Module 7.0

ALG & B2BUA Configurations with SIP Header Manipulation



edgewater NETWORKS

Module 7.0: Performance Objectives

1. Examine EdgeMarc SIP specific functionality.
2. Explore ALG & B2BUA deployment configurations.

Module 7.0: Hands On Labs

- Lab 1: Planning SIP Traffic Flow between LAN endpoints & SIP
- Lab 2: VoIP NAT Traversal Troubleshooting Asterisk WAN IP PBX with LAN &WAN side IP Phones – No EdgeMarc SIP ALG configured
- Lab 3: Configure EdgeMarc SIP ALG with WAN based IP PBX / SIP Server
- Lab 4: Deploy LAN based PSTN Gateway with WAN SIP Server & SIP ALG Trunking Redirect Rule
- Lab 5: Configure LAN side Asterisk IP PBX with EdgeMarc B2BUA for WAN SIP Trunking connectivity

Module 7.0 Lessons

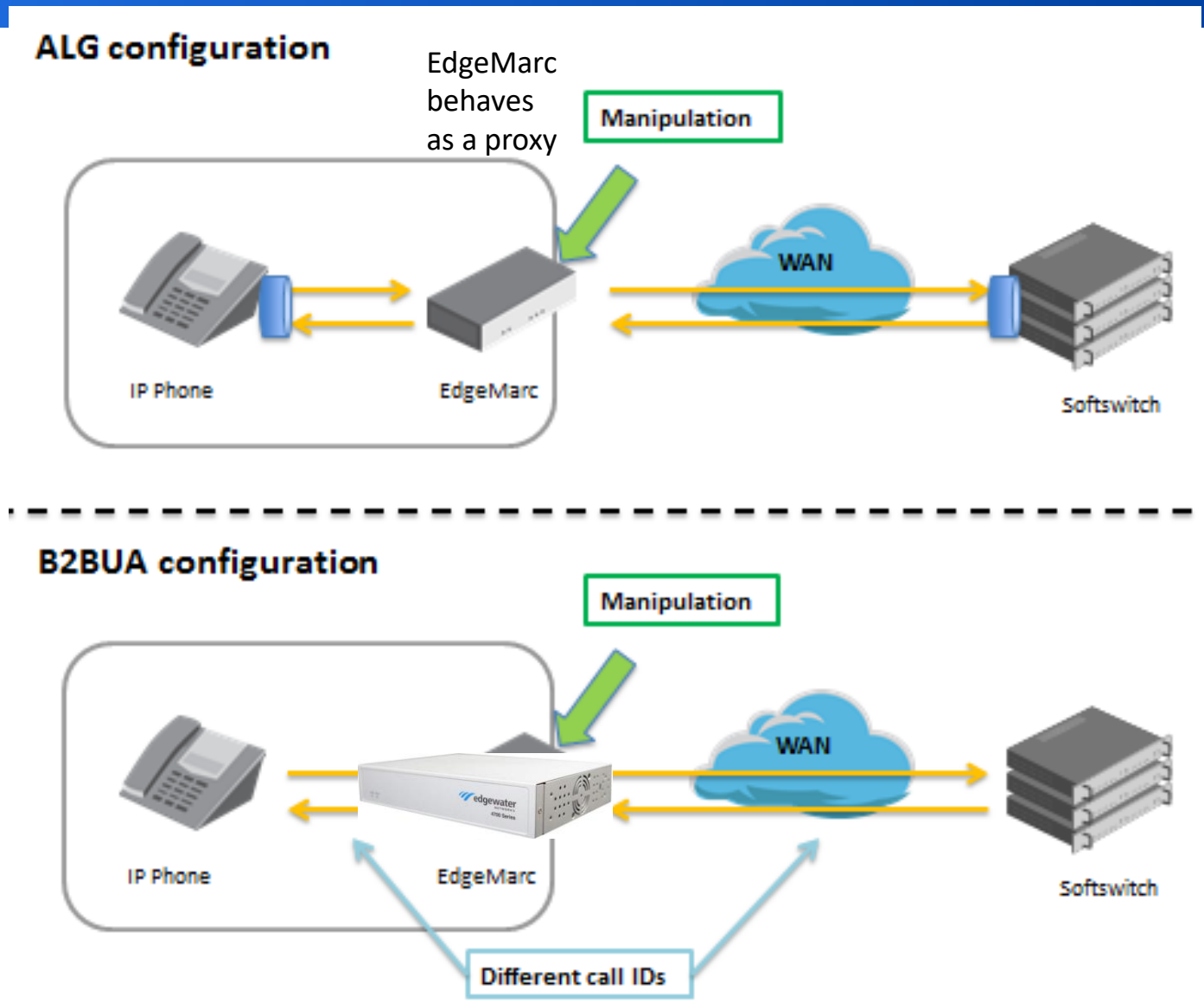
- Lesson 1.0 EdgeMarc VoIP Configuration & Deployment Options
- Lesson 2.0 LAN & WAN Based SIP Server Configuration
- Lesson 3.0 EdgeMarc Advanced VoIP Network Capabilities

7.0: ALG vs B2BUA

- The ALG (Application Layer Gateway) provides basic Proxy function with simple Header manipulation (solving NAT traversal deployment issue)

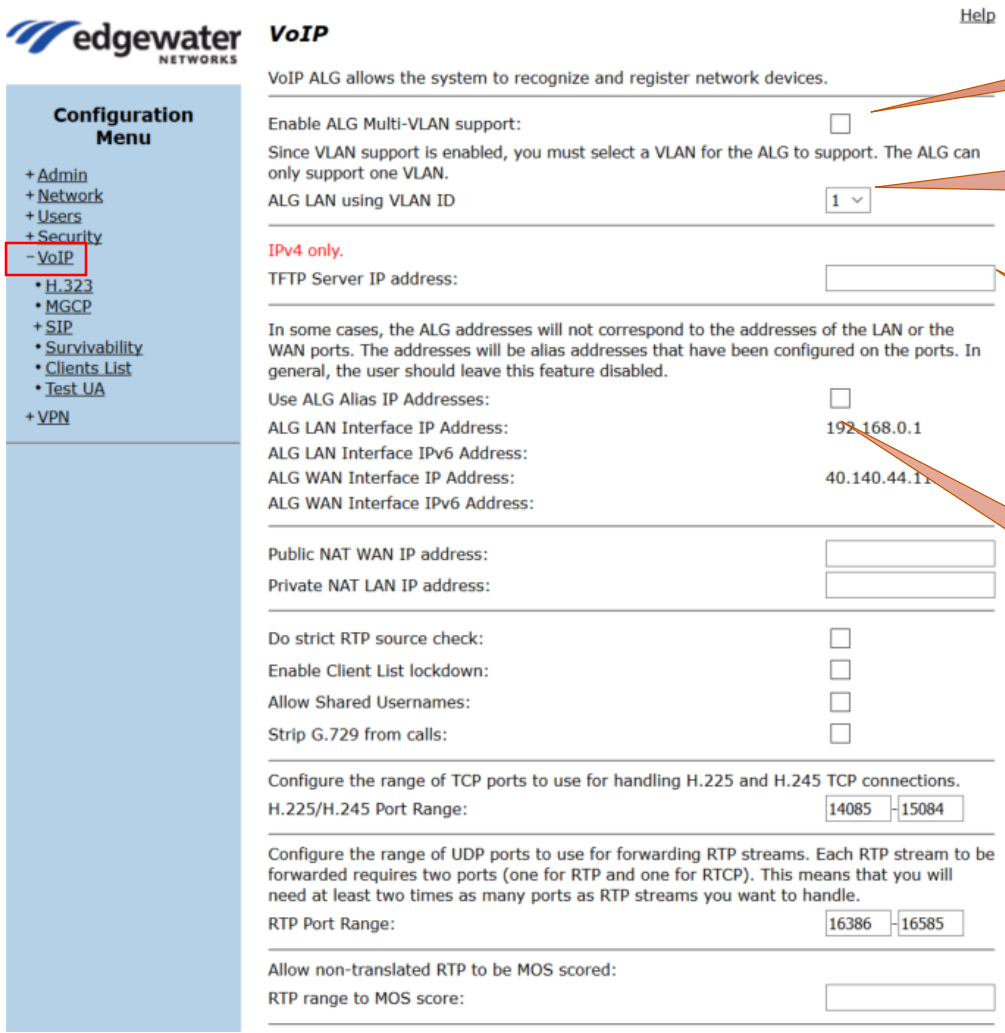
- The B2BUA (Back to Back User Agent) provides more advanced proxy capability with advanced Header Manipulation
  - In the originating call leg the B2BUA acts as a user agent server (UAS) and processes the request as a user agent client (UAC) to the destination end, handling the signaling between end points back-to-back
- Only when the ALG is configured, MOS scores, Traffic Shaper differentiating voice versus data are available.

7.0: Difference between ALG and B2BUA



Company Confidential

7.0: VoIP Settings



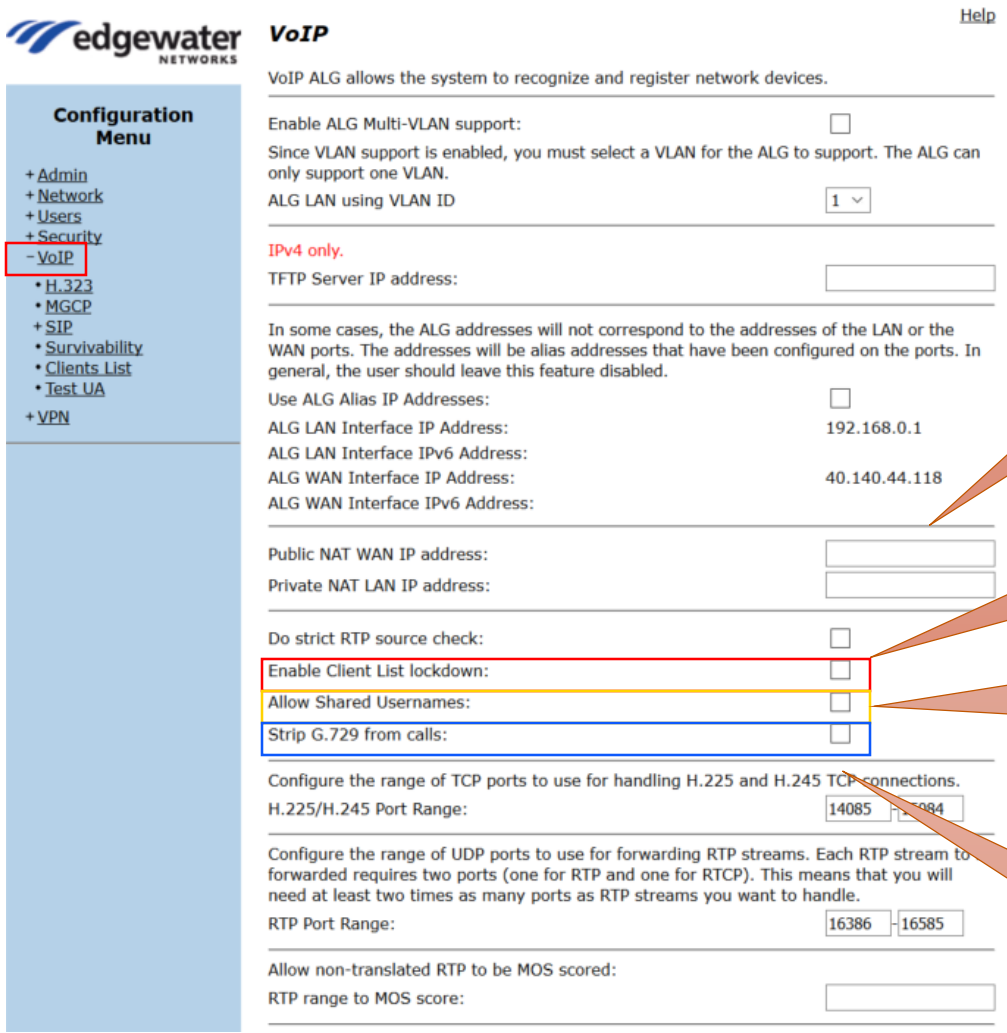
Multi VLAN ALG – added in VOS 14.7.0

If VLANs enabled, select the VLAN that the ALG should be listening on

If phones are getting their config from a hosted TFTP server in the cloud, put in the TFTP server IP here

Leave this unchecked. It's only if you need to modify the signaling IP that it NOT the WAN IP of the EdgeMarc

7.0: VoIP page Settings - continued



EdgeMarc behind a FW in a DMZ feature. EdgeMarc has a DMZ IP and NAT WAN IP is the main IP on the FW. Make sure all relevant ports are forwarded to the EdgeMarc.

Client list lockdown locks the EdgeMarc client list. Nothing can register behind the EdgeMarc once this is enabled.

Allow Shared Usernames should be enabled if you have multiple lines behind the same EdgeMarc with the same Authname / DID and they are all registering.

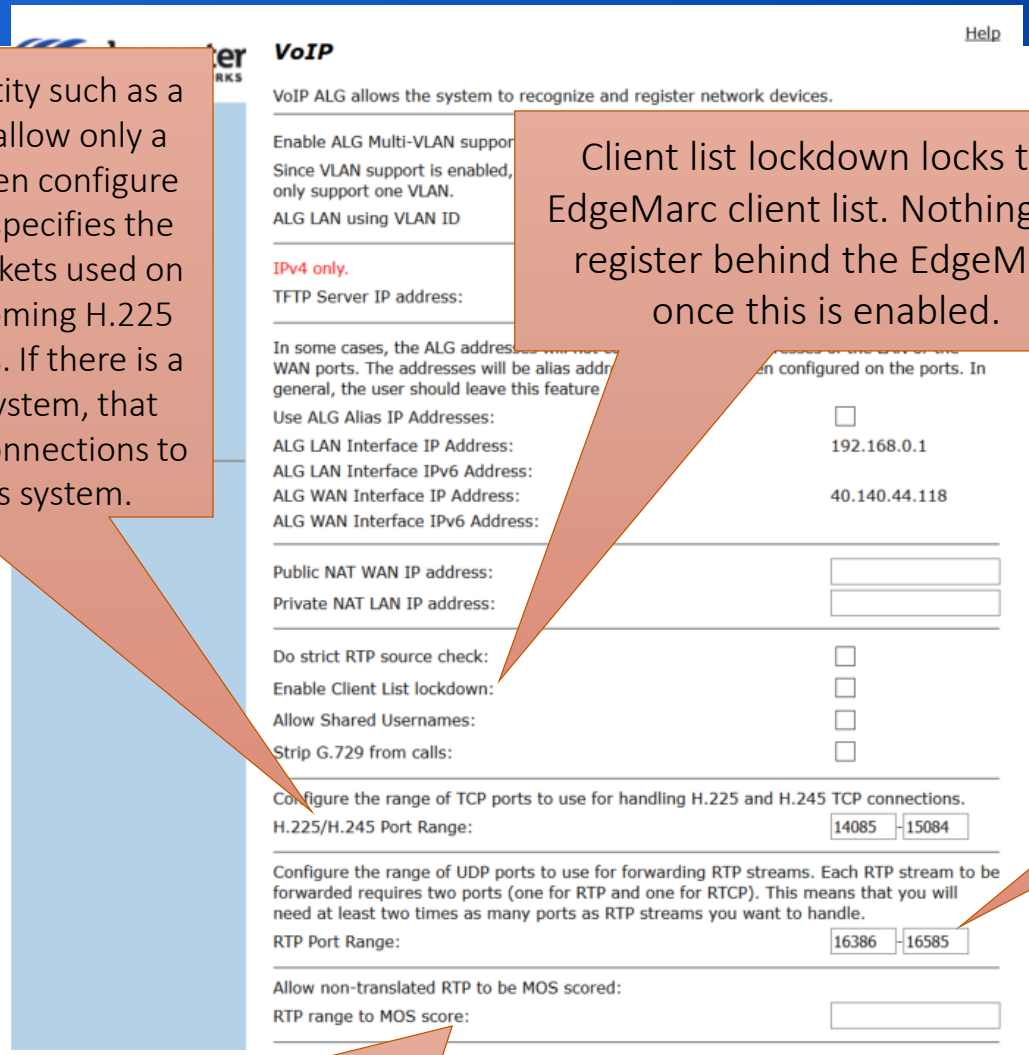
It is possible to strip G.729 from the SDP of all SIP and MGCP messages by enabling this checkbox. Only applicable to SIP.

7.0: VoIP page (3)

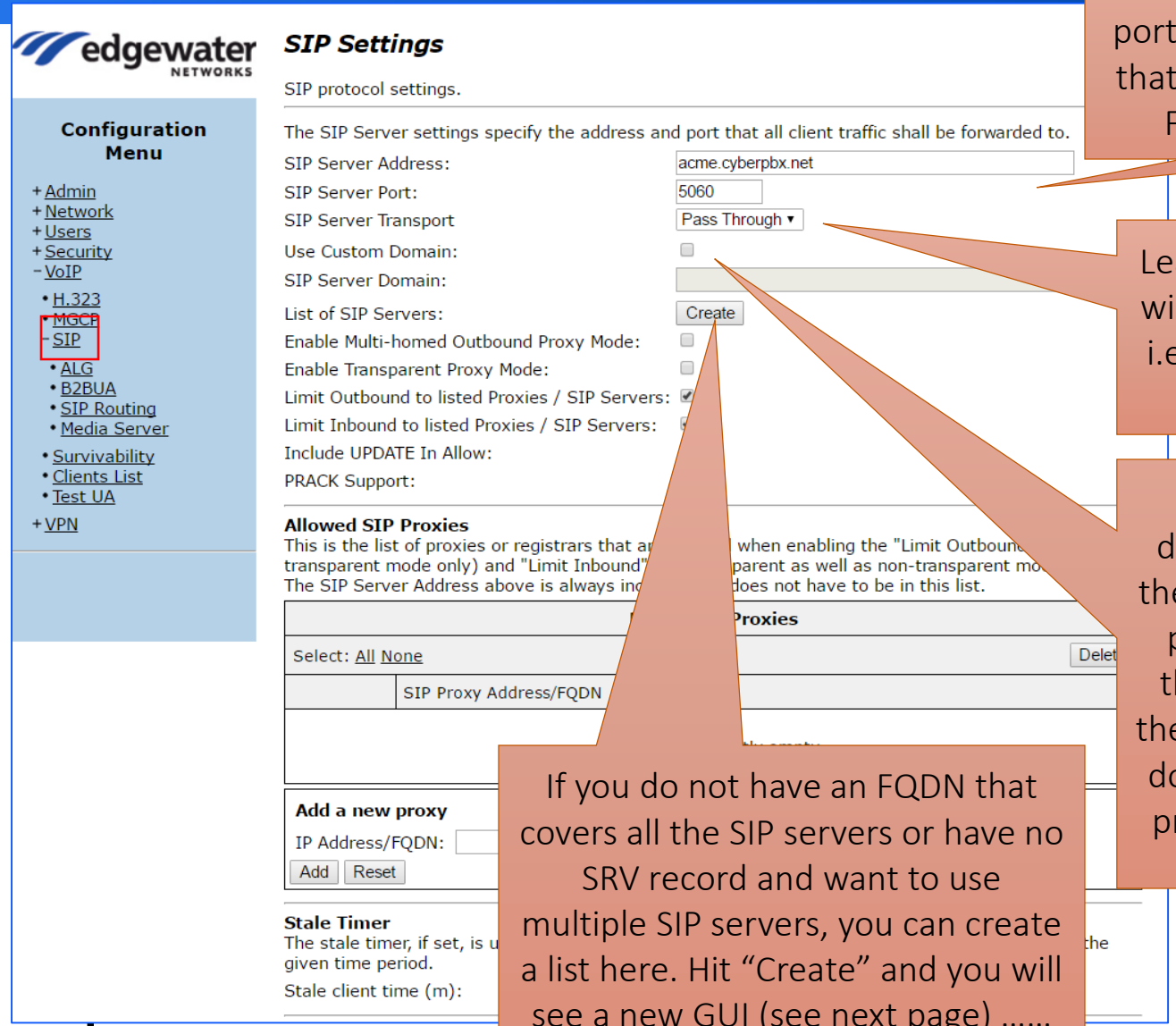
If an external network entity such as a firewall is configured to allow only a range of ports for TCP, then configure the port range here. his specifies the range of TCP listening sockets used on the device to accept incoming H.225 or H.245 TCP connections. If there is a firewall in front of the system, that firewall must allow TCP connections to this range to reach this system.

Client list lockdown locks the EdgeMarc client list. Nothing can register behind the EdgeMarc once this is enabled.

RTP port range used by the EdgeMarc. (This ports are reserved and in the NOTRACK range)



If you have the license “RTP range MOS scoring: ON”. Otherwise, this field is not there. Basically, the EdgeMarc can score RTP out of the normal range



SIP server address and signaling port of the SIP server. Blank means that ALG disabled. When putting a FQDN, make sure it resolves

Leave it as “Pass Through”. The ALG will not alter the transport protocol i.e. if it receives SIP TCP, it will pass through SIP TCP.

If you need to use a custom domain, check this box and enter the domain. The ALG will only allow packets that match that domain through. Also, in Registrar mode, the EdgeMarc will substitute the SIP domain on the phone with what is programmed here and send it out the WAN.

