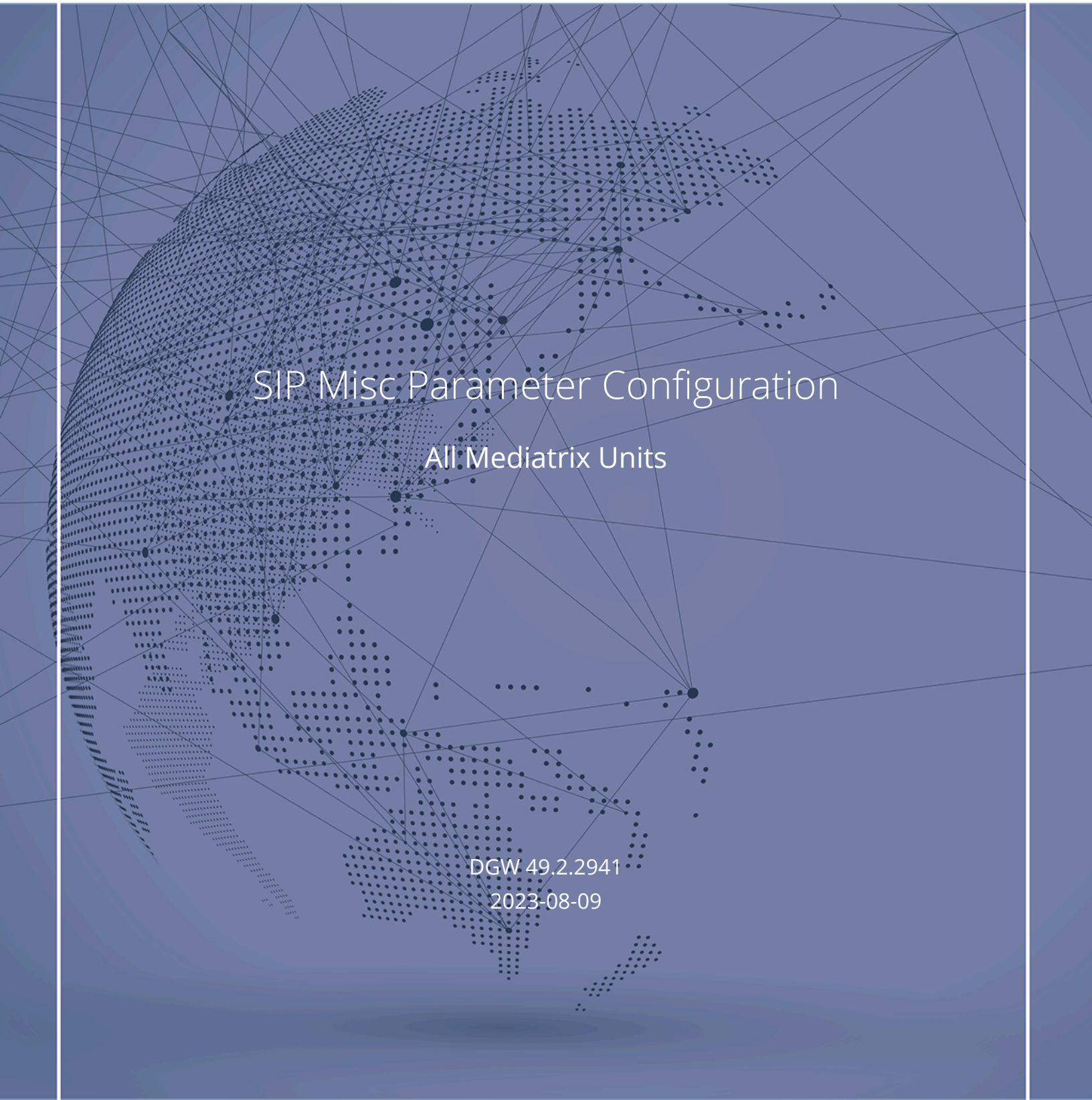


SIP Misc Parameter Configuration

All Mediatrix Units

DGW 49.2.2941

2023-08-09

Table of Contents

Basic Concepts

SIP Penalty Box

The penalty box feature is useful when a given host FQDN resolves to a non-responding address. When the address times out, it is put into the penalty box for a given amount of time. During that time, this address is considered as “non-responding” for all requests

This feature is useful when DNS requests return multiple or varying addresses for a host FQDN. It makes sure that, when a host is down, no SIP request is sent to it for a minimal amount of time. When enabled, this feature takes effect immediately on the next call attempt.

