Last updated: May 24, 2016

Question

Describe the EdgeMarc's VoIP Survivability facility; how it works and how it is configured.

Answer

Based on VOS: v 14.6.0 or later

1.0 Overview

Edgewater's VoIP survivability enhances the reliability of VoIP services to branch offices by providing local call switching in the event of WAN link failures or other loss of connectivity to network-based call-processing servers. VoIP survivability is a licensed option for Edgewater's EdgeMarc Series appliances.

The primary features of this facility include:

- Local call switching between VoIP endpoints and premises based PSTN gateways during WAN link failures or other failures that prevent connectivity to network based call processing servers
- Calling features of transfer, hold and conference during Local call switching
- Automated setup that creates a local dial plan in the EdgeMarc appliance by monitoring traffic to the softswitch (Broadsoft softswitch only)
- Enhanced Application-layer monitoring of softswitches to determine connectivity
- Automatic detection of loss of connectivity to softswitches and automatic return of call control when connectivity has been restored
- Configurable timers to determine server connectivity
- Call processing server connectivity status indicators in EdgeMarc GUI. Change-of-status reporting in EdgeMarc syslog messages
- Support for multiple call processing servers in primary and backup configuration

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

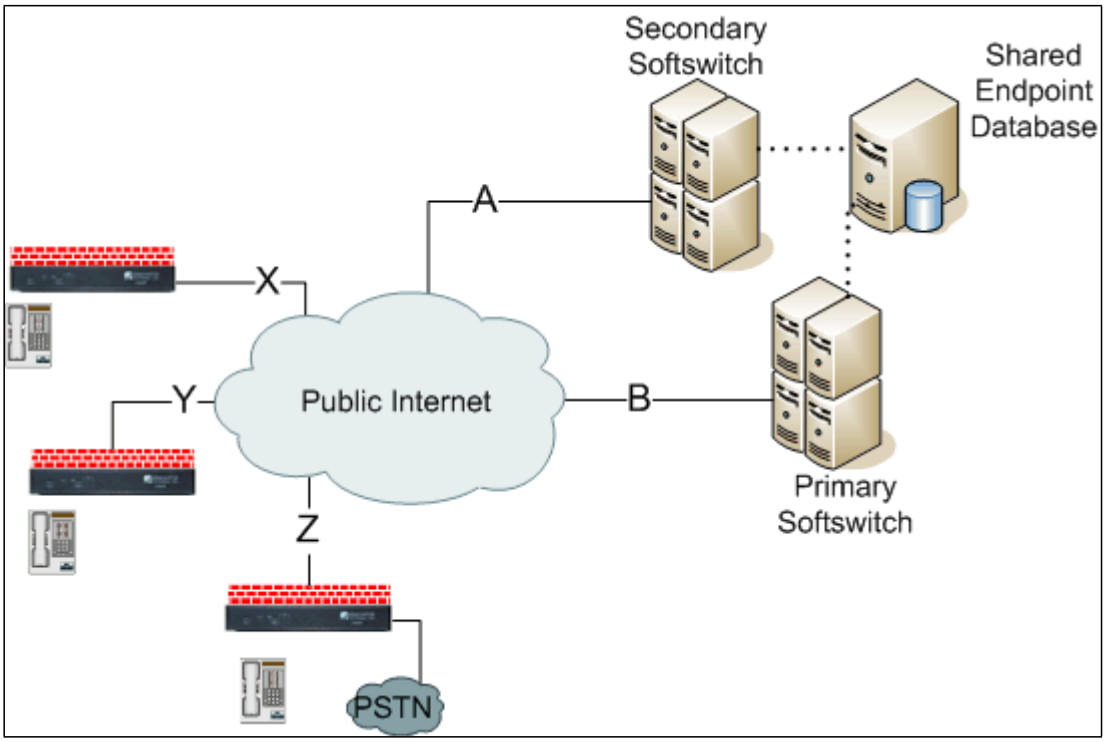
2.0 Supported Softswitch Topologies

EdgeMarc's VoIP Survivability supports two redundant-softswitch deployment models. The first assumes the use of no Session Border Controller (SBC) or the use of Session Border Controllers that share a single ("virtual") IP address. The second model assumes geographically separated SBCs each with unique IP addresses. In both models the EdgeMarc is configured with or dynamically learns the IP address of the primary softswitch/SBC and, optionally, a backup softswitch/SBC.

The models differ with respect to endpoint IP addressing as viewed from the softswitches' perspective. In the first model, named Static Endpoint Addressing, the address of an endpoint (eg. an EdgeMarc) remains unchanged regardless of whether the endpoint is reached via the primary or the secondary softswitch. In the second model, named Varying Endpoint Addressing, the IP address of the endpoint varies depending on whether it is reached through the primary SBC or through the secondary SBC.

This difference is made clearer in the pictures below:

2.1 Model 1: Redundant softswitches using static endpoint addressing



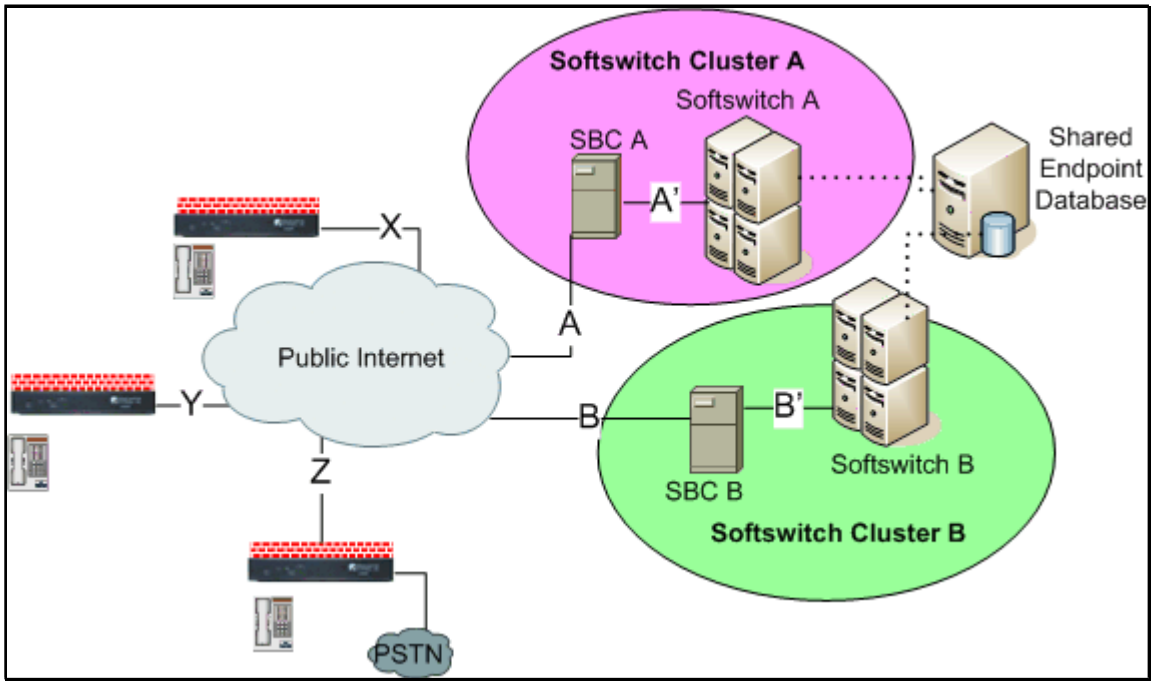
In this configuration, the primary and secondary softswitches are known at each EdgeMarc by two different IP addresses (A and B, above). Each EdgeMarc and the endpoints behind it are reached by the softswitches using a single IP address (X, Y and Z, above). Registered URIs, along with their associated EdgeMarc IP address, are stored in the shared endpoint database.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

When an EdgeMarc detects loss of its primary softswitch (using the algorithm described in detail below), it directs all SIP messaging to the secondary softswitch. The SIP URIs and associated IPs in the shared endpoint database do not need to be updated when an EdgeMarc shifts from primary to secondary softswitch. The destination IP for each SIP URI remains unchanged. This is the key difference between this model and the one following.

2.2 Model 2: Redundant softswitches using varying endpoint addressing

This is the more common configuration for today's service providers.

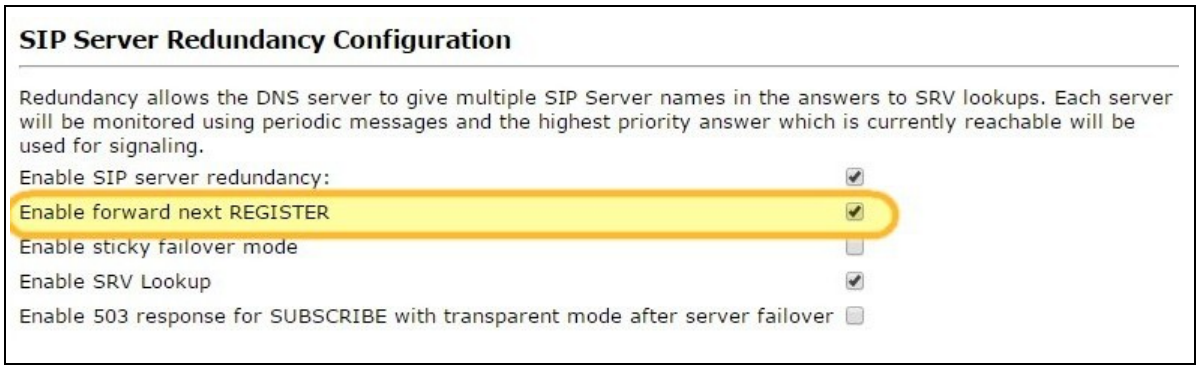


As with the first configuration, the primary and secondary softswitches are known at each EdgeMarc by two different IP addresses (A and B, above). However, unlike the first model, each EdgeMarc and the endpoints behind it are reached by the primary and secondary softswitches using different IP addresses (A' and B', above).
Softswitch A reaches all endpoints via SBC A, only, and Softswitch B reaches all endpoints via SBC B, only. Each Registered SIP URI, along with its most recently registered address (A' or B') is stored in the shared endpoint database.