If you do not have an FQDN that covers all the SIP servers or have no SRV record and want to use multiple SIP servers, you can create a list here. Hit “Create” and you will see a new GUI (see next page) ……

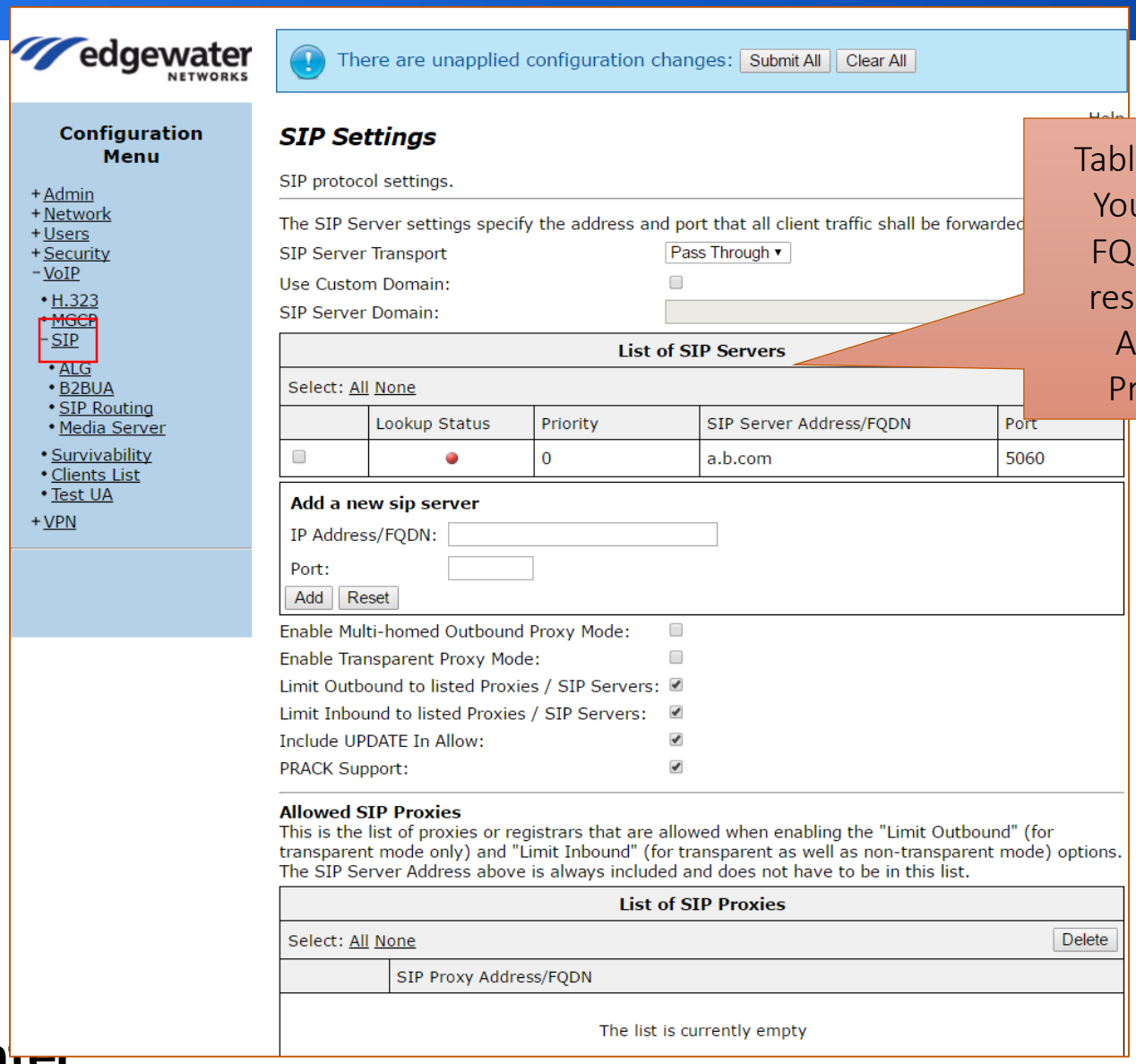
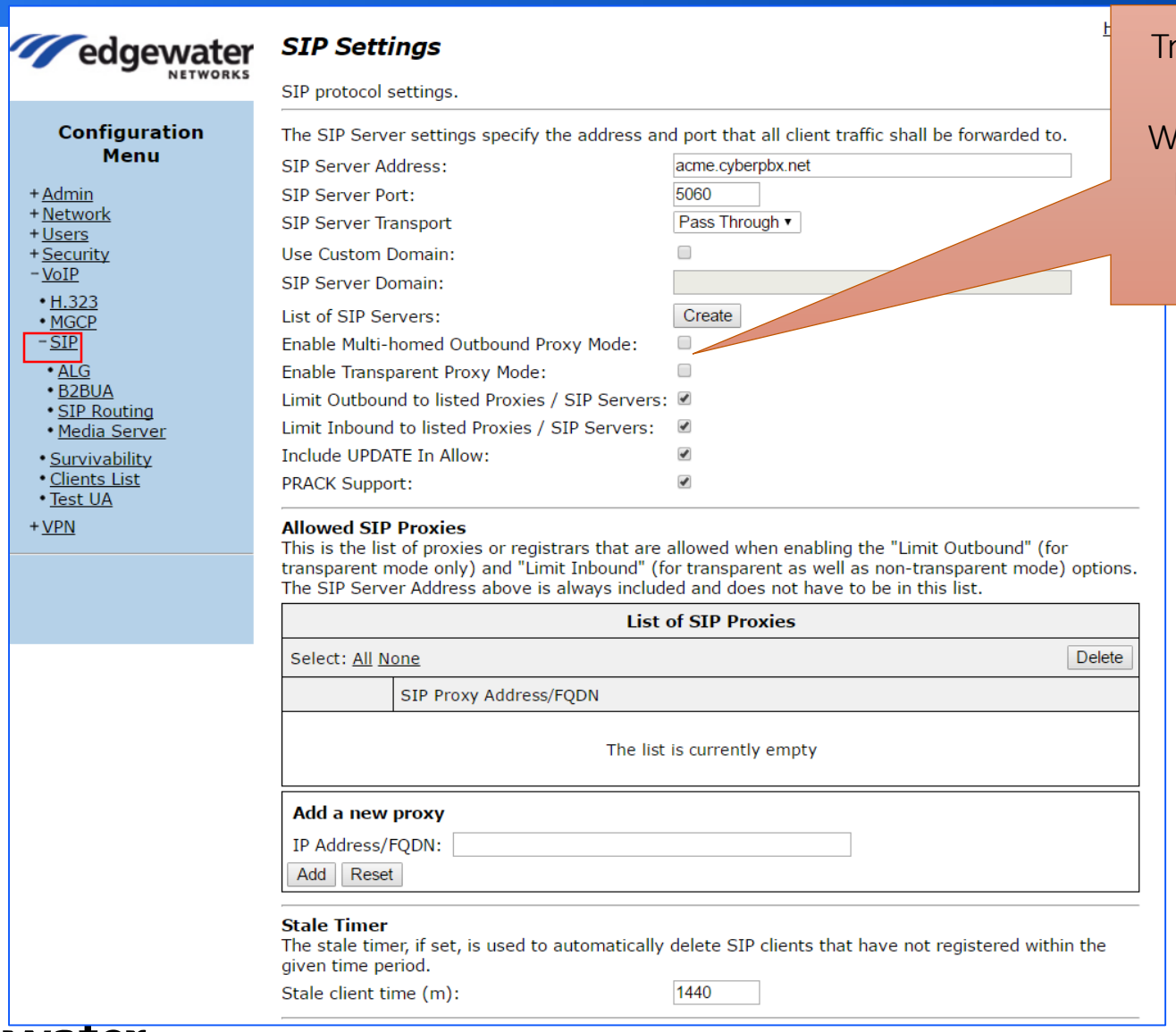


Table to enter list of SIP servers. You can enter IP addresses or FQDN. Make sure they can be resolved. Note: The SIP server Address field disappeared. Priority 0 is highest priority.

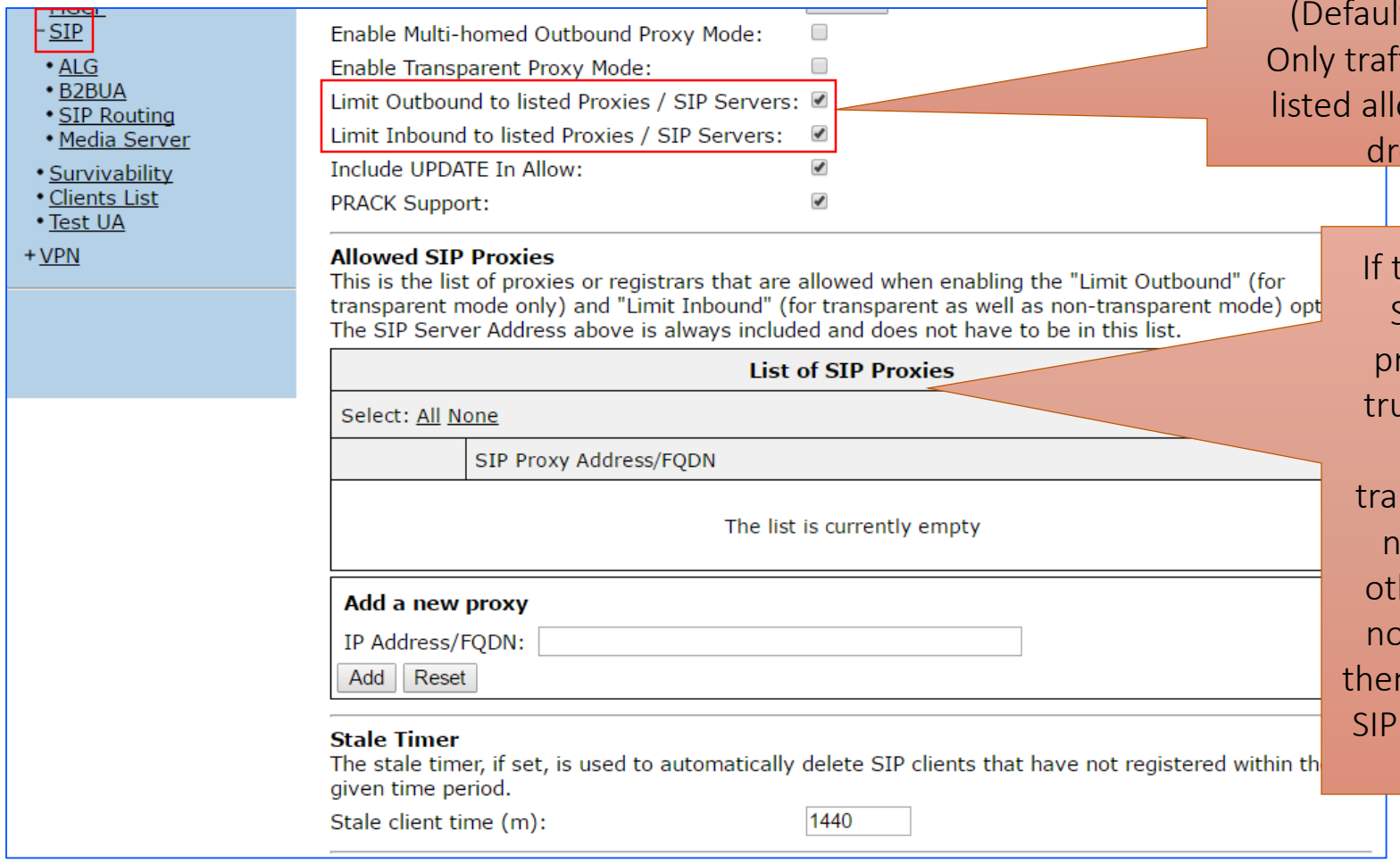
SIP page 2



Transparent Mode / Multi homes ORP mode. (default = off)
When phone SIP Server is not the EdgeMarc (pointing directly to cloud), you need to enabled transparent mode.

Terminology to learn
Registrar mode
Proxy mode
OBP mode
Transparent mode
Multi-homed mode

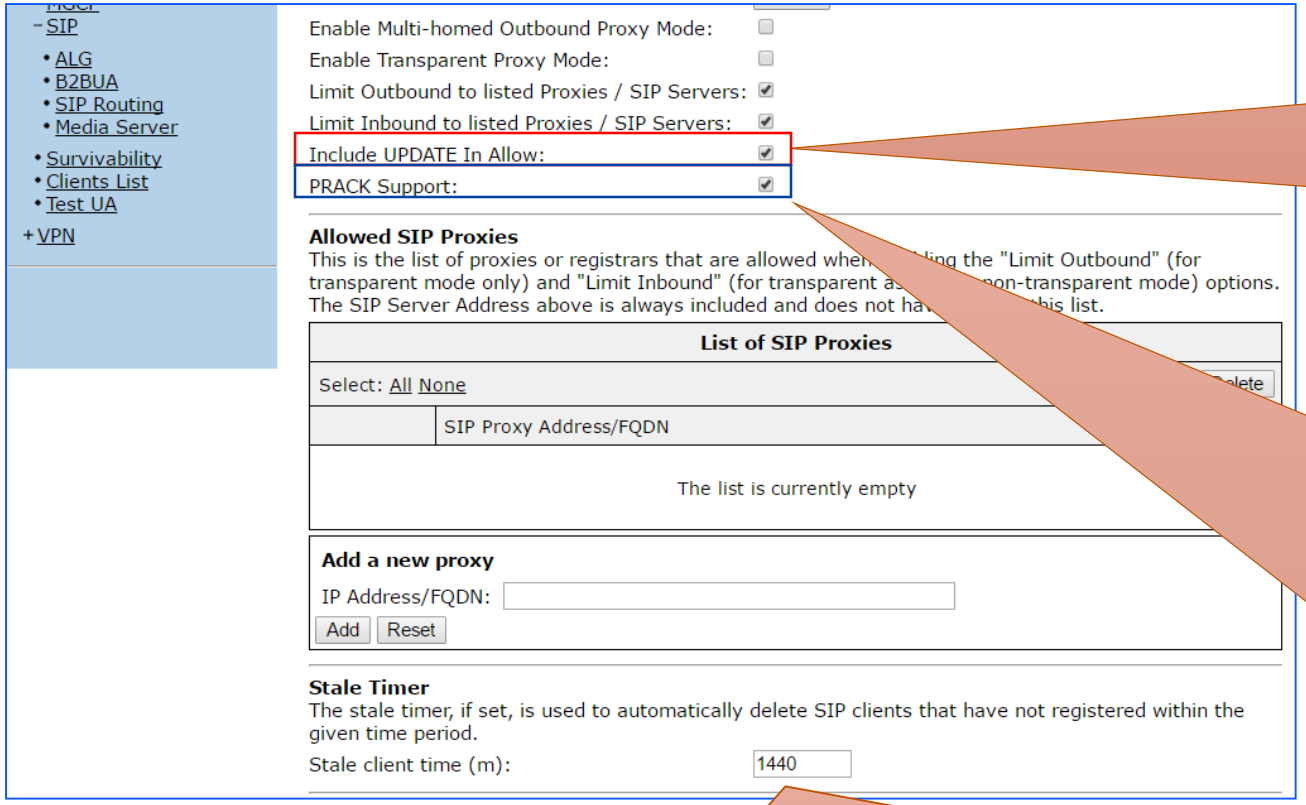
7.0: SIP page 3



Security feature – prevent unauthorized SIP calls (Default = Enabled) Only traffic SIP servers listed allowed. Others dropped.

If there are other SIP servers or proxies that are trusted (example phones in transparent mode need to talk to other SIP servers not listed), enter them into the list of SIP proxies (white-list)

7.0: SIP page 4



Include Update is Allow – only applicable in B2BUA mode.

The default behavior is to add the UPDATE method in the Allow header. Turning off this setting will exclude the UPDATE method from the Allow header.

PRACK Support (B2BUA)

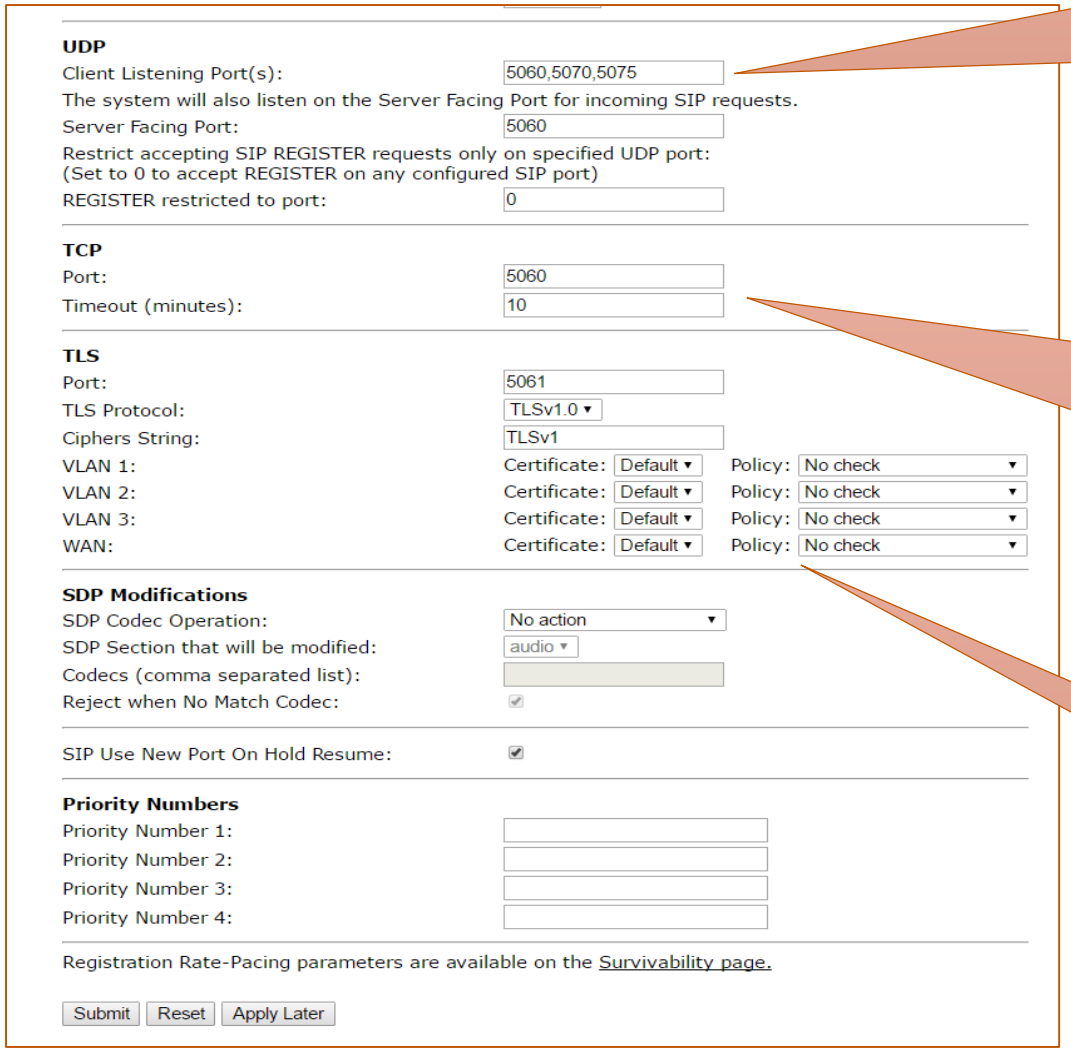
SIP PRACK interoperability provides B2BUA support to allow an endpoint that does not support PRACK to interoperate with an endpoint that requires PRACK support.

When enabled, the system will add **Supported: 100rel** in the SIP INVITE or add **Required: 100rel** in the 18X response messages the systems B2BUA sends out.

Stale Timer. Default = 1 day

If the client is in the client list and is no longer online, the client list will purge out after 1 day. This is to cater for clients that may fill up the client list but are no longer online. If the value = 0, table never flushes

7.0: SIP page 5

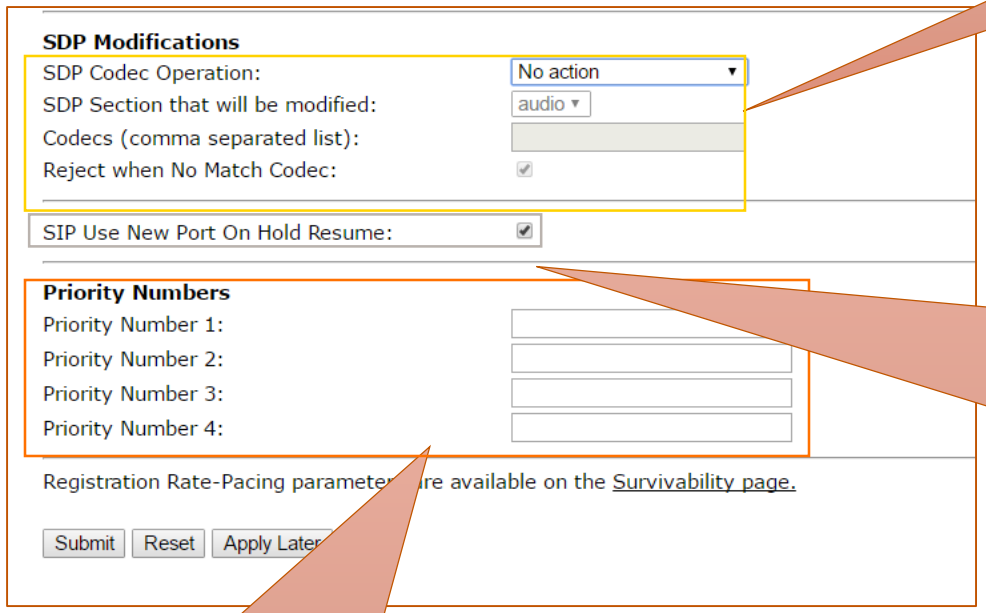


UDP SIP ports.
Client listening port = ALG will listen to those ports for any SIP request
Server Facing port = port that the SIP server is listening to.

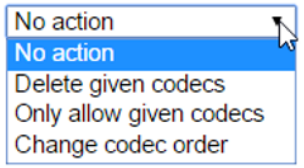
TCP SIP ports.
TCP port that the EdgeMarc WAN will listen for TCP SIP.
Timeout = when there is no activity for the amount of time, the ALG will close the TCP port until a new request

Configure TLS settings here

7.0: SIP page 6



You can configure the ALG to reorder from the INVITE



Prior to 14.1.1, a Hold and Resume resulted in the ALG re-using the same RTP port. Some cases if caused 1-way audio.

Version 14.1.1 introduced feature to use new port. However, it caused problems with other customers. So, in 14.2.0, toggle added.