The penalty box feature is applied only when using UDP or TCP connections established with a FQDN. A similar penalty box feature for the TLS persistent connections is available via the **TLS Persistent Retry Interval** parameter.

Note: The Penalty Box feature works only with Trunk Gateways, i.e. it is disabled when an Endpoint Gateway type is configured.

SIP Penalty Box vs Transport Types

Media5 recommends to use this feature with care when supporting multiple transports or you may experience unwanted behaviours. When the Mediatrix unit must send a packet, it retrieves the destination from the packet. If the destination address does not specify a transport to use and does not have a DNS SRV entry that configures which transport to use, then the Mediatrix unit tries all transports it supports, starting with UDP. If this fails, it tries with TCP. The unit begins with UDP because all SIP implementations must support this transport, while the mandatory support of TCP was only introduced in RFC 3261.

Note: It is not the destination itself that is placed in the penalty box, but rather targets, which are a combination of address, port, and transport. Targets put in penalty box are not used unless all the targets are in the penalty box. In that case, the highest priority target is used.

Let’s say for instance that the Mediatrix unit supports both the UDP and TCP transports. It tries to reach endpoint “B” for which the destination address does not specify a transport and there is no DNS SRV entry to specify which transports to use in which order. It turns out that this endpoint “B” is also down. In this case, the Mediatrix unit first tries to contact endpoint “B” via UDP. After a timeout period, the UDP target is placed in the penalty box and the unit then tries to contact endpoint “B” via TCP. This fails as well and the TCP target is also placed in the penalty box.

Now, let’s assume endpoint “B” comes back to life and the Mediatrix unit tries again to contact it before UDP and TCP targets are released from the penalty box. First, the unit tries UDP, but it is currently in the penalty box and there is another transport left to try. The Mediatrix unit skips over UDP and tries the next target, which is TCP. Again, TCP is still in the penalty box, but this time, it is

the last target the Mediatrix unit can try, so penalty box or not, TCP is used all the same to try to contact endpoint “B”.

There is a problem if endpoint “B” only supports UDP (RFC 2543-based implementation). Endpoint “B” is up, but the Mediatrix unit still cannot contact it: with UDP and TCP in the penalty box, the unit only tries to contact endpoint “B” via its last choice, which is TCP.

The same scenario would not have any problem if the penalty box feature was disabled. Another option is to disable TCP in the Mediatrix unit, which makes UDP the only possible choice for the unit and forces to use UDP even if it is in the penalty box.

You must fully understand the above problem before configuring this feature. Mixing endpoints that do not support the same set of transports with this feature enabled can lead to the above problems, so it is suggested to either properly configure SRV records for the hosts that can be reached or be sure that all hosts on the network support the same transport set before enabling this feature.

Default Conversion of Standard SIP Error Codes To ISDN Q.850 Cause Codes

Mediatrix devices internally use Q.850 ISDN cause codes as the common representation for call errors and call terminations. Mediatrix devices are gateways used between SIP and conventional (i.e. non-SIP) telephony technologies; therefore converting SIP error codes to Q.850 ISDN cause codes is required in both directions i.e. from SIP to ISDN and ISDN to SIP.

The following table presents the conversion of SIP Error Codes to Q.850 ISDN Cause Codes. It is possible to override these default conversions and to configure the conversions of any other SIP error code between 400 and 699. (Refer to the Basic tasks)

SIP Error Codes	Q.850 ISDN Cause Codes
400: Bad Request	41 Temporary Failure
401: Unauthorized	21 Call rejected
402: Payment required	21 Call rejected
403: Forbidden	21 Call rejected
404: Not found	1 Unallocated number
405: Method not allowed	63 Service or option unavailable
406: Not acceptable	79 Service/option not implemented
407: Proxy authentication required	21 Call rejected
408: Request timeout	102 Recovery on timer expiry
410: Gone	22 Number changed (w/o diagnostic)
413: Request Entity too long	127 Interworking
414: Request-URI too long	127 Interworking
415: Unsupported media type	79 Service/option not implemented
416: Unsupported URI Scheme	127 Interworking
420: Bad extension	127 Interworking
421: Extension Required	127 Interworking
423: Interval Too Brief	127 Interworking
480: Temporarily unavailable	18 No user responding
481: Call/Transaction Does not Exist	41 Temporary Failure
482: Loop Detected	25 Exchange - routing error
483: Too many hops	25 Exchange - routing error
484: Address incomplete	28 Invalid Number Format
485: Ambiguous	1 Unallocated number
486: Busy here	17 User busy
500: Server internal error	41 Temporary failure
501: Not implemented	79 Not implemented, unspecified
502: Bad gateway	38 Network out of order
503: Service unavailable	41 Temporary failure
504:Server time-out	102 Recovery on timer expiry
504: Version Not Supported	127 Interworking
513: Message Too Large	127 Interworking