When an EdgeMarc detects loss of its primary softswitch (using the algorithm described in detail below), it directs all SIP messaging to the secondary softswitch/SBC. The SIP URIs and associated IPs in the shared endpoint database now do need to be updated. The backup softswitch can only reach the endpoint URIs via its local SBC; if the IP address associated with a given SIP URI is not updated to be the backup softswitch's SBC, then the backup softswitch will not be able to reach the endpoint. This is the key difference between this model and the first one.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

It is vital, therefore, that when an EdgeMarc detects loss of its primary softswitch, that it immediately re-Register all endpoints behind it, so that the shared endpoint database is updated. The EdgeMarc is able to do this – without burdening the softswitch with excess Register messages during normal operation. This is already enabled by default.



Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

3.0 How Survivability Behaves: An Overview

3.1 Without the EdgeMarc: A stand-alone SIP phone

A SIP phone without an EdgeMarc in front of it will typically be configured with Primary and Backup SIP proxy addresses. The phone will always try to contact the primary softswitch first, resending a message several times if it does not get an immediate response. After a specified number of tries to the primary, the phone will then retry the same message to the backup softswitch address.

This is a simple algorithm but with the following behavior: While the primary softswitch is down, every outbound phone call is delayed by the number of seconds required to time out with the primary softswitch.

3.2 With an EdgeMarc

Phones behind an EdgeMarc are usually configured with a single SIP Proxy server and an optional Outbound Proxy server. Either the SIP Proxy server address or the outbound proxy address is set to the EdgeMarc's LAN IP address. The EdgeMarc then proxies all the phones' messages.

The EdgeMarc is configured with and/or determines the IP addresses of the primary and backup softswitch. This process is described in more detail below.

The EdgeMarc continuously monitors the status of connectivity to the network-based softswitches by watching the phones' application messages or, if configured, inserting its own application layer "ping" messages. This application-layer monitoring provides the benefit of detecting when a softswitch hardware platform is reachable but the softswitch service itself is not functioning properly.

The EdgeMarc maintains state information for each softswitch. The highest-priority reachable softswitch is called the Active softswitch.

When the Active softswtich is declared unreachable, the EdgeMarc notes this and changes the Active softswitch to the next highest priority reachable softswitch (if any). If the primary and secondary softswitches are all declared unreachable, then the EdgeMarc enters "Local" mode (only if this is licensed on the EdgeMarc and enabled) and performs call processing locally for the LAN- side SIP user agents.

Optionally, the EdgeMarc can be locally connected to the PSTN by an internal FXO port (certain models) or via an external gateway. This PSTN connection can be used for inbound and outbound calling during Local mode. (To maximize utilization of this gateway it can also be used when call switching is being performed by the network-based softswitch, this is sometimes referred to as an Enterprise Gateway). Once connectivity to a softswitch is restored, the EdgeMarc will automatically turn control of all subsequent call requests over to the softswitch. Calls in progress that were established while the EdgeMarc appliance was in Local mode will not be disrupted when connectivity is restored to the network softswitch.

3.2.1 Local Mode dialing plans

The EdgeMarc appliance automatically creates a local dialing plan by monitoring the registration requests sent by LAN-based SIP user agents as they register with the network-based server (Broadsoft softswitch only). This dial plan will be used during

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

Local mode to process dialed digits and forward calls between local phones or out a LAN-side PSTN gateway.

In addition to any dial plan learned by watching network registrations, the EdgeMarc will automatically build 10-, 7- and 4-digit dial plans using the last characters of the endpoint's username (usually the DID). The EdgeMarc can also be configured to create a dialing plan using a user-specified last N digits of each endpoint's username.

3.3 Survivability when using Transparent Mode

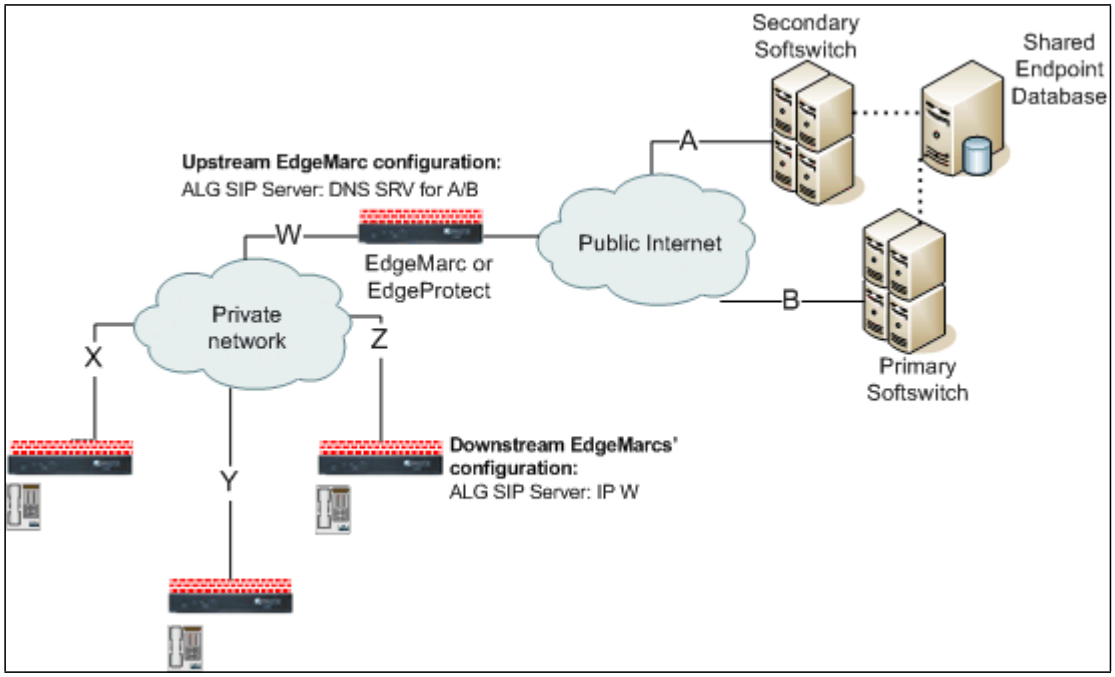
As described above in section 3.2, typically phones behind an EdgeMarc point to the EdgeMarc as the SIP Proxy or Outbound Proxy. We call this Registrar Mode or Outbound Proxy Mode. The SIP messages generated by the phone will have a destination IP address of the EdgeMarc itself.

There are cases, however, where the phone behind the EdgeMarc is configured to point directly to the IP address of the network softswitch or Session Border Controller. This is called "Transparent mode". Survivability mode supports endpoints configured in Transparent mode.

See Edgewater Knowledgebase article: *Flexible SIP Routing - Overview* for further details on Transparent mode.

3.4 Survivability with chained EdgeMarcs

The EdgeMarc supports chained configurations, as shown below:



Survivability is supported in this configuration. The upstream EdgeMarc is aware of the public softswitches. It maintains connectivity status to each network softswitch as

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

well as responsibility for forwarding SIP messages to the highest-priority active softswitch. The downstream EdgeMarcs are only aware of the upstream as the one reachable softswitch.

If one of the downstream EdgeMarcs loses WAN connectivity it will individually switch to Local mode. If connectivity is lost by the upstream EdgeMarc, then all downstream EdgeMarcs will immediately switch to Local mode.

4.0 How Survivability Behaves: The Details

4.1 Determining softswitch IP address(es)

The IP address of the softswitch (or softswitches) must be known to the EdgeMarc. This address (or addresses) is set on the VoIP ALG -> SIP page of the EM GUI. The address can be specified in any of four ways:

- DNS Name w/ SRV records
  A single softswitch DNS name that is configured to provide multiple SIP addresses, with associated weights and priorities, via DNS SRV record.

- DNS Name w/o SRV records
  A single softswitch DNS name that maps to an "A" record IP address. The EdgeMarc supports return of a single A record. Multiple (or more specifically, rotating) IP address are not supported.

- Single IP address
  A single softswitch IP address.

- List of IP addresses
  A list of softswitch IP addresses in priority order.

4.2 Determining softswitch availability

The EdgeMarc selects and monitors the Active softswitch. The active softswitch is initially the highest priority network softswitch known to the EdgeMarc. Over time the active softswitch can change, becoming the secondary network softswitch, the EdgeMarc's internal softswitch, none (if the EdgeMarc's Survivability feature is not enabled), or back to the primary.