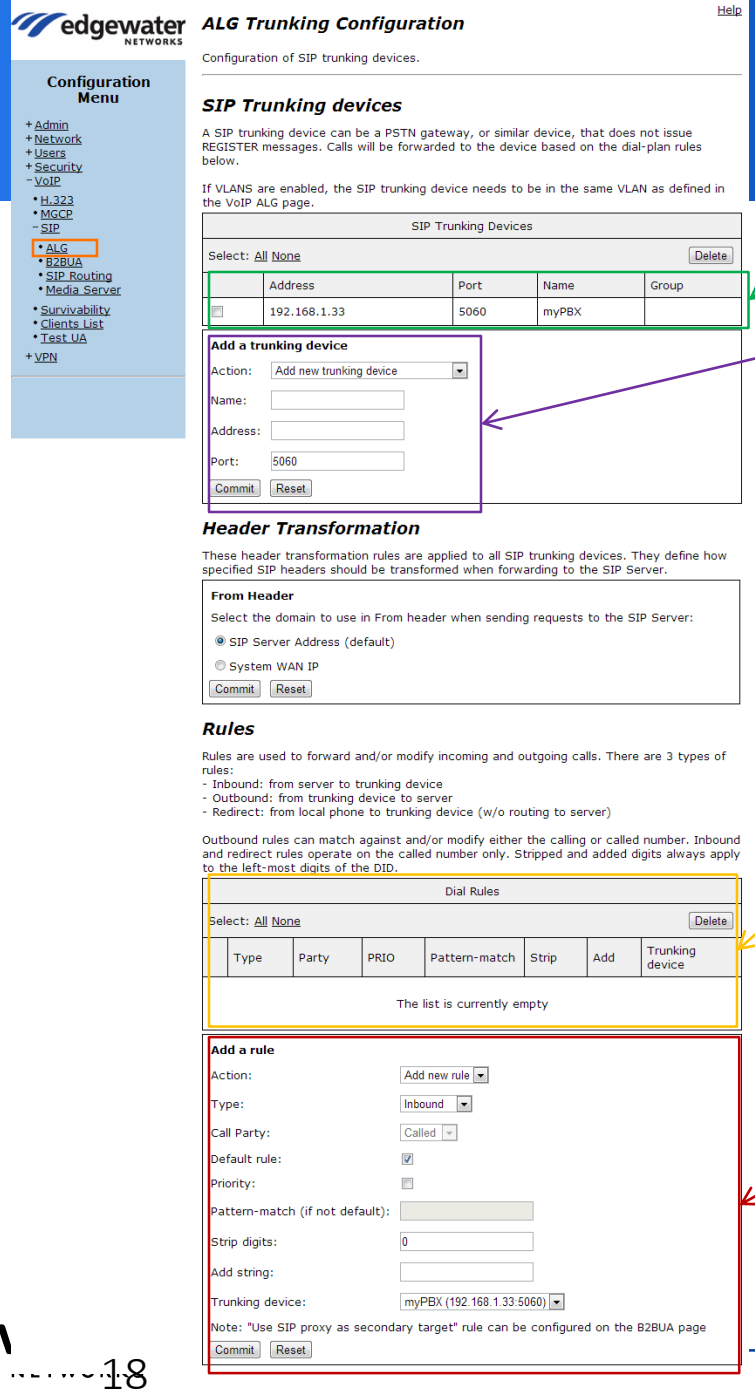
ON by default = New behavior

A call to (up to) 4 Priority Calling numbers (from any ALG/B2BUA Trunking Devices or Registered lan clients) are processed even after CAC limit is reached, by pre-empting any non-priority call.

How to route calls with ALG

- The ALG can provide routing capability based on regular expression detection on incoming or outgoing or redirect calls to a defined trunk group:
  - Legacy PBX or IP PBX
  - Local Gateway
  - PRI
  - FXO/FXS
- It can also remove digits and add digits from the

Company Confidential



List of Trunking Device

Create a new Trunking Device on the LAN side

List of Rules

Add rule:
- Select type: inbound, outbound, redirect
- Call party: Called or calling
- Default rule or match pattern
- Strip and/or add digit from the called number
- Send to Trunking device

Company Confidential

18

Matching rules

- Pattern definitions

.	Matches one or more digits.
[x-y]	Matches any single digit between x and y (inclusive). For example, [1-3], matches 1, 2 or 3
X	Matches any digit between 0 and 9, equivalent to [0-9]
Z	Matches any digit between 1 and 9, equivalent to [1-9]
N	Matches any digit between 2 and 9, equivalent to [2-9]

- Pattern examples

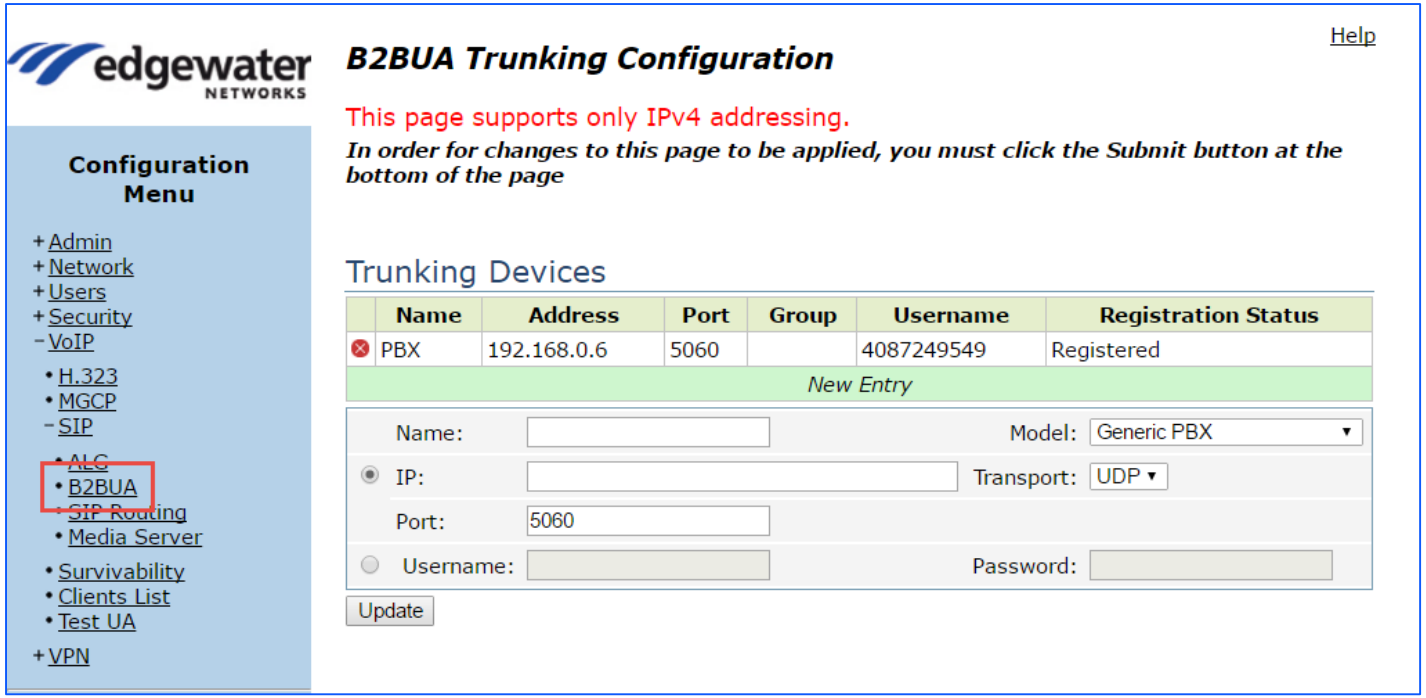
1XXX	Matches any four-digit number starting with 1, e.g. 1000, 1200, 1234
9NXXXXXX	Local calls preceded by a 9, e.g. 95551234
91NXXNXXXXXX	Long distance calls preceded by a 9, e.g. 914085551234

Company Confidential

How use the B2BUA

- The B2BUA can provide routing capability based on regular expression detection on incoming or outgoing or redirect calls to a defined trunk group:
  - Legacy PBX or IP PBX
  - Local Gateway
  - PRI
  - FXO/FXS
- Use it when Advanced SIP Header Manipulation needed
- It also allows the EdgeMarc to register to the Softswitch (for example for the SIP trunking deployment) on behalf of the PBX

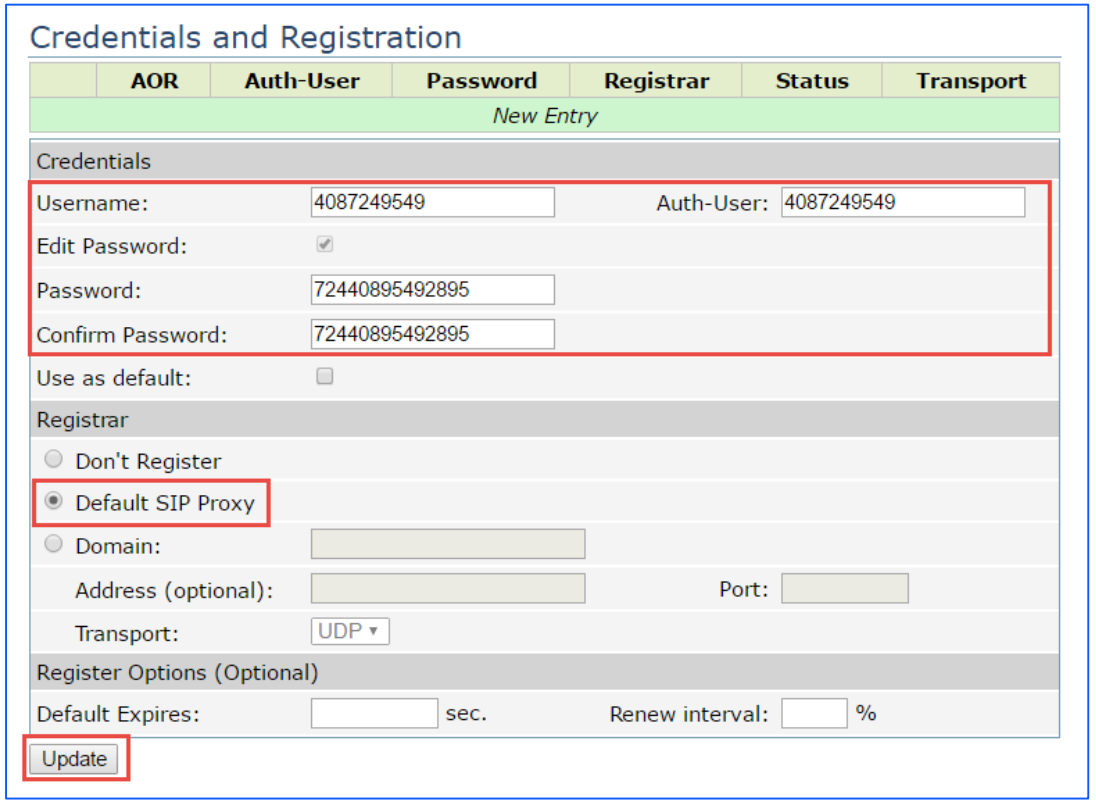
B2BUA page – Trunking Device



Enter the trunking device on the LAN side here.

You can either enter a static IP address or Username/Password (credentials) that the PBX is Registering with.
In this example, I entered the Username/Password and when the PBX registered, it filled in the IP address.

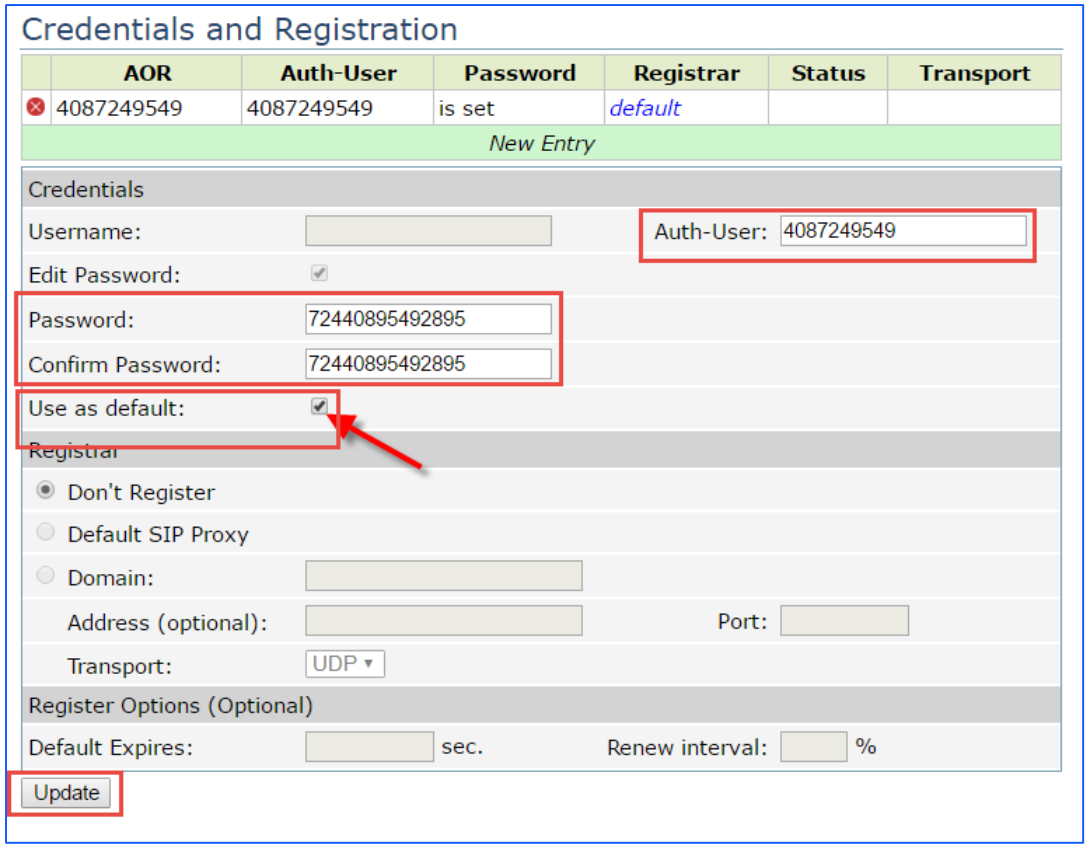
B2BUA – Credentials & Registration



Configure the credentials that the B2BUA will use to register on behalf of the PBX. Also select the Registrar method.

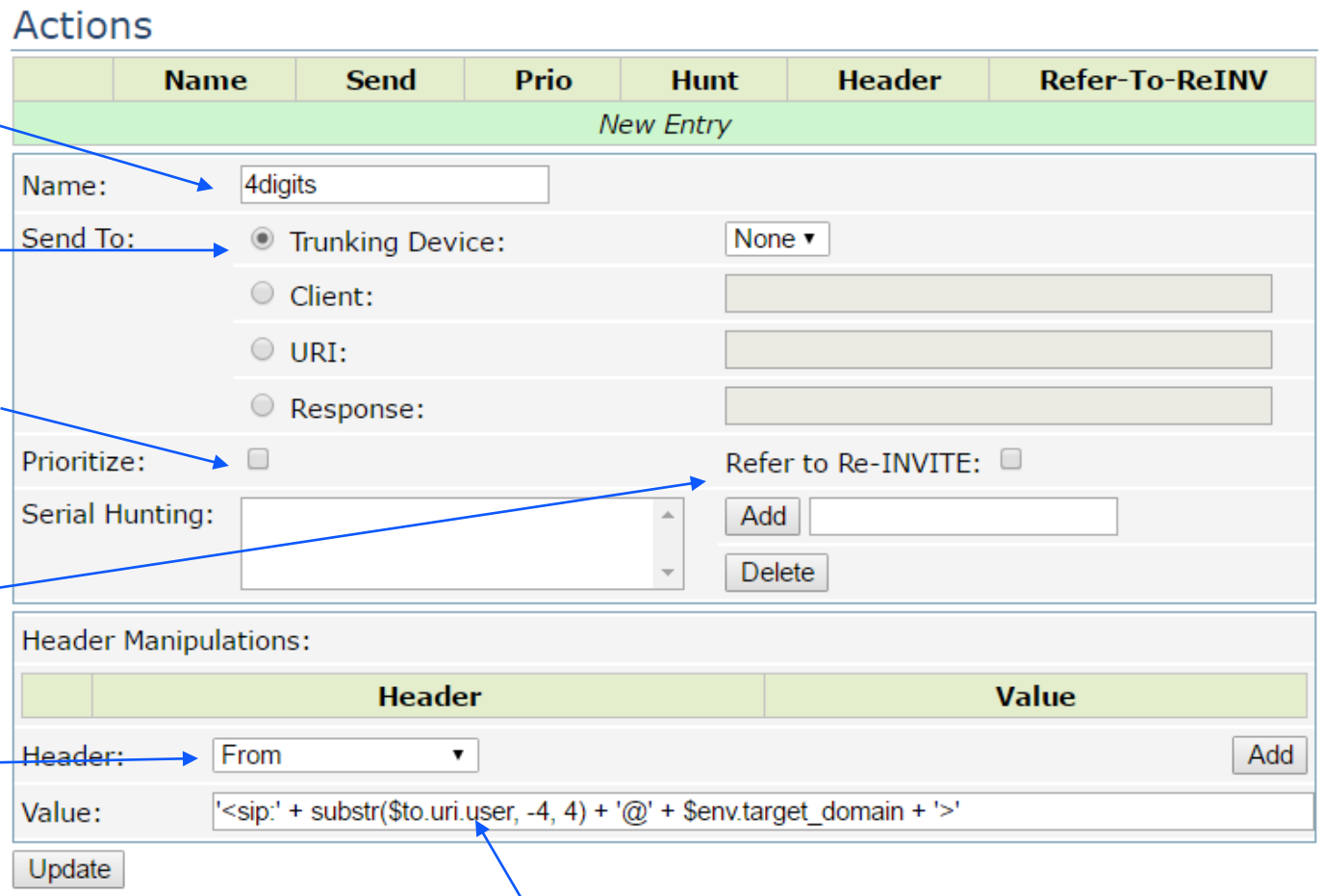
Default SIP proxy means that the SIP server address defined on the SIP page

B2BUA – Credentials & Registration



If the SIP server is set to challenge the INVITE, and the PBX doesn't support any Authentication, then you want the B2BUA to respond to the 401 Unauthorized sent by the SIP server. Configure the 'Use as Default' for the B2BUA to respond to 401s and not pass it through to the PBX.

B2BUA – Actions



Enter the Action name

Select the type of target and enter/select the target

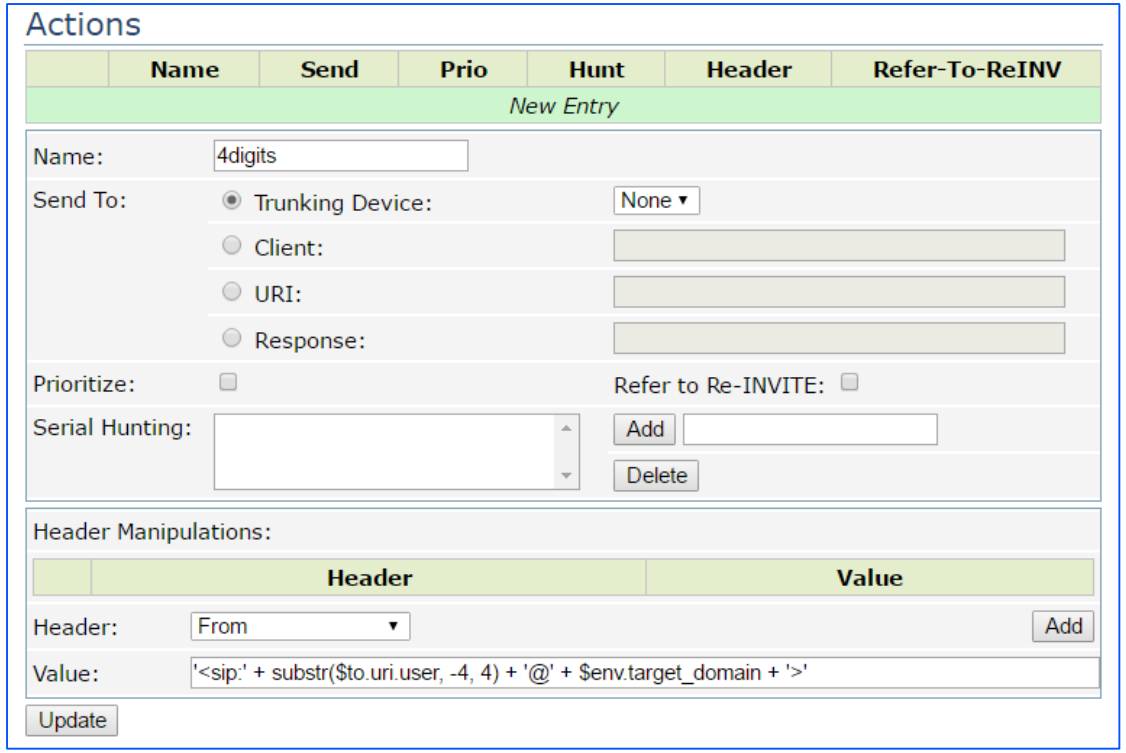
Prioritize: if the FXO lines are all busy it will force a call to be stopped and this one to be placed

Convert Refer to Re-invite (only if SIP server doesn't support REFER messages

Select the Header you want to change

Add the rule you want to be applied

B2BUA – Actions



Action added to strip 6 leading digits and only send 4 digits

B2BUA – Match rule

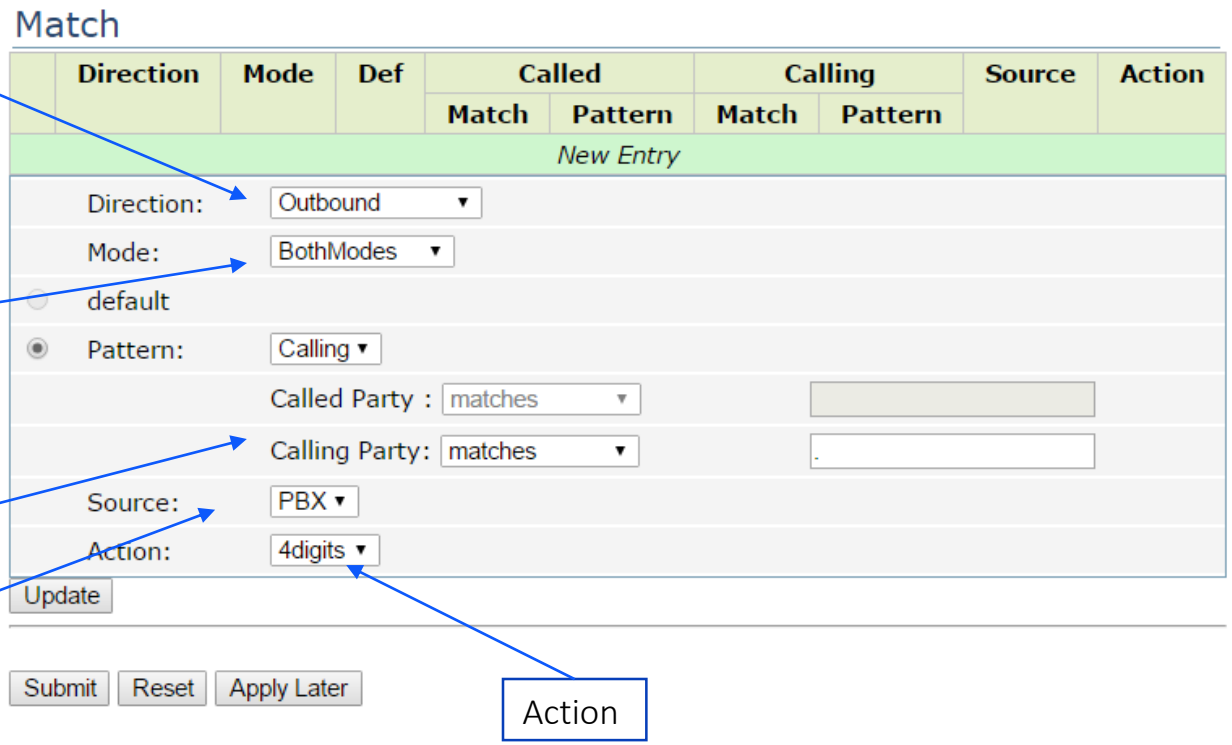
Add a match rule to apply the Actions

Apply in this direction only
Outbound = from PBX to SS
Inbound = incoming from SS
REFER intiated = for Refer to Reinvite only

When to apply this rule
Both modes = all the time
Local Mode off = only in remote mode
Local Mode on = only in local mode

Pattern Match

Source



Action

Hit Update
Hit Submit

Header Manipulation

- Enable to customize the SIP headers content
- Add custom headers
- Allow the usage of global variables issued from the SIP headers
- Allow the usage of function to manipulate the global variables

HMR syntax

- The header value is entered as a concatenation of segments using the "+" sign:
  - segment#1 + segment#2 +…+ segment#n
- Each segment can be:
  - *Literal:* A string literal should be enclosed in single quotes. Example **'sip:'**.
  - *Variable:* One of the pre-defined variables (extracted values from the received SIP message or the environment). Variables are written preceded with a '$' sign. Example: **$from.uri.user**.
  - *Function:* They operate on the variables and insert the result into the value.