SIP Error Codes	Q.850 ISDN Cause Codes
600: Busy everywhere	17 User busy
603: Decline	21 Call rejected
604: Does not exist anywhere	1 Unallocated number

Default Conversion of Standard Q.850 ISDN Cause Codes to SIP Error Codes

Mediatrix devices internally use Q.850 ISDN cause codes as the common representation for call errors and call terminations. Mediatrix devices are gateways used between SIP and conventional (i.e. non-SIP) telephony technologies; therefore, converting SIP error codes to Q.850 ISDN cause codes is required in both directions i.e. from SIP to ISDN and ISDN to SIP.
The following table presents the conversion of Q.850 ISDN Cause Codes to SIP Error Codes. It is possible to override these default conversions and to configure the conversions of any other Q.850 ISDN Cause Codes between 1 and 127. (Refer to the Basic tasks.)

Normal Event

Q.850 ISDN Cause Codes	SIP Error Codes
1: Unassigned (unallocated) number.	404 Not Found
2: No route to specified transit network.	404 Not Found
3: No route to destination.	404 Not Found
6: Channel unacceptable.	500 Internal Server Error
7: Call awarded and being delivered in an established channel.	500 Internal Server Error
16 normal call clearing	--- BYE or CANCEL
17: User busy.	486 Busy Here
18: No user responding.	408 Request Timeout
19: User alerting, no answer.	480 Temporarily unavailable
20: Subscriber absent.	480 Temporarily unavailable
21: Call rejected.	403 Forbidden
22: Number changed (w/o diagnostic).	410 Gone
22: Number changed (w diagnostic).	301 Moved Permanently
23: Redirection to new destination.	410 Gone
26: Non-selected user clearing.	404 Not Found
27: Destination out of order.	502 Bad Gateway
28: Invalid number format (incomplete number)	484 Address incomplete
29: Facility rejected.	501 Not implemented
30: Response to STATUS ENQUIRY.	500 Internal Server Error
31 normal unspecified	480 Temporarily unavailable

Resource unavailable

ISUP Cause Value	SIP Response
34: No circuit/channel available.	503 Service unavailable
38: Network out of order.	503 Service unavailable
41: Temporary failure.	503 Service unavailable
42: Switching equipment congestion. .	503 Service unavailable
43: Access information discarded.	500 Internal Server Error
44: Requested circuit/channel not available.	500 Internal Server Error
47: Resource unavailable, unspecified	503 Service unavailable

Service or option not available

ISUP Cause Value	SIP Response
55: Incoming calls barred within CUG.	403 Forbidden
57: Bearer capability not authorized.	403 Forbidden
58: Bearer capability not presently available.	503 Service unavailable
63: Service or option not available, unspecified.	500 Internal Server Error

Service or option not implemented

ISUP Cause Value	SIP Response
65: Bearer capability not implemented.	488 Not Acceptable Here
66: Channel type not implemented.	500 Internal Server Error
69: Requested facility not implemented.	500 Internal Server Error
70: Only restricted digital information bearer. .	488 Not Acceptable Here
79: Service or option not implemented, unspecified	501 Not Implemented

Invalid Message

ISUP Cause Value	SIP Response
81: Invalid call reference value.	500: Internal Server Error
82: Identified channel does not exist.	500 Internal Server Error
83: A suspended call exists, but this call identity does not.	500 Internal Server Error
84: Call identity in use.	500 Internal Server Error
85: No call suspended.	500 Internal Server Error
86: Call having the requested call identity has been cleared.	500 Internal Server Error
87: user not member of CUG.	403 Forbidden
88: Incompatible destination..	503 Service unavailable
91: Invalid transit network selection.	500 Internal Server Error
95: Invalid message, unspecified	500 Internal Server Error

Protocol error

ISUP Cause Value	SIP Response
96: Mandatory information element is missing.	500: Internal Server Error
97: Message type non-existent or not implemented.	500: Internal Server Error
98: Message not compatible with call state or message type non-existent or not implemented.	500: Internal Server Error
99: Information element non-existent or not implemented.	500: Internal Server Error
100: Invalid information element contents.	500: Internal Server Error
101: Message not compatible with call state.	500: Internal Server Error
102: Recovery on time expiry.	504 Gateway timeout
111: Protocol error, unspecified.	500 Server internal error

Interworking

ISUP Cause Value	SIP Response
127: Interworking, unspecified	500 Server internal error

PRACK

Reliable provisional responses (PRACK) is supported as per RFC 3262.