Three events will cause the EdgeMarc to return to the primary:

- If the secondary fails, and the primary is up, the EdgeMarc will switch back to the primary.
- If the EdgeMarc goes to Local mode, then whichever softswitch is detected first the EdgeMarc will use. (Note, if the secondary is detected first, then the EdgeMarc will stay with the secondary.)
- Clicking Submit on the Survivability GUI page will cause the highest-priority softswitch to be chosen.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

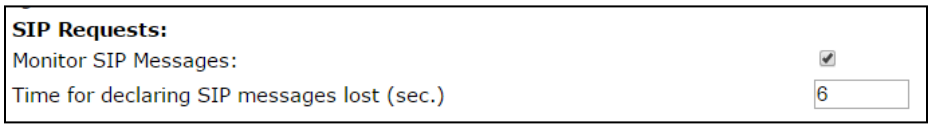
4.2.1 Monitoring the Active softswitch

Active Softswitch availability is determined using one or both of the following techniques:

- SIP message monitoring

  The EdgeMarc monitors SIP messages (Requests) from itself to the current active softswitch. If no outstanding Requests are responded to (and no incoming requests are received) for 6 seconds, then the softswitch will be declared down. The default 6-second time is configurable. This method of monitoring is recommended to be always enabled.

  Note: If Monitoring SIP Messages was disabled, the EdgeMarc will not be able to detect any SIP failures and will not know if the softswitch is still reachable or not. The status of the softswitch on the SIP server reachability section at the top of the Survivability page will always be green / reachable, even though it's not. That is why it is recommended to always have it enabled.

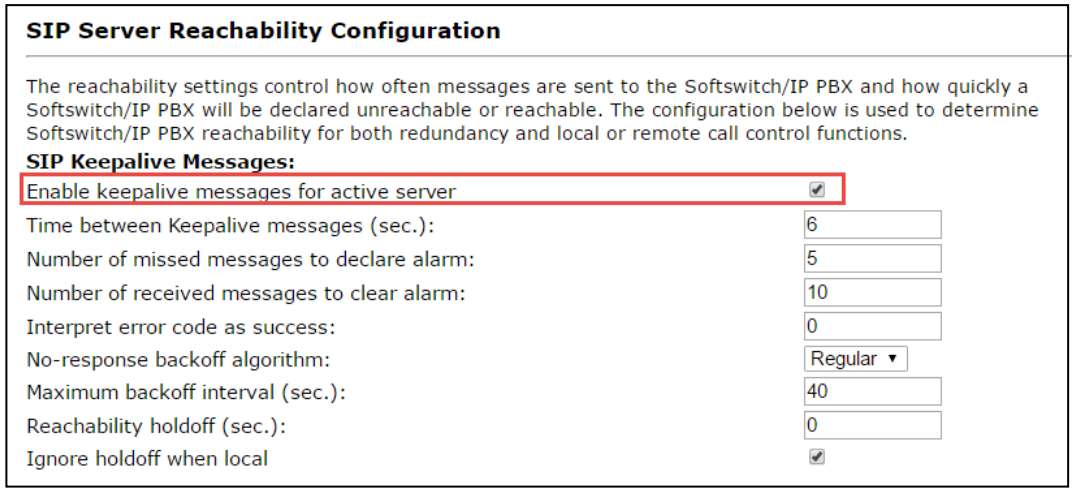


- Active-softswitch monitoring

  Optionally, the EdgeMarc can be told to additionally always send SIP Options messages to the active softswitch. In addition to the above monitoring the EdgeMarc will issue SIP Options message "pings" to the softswitch at a specified interval. This. will enable the EdgeMarc to detect that a softswitch (or connectivity thereto) has failed while no other phone activity is being initiated from the site.
  The rate at which these messages are sent, as well as how many are necessary to declare that the softswitch is down, can be set in the Survivability page GUI as shown on the diagram below.

  Note: Disabling the 'Enable keepalive messages for active server' does NOT disable all the other settings below it. The OPTIONS messages will still follow what is configured in those settings. OPTION messages will still be sent out the EdgeMarc whenever one or more of the SIP servers become unreachable.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved



When either of the above techniques indicate that the current active softswitch is unavailable, a new active softswitch will be assigned and the prior softswitch will be monitored, via SIP Options "pings", for recovery, as described below.

4.2.2 Monitoring inactive / down softswitches

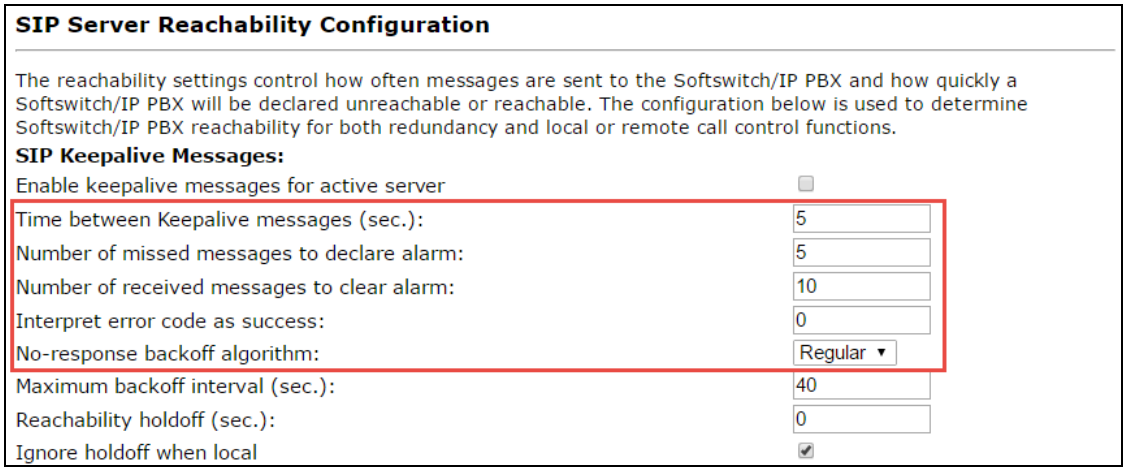
When the EdgeMarc is using a secondary softswitch or its internal softswitch as the Active one, it will monitor the higher priority softswitch(es) for availability. It does this by sending SIP Options messages. The interval between the OPTIONS messages that the EdgeMarc sends out is controlled by the '*Time between Keepalive Messages*'. The default value is 5 sec.

The EdgeMarc will expect a 200 OK response to the OPTION messages. If the softswitch responds with anything other than a 200 OK, that code will need to be added to the field '*Interpret error code as success'*. The default is '0' which means 200 OK.

The '*Number of received messages to clear alarm*' determines the number of consecutive successful responses the EdgeMarc expects before declaring the down softswitch as Active again. In this case, it will look for 10 consecutive successful responses to SIP Options messages before it declares a softswitch to be available.

When a higher-priority softswitch is determined to again be available the EdgeMarc will assign this softswitch as the Active softswitch and direct all future messages to this softswitch. (Control of re-assignment to a higher-priority softswitch can be controlled, see section 4.5 Choosing NOT to return to the Primary softswitch, below.)

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved



SIP Options message "ping" interval – down softswitch		
First ping interval		5 seconds
Each following interval, if no response		double each prior waiting period (ie 10 secs, then 20 secs, then 40
Each following interval, if prior successful		5 seconds
Maximum ping period	Remote mode	160 seconds
	Local mode	40 seconds
Number of successful ping to declare up		Set on GUI page: "Number of received messages to clear alarm",

4.2.3 SIP Options message pacing

The EdgeMarc's Survivability design is architected to minimize the impact of SIP Options messages on the softswitch. As the CPE network scales it is important that the keep-alive mechanism not overwhelm the infrastructure.

The EdgeMarc uses two different Options message pacing techniques, one to monitor a down softswitch, the other to monitor the Active softswitch.

4.2.3.1 Monitoring a down softswitch

When the Active softswitch is either a secondary softswitch or the internal EdgeMarc softswitch, the EdgeMarc will monitor the higher-priority softswitch(es) for reachability. See Section 4.2.2 for details.

4.2.3.2 Monitoring the active softswitch

If requested, the EdgeMarc can actively monitor the health of the softswitch. *'Enable Keepalive messages for active server'* must be enabled for this feature.

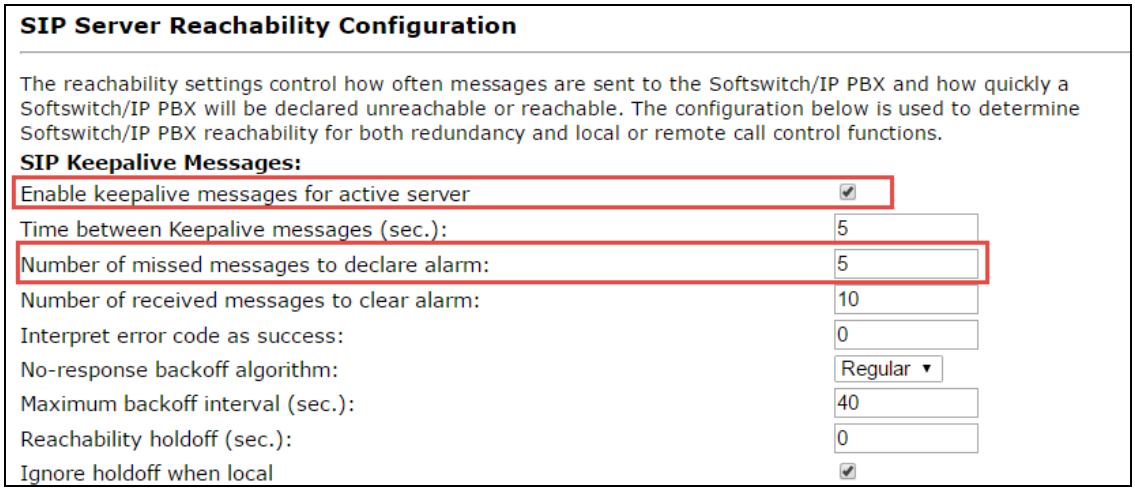
In the Active Monitoring mode, the EdgeMarc will send out OPTION messages even though there are no phones plugged into the LAN side of the EdgeMarc. The EdgeMarc will actively monitor the reachability of the provider's softswitch even where there is no

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

other SIP traffic flowing through the Edgemarc. Usually, service providers use this feature when they drop ship an EdgeMarc to the customer premises and their installers want to test the circuit before the customer installs the phones.

