-1---21019d324b6d792c
    Record-Route: <sip:10.4.254.14:5060;transport=tcp;lr>
    Contact: <sip:8773@10.180.240.228:5060;transport=TCP;user=phone>
    Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,REGISTER,REFER,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PRACK,UPDATE
    Supported: replaces,UPDATE,INFO
    User-Agent: Ericsson-LG Enterprise iPECS-UCP UCP600 2.1.42
```

Trouble Shooting

SIP call has one-way mute problem.

- When SIP ALG feature is set in F/W, VOIM Local IP can be used.
- When Port Forwarding rule is used, VOIM Firewall IP must be used.
- If user has mute problem even RTP IP is right, Wireshark trace in front of UCP and VOIM will be helpful to find error.
  - Sometimes F/W device blocks RTP packet from server side.

SDP IP rule

PGM132-Firewall IP Address(VOIM)	PGM133-Firewall IP Apply	SDP IP Address
O	O	VOIM Firewall IP
Don’t care	X	VOIM Local IP