HMR: SIP messages

- *Extract of SIP message:*

INVITE sip:1119653046@192.20.137.98:5060 SIP/2.0

Via: SIP/2.0/UDP182.19.6.115:5060;branch=z9hG4bK1sansay3598643rdb80

Record-Route:<sip:sansay3598643rdb80@182.19.6.115:5060;lr;transport=udp>

To: <sip:3239653046@192.20.137.98>

From: "JOHN DOE "<sip:+18282868990@182.19.6.115>;tag=sansay3598643rdb80

Call-ID: 2100413-0-651057500@123.149.209.113

CSeq: 1 INVITE

Contact: <sip:+18282868990@182.19.6.115:5060>

Supported: replaces

Max-Forwards: 26

List of headers:

- Request URI
- To
- From
- Contact

HMR variables (see Help page)

Header Name	Variable	Remark
From	$from.dispname	Display name
	$from.uri.user	User name portion of the URI
	$from.uri.host	
	$from.uri.port	
	$from.uri.parameter[user	
	$from.uri.header[h1]	
	$from.parameter	
To	Same as From	
Contact	Same as From	
Route	Same as From	
Record-Route	Same as From	
P-Asserted-Identity (PAI)	Same as From	
P-Preffered-Identity (PPF)	Same as From	
Via	$via.ip.host	Value of sent-by
	$via.ip.port	sent-by port
	$via.parameter[branch	Value of parameter 'branch'
Request URI	$request.method	SIP method
	$request.uri.user	Request-URI user
	$request.uri.host	Request-URI host
	$request.uri.port	Request-URI port
Other headers	$diversion.text	Extract the entire diversion header from the received message

Environment variables

Variable Name	Value
$env.in_intf_host	IP Address of the interface on which the message was received
$env.in_intf_port	TCP/IP Port on which the message was received
$env.out_intf_host	IP Address of the interface from which the message will leave EM
$env.out_intf_port	Source port that will be used for sending the message
$env.target_host	IP Address of the destination of the message
$env.target_port	Destination port of the message
$env.target_domain	Domain name of the destination of the message

HMR: Examples with variables

- From header:

From: "JOHN DOE "<sip:+18282868990@182.19.6.115>;tag=sansay3598643rdb80

- $from.dispname = *JOHN DOE*
- $from.uri.user = *+18282868990*
- $env.*target_domain* = *182.19.6.115*

Without modification, this is what you would enter in the Header's Value:

$from.dispname + '<sip:' + $from.uri.user + '@' + $env.target_domain + '>;tag=sansay3598643rdb80'

- Contact header:

Contact: <sip:+18282868990@182.19.6.115:5060> sip:+18282868990@182.19.6.115:506

- $contact.uri.user = *+18282868990*
- $env.target_domain = *182.19.6.115*
- $contact.target.port = *5060*

Without modification, this is what you would enter in the Header's Value:

'<sip:' + $contact.uri.user + '@' + $env.target_domain + ':' + $contact.target.port + '>'

Function: substr()

- substr() function extracts a sub-string of length "*len*" from the src_string starting at index "*start_index*“
- The first character is index "0", and the second character is index "1".
- If the start_index is negative, counting starts from the end of the string.
- For example "-1" would mean the last character, and "-2" would mean the 2nd to last character. If "*len*" is zero this means the entire string.

Substr() example

- From the following string abcdefghijk, here is the table with the index



1	2	3	4	5	6	7	8	9	10	11
A	B	C	D	E	F	G	H	I	J	K
-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1

substr ($var, # of digits to strip, # of digits to return after that point)

Striping the 2 first digits: substr($var, 2, 0) gives cdefghijk as result (good example to strip the +1 from the from)

Extract 4 letters from the right: substr($var, -4, 4), the output is hijk

Drop the 5 last letters: substr($var, 0, 6)

Substr() example (google it)

http://php.net/manual/en/function.substr.php

HMR examples

- From header:

From: "JOHN DOE "<sip:+18282868990@182.19.6.115>;tag=sansay3598643rdb80

- $from.dispname = JOHN DOE
- $from.uri.user = +18282868990
- $env.target_domain = 182.19.6.115

Remove the +1 from the FROM header:

$from.dispname + *'<sip:'* + *substr*($from.uri.user,*2,0)* + *'@'* + $env.target_domain + *'>;tag=sansay3598643rdb80'*

- To add 1 to the To header:

'<sip:1' + $to.uri.user + '@' + $env.target_domain + '>'

- To remove the 6 first digits from the To and Request URI Header:

'sip:' + substr($request.uri.user, 6, 0) + '@' + $env.target_host

Function: replace()

- replace() function searches the "src_string" for all occurrences of "search_string" and replaces them with "replace_value“
- For example: to replace in a variable, 88 by 101
  - replace($var, ’88’,’101’)
  - If the value of $variable was 192.168.88.22, the result of the function is going to be:
    - 192.168.101.22

Reminder with HMR

- When you are modifying the number called, you must apply HMR to the To and the Request URI headers
- When you are modifying the calling number, you must apply the HMR to the From and Contact headers
  - the uri part must be identical

- *When you are changing the Request URI Header there is no '< >' in the header!!!*

B2BUA – Example (Change From to 4 digits)

LAN

21:10:02.877193 192.168.0.6.50289 > 192.168.0.1.5060:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
INVITE sip:14083517226@192.168.0.1;user=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.0.6:5060;branch=z9hG4bK42c0a5fd
From: "9549"
<sip:4087249549@192.168.0.1>;tag=003094c317c6924c3323d156-1973cb1a
To: <sip:14083517226@192.168.0.1;user=phone>
Call-ID: 003094c3-17c60004-7c246695-5b0e9d5d@192.168.0.6
Max-Forwards: 70
CSeq: 101 INVITE
User-Agent: Cisco-CP7960G-#7/8.0
Contact: <sip:4087249549@192.168.0.6:5060;transport=udp>
Expires: 180
Accept: application/sdp
Allow:
ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE
Supported: replaces;join;norefersub
Content-Length: 270
Content-Type: application/sdp
Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 2392 0 IN IP4 192.168.0.6
s=SIP Call
t=0 0
m=audio 26220 RTP/AVP 0 8 18 101
c=IN IP4 192.168.0.6
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/0
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv

WAN

21:10:02.907704 40.140.44.118.5060 > 74.112.29.118.7281:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
INVITE sip:14083517226@acme.cyberpbx.net:7281 SIP/2.0
Via: SIP/2.0/UDP 40.140.44.118:5060;branch=z9hG4bK1760566199
Route: <sip:74.112.29.118:7281;transport=udp;lr>
From:
<sip:7226@acme.cyberpbx.net>;tag=3az08xr7xj4hDIJ5I3947B83550babe0
To: <sip:14083517226@acme.cyberpbx.net>
Call-ID: 2026855649@40.140.44.118
CSeq: 786 INVITE
Contact: <sip:4087249549@40.140.44.118:5060>
Supported: 100rel
Max-Forwards: 70
User-Agent: ewb2bua/14.7.0
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER, UPDATE
Content-Type: application/sdp
Content-Length: 274

v=0
o=Cisco-SIPUA 2392 0 IN IP4 40.140.44.118
s=SIP Call
t=0 0
m=audio 16584 RTP/AVP 0 8 18 101
c=IN IP4 40.140.44.118
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/0
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv

From	'<sip:' + substr($to.uri.user, -4, 4) + '@' + $env.target_domain + '>'

B2BUA – Example (only send 4 digits in Request URI)

LAN

23:28:41.246786 192.168.0.6.50289 > 192.168.0.1.5060:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
INVITE sip:14083517226@192.168.0.1;user=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.0.6:5060;branch=z9hG4bK2a0b3281
From: "9549"
<sip:4087249549@192.168.0.1>;tag=003094c317c692ea6833d4b1-05ff8c02
To: <sip:14083517226@192.168.0.1;user=phone>
Call-ID: 003094c3-17c6000d-4426c4b9-47fb68a2@192.168.0.6
Max-Forwards: 70
CSeq: 101 INVITE
User-Agent: Cisco-CP7960G-#7/8.0
Contact: <sip:4087249549@192.168.0.6:5060;transport=udp>
Expires: 180
Accept: application/sdp
Allow:
ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE
Supported: replaces;join;norefersub
Content-Length: 271
Content-Type: application/sdp
Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 23165 0 IN IP4 192.168.0.6
s=SIP Call
t=0 0
m=audio 26238 RTP/AVP 0 8 18 101
c=IN IP4 192.168.0.6
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/0
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv

WAN

23:28:41.275614 40.140.44.118.5060 > 74.112.29.118.5060:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
INVITE sip:7226@74.112.29.118 SIP/2.0
Via: SIP/2.0/UDP 40.140.44.118:5060;branch=z9hG4bK1681630567
From: "9549"
<sip:4087249549@acme.cyberpbx.net>;tag=3az08hPD5mraGWKok246578256c68051
To: <sip:14083517226@acme.cyberpbx.net>
Call-ID: 2003091281@40.140.44.118
CSeq: 786 INVITE
Contact: <sip:4087249549@40.140.44.118:5060>
Supported: 100rel
Max-Forwards: 70
User-Agent: ewb2bua/14.7.0
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER, UPDATE
Content-Type: application/sdp
Content-Length: 275

v=0
o=Cisco-SIPUA 23165 0 IN IP4 40.140.44.118
s=SIP Call
t=0 0
m=audio 16584 RTP/AVP 0 8 18 101
c=IN IP4 40.140.44.118
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/0
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv

Request-URI	'sip:' + substr($request.uri.user, -4,4) + '@' + $env.target_host

B2BUA – Example (Add +1 to Request URI and To)

LAN

```
19:37:40.226851 192.168.0.6.50289 > 192.168.0.1.5060:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
INVITE sip:4083517200@192.168.0.1;user=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.0.6:5060;branch=z9hG4bK0c671e12
From: "9549"
<sip:4087249549@192.168.0.1>;tag=003094c317c6980b264a7f8a-
1d5f1ebc
To: <sip:4083517200@192.168.0.1;user=phone>
Call-ID: 003094c3-17c6000e-44e02e18-675af8c2@192.168.0.6
Max-Forwards: 70
CSeq: 101 INVITE
User-Agent: Cisco-CP7960G-#7/8.0
Contact: <sip:4087249549@192.168.0.6:5060;transport=udp>
Expires: 180
Accept: application/sdp
Allow:
ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE
Supported: replaces;join;norefersub
Content-Length: 271
Content-Type: application/sdp
Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 18516 0 IN IP4 192.168.0.6
s=SIP Call
t=0 0
m=audio 26240 RTP/AVP 0 8 18 101
c=IN IP4 192.168.0.6
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/0
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

WAN

```
19:37:40.243713 40.140.44.118.5060 > 74.112.29.118.5060:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
INVITE sip:+14083517200@74.112.29.118 SIP/2.0
Via: SIP/2.0/UDP 40.140.44.118:5060;branch=z9hG4bK2036678705
From: "9549"
<sip:4087249549@acme.cyberpbx.net>;tag=3az08Z57hncri1k56C4323A02
670518e
To: <sip:+14083517200@74.112.29.118>
Call-ID: 818091304@40.140.44.118
CSeq: 787 INVITE
Contact: <sip:4087249549@40.140.44.118:5060>
Supported: 100rel
Max-Forwards: 70
User-Agent: <testing>
Allow: ACK, BYE, CANCEL, INVITE, NOTIFY, OPTIONS, REFER, REGISTER,
UPDATE
Content-Type: application/sdp
Content-Length:   275

v=0
o=Cisco-SIPUA 18516 0 IN IP4 40.140.44.118
s=SIP Call
t=0 0
m=audio 16584 RTP/AVP 0 8 18 101
c=IN IP4 40.140.44.118
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/0
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

To	'<sip:+1' + $to.uri.user + '@' + $env.target_host + '>'
Request-URI	'sip:+1' + $request.uri.user + '@' + $env.target_host
User-Agent	'<testing>'

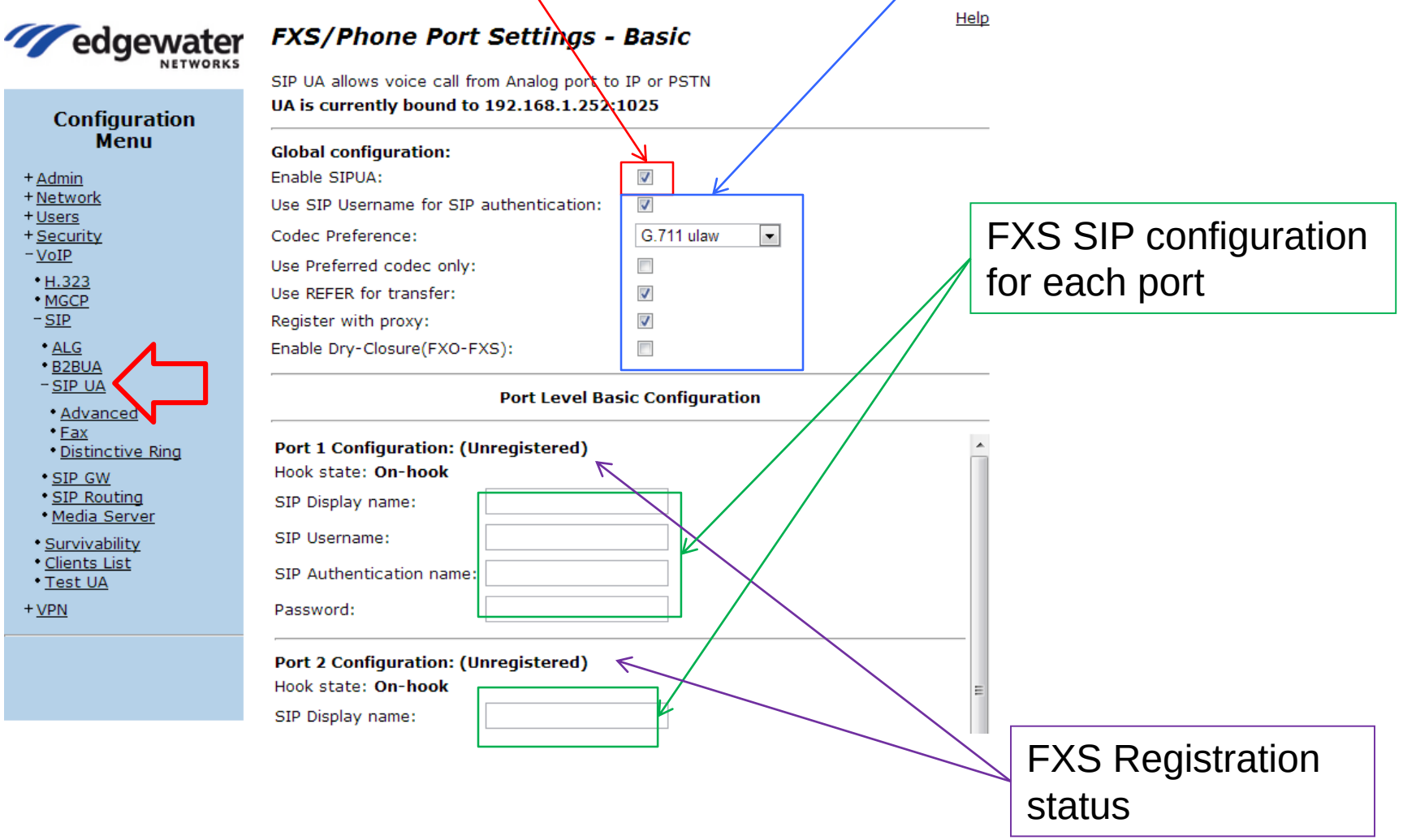
FXS

- Some EdgeMarc models have embedded FXS (Foreign eXchange Subscriber) ports
  - 2, 6 ,8, 24 ports
  - Enabling to connect analog phones, Fax, modem…
  - This allows to recycle the existing implementation (phones and wiring)
- Once enabled the UA is assigned to the IP address .252 (same subnet than the ALG) with the port 1025
- Provides Hunt group capability
- Fax T38
- VAD
- Distinctive ringing