If the softswitch were to stop responding to Options (for whatever reason), it will take 5 consecutive non-responses before the EdgeMarc declares that the softswitch is down. (This value is the '*Number of missed messages to declare alarm*').

At this point, the algorithm in Section 4.2.2 goes into effect.



SIP Options message "ping" interval – Active softswitch keep-alive	
Each ping interval	Set on GUI page: "Time (s) between Keepalive messages:",
Number of failed pings to declare down	Set on GUI page: "Number of missed messages to declare

4.4 Registration Rate-Pacing

The use of frequent Register messages from phone to softswitch is a common method of ensuring that NAT tunnels remain open for a session border controller. When an EdgeMarc is used there is no need to pass Register messages through to a softswitch (or SBC) at a high frequency. Once an hour is normally sufficient. There is, however, a need to have the phone register frequently with the EdgeMarc! Here's why:

The phone and softswitch usually share a common password that is strongly encrypted in the Register message flow. The EdgeMarc does not share this password. Therefore, the EdgeMarc cannot generate a Register message on behalf of an endpoint; rather, the phone must always generate a Register and the EdgeMarc either passes that register through to the softswitch or responds to it locally. (Note, the EdgeMarc will never respond positively (200 OK) to a Register until the softswitch has already done so.)

When properly configured, this Register rate-pacing will limit the rate at which the softswitch or SBC is hit with these Register messages. The softswitch/SBC will be

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

able to maintain a reasonably up-to-date address of record for each DID, it will not be overburdened by Register messages, and the EdgeMarc will be able to cause a fast failover at the time of a network connectivity change.

After recovery from a site outage (where the EdgeMarc has entered Local mode), it is important to pass a Register through to the softswitch as soon as connectivity has been restored. If the outage was longer than the last Register's expiration period – of if the softswitch itself restarted – then the phone will appear offline to the softswitch.

See section 2.2 for more information.

4.5 Notifying softswitch upon availability change

When returning control at the end of a failover event, the EdgeMarc will always pass each phone's next Register message through to the softswitch. This ensures all phones are (re)Registered with the softswitch.

The EdgeMarc does not normally forward phones' Register messages upon failover from primary-to-secondary or secondary-to-primary. However, for scenario *2.2, Model 2: Redundant softswitches using varying* endpoint addressing, it is critical that each phone re-Register upon change of the Active softswitch. The EdgeMarc can be configured to Forward Next Register whenever the EdgeMarc changes the Active softswitch, thereby updating the softswitch's address-of-record for each phone's SIP URI.

4.5.1 Choosing NOT to return to the Primary softswitch

It may be preferred that the EdgeMarc not automatically return to the primary softswitch after a failure event has ended. The EdgeMarc can be told to remain with the secondary softswitch even if the primary is available. When selected, the EdgeMarc will stay with the secondary softswitch even when the primary returns to service. See '*Enable Sticky Failover mode*'. It will only return to the main server when you hit Submit on the Survivability page.

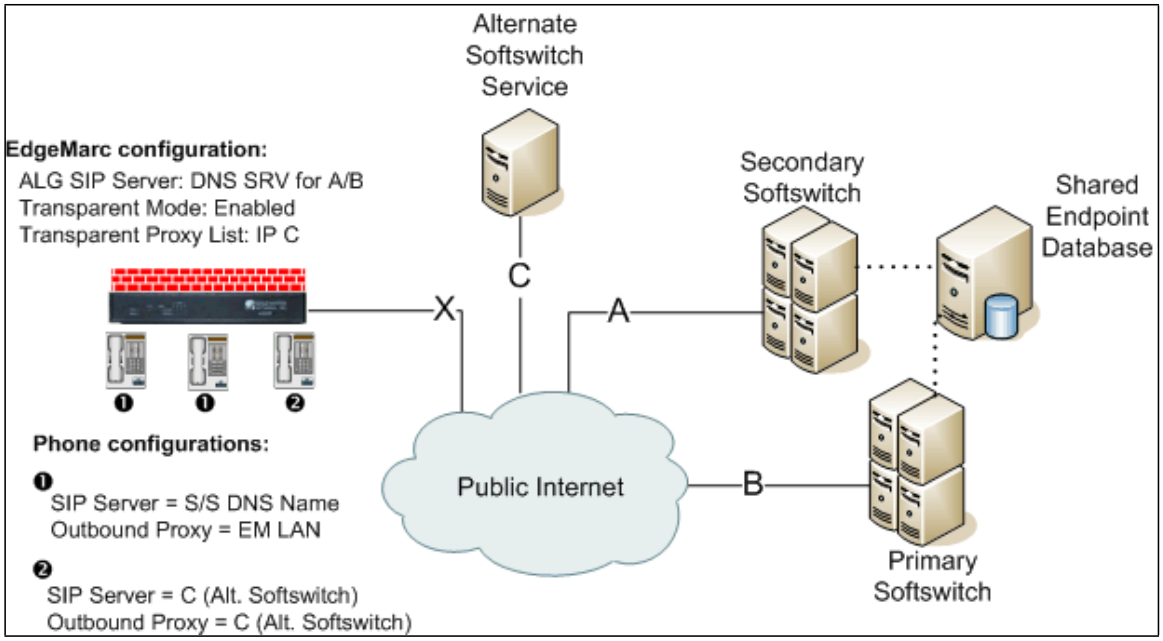
4.6 Survivability and Transparent Mode interaction

The interaction of the EdgeMarc's Survivability function with phones configured in "Transparent" mode needs detailed explanation. Transparent mode can be used for many different scenarios, a few are described below.

A consistent behavior applies for all Transparent mode configurations: The EdgeMarc will monitor the Active softswitch IP as described earlier. It will monitor SIP requests and responses to the Active softswitch IP, as well as, optionally, send Options pings to the active softswitch. Messages to other softswitch IP addresses will not be monitored and will not determine up/down state with respect to survivability.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

4.6.1 Single Transparent mode phone



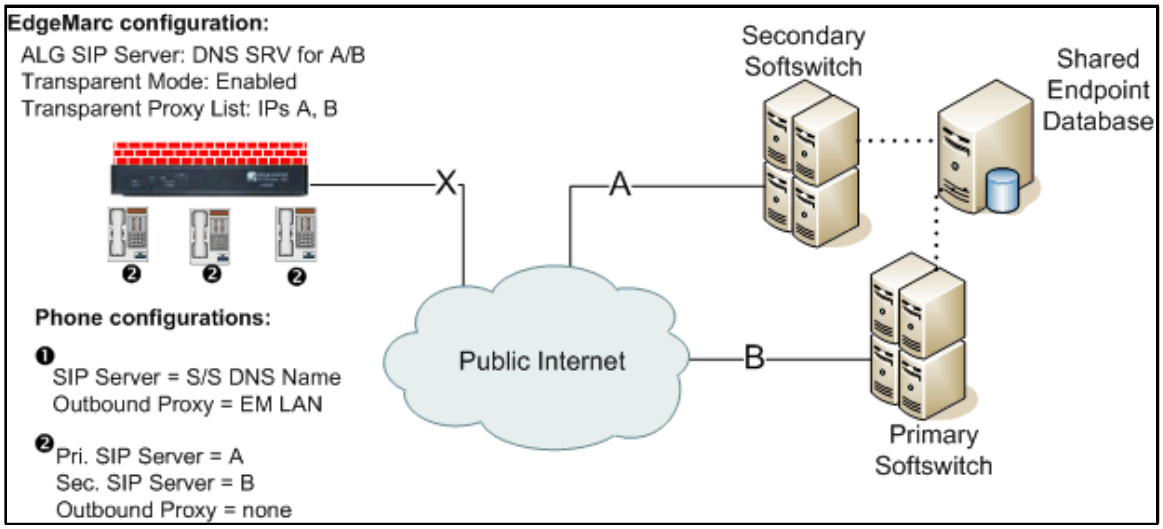
In this scenario it is the exception that a phone is configured for Transparent mode. Most phones are pointing directly to the EM as the SIP Server and the EM decides if packets are forwarded to softswitch A or B. The survivability logic as described above applies to these phones.

There are one or more phones set with configuration 6, in the above diagram. This phone is communicating directly with an alternate softswitch. It is the phone that determines the destination of SIP Requests, not the EM. While the EdgeMarc is in Remote mode, the Active softswitch (A or B) as will have no knowledge of the messages sent by this alternate phone.

If the EdgeMarc determines that both the primary and secondary softswitches are down, then it will enter Local mode. When that occurs, the SIP server inside the EdgeMarc will take over. It will intercept and process all SIP messages, including those addressed to the alternate softswitch (IP address C, above).