It is possible to define the type of PRACK support when acting as a:

- user agent client
- user agent server

Session Timer Extension

The session timer extension allows detecting the premature end of a call caused by a network problem or a peer's failure by resending a refresh request periodically.

This refresh request sent by the Mediatrix unit is either a reINVITE or an UPDATE, according to the configuration of the **Session Refresh Request Method** parameter.

A successful response (200 OK) to this refresh request indicates that the peer is still alive and reachable. A timeout to this refresh request may mean that there are problems in the signalling path or that the peer is no longer available. In that case, the call is shut down by using normal SIP means.

SDP in Session Timer reINVITEs or UPDATEs

The reINVITE is sent with the last SDP that was negotiated. Receiving a session timer reINVITE should not modify the connection characteristics. If the reINVITE method is used, it is sent with the last SDP that was negotiated. Reception of a session timer reINVITE should not modify the connection characteristics. If the UPDATE method is used, it is sent without any SDP offer.

Relation Between Minimum and Maximum Values

A user agent that receives a Session-Expires header whose value is smaller than the minimum it is willing to accept replies a “422 Timer too low” to the INVITE and terminates the call. The phone does not ring.

It is up to the caller to decide what to do when it receives a 422 to its INVITE. The Mediatrix unit will automatically retry the INVITE, with a Session-Expires value equal to the minimum value that the user agent server was ready to accept (located in the Min-SE header). This means that the maximum value as set in the Mediatrix unit might not be followed. This has the advantage of establishing the call even if the two endpoints have conflicting values. The Mediatrix unit will also keep retrying as long as it gets 422 answers with different Min-SE values.

Session Refresh

Sending a session timer reINVITE or UPDATE is referred to as refreshing the session.

Normally, the user agent server that receives the INVITE has the last word on who refreshes. The Mediatrix unit always lets the user agent client (caller) perform the refreshes if the caller supports session timers. In the case where the caller does not support session timers, the Mediatrix unit assumes the role of the refresher.

Event Handling

The Mediatrix unit supports receiving event handling Notifications to start a remote reboot or a sync of configuration for specific endpoint(s).

The event handling Notifications "reboot" or "check-sync" is not specified in an Allow-Events header. The Mediatrix unit supports the Notify without subscription.

Note: It is recommended to use these event handling notifications only when the SIP transport is secure (TLS) or when the firewall filters the requests sent to the unit.

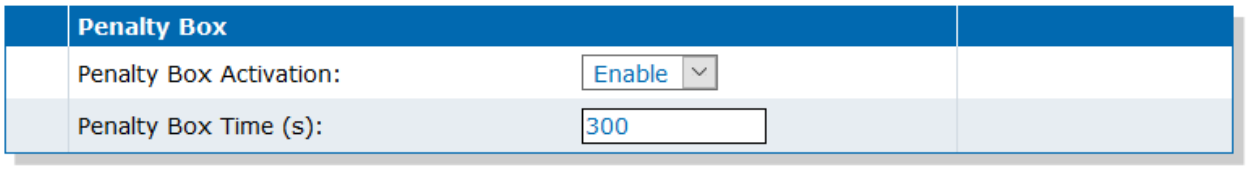
Basic Tasks

Configuring the SIP Penalty Box

Steps

1) Go to **SIP**/**Misc**.
2) In the **Penalty Box** table, from the **Penalty Box Activation**list, choose **Enable**.
3) In the **Penalty Box Times** field, enter the duration during which the SIP target will remain in the SIP penalty box.

Result



Overriding the Default Mapping for SIP Error Code to ISDN Cause

Steps

1) Go to **SIP**/**Misc**.
2) In the **SIP to Cause Error Mapping** table, click .
3) In the **Configure New SIP to Cause Error Mapping** table, from the **Suggestion** list, choose a SIP code and cause.
4) Click **Apply**.