How to configure FXS

Enable SIPUA for FXS usage

Global FXS configuration

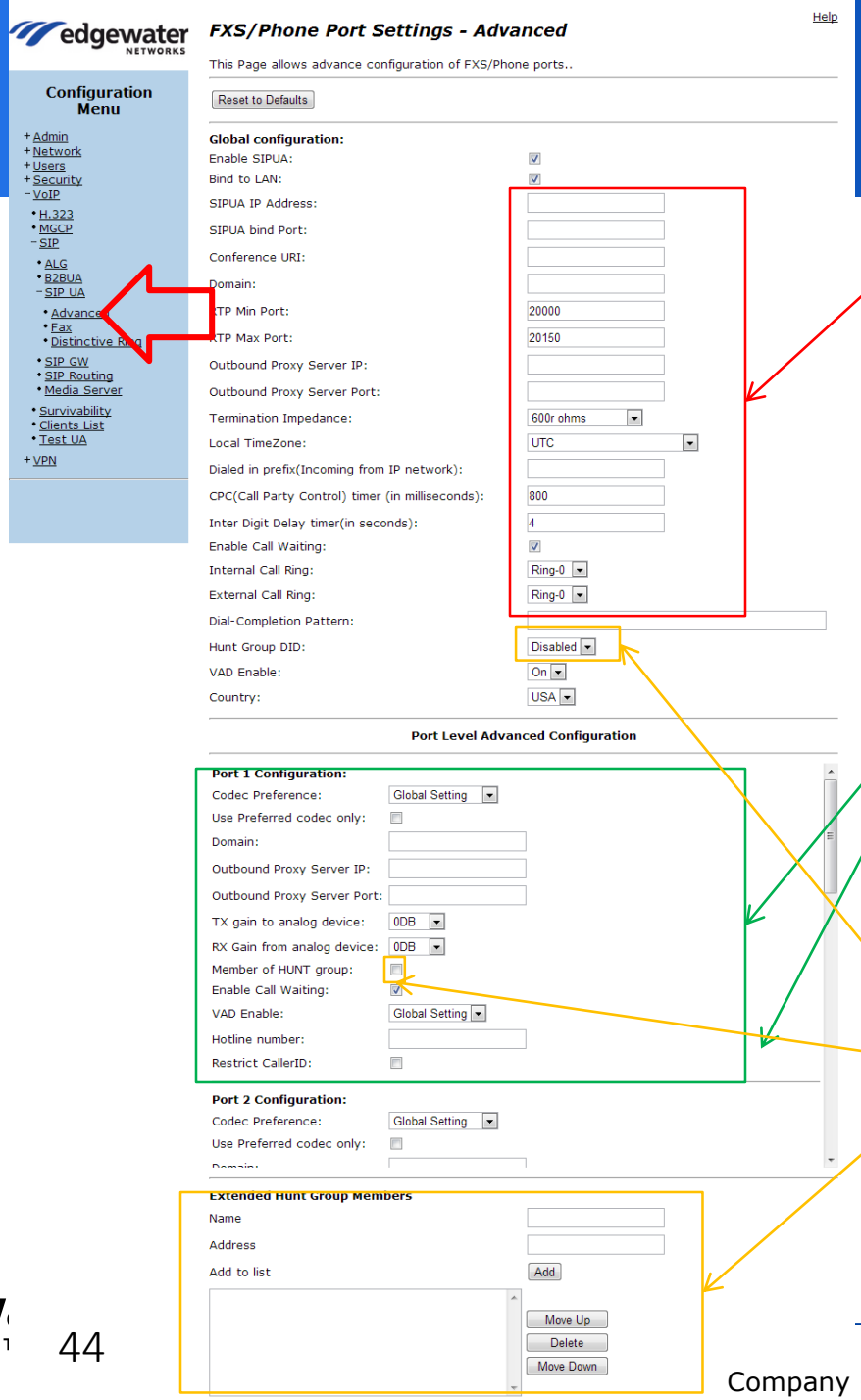


FXS SIP configuration for each port

FXS Registration status

Company Confidential

43



Deeper Global FXS configuration

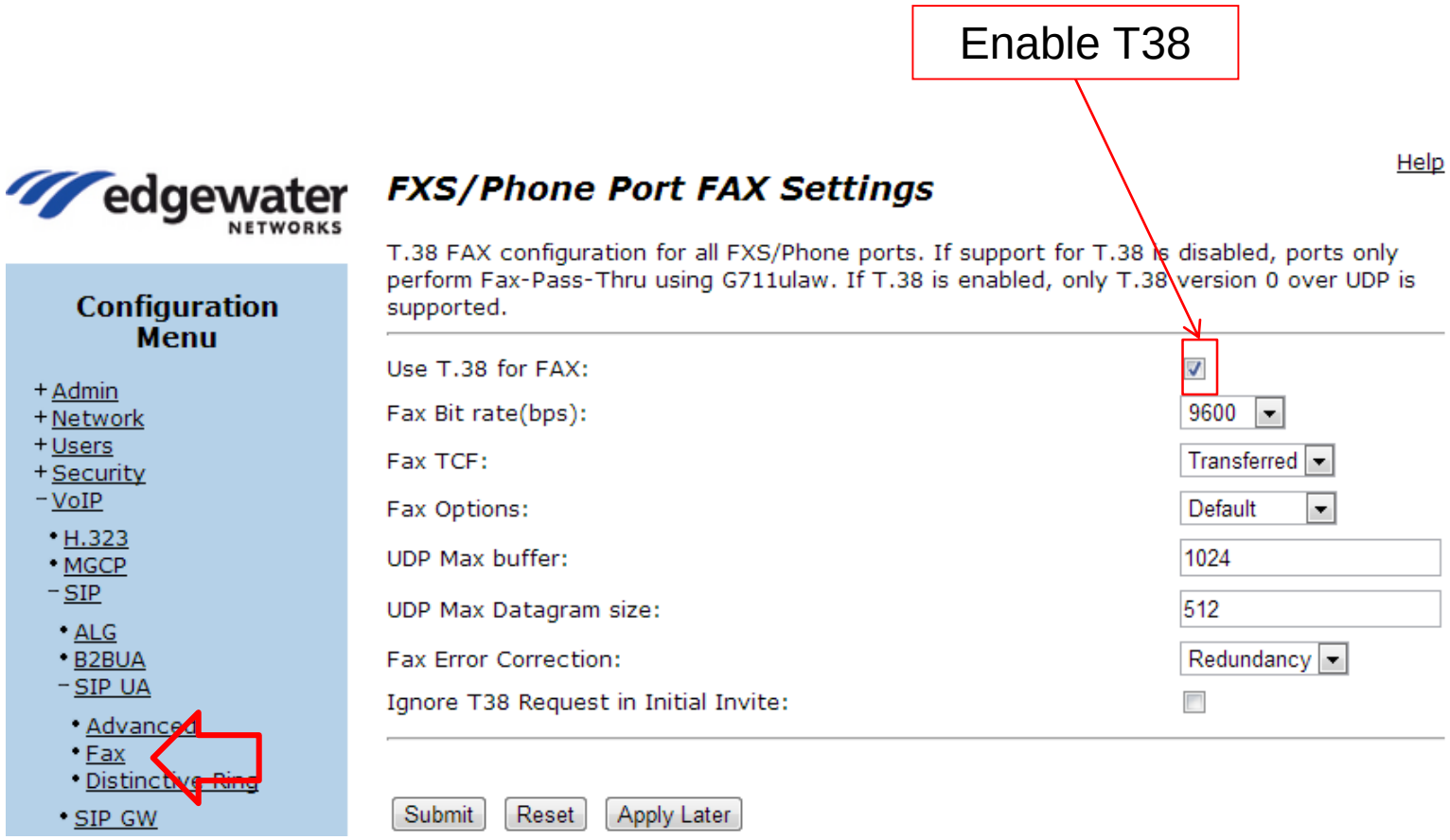
Each FXS port can inherit from the global configuration and be tuned

Hunt group can be configured with FXS (check the hunt group checkbox in the port x configuration). When a call comes to the hunt group, the call is going to go the next available person (make sure that the Call waiting is disabled). You can add none FXS phone to the group and change the order within the list

Company Confidential

44

How to configure Fax and T38

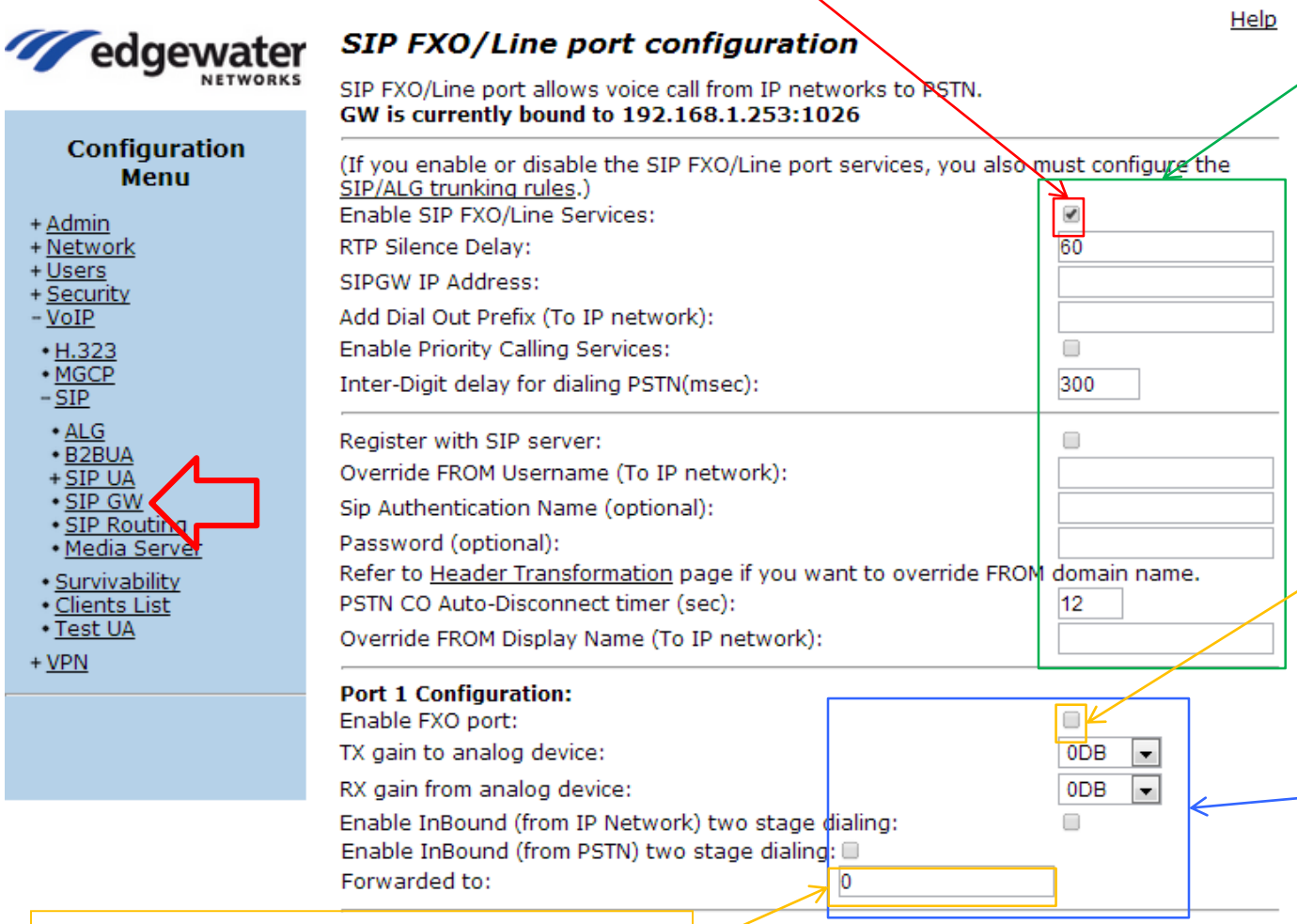


FXO

- Some EdgeMarc models have embedded FXO (Foreign eXchange Office) ports
  - 1, 2 ports
  - Enabling to connect to the PSTN
- Once enabled the ALG is assigning to the IP address .253 (same subnet than the ALG) with the port 1026
- This allows in the event of a WAN failure to enable incoming and outgoing calls from the EdgeMarc (in conjunction with Survivability and call routing)

How to configure FXO

Enable SIPGW for FXO usage



Configure the FXO global configuration

Enable this port

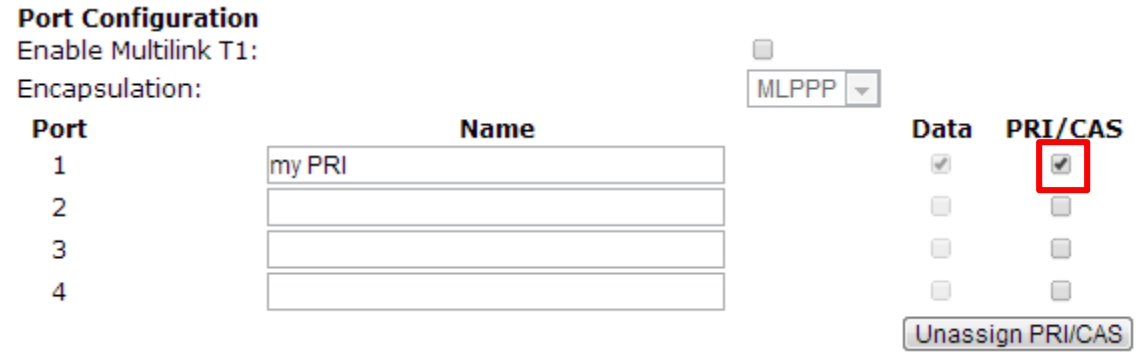
Configure the FXO specific ports

Forward to specific destination

Company Confidential

EdgeMarc and PRI

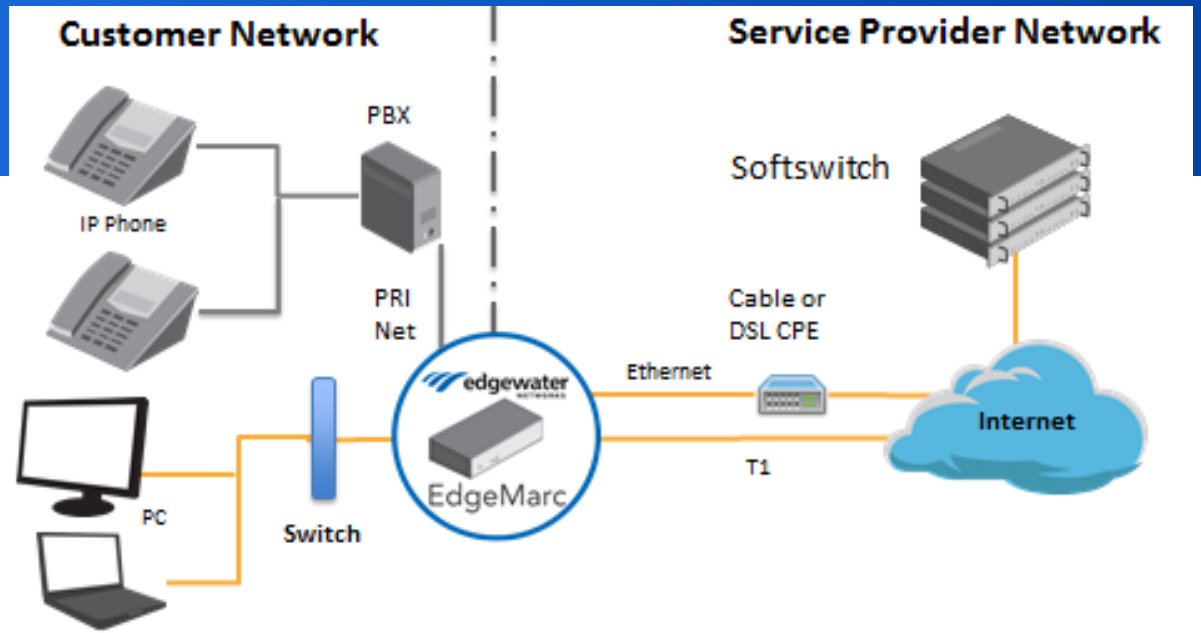
- EdgeMarc can provide PRI connectivity to a Legacy PBX (PRI/Network side) and also to the PSTN (PRI/Client side)
- There is also the CAS (Network and Client side) version
- In the T1/E1 configuration menu, select the PRI/CAS check box for the PRI port



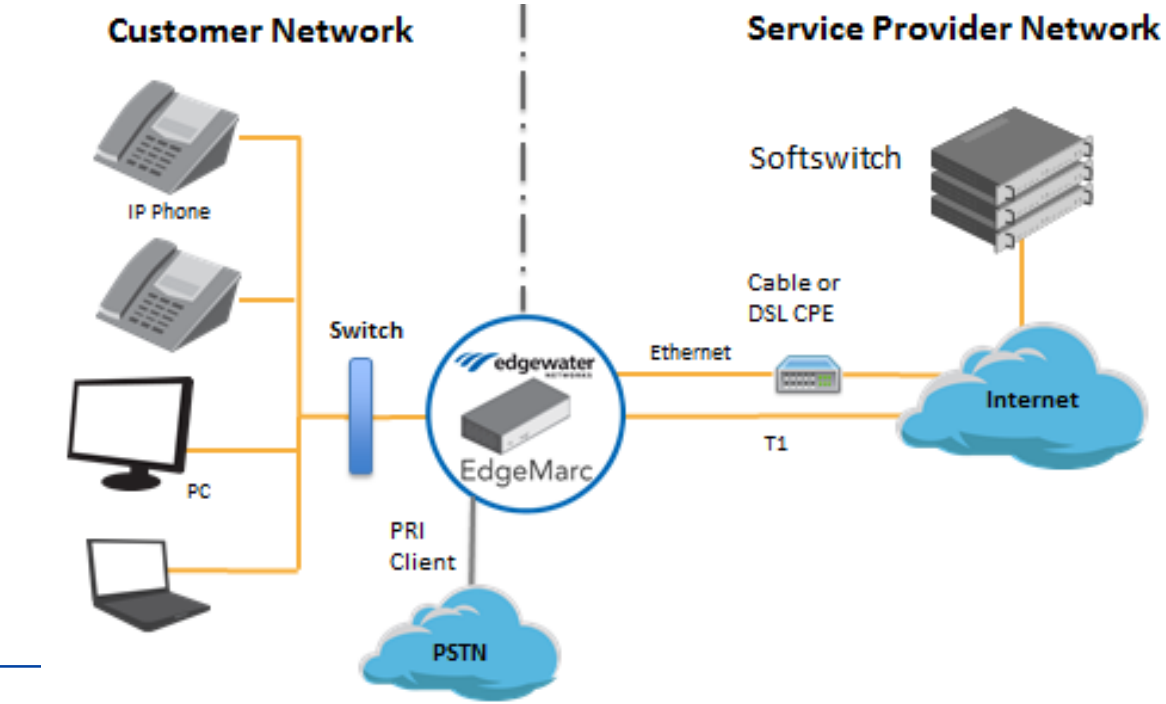
NOTE: On a 4601, if you have a PRI and a T1 data WAN, make sure that the T1 Data WAN is on a lower port compared to the PRI port.
Example: Data = Port 1, PRI = Port 2.

48
Company Confidential

PRI NET

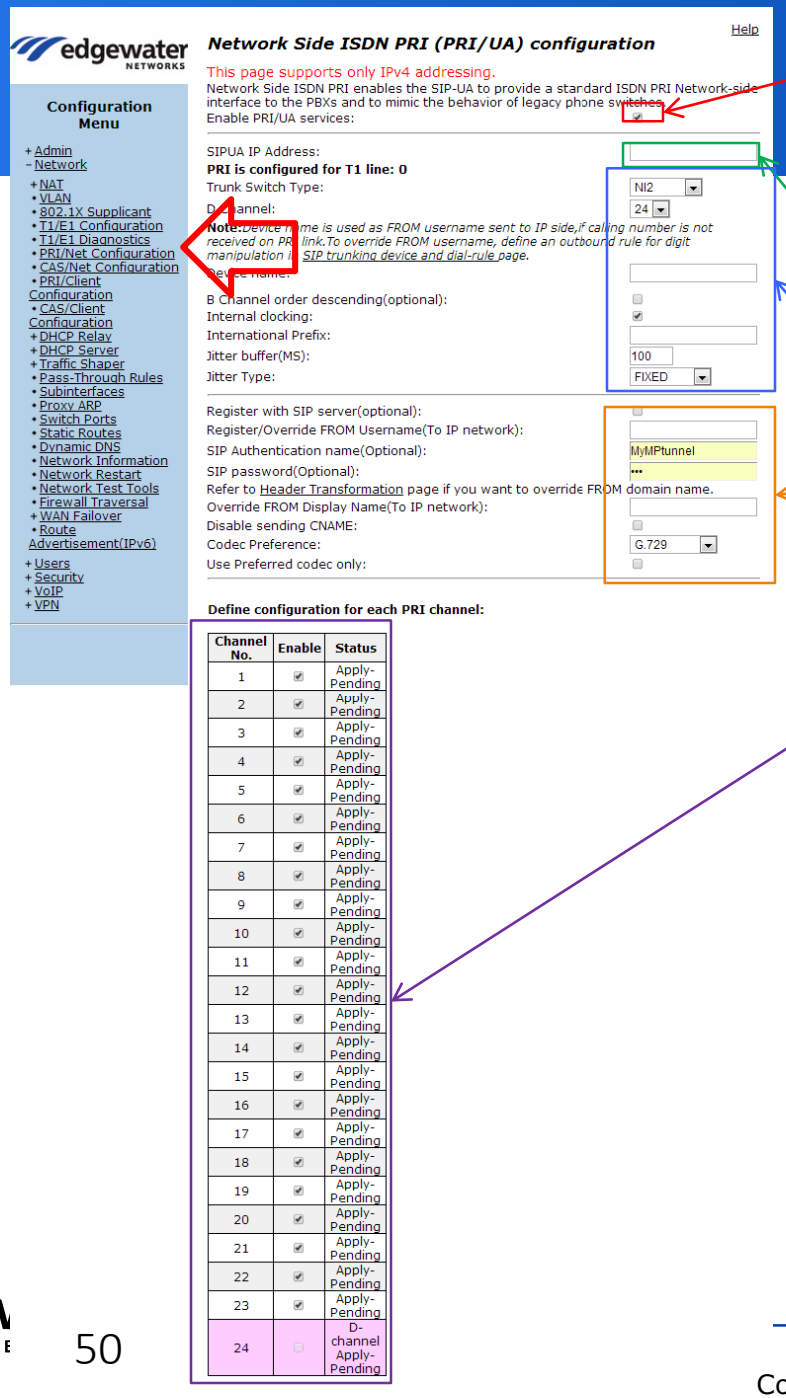


PRI CLIENT



Company Confidential

49



Enable PRI/Net configuration for interconnection with legacy PBX

Leave this empty except instructed otherwise

Configure the PRI

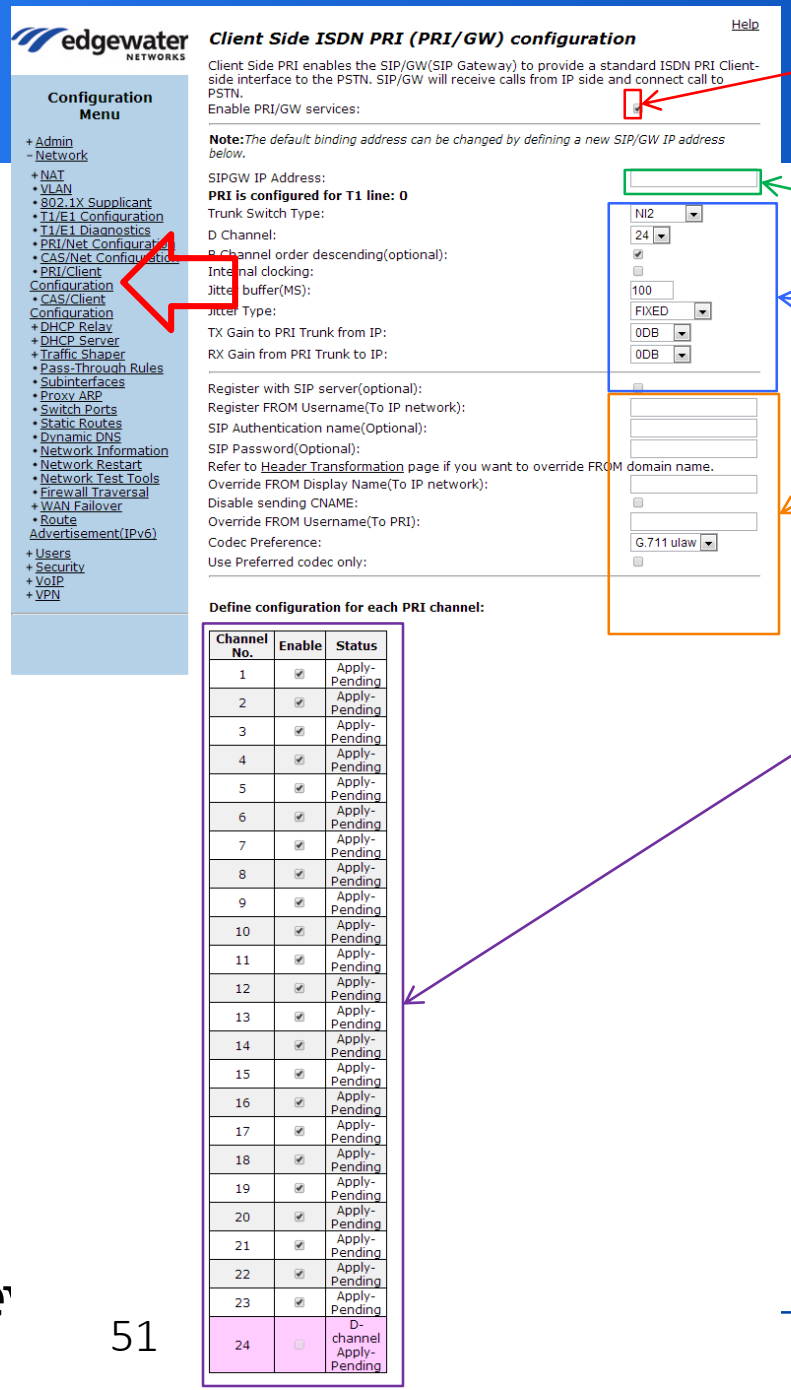
Configure the SIP registration configuration if needed on behalf of the PBX