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

4.6.2 All phones transparent mode



In this scenario all phones are configured in Transparent mode. The EdgeMarc is aware of the two softswitches used by the phones (A and B). However it is not the EdgeMarc ALG that determines if the phones communicate with Server A or Server B, that decision is made by the phones' internal logic. The EdgeMarc does need to be aware of the softswitches to which the phones are sending their messages. This is done via the EdgeMarc's Transparent Proxy List (even if the softswitches are the same IPs as the DNS SRV record specifies).

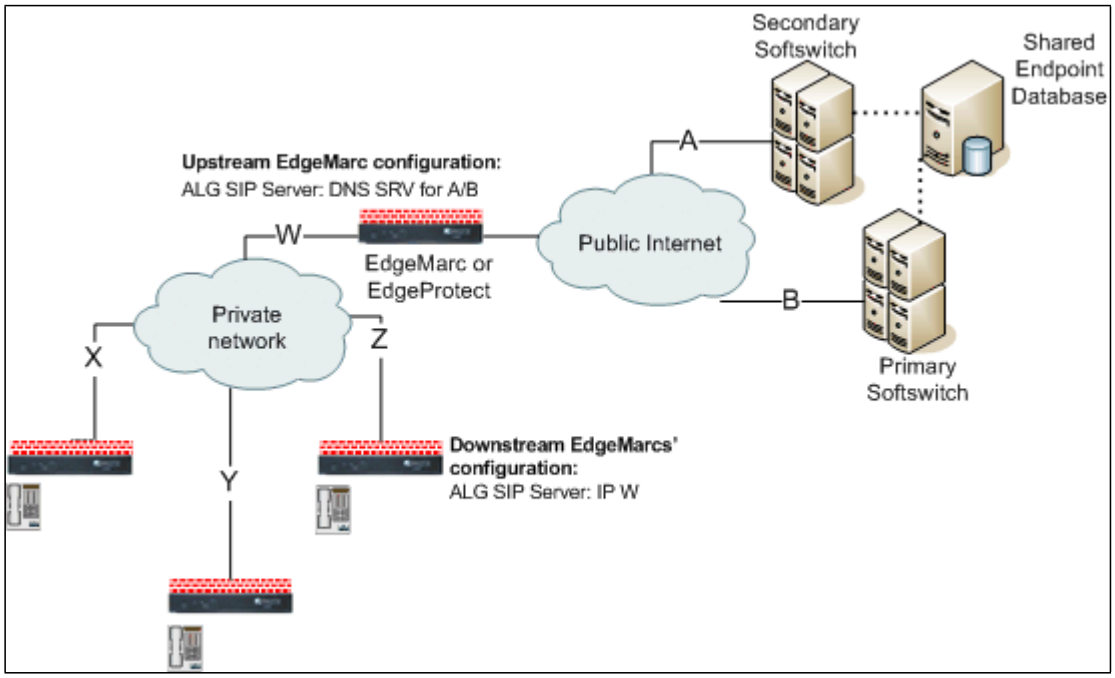
The EdgeMarc will monitor the Primary softswitch – which is initially the Active softswitch – using one or both of the methods described earlier: SIP Message Monitoring and/or Active Softswitch Keep-alive. When the primary fails as determined by either method, the EdgeMarc will change the Active softswitch to the Secondary. As described, this has no effect on whether the phones communicate with Server A or Server B, they are making that decision independently.

If both the primary and secondary softswitches are declared down, then the EdgeMarc will switch into Local mode and take over SIP processing using its internal softswitch. Regardless of whether the phones attempt to communicate with softswitch A or B, the EdgeMarc's internal softswitch will process and respond to all SIP messages.

During this time the EdgeMarc will use SIP Options keep-alive messages to determine if softswitch A or B return to service. When either does, it will then stop processing SIP messages and return to forwarding those messages to the softswitch requested by the endpoint (A or B).

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

4.7 Survivability with chained EdgeMarcs



The EdgeMarc supports chained configurations, similar to the above. Survivability is supported in this configuration. There are, however, some differences in configuration and the underlying behavior of SIP Options messages.

In a chained configuration, the upstream EdgeMarc is configured as described in the above sections. It is aware of the primary and secondary softswitches and maintains which is the Active softswitch.

The downstream EdgeMarc is aware of only one “softswitch”, that is the upstream EdgeMarc’s IP address. The downstream EdgeMarcs are essentially monitoring link connectivity.

Rather than forward SIP Options messages from each downstream EdgeMarc to the Active softswitch, the upstream EdgeMarc answers these downstream keep-alive Options pings itself. As long as the upstream EdgeMarc has reachability to one of the network softswitches, then it will reply to a downstream Options ping with a success response. When connectivity is lost to both softswitches the upstream EdgeMarc will respond with a SIP Options failure response.

The downstream EdgeMarcs will enter Local mode immediately upon receiving a failure response. Similarly, they will enter Remote mode immediately upon receiving a success response. These downstream EdgeMarcs will not wait for the specified number of pings to declare up or down, they will act immediately. The net effect is that the upstream EdgeMarc will follow the earlier timing rules to declare a softswitch up or down and the downstream EdgeMarcs will immediately confirm without having to repeat the timeout periods.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

5.0 Sample Configurations

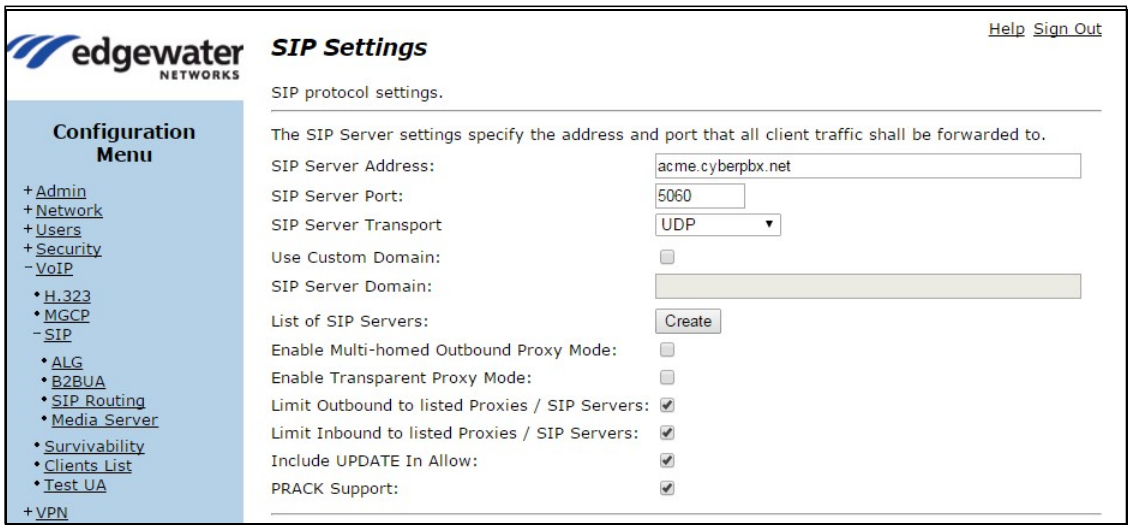
5.1 Redundant softswitches with varying endpoint addressing.

The following example steps through the EdgeMarc GUI configuration to implement the scenario described in 2.2, Model 2: Redundant softswitches using varying endpoint addressing, on page 3. This example assumes:

- DNS SRV record is used to learn primary and secondary softswitches
- EdgeMarcs running VOS v11.x or later

Step 1: Set ALG SIP Server Address

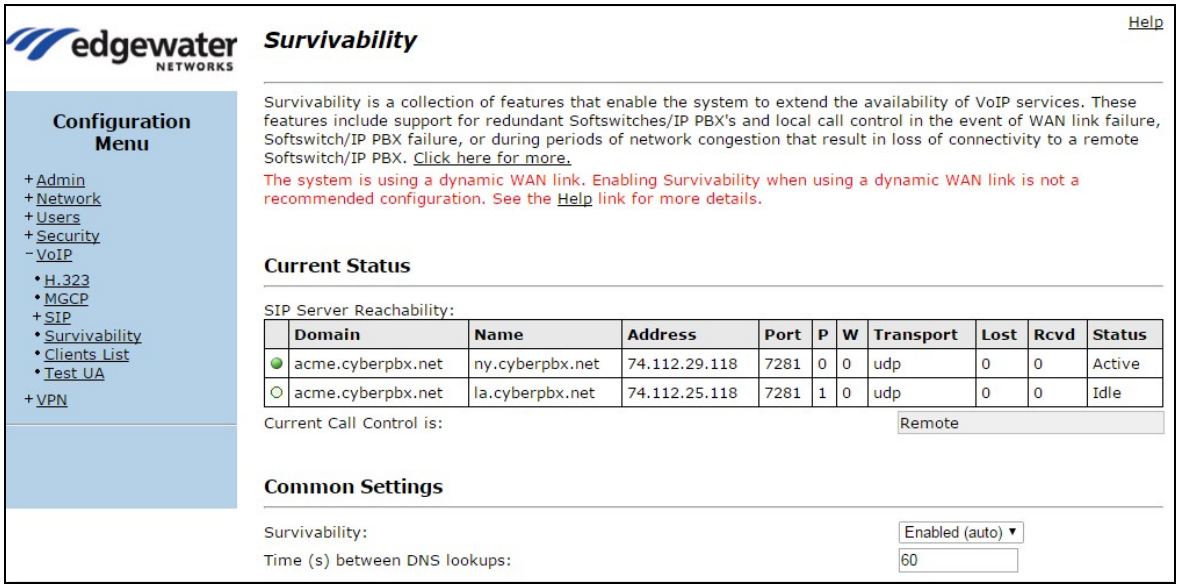
On VoIP -> SIP page set SIP Server address to proper DNS SRV name. acme.cyberpbx.net in the screenshot below:



Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

5.2 Survivability Status and Configuration

SURVIVABILITY configuration page is a sub-menu of **VoIP** page as seen in below diagram. In this example, the EdgeMarc is configured with a SIP Server name with SRV records for primary and secondary servers based on priority. It also indicates that the EdgeMarc is in Remote mode, meaning the SIP Server is currently reachable, also indicated by the green radio button to the left of the server.