Result

For example:

Overriding the Default Mapping for ISDN Cause to SIP Error Codes

Steps

1) Go to **SIP**/**Misc**.
2) In the **Cause to SIP Error Mapping** table, click ➕.
3) In the **Configure New Cause to SIP Error Mapping** table, from the **Suggestion** list, choose a SIP code and cause.
4) Click **Apply**.

Result

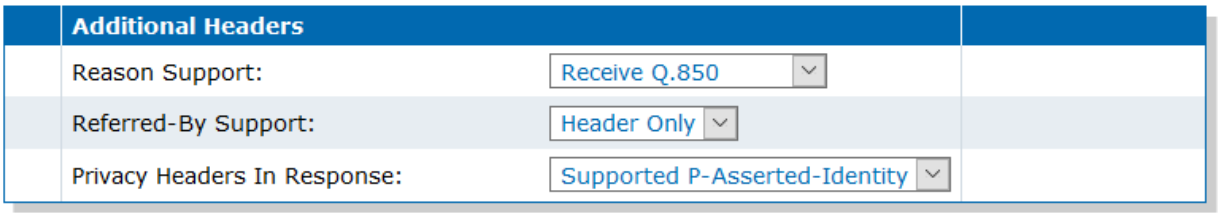
Choosing to Use Additional Headers

Steps

1) Go to **SIP**/**Misc**.
2) In the **Additional Headers** table, set the **Reason Support**, the **Referred-By Support** and the **Privacy Headers In Response** fields as required.
3) Click **Apply**.

Result

The Reason and the Referred-By SIP Headers will be handled as chosen.



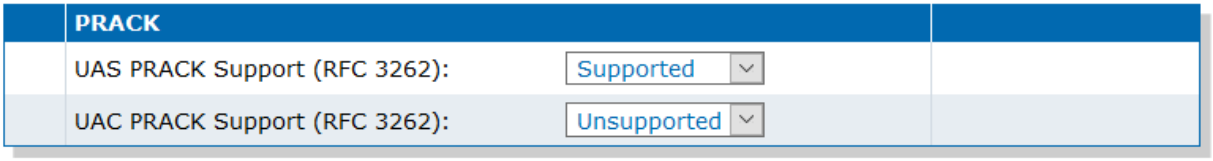
Defining the Type of PRACK Support

Steps

1) Go to **SIP/Misc**.
2) In the **Prack** table, set the **UAC PRACK Support (RFC 3262)** and **UAS PRACK Support (RFC 3262)** fields as required.
3) Click **Apply**.

Result

When acting as a user agent server or client, the RFC 3262 (PRACK) will or not be supported.



Setting the Session Refresh Information

Steps

1) Go to **SIP/Misc**.
2) In the **Session Refresh**, table, set the **Session Refresh Timer Enable** selection list to **Enable**.

   Note: Disabling this parameter is not recommended since it will make 'dead' calls impossible to detect.

3) Set the **Minimum Expiration Delays** field.

   Note: The value of the **Minimum Expiration Delays** must be equal or smaller than the **Maximum Expiration Delays** value.

4) Set the **Maximum Expiration Delays** field.

   Note: The value of the **Maximum Expiration Delays** must be equal or higher than the **Minimum Expiration Delays** value.

   Note: When the **Maximum Expiration Delays** value is lower than the **Minimum Expiration Delays** value, the minimum and maximum expiration delay values in INVITE packets are the same as the value set in the Minimum Expiration Delay field.

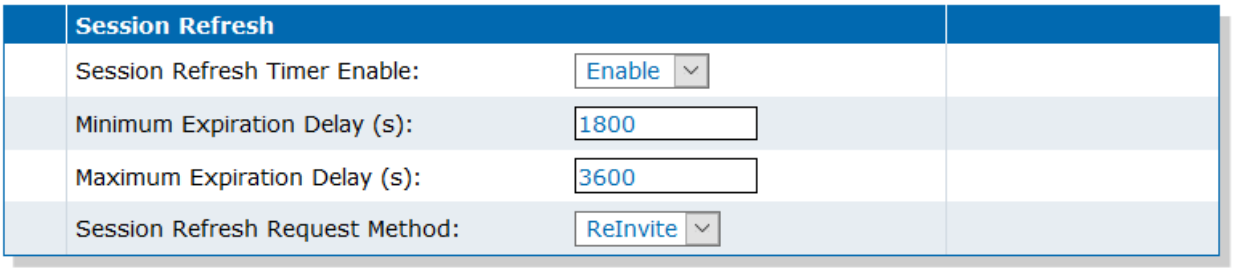
5) Set the **Session Refresh Request Method** field.