Status of the PRI channels

Configuration of PRI/NET

Company Confidential

50



Enable PRI/Client configuration for interconnection with legacy PBX

Leave this empty except instructed otherwise

Configure the PRI

Configure the SIP registration configuration if needed on behalf of the PBX

Status of the PRI channels

Configuration of PRI/Client

Company Confidential

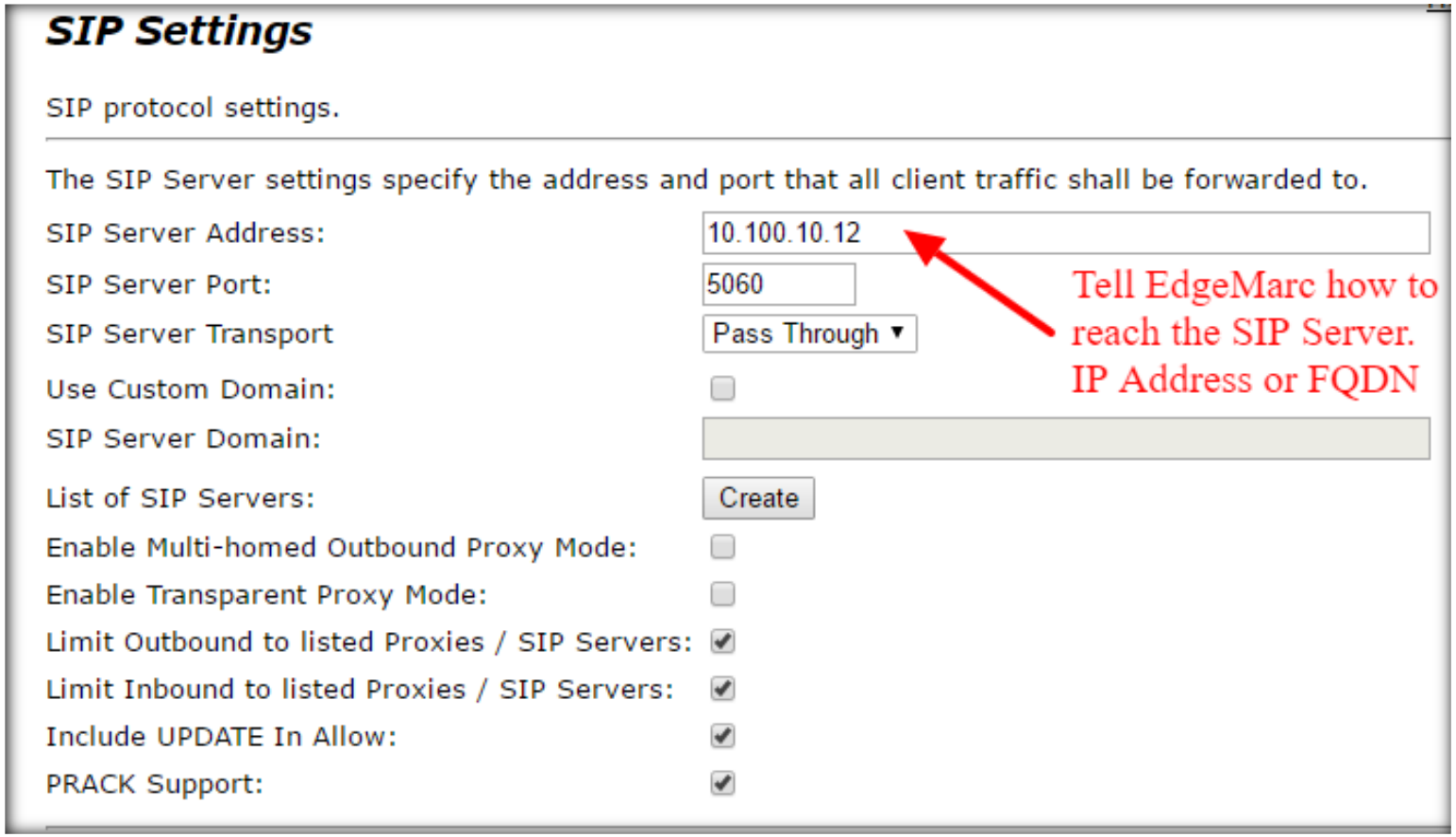
51

Lesson 7.2: LAN & WAN Based SIP Server Configuration

1. Understanding EdgeMarc ALG + Firewall operations
2. EdgeMarc SIP Configuration Approaches
3. B2BUA vs SIP ALG configurations
4. Determining EdgeMarc action requirements for both/either Inbound & Outbound SIP INVITEs
5. Defining EdgeMarc call engagement Scope for both Inbound & Outbound
6. Working with multi-vendor SIP deployments
7. Working with Legacy VoIP/SIP/Traditional PBX equipment with/without SIP Registration capabilities
8. Configure EdgeMarc with LAN & WAN based IP PBX & SIP Server
9. Configuration support for ALG SIP Trunking
10. EdgeMarc SIP B2BUA configuration options

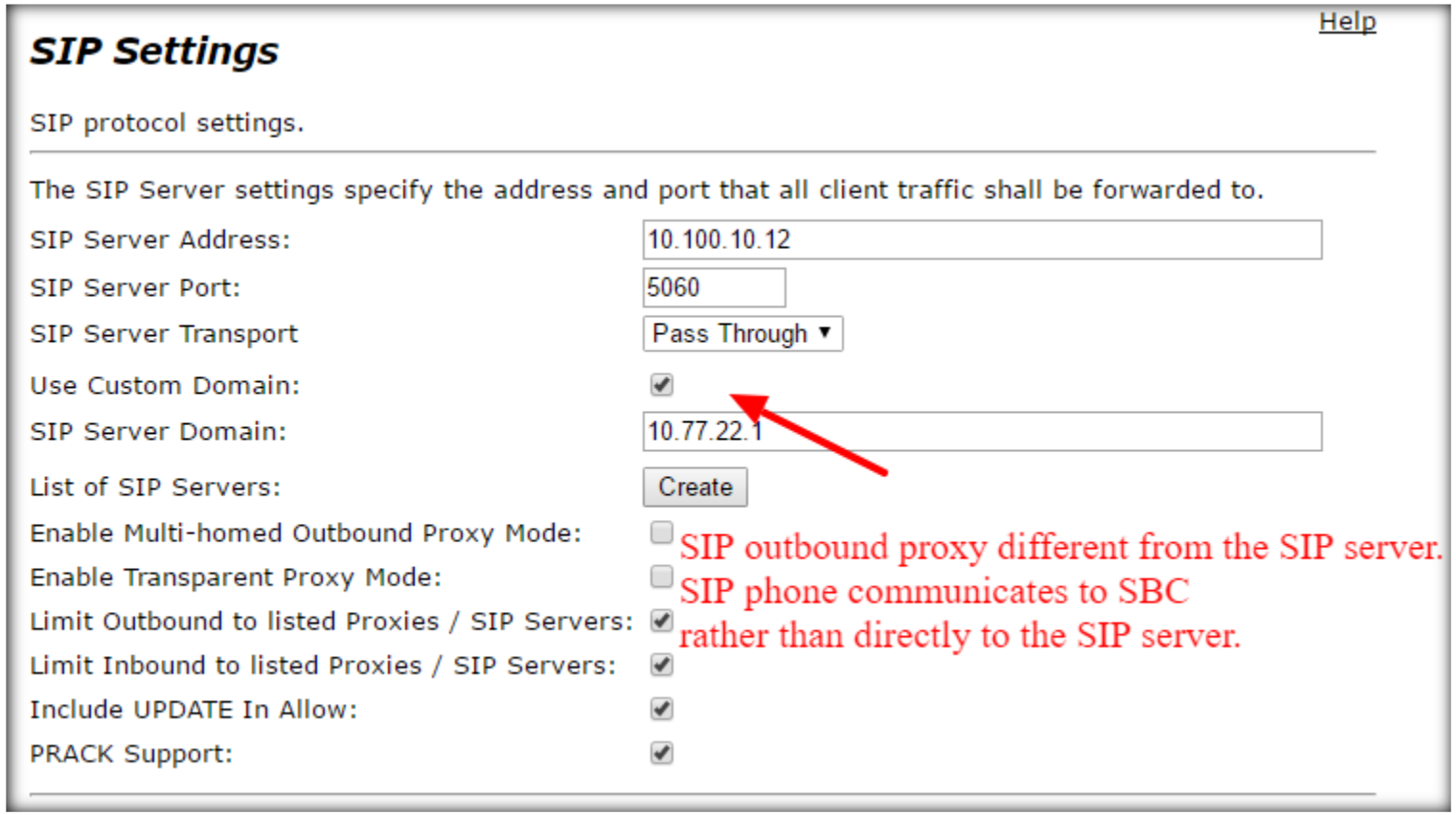
7.2: Basic VoIP & SIP Settings

- It's easy to solve the NAT Traversal issue with EdgeMarc
- Works for Phones or IP PBX passing SIP & RTP from LAN to/from WAN
- Just a great and easy implementation in EdgeMarc to solve a massive issue in VoIP
- Work buying EdgeMarc just for this one function!



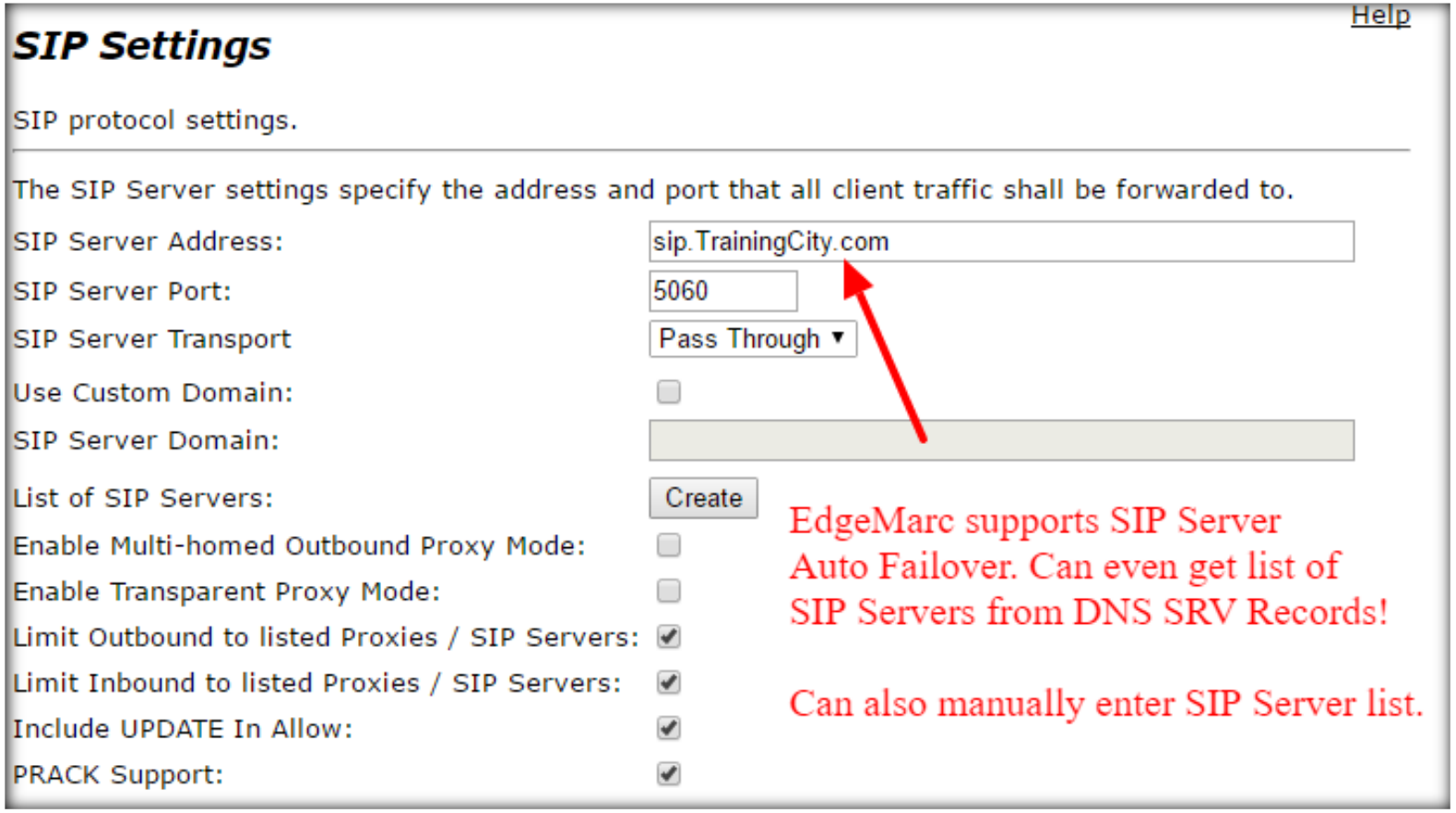
7.2: SIP Settings – Custom Domain

- Specifying a custom domain is commonly done in configurations where the SIP outbound proxy is different from the SIP server address.
- An example of this configuration is where a SIP phone communicates to a Session Border Controller (SBC) rather than directly to the SIP server.



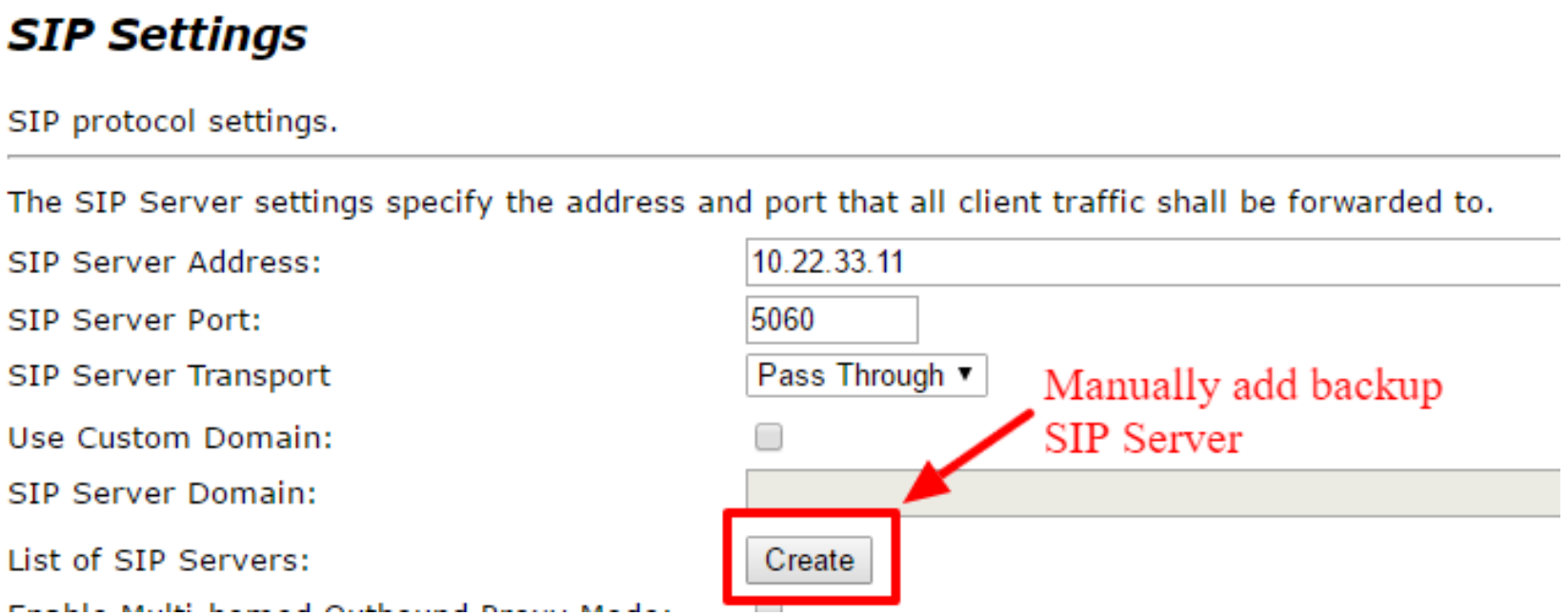
7.2: SIP Settings - SIP Server Auto Failover & Server List

- This is a great feature and easy to implement
- Just Give EdgeMarc a URL in the SIP Server settings
- EdgeMarc does a DNS SRV Record lookup request and builds the list of main and backup SIP Servers
- We will see more details when we look at "Survivability" section



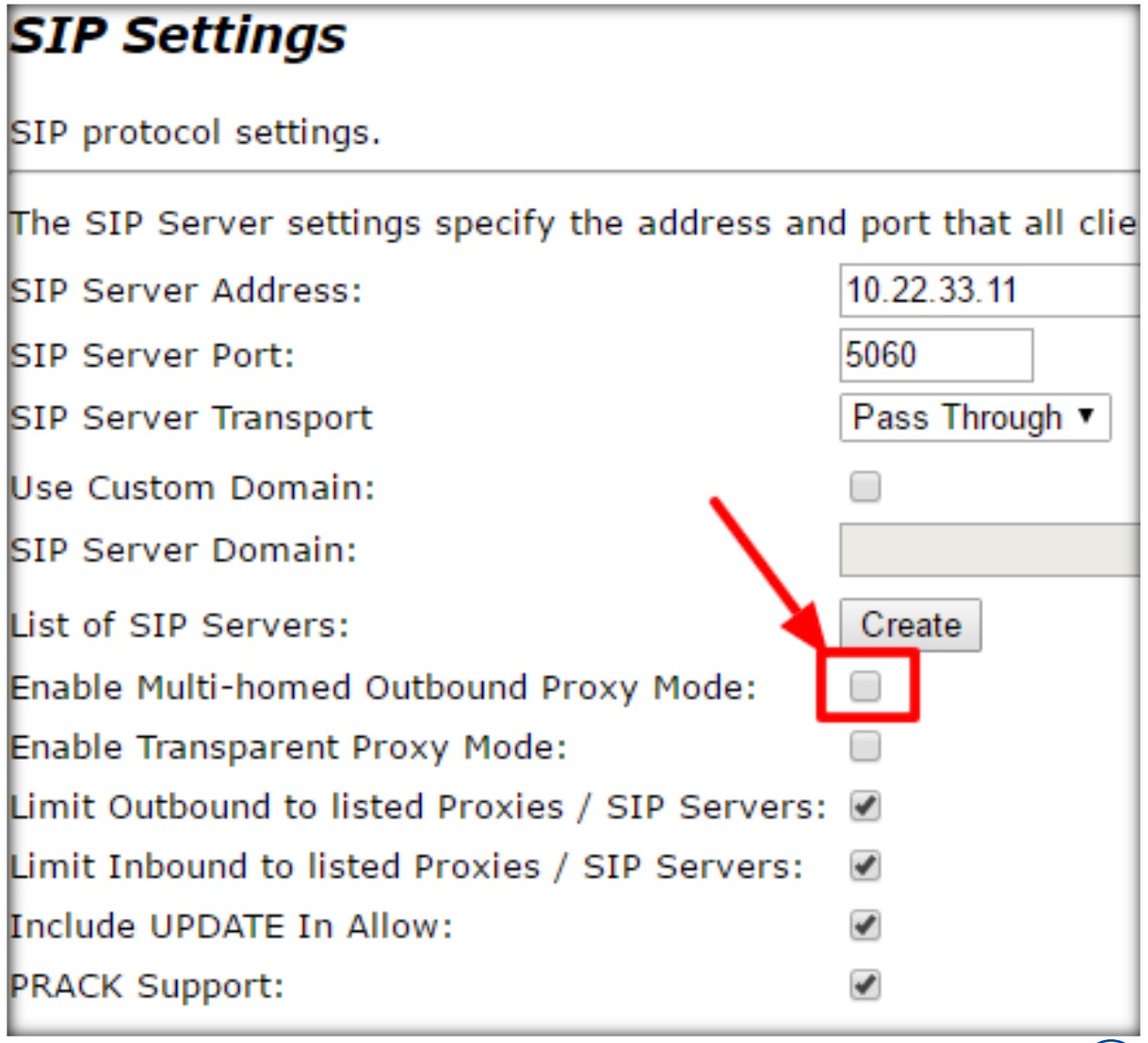
7.2: SIP Settings SIP Server Auto Failover & Server List

- You can also manually enter the SIP Servers in the list on the SIP Settings page and Auto Failover “just works”.