When licensed, **SURVIVABILITY** can be set to Enabled (auto), Always Local and Disabled.

ENABLED (AUTO) = this is the most common setting in which the EdgeMarc starts in Remote Mode where call-routing is handled by the SIP Servers, until both SIP Servers becomes unresponsive, at this point, Current Call Control will change to Local or enter Survivability.

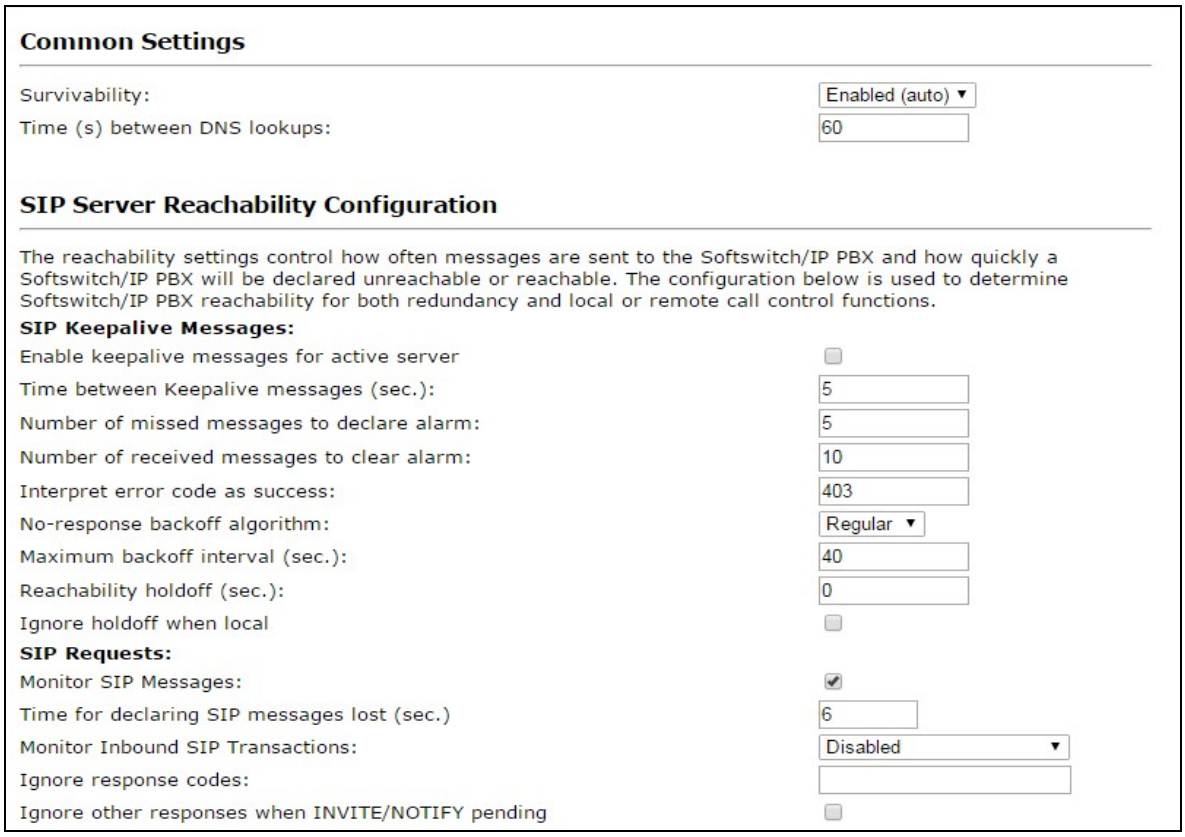
DISABLED = to turn-off Survivability which is similar to not being a licensed option.

ALWAYS LOCAL = to enable Local Mode or enter Survivability permanently.

TIME BETWEEN DNS LOOKUPS – default value is 60 seconds, is the time between DNS SRV lookups.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

5.3 SIP Server Reachability Configuration



The following fields are relevant for this configuration.

ENABLE KEEPALIVE MESSAGES FOR ACTIVE SERVER = keepalive pings in the form of SIP Option messages are sent to the active SIP Server. This is disabled by default.

TIME BETWEEN KEEPALIVE MESSAGES = time in seconds between two keepalive messages

NUMBER OF MISSED MESSAGES TO DECLARE ALARM = consecutive SIP Option messages without a response before SIP Server is considered unreachable and failover to backup SIP Server or Local mode.

NUMBER OF RECEIVED MESSAGES TO CLEAR ALARM = consecutive SIP Option messages with a response before SIP Server is considered reachable after being unreachable, or from Local mode to Remote mode. This is also true even if keepalive messages for active server is disabled.

INTERPRET ERROR CODE AS SUCCESS = expected SIP response (aside from 200 OK) to SIP Option messages sent to both active, backup and inactive SIP Servers. This is required for SIP Server to be declared reachable. Example values are 403,404 and 405.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

NO-RESPONSE BACKOFF ALGORITHM = REGULAR OR RANDOM

> **REGULAR** - working in conjunction with "Time Between Keepalive Messages", when the EdgeMarc does not receive any response to keepalives, it doubles the interval for the next keepalive until the "Maximum backoff interval" is reached.
>
> **RANDOM** – keepalives is sent from anywhere between 3 seconds and "Maximum backoff interval"

MAXIMUM BACKOFF INTERVAL = the maximum interval between keepalive messages. Default value is 40 seconds

REACHABILITY HOLDOFF = the time it waits before marking a SIP Server active once it's been declared reachable. Default value is 0 second.

IGNORE HOLDOFF WHEN LOCAL = when Reachability Holdoff is set to other than 0 seconds, you can enable this option to ignore Reachability Holdoff when transitioning from Local Mode to Remote Mode.

MONITOR SIP MESSAGES = enabled by default, this option monitors SIP requests to the active server, if timeout is reached, server is marked unreachable. This is independent of the Keepalive Messages sent by the EdgeMarc.

TIME FOR DECLARING SIP MESSAGES LOST = time in seconds when SIP Requests timeout is reached. Default value is 6 seconds.

MONITOR INBOUND SIP TRANSACTIONS

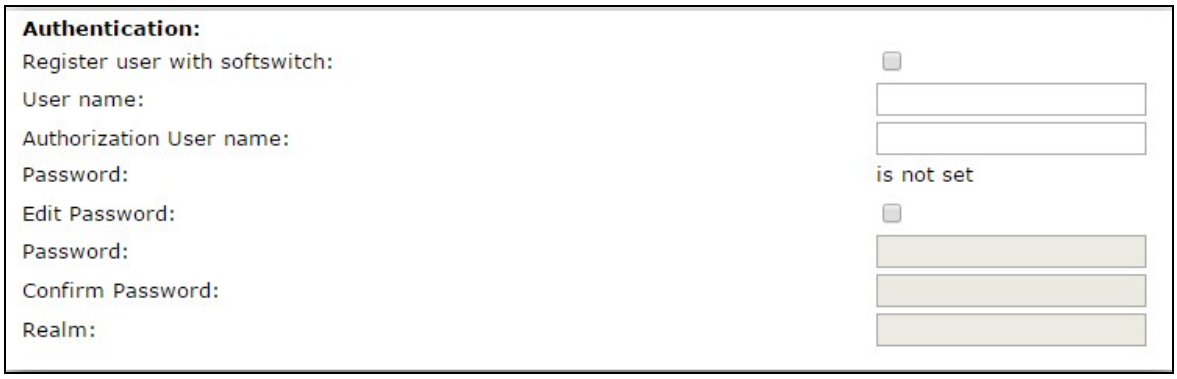
> **DISABLED** – inbound SIP messages are not able to cancel SIP messages timeout
>
> **ALL SIP REQUESTS** – when received, inbound SIP Requests can cancel SIP timer for outgoing SIP Requests.
>
> **ALL EXCEPT SIP OPTIONS** – when received, inbound SIP Requests except OPTIONS can cancel SIP timer for outgoing SIP Requests.