   Note: Session Refresh Requests can be received via both methods, regardless of how this parameter is configured.

6) Click **Apply**.

Result

For example :



Overriding the SIP Domain Used

Steps

1) Go to **SIP**/**Misc**.
2) In the **Gateway Configuration** table, in the **SIP Domain Override** field, enter the SIP domain name that should be used instead of the home domain proxy.
3) Click **Apply**.

Result

The specified SIP domain name will be used instead of the home domain proxy (**Proxy Host** field under **SIP**/ **Servers**) in the address of record and the request-URI. When it overrides the home domain proxy in the request-URI, the request-URI also contains a maddr parameter with the resolved home domain proxy to make sure the requests are routable.

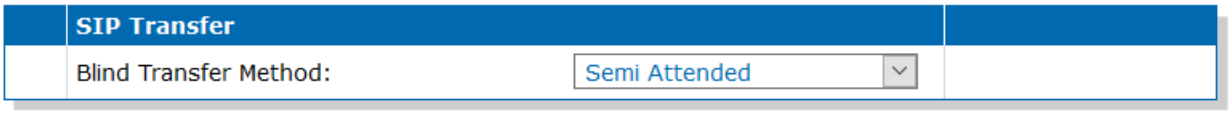
Setting the Blind Transfer Method

Steps

1) Go to **SIP**/**Misc**.
2) In the **SIP Transfer** table, from the **Blind Transfer Method** choose the required method.
3) Click **Apply**.

Result

The blind transfer will be achieved as set when participating in a transfer as the transferor. For example:



Configuring Call Diversion

Information

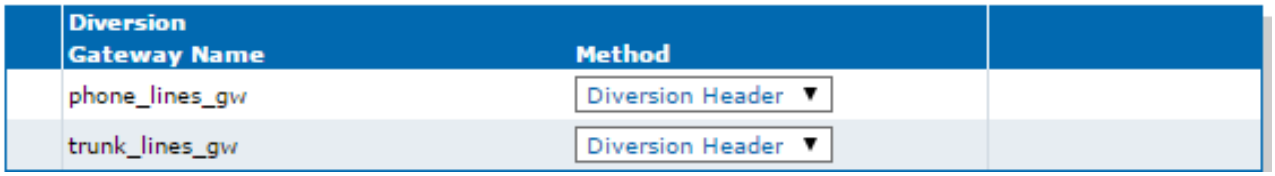
The Diversion feature is not available in the NI2 and QSIG signalling protocols. For more details on ISDN PRI interfaces, refer to the DGW Configuration Guide - ISDN user guide published on the Media5 Documentation Portal.

Steps

1) Go to **SIP**/**Misc**.
2) In the **Diversion** table, from the selection list, choose the required **Method**.
3) Click **Apply**.

Result

The Gateway will use the SIP method selected to receive/send call diversion information in an INVITE. For example:



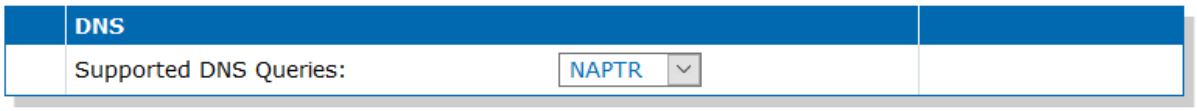
Configuring Supported DNS Queries

Steps

1) Go to **SIP**/**Misc**.
2) In the **DNS** table, from the **Supported DNS Queries** selection , select the type of DNS queries that the SipEp service supports.
3) Click **Apply**.