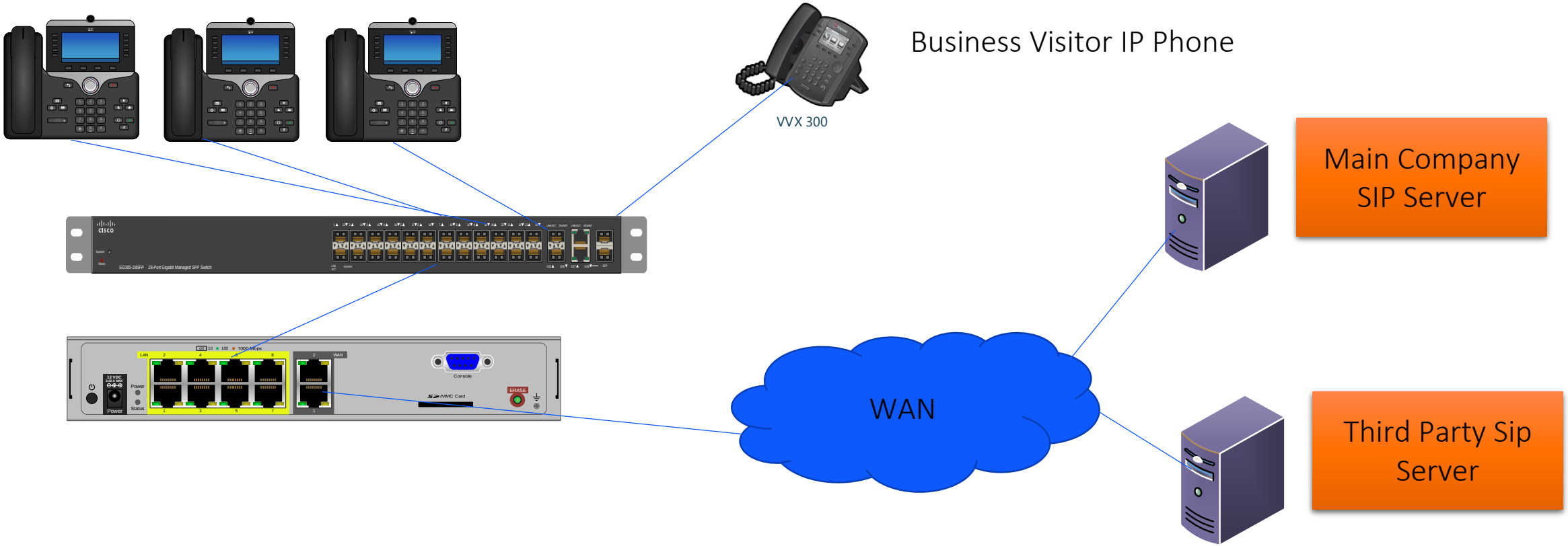


7.2: SIP Settings - Multi-Homed Outbound Proxy Mode

- This option allows or prevents IP Phones on the LAN from using a softswitch FQDN *while using the Edgemarc LAN IP as it's outbound proxy*.
- If the phone uses an IP address instead of a url, this option does not prevent it

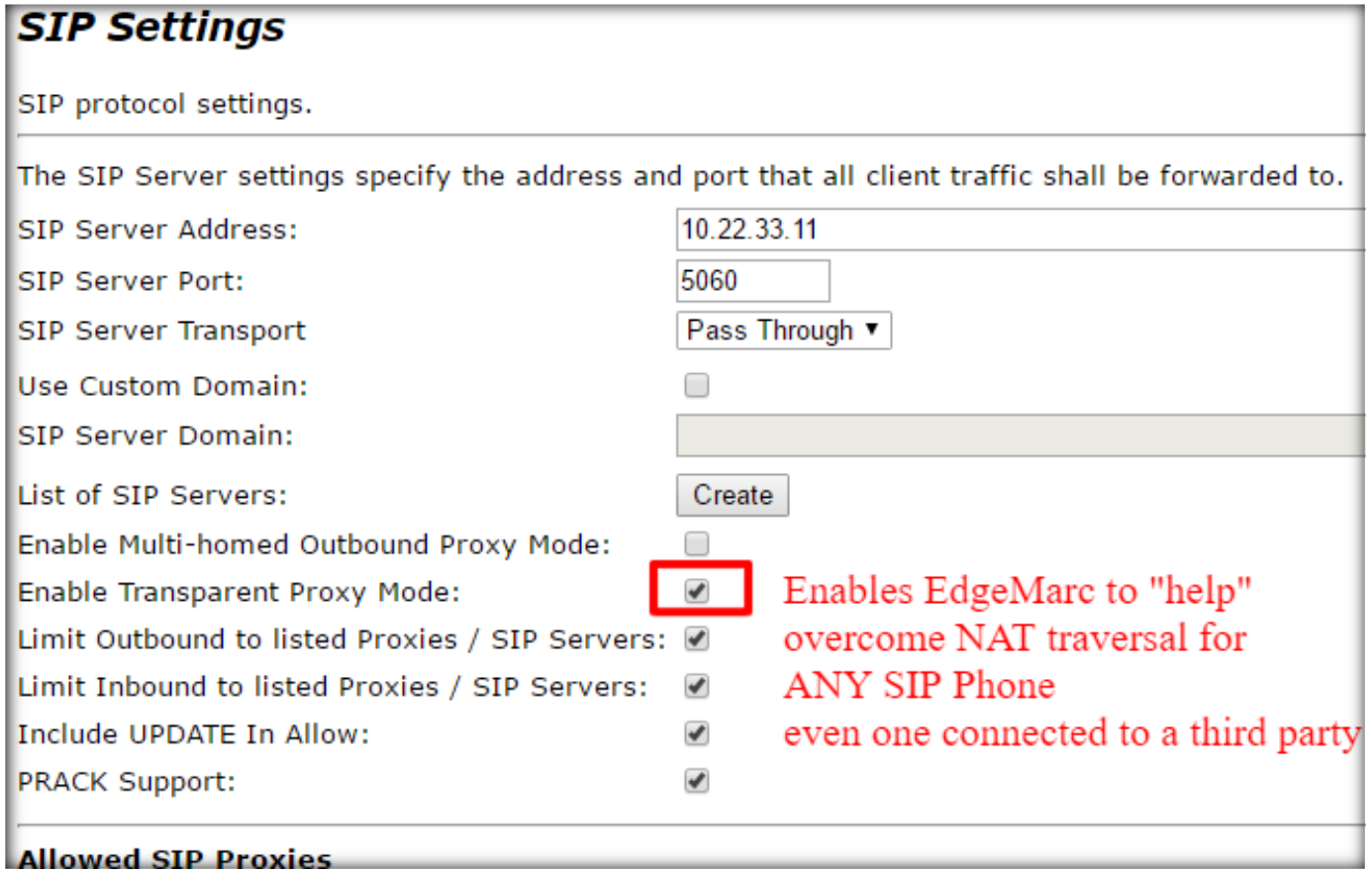


7.2: SIP Settings - Transparent Mode

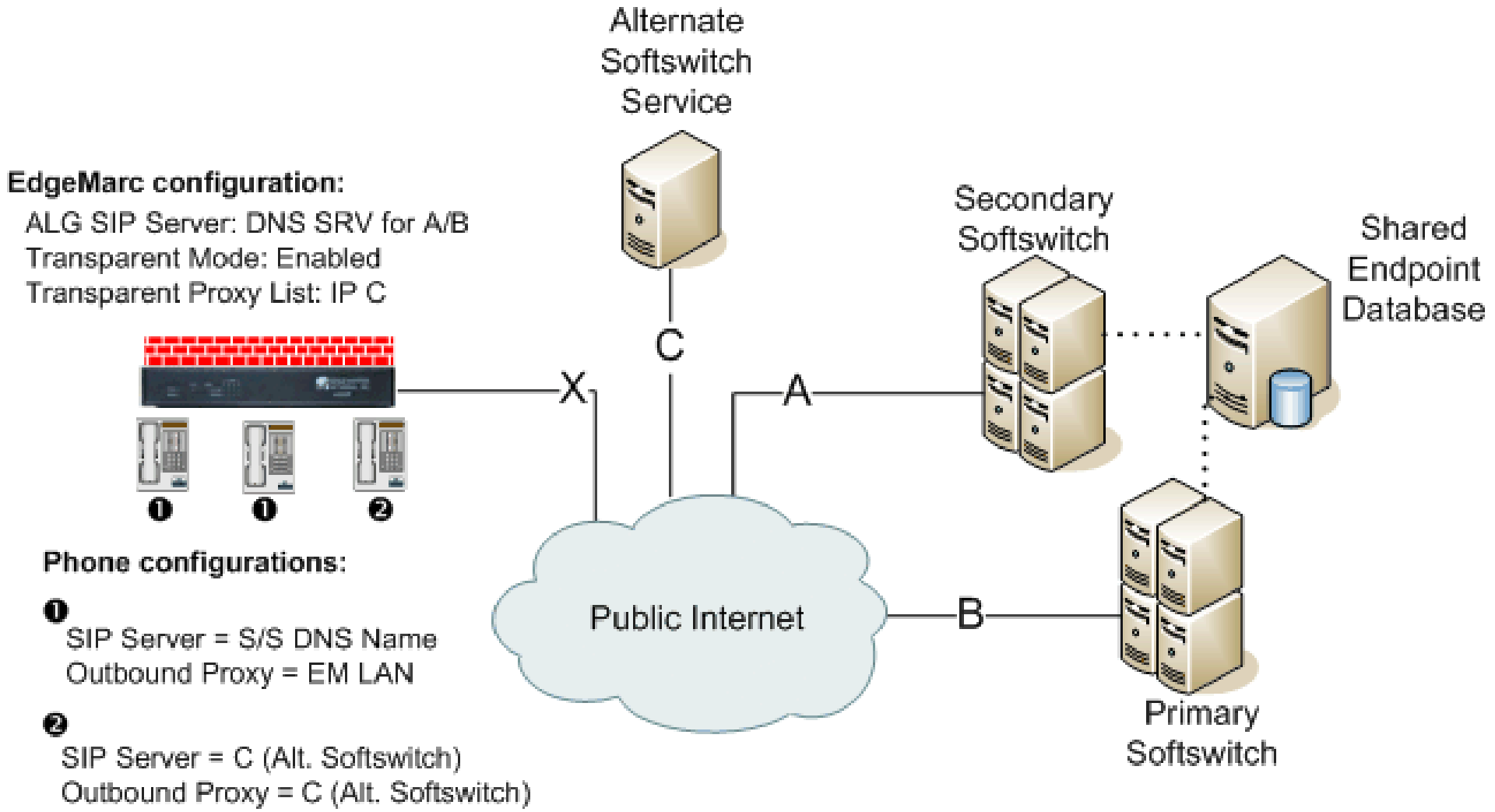


7.2: SIP Settings – Transparent Mode

- EdgeMarc intercepts ALL SIP messages from a LAN-side phone regardless of the Outbound Proxy and SIP Proxy values configured in the phone
- However, if the signalling is TCP-based AND used for 3rd-party servers not configured in the system, then the signalling will not be intercepted and hence with go through the NAT process



7.2: SIP Settings – Transparent Mode

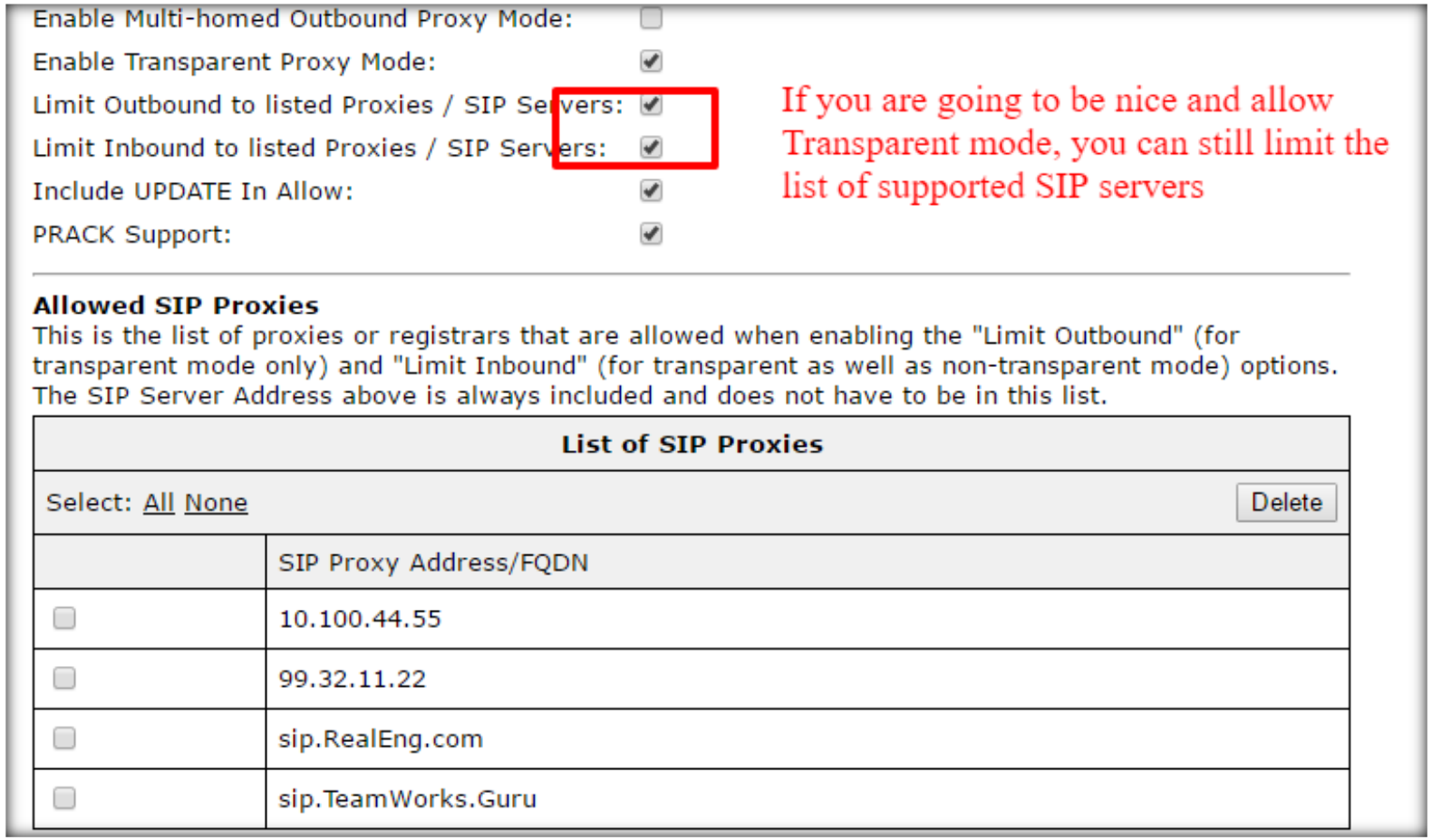


7.2: SIP Settings-Transparent Mode: Limits to being Nice!

- **Limit Outbound to listed Proxies / SIP Servers** The default behavior in Transparent Proxy Mode is to Limit Outbound to listed Proxies / SIP Servers. This means that the System will only process outbound messages intended for a pre-configured list of proxies and SIP servers. Turning off this setting will allow the System to process all outbound messages for any SIP proxy/server.
- **Limit Inbound to listed Proxies / SIP Servers** This option, if checked, means that the System will only process inbound messages from a pre-configured list of proxies and SIP servers. Turning off this setting will allow the System to process all inbound messages from any SIP proxy/server.

7.2: SIP Settings-Transparent Mode: Limits to being Nice!

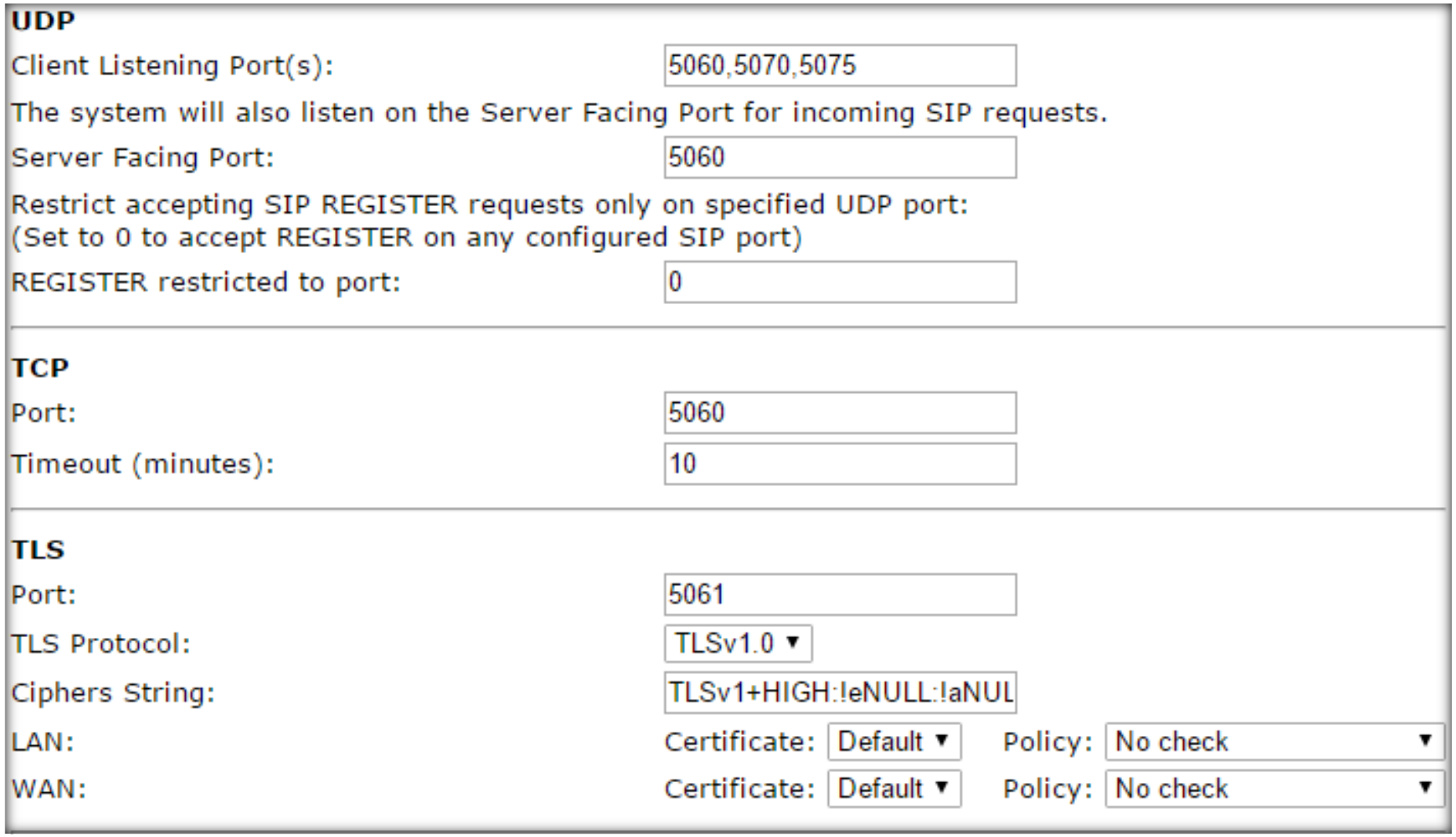
- Just because you decided to be nice and turn on support for Transparent Mode so that other SIP Phones on the LAN can take advantages of EdgeMarc SIP ALG NAT Traversal, doesn't mean you have to be wide open to any SIP connection



7.2: SIP Settings – Nice little features

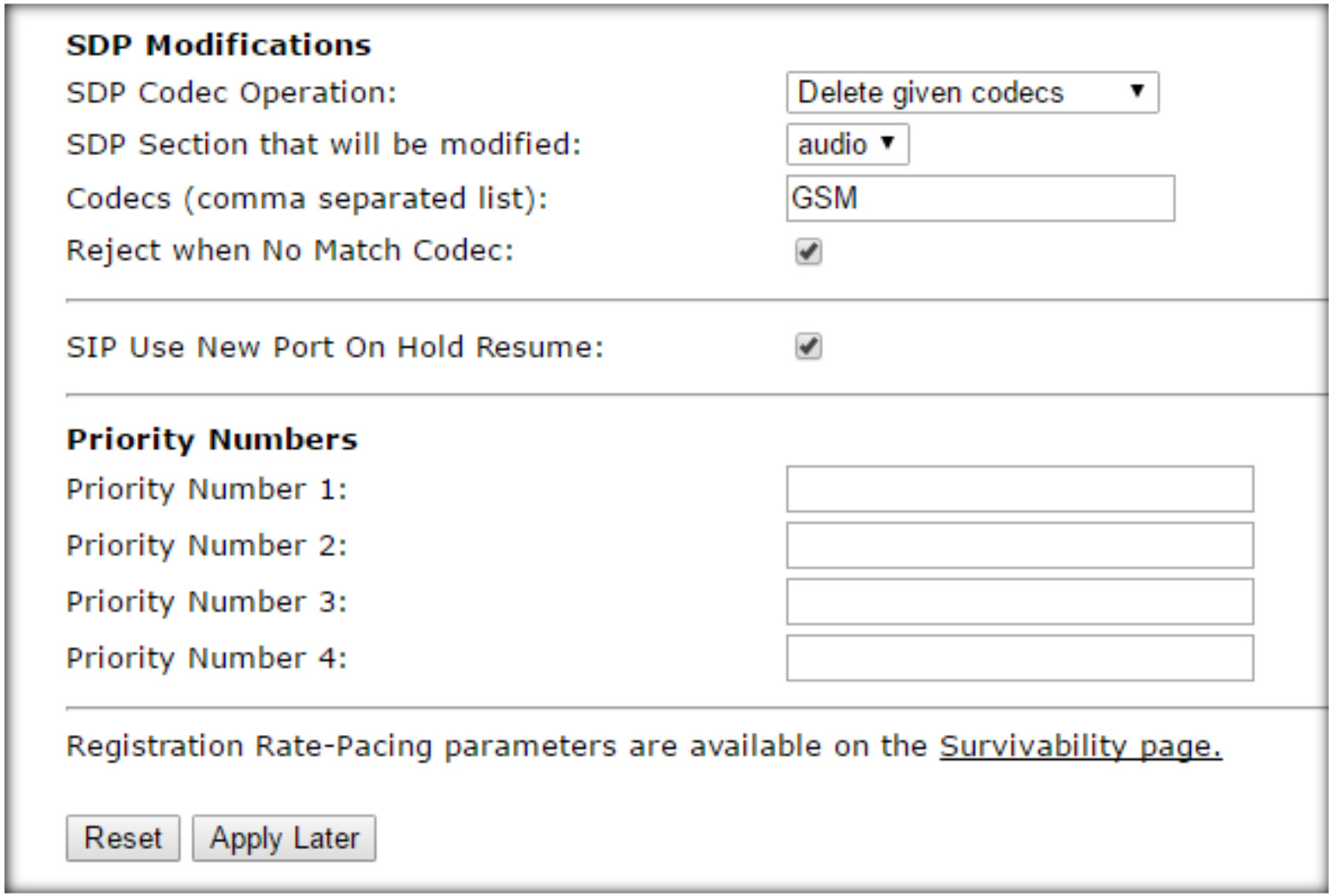
- **Include UPDATE In Allow** This option is applicable for B2BUA calls only. The default behavior is to add the UPDATE method in the Allow header.
- **PRACK Support** - When enabled, the system will add **Supported: 100rel** in the SIP INVITE or add **Required: 100rel** in the 18X response messages the systems B2BUA sends out.
- **Stale Timer** - If no REGISTER request have been received from the client during this time, the client will be automatically deleted.

7.2: SIP Settings – Transport Layer Options



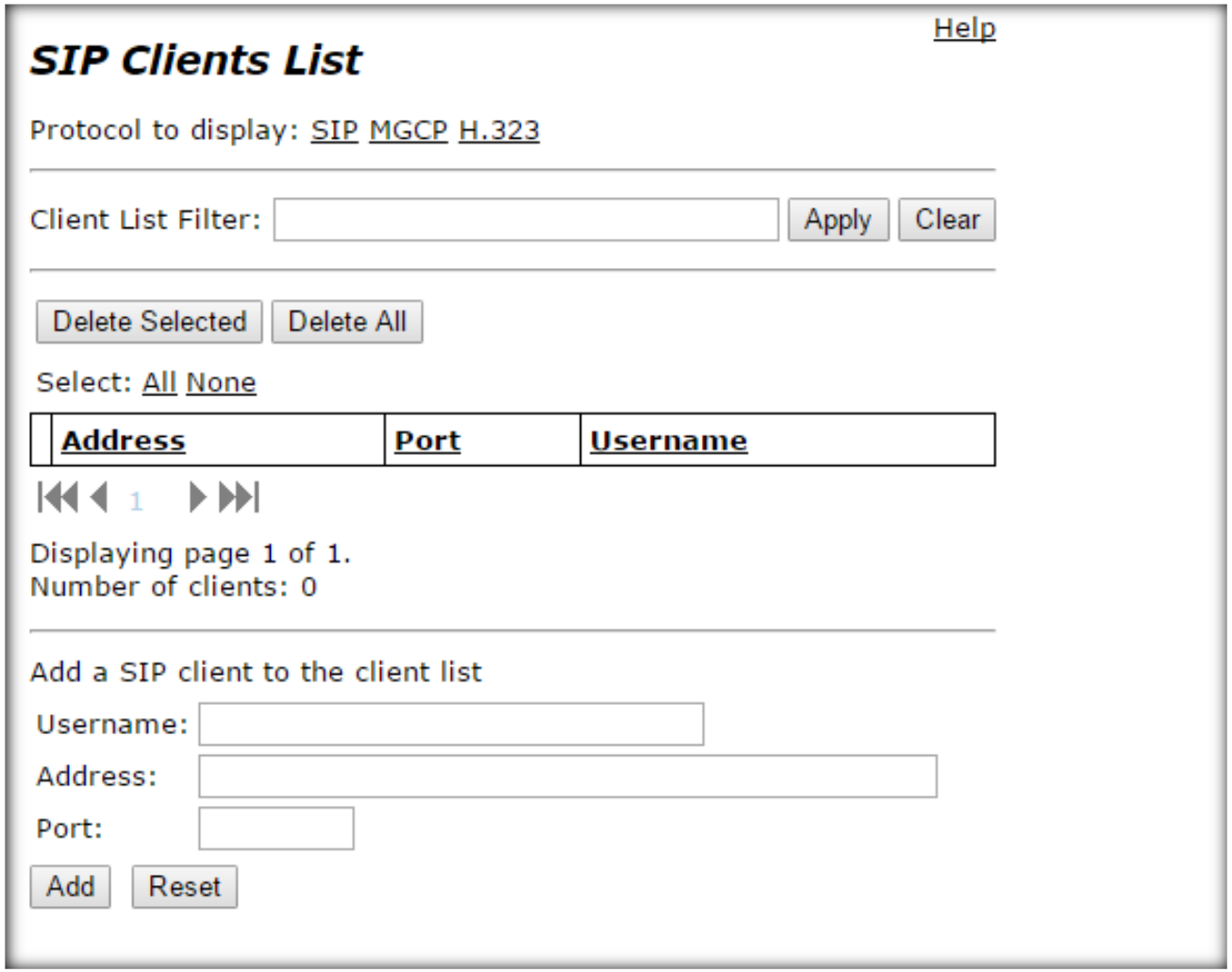
7.2: SIP Settings – More, More, More!

- modifications to SIP/SDP messages as they pass through the device
- Priority numbers call to these numbers processed even after Call Admission Control - CAC limit is reached, by pre-empting any non-priority call



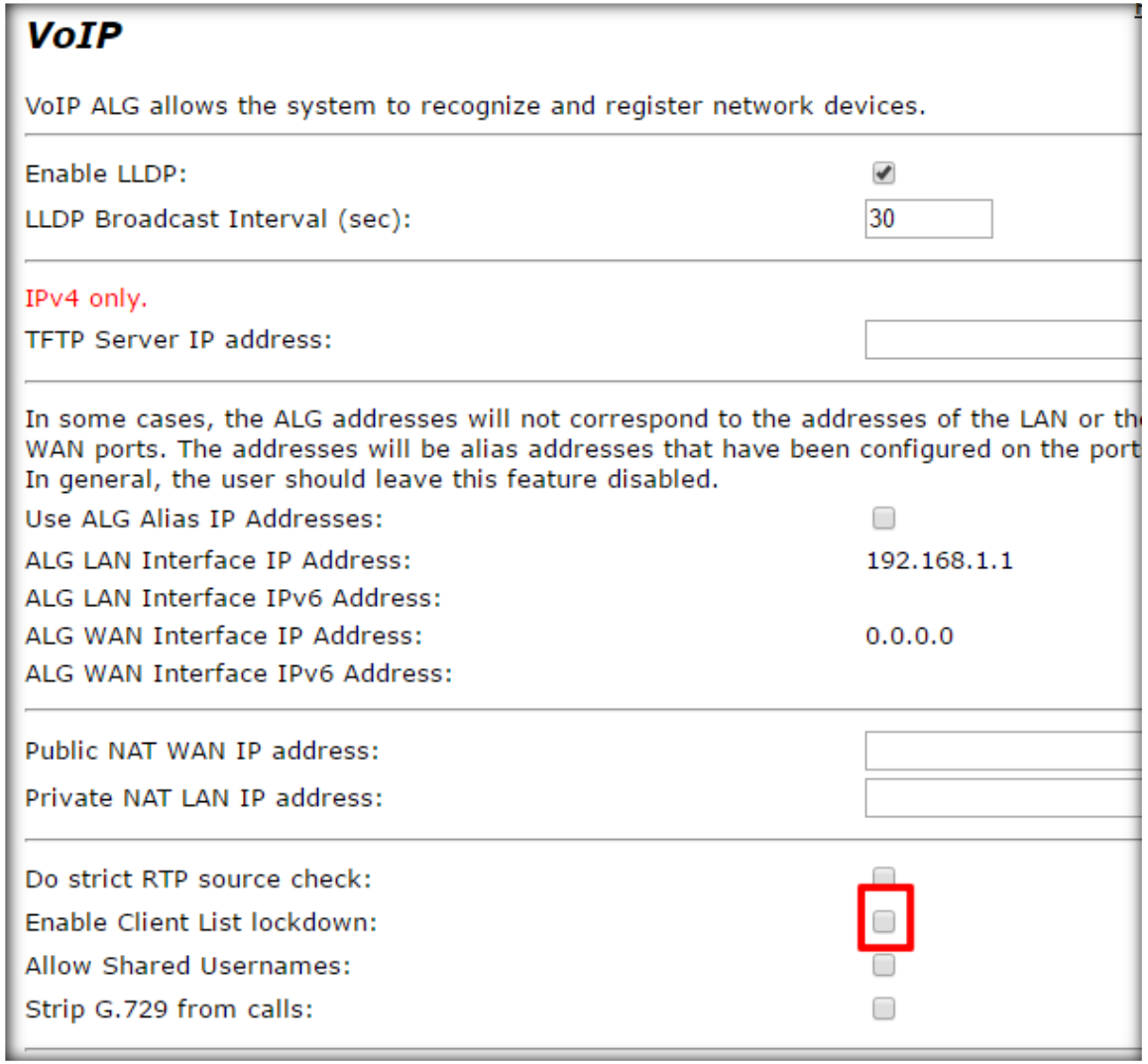
7.2: Client List & Lockdown

- The clients lists contain entries for devices that have registered with the system. The displayed clients can be filtered, sorted, queried for information, and deleted. It is also possible to add clients to the clients list.
- Clients can be added and deleted without restarting the system.
- You can choose to “lock” the client list, preventing any additional SIP devices to communicate



7.2: Client List & Lockdown

- You can choose to “lock” the client list, preventing any additional SIP devices to communicate



7.3: EdgeMarc SIP Configuration Approaches

1. ALG - Application Layer Gateway
2. B2BUA – Back to Back User Agent

7.3: SIP Server Configuration – ALG & B2BUA

- Making changes to SIP headers as they pass through a SIP Server or SBC is very common and generally speaking a needed service for SIP Phones / endpoints
- For example, a SIP Phone will insert it's RFC 1918 Address in the "contact" field. Sending this into The Internet is useless, and exposes the internal network architecture
- EdgeMarc ALG – Minimal awareness of SIP call flow (Stateless)
- EdgeMarec B2BUA – "All in" changing many aspects of the SIP header. This is useful for security and compatibility

7.3: SIP Server Configuration – ALG & B2BUA

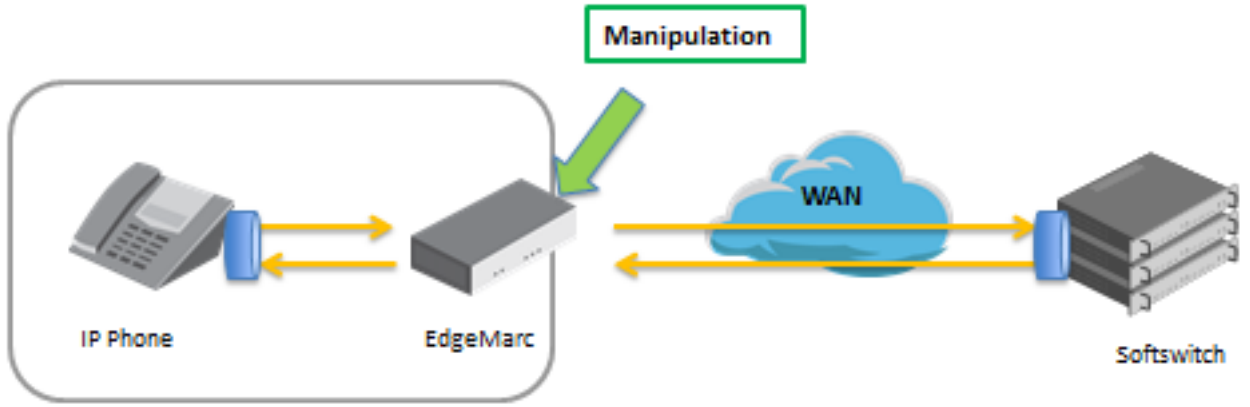
- The ALG (Application Layer Gateway) provides basic Proxy function with simple Header manipulation (solving NAT traversal deployment issue)
- The B2BUA (Back to Back User Agent) provides more advanced proxy capability with advanced Header Manipulation
  - In the originating call leg the B2BUA acts as a user agent server (UAS) and processes the request as a user agent client (UAC) to the destination end, handling the signaling between end points back-to-back

7.3: SIP Server Configuration – ALG & B2BUA

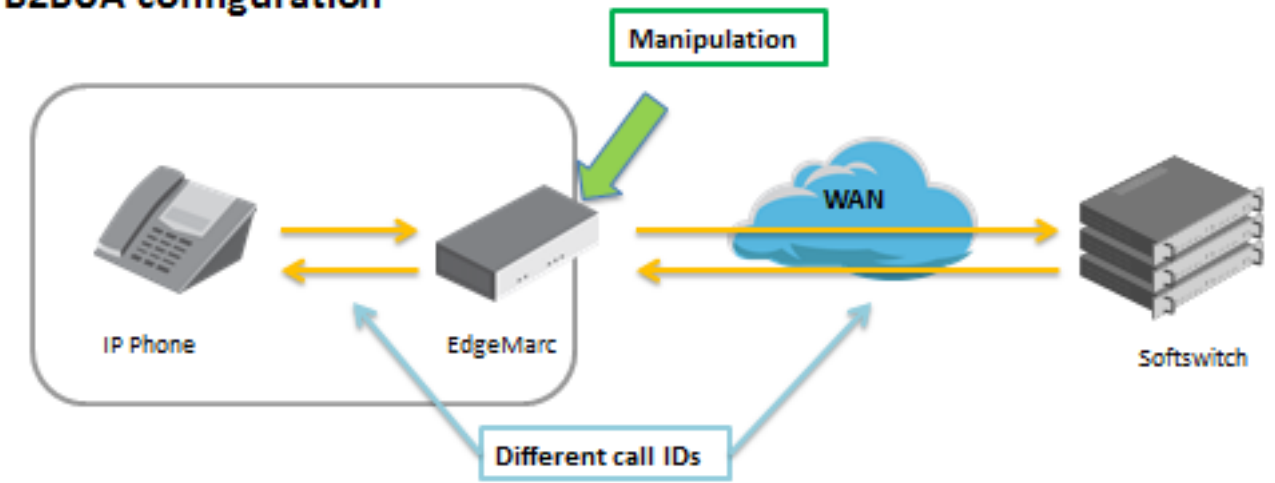
- ALG - Stateless Very fast, but only basic header manipulation and control as no knowledge of “SIP Call Flow”
- B2BUA - Stateful process – Full Awareness of SIP Call Flow and RTP payload
  - The stateful B2BUA has a powerful header manipulation capability
  - Tradeoff – CPU & memory requirements

7.3: SIP Server Configuration – ALG & B2BUA

ALG configuration



B2BUA configuration



7.3: EdgeMarc ALG

- EdgeMarc SIP ALG supports the following limited transformations:

1. Digit manipulation
2. Insert specific predefined headers:
   - requesting broadworks subscriber data header into a Registration packet
   - Record-route header ensuring the ALG is part of any further SIP conversation
3. Replace LAN side IP address with a SIP Server Address or EdgeMarc WAN IP
4. Select between using the upstream SIP server address or the WAN side EdgeMarc address in the from header

7.3: EdgeMarc ALG - How to route calls with ALG

- The ALG can provide routing capability based on regular expression detection on incoming or outgoing or redirect calls to a defined trunk group:
  - Legacy PBX or IP PBX
  - Local Gateway
  - PRI
  - FXO/FXS
- It can also remove digits and add digits from the SIP To: field

Company Confidential

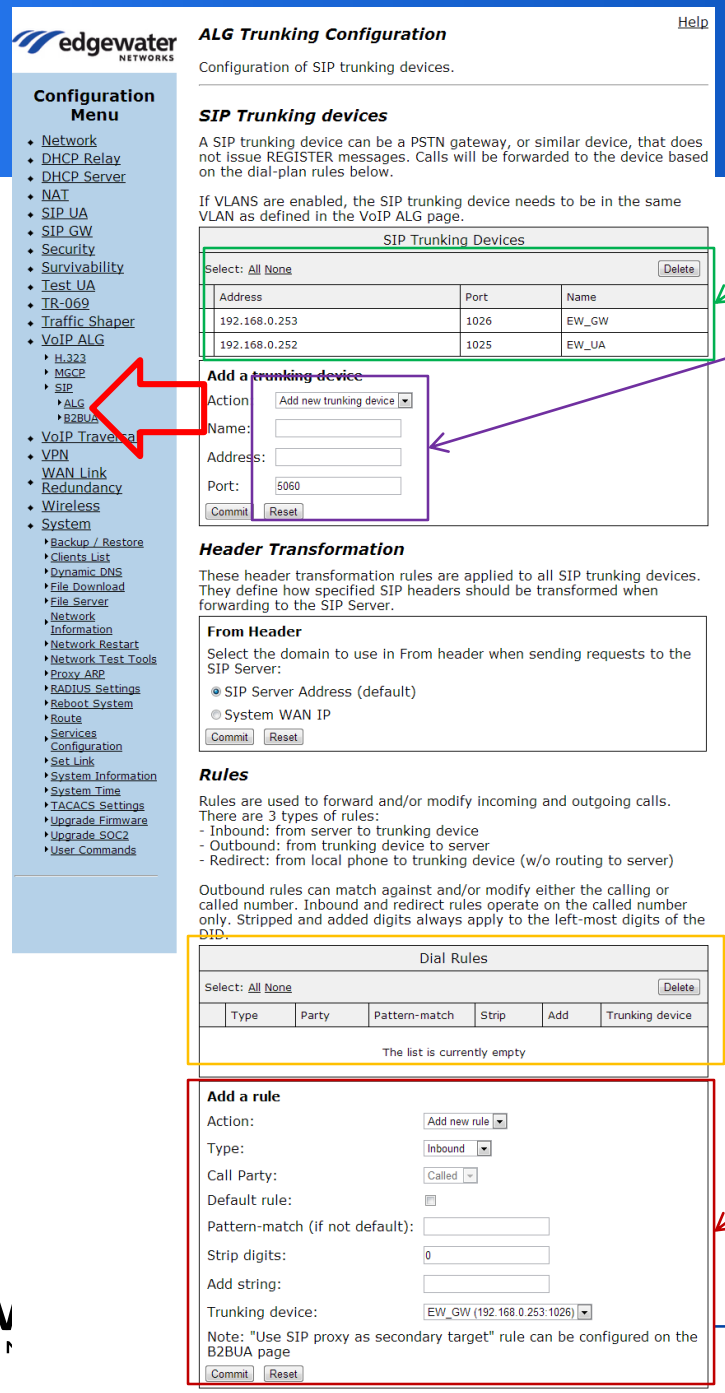
Lesson 4.4: EdgeMarc ALG - Matching rules

- Pattern definitions

.	Matches one or more digits.
[x-y]	Matches any single digit between x and y (inclusive). For example, [1-3], matches 1, 2 or 3
X	Matches any digit between 0 and 9, equivalent to [0-9]
Z	Matches any digit between 1 and 9, equivalent to [1-9]
N	Matches any digit between 2 and 9, equivalent to [2-9]

- Pattern examples:

1XXX	Matches any four-digit number starting with 1, e.g. 1000, 1200, 1234
9NXXXXXX	Local calls preceded by a 9, e.g. 95551234
91NXXNXXXXX X	Long distance calls preceded by a 9, e.g. 914085551234



List of Trunking Device

Create a new Trunking Device on the LAN side

List of Rules

Add rule:
- Select type: inbound, outbound, redirect
- Call party: Called or calling
- Default rule or match pattern
- Strip and/or add digit from the called number
- Send to Trunking device

7.4: EdgeMarc B2BUA - How use the B2BUA

- The B2BUA can provide routing capability based on regular expression detection on incoming or outgoing or redirect calls to a defined trunk group:
  - Legacy PBX or IP PBX
  - Local Gateway
  - PRI
  - FXO/FXS
- It can also perform advanced SIP Header Manipulation
- It also allows the EdgeMarc to register to the Softswitch (for example for the SIP trunking deployment) on behalf of the PBX

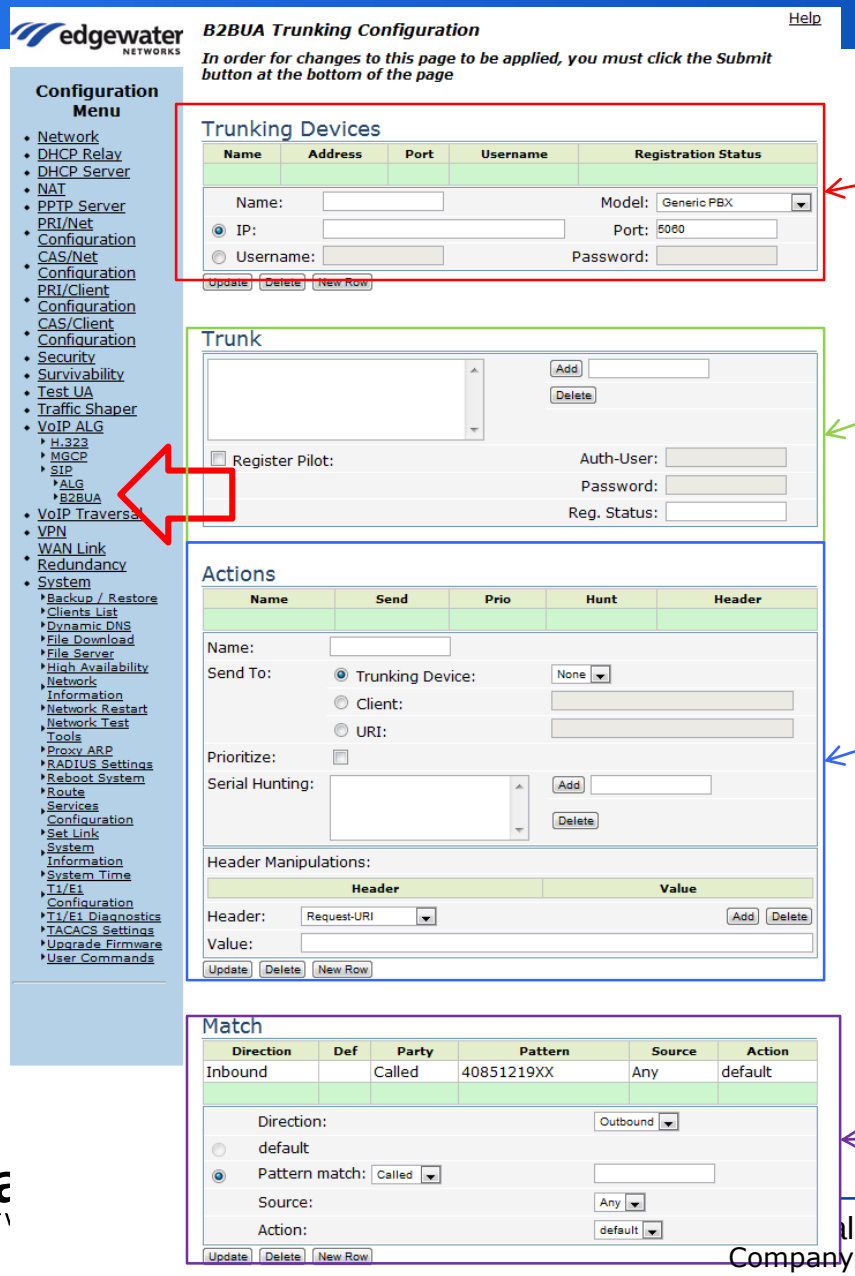
Company Confidential

7.4: B2BUA – Back to Back User Agent

EdgeMarc B2BUA supports flexible SIP header manipulation:

1. Homogenization of core SIP signaling
2. Proxy registration
3. Insertion of custom SIP headers
4. Translating a “REFER” call transfer flow into a “RE-INVITE” call transfer flow
5. Transforming SIP response codes

7.4: EdgeMarc B2BUA - GUI



Adding Trunking device

Define Trunk and register Trunk credentials

Add action to be sent to a specific device, hunt group and HMR (please check the advanced presentation on HMR)

Create an Action First then create the Match

Add Match Pattern case

Company Confidential

79

Module 7.0: Review

Module 7.0: Quiz