IGNORE RESPONSE CODES – SIP responses from the active SBC are ignored as valid responses to stop SIP timeout. Multiple SIP responses are separated by a comma. Example 100, 403

IGNORE OTHER RESPONSES WHEN INVITE/NOTIFY PENDING – when enabled, no response for non-Invite or non-Notify requests cannot cancel SIP message timeout when Invite/Notify Request is already pending.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

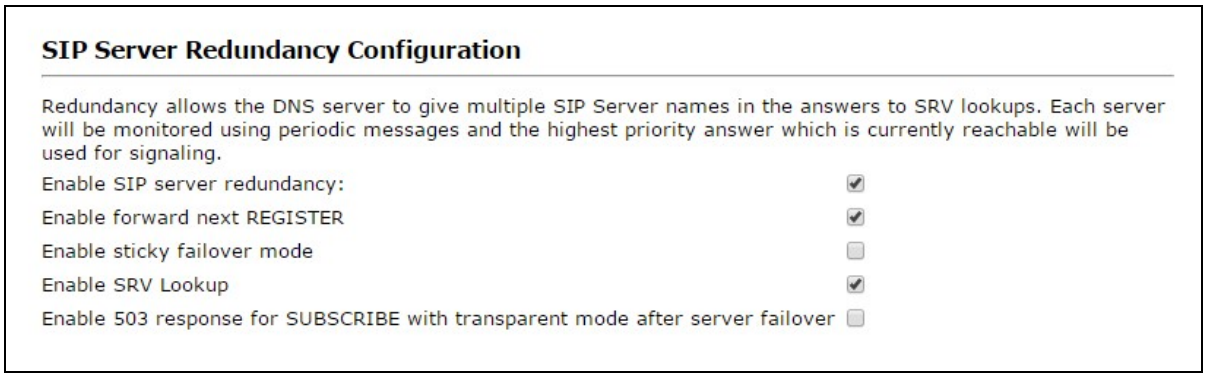
5.4 Authentication Configuration



REGISTER USER WITH SOFTSWITCH = When enabled, the next few parameters allow credentials to be used for Register messages to the active server. SIP Option messages will use these credentials when sending keepalive messages.

USERNAME, AUTHORIZATION NAME and PASSWORD

5.5 SIP Server Redundancy Configuration



The following fields are relevant for this configuration.

ENABLE SIP SERVER REDUNDANCY = Tells the EdgeMarc to use DNS SRV resolution for the SIP Server DNS name provided on the VoIP -> SIP page. This is enabled by default.

ENABLE FORWARD NEXT REGISTER = Tells the EdgeMarc to forward the next register from every phone after a change in the Active softswitch. This ensures the address of record for each phone's DID is updated. This is enabled by default.

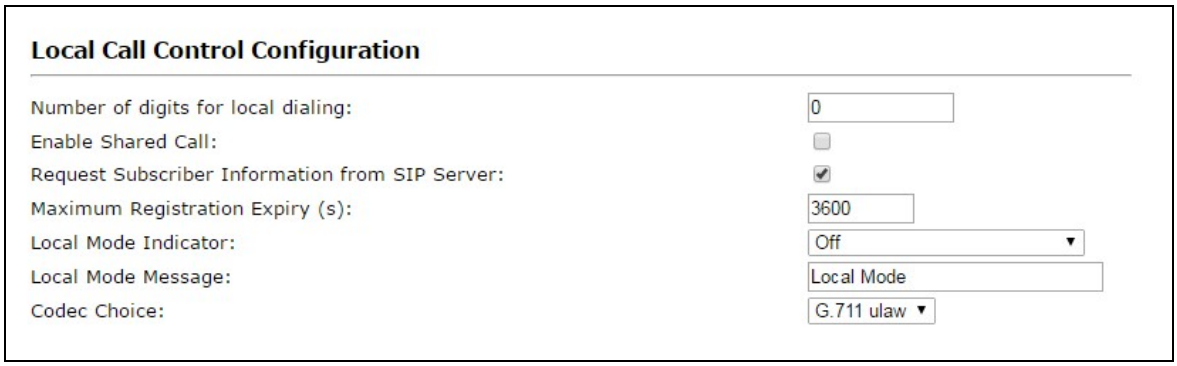
ENABLE STICKY FAILOVER MODE = When enabled, the active server will remain active regardless of a higher priority server becoming available/reachable. This is disabled by default.

ENABLE SRV LOOKUP = When enabled, the EdgeMarc performs a DSN SRV lookup of the SIP Server domain name in the VoIP -> SIP Settings Page. Example DNS SRV query using SIP Server in page 16: **SRV _sip._udp.acme.cyberpbx.net**

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved - Page 20 of 27

ENABLE 503 RESPONSE FOR SUBSCRIBE WITH TRANSPARENT MODE AFTER SERVER FAILOVER = When multiple redundant SIP Servers are in use, upon a failover event where a new SIP server becomes the active SIP Server for the system, this feature when enabled will respond with a "503" to the next SUBSCRIBE from an endpoint to indicate to the endpoint that it needs to refresh its subscription with a new server.

5.6 Local Call Control Configuration



The following fields are relevant for this configuration.

NUMBER OF DIGITS FOR LOCAL DIALING = The number of digits used to process extension to extension calling. Default setting is 0, meaning the whole phone number is used.

ENABLE SHARED CALL = When enabled, calls to any line appearances will be routed to the primary line of a SIP endpoint. This is disabled by default, meaning, calls to none primary line appearance will be ignored.

REQUEST SUBSCRIBER INFORMATION FROM SIP SERVER = When enabled and supported by the softswitch, the EdgeMarc will request subscriber information during phone registration from the active server.

MAXIMUM REGISTRATION EXPIRY = This is the maximum registration expiry timeout in seconds that the local call control server will accept from SIP endpoints. Default setting is 3600 seconds.

LOCAL MODE INDICATOR =

OFF - No local mode indicator is used. Default setting.

SUPRESS REGISTER RESPONSE - The EdgeMarc ignores Register messages in Local-Mode.

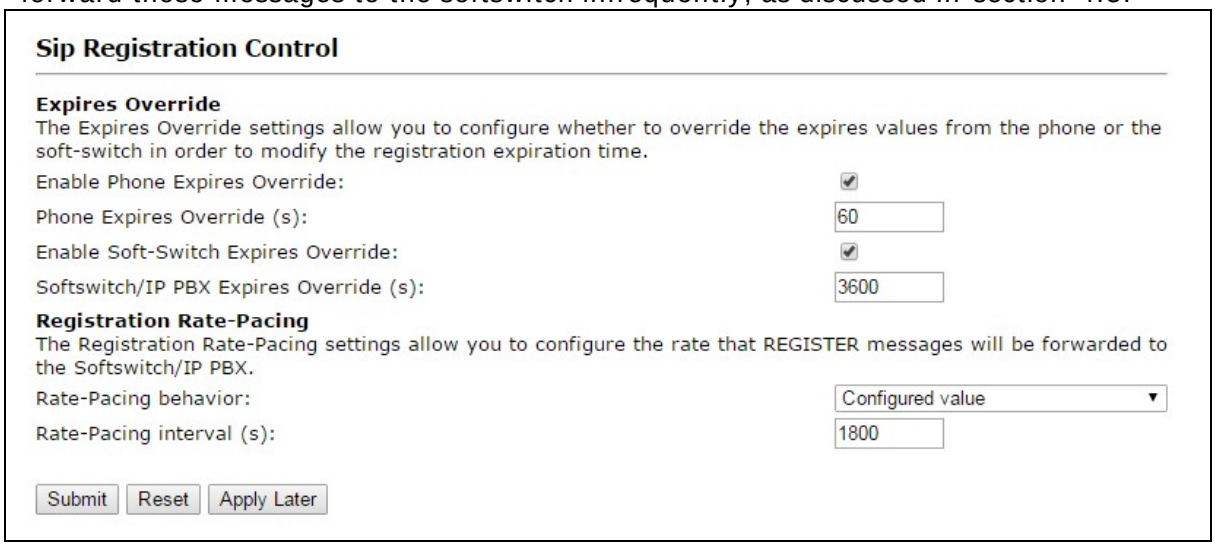
SEND RESPONSE INFORMATION – The EdgeMarc responds with specific message displayed by the phone while in Local Mode.

LOCAL MODE MESSAGE – Specific string the EdgeMarc sends within the SIP Register 200 OK response the endpoint can display while in Local Mode.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

5.7 Registration Rate-Pacing Configuration

Configure the phones to register frequently with the EdgeMarc but have the EdgeMarc forward those messages to the softswitch infrequently, as discussed in section 4.3.



EXPIRES OVERRIDE =

ENABLE PHONE EXPIRES OVERRIDE – The EdgeMarc responds to client Register messages with specified expiry timer. This is enabled by default.

PHONE EXPIRES OVERRIDE – Time in seconds that the EdgeMarc set as the expiry timer in the 200 OK response for client Register message. Default setting is 60 seconds.

ENABLE SOFT-SWITCH EXPIRES OVERRIDE – The EdgeMarc forwards the client Register message to the softswitch with a valid Registration for x duration. This is enabled by default.

SOFTSWITCH / IP PBX EXPIRES OVERRIDE – Time in seconds that the EdgeMarc set as the duration for the client's valid Registration with the softswitch. Default setting is 3600 seconds.

REGISTRATION RATE-PACING =

RATE-PACING BEHAVIOR – NONE, Softswitch Provided Value or Configured Value.

NONE – Rate-pacing is disabled. All Register messages from the endpoints are forwarded to the softswith.

SOFT-SWITCH / IP PBX PROVIDED VALUE – Register messages from the endpoints are rate-paced/forwarded based on the expiry timer within the 200 OK response from the softswitch.

CONFIGURED VALUE – Rate-Pacing Interval – Default setting is 1800 seconds. This is normally set to half the duration of Soft-switch Expires Override or whatever

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

duration the softswitch keeps an endpoint Registration valid.

6.0 Shared-Call support in Local mode

The EdgeMarc provides limited support when in Local mode for Polycom phones configured for Broadsoft's and Polycom's Shared-Call facility (sometimes known as Bridged Line Appearance [BLA]).