Result

The SipEp service will support and use the selected DNS queries. For example:



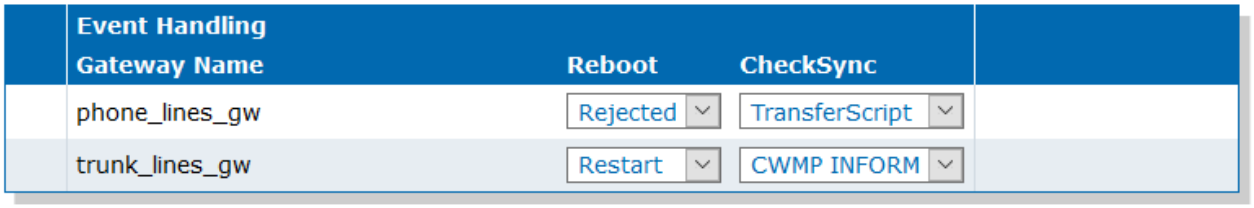
Configuring Event Handling

Steps

1) Go to **SIP**/**Misc**.
2) In the **Event Handling** table, for each gateway, from the **Reboot** selection list, choose how the gateway handles the reboot SIP NOTIFY messages.
3) From the **Check Sync** selection list, choose how the gateway handles check-sync SIP NOTIFY messages.
4) Click **Apply**.

Result

The SIP Gateway will handle reboot SIP NOTIFY messages and the check-sync SIP NOTIFY messages as configured.



Enabling Messaging Subscription

Steps

1) Go to **SIP**/**Misc**.
2) In the **Messaging Subscription** table, from the selection list, choose **Enable**.
3) Click **Apply**.

Result

The unit will add the username in the request URI of MWI SUBSCRIBE requests.

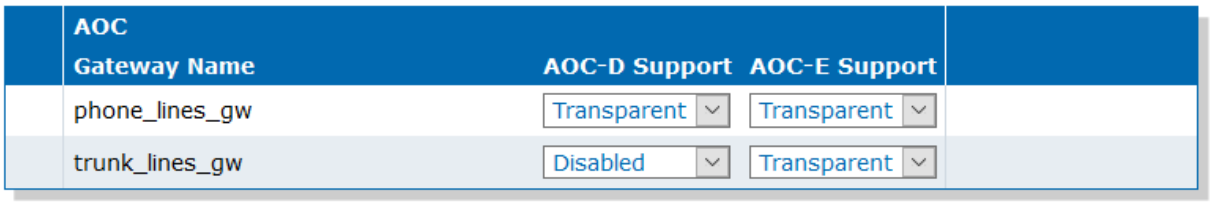
Configuring Advice of Charge (AOC)

Steps

1) Go to **SIP**/**Misc**.
2) In the **AOC** table, for each gateway, choose from the **AOC-D Support** and **AOCE Support** fields how the AOC-D and AOC-E messages are sent.
3) Click **Apply**.

Result

The current charge will be sent either (D)uring the call in AOC-D messages or at the (E)nd of the call in AOC-E messages.



AOC Gateway Name	AOC-D Support	AOC-E Support
phone_lines_gw	Transparent	Transparent
trunk_lines_gw	Disabled	Transparent

Enabling the Media Security Agreement Parameter

Steps

1) Go to **SIP**/**Misc**.
2) In the **Security Mechanism Agreement** table, from the **Media Security Agreement** selection list, choose **Enable**.
3) Click **Apply**.

Result

Once enabled, security headers are added to the SIP signalling to agree upon the security mechanism to be used for the media, i.e. SRTP with SDES.

Security Mechanism Agreement	
Media Security Agreement:	Enable

Advanced Misc SIP Parameters

Although most of the DGW parameters can be configured in the Web browser, some aspects of the configuration can only be completed with the configuration parameters by:

- using a MIB browser
- using the CLI
- creating a configuration script containing the configuration parameters

For more details on the following parameters, refer to the DGW Configuration Guide - Reference Guide published on the Media5 Documentation Portal.

- To set the forked provisional responses behaviour:: **SipEp.interopForkedProvisionalResponsesBehavior**
- To set the DNS failure concealment parameter: **Sip.DnsFailureConcealment**

  Note: This parameter applies only to Endpoint Gateway types; it has no effect on Trunk Gateways. The behavior on Trunk Gateways always matches the "none" value.

Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will bedisplayed.

DGW Documentation

Mediatrix devices are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the Media5 Documentation Portal.

Several types of documents were created to clearly present the information you are looking for. Our documentation includes:

- **Release notes**: Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes**: These documents are created to facilitate the configuration of a specific use case. They address a configuration aspect we consider that most users will need to perform. However, in some cases, a configuration note is created after receiving a question from a customer. They provide standard step-by-step procedures detailing the values of the parameters to use. They provide a means of validation and present some conceptual information. The configuration notes are specifically created to guide the user through an aspect of the configuration.
- **Technical bulletins**: These documents are created to facilitate the configuration of a