The following steps describe how to configure the EdgeMarc to support phones configured in a BLA mode.

Overview

Shared-Call, or Shared Call Appearance (SCA), as defined for this feature, is a Broadsoft softswitch function that allows one DID to map to multiple endpoint Line SIP URIs. When the softswitch receives a call for that DID, it automatically sends Invites to the main URI associated with that DID as well as one or more Shared Call Appearance URIs. When a call is made from one of the SCA URIs, the calling-line number presented is the associated DID.

Polycom phones in conjunction with Broadsoft take this a step farther, providing a more advanced Shared Call Appearance where each phone continuously sees the status of the shared line. If one phone puts that line on hold, all other phones show the line on hold. Any of the phones can then take the line off hold. This capability is referred to as Bridged Line Appearance (BLA). The BLA capability is turned on simply by setting a parameter in the Polycom phone configuration file to "type=shared".

The EdgeMarc Shared Call Appearance Survivability function is the ability to offer a limited SCA function when the EdgeMarc switches into fallback mode, taking over call signaling processing.

Supported function

The goal of the EdgeMarc SCA function is to work in an environment where:

- Only Polycom phones are in use
- Shared lines are all configured as type=shared (ie. BLA functionality is in use)

In a WAN outage, when the EdgeMarc takes over call control, incoming calls to shared-line DIDs will ring on the same phones as normally occurs. Any phone can pick up the call and can transfer it to any other phone. BLA functionality, however, is not provided.

The private BLA protocol used between the Polycom phone and the Broadsoft switch is not available in the EdgeMarc, therefore a specific, restricted configuration must be deployed to allow a limited SCA-style function to operate when the EdgeMarc is in fallback mode. This is accomplished by providing each phone with at least one Line – always including the first line – with a non-shared DID (type=private in the Polycom configuration file). The EdgeMarc will then map the other DIDs (those whose Lines are type=shared) to ring in on Line 1 when they are called during Local mode. These BLA lines cannot be used to make outbound calls when in fallback mode, the first line must always be used.

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

Configuration requirements

The EdgeMarc's ability to implement Shared Call Appearance requires that the EdgeMarc understand which phone Lines (which SIP URIs) represent a BLA (type=shared) Line and which represent a standard (type=private) Line.

The EdgeMarc, as of release v6.1.5, makes this determination by examining the SIP URI value itself.

The EdgeMarc assumes that a SIP URI of the following form is for a "type=shared" line:

nnnnnnnnnnXXXa
where:
nnnnnnnnnn is the 10-digit DID
XXX is an alpha string (recommended "sca")
a is a digit (recommended 0 thru 9)

The EdgeMarc assumes that a SIP URI of the following form is for a "type=private" line:

nnnnnnnnnn
where:
nnnnnnnnnn is the 10-digit DID

The EdgeMarc uses this implied knowledge of the line type, along with some additional assumptions detailed below, to build a valid dialing plan that will work when faillback mode is active.

For someone who is used to configuring a Broadsoft without prerequisites for the format of URIs, this may mean a change in how you might otherwise configure Line names. You must use the URI format described above.

The following is a summary of the rules that will result in a valid phone configuration that works in fallback mode:

1) Line 1 of each phone must be a type=private line using the above URI format for the Line
2) Lines 2+ of each phone must be a type=shared line using the above URI format for each Line
3) Any Line that is an SCA Line (either on the primary phone or a phone that has the shared call appearance) must use a type=shared URI for that line

These simple rules imply other characteristics that you must follow:

4) The "primary owning" phone for a given shared DID, say a DID of 2125551212, must have this DID assigned to its 2nd or greater line (ie not Line 1) AND must use the type=shared format. So a valid URI for this DID on the primary phone would be: "2125551212sca0" (0=zero), assigned to Line 2.

5) Line 1 on a phone that owns a shared DID must be a unique number that is type=private and has the above type=private format URI. In the above

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

6) example, the phone that "owns" 21255551212 cannot have that DID on Line 1. Line 1 must have a different, private DID and type=private URI.

A few more related rules/reminders:

7) On the Survivability page you must enable:
"Enable Local-Mode Indicator" and "Enable Shared Call", as described above in Step 2.

8) On the VoIP ALG -> SIP page you must configure:
"Registration rate pacing: 30/3600/1800", as described above in Step 3.

9) If you make changes in the phones' URIs, particularly changing any Line from a type=private URI to a type=shared URI, then you must clear out the EdgeMarc Clients List in order to flush out the prior URI. Otherwise the old URI will stay around until it times out (1 day) and will impact the dialing plan that is built.

Example Polycom configuration files

Below are example Polycom configuration files that are properly defined to support SCA Survivability function.

Phone 1:

- 4 Lines
- The first two Lines are private to this phone
- The third is an SCA Line for a DID owned primarily by Phone 2
- The fourth is an SCA Line for a DID owned primarily by this phone

`reg.1.displayName=""`	
`reg.1.address="2408881040"`	This DID rings on no other phone. Its URI is all numeric.
`reg.1.label="1040"`	
`reg.1.type="private"`	The 1st Line must be type=private. This is the line on which the EdgeMarc will ring all incoming calls for the other type=shared lines.
`reg.1.auth.userId="2408881040"`	
`reg.1.auth.password="2408881040"`	
`reg.2.displayName=""`	
`reg.2.address="2408881039"`	This particular phone has a second private line. This is optional. The URI is all numeric.
`reg.2.label="1039"`	
`reg.2.type="private"`	All lines that ring nowhere else must have type=private.
`reg.2.auth.userId="2408881039"`	
`reg.2.auth.password="2408881039"`	
`reg.2.server.dnsLookupOption="0"`	
`reg.3.displayName=""`	

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

reg.3.address="2408881034sca1"	This DID is a Shared Call Appearance for a number primarily owned by another phone. Its URI contains the string “sca” after the DID itself.
reg.3.label="1034"	
reg.3.type="shared"	All lines that ring on multiple phones must use type=shared.
reg.3.auth.userId="2408881034"	
reg.3.auth.password="2408881034"	
reg.4.displayName=""	
reg.4.address="2408881033sca0"	This DID has a Shared Call Appearance on one or more other phones. Because this is an SCA DID, its URI has the string “sca” after the DID. Because this is the phone that is the primary owner of this DID, the value “0” was chosen after the “sca” string.
reg.4.label="1033"	
reg.4.type="shared"	All lines that ring on multiple phones must use type=shared.
reg.4.auth.userId="2408881033"	
reg.4.auth.password="2408881033"	

Phone 2:

- 3 Lines
- The first Line is private to this phone
- The second is an SCA Line for a DID owned primarily by this phone
- The third is an SCA Line for a DID owned primarily by Phone 1

reg.1.displayName=""	
reg.1.address="2408881041"	This DID rings on no other phone. Its URI is all numeric.
reg.1.label="1041"	
reg.1.type="private"	The 1st Line must be type=private. This is the line on which the EdgeMarc will ring all incoming calls for the type=shared lines.
reg.1.auth.userId="2408881041"	
reg.1.auth.password="2408881041"	
reg.2.displayName=""	
reg.2.address="2408881033sca1"	This DID is a Shared Call Appearance for a number primarily owned by another phone. Its URI contains the string “sca” after the DID itself.
reg.2.label="1033"	
reg.2.type="shared"	All lines that ring on multiple phones must use type=shared.
reg.2.auth.userId="2408881033"	
reg.2.auth.password="2408881033"	
reg.3.displayName=""	

Copyright © 2016. Edgewater Networks, Inc - All Rights Reserved

reg.3.address="2408881034sca0"	This DID has a Shared Call Appearance on one or more other phones. Because this is an SCA DID, its URI has the string "sca" after the DID. Because this is the phone that is the primary owner of this DID, the value "0" was chosen after the "sca" string.
reg.3.label="1034"	
reg.3.type="shared"	All lines that ring on multiple phones must use type=shared.
reg.3.auth.userId="2408881034"	
reg.3.auth.password="2408881034"	

Phone 3:

- 2 Lines
- The first Line is private to this phone
- The second is an SCA Line for a DID owned primarily by Phone 1

reg.1.displayName=""	
reg.1.address="2408881042"	This DID rings on no other phone. Its URI is all numeric.
reg.1.label="1042"	
reg.1.type="private"	The 1st Line must be type=private. This is the line on which the EdgeMarc will ring all incoming calls for the type=shared lines.
reg.1.auth.userId="2408881042"	
reg.1.auth.password="2408881042"	
reg.2.displayName=""	
reg.2.address="2408881033sca2"	This DID is a Shared Call Appearance for a number primarily owned by another phone. Its URI contains the string "sca" after the DID itself.
reg.2.label="1033"	
reg.2.type="shared"	All lines that ring on multiple phones must use type=shared.
reg.2.auth.userId="2408881033"	
reg.2.auth.password="2408881033"	

Local-Mode Indicator

Local-Mode Indicator tells the EdgeMarc to indicate on the phone that fallback mode is active. This is intended to signal to the phone user that softswitch capabilities, such as inter-site 4-digit dialing, are not presently available.

As of VOS v6.x, this indication is provided by causing the Line icon on Polycom phones to turn hollow. (The same indication as when a phone is unable to Register with a softswitch.)

If Local Mode Indicator is not selected, then when the EdgeMarc enters fallback mode no change is seen on the phone itself.

Copyright © 2016, Edgewater Networks, Inc. All rights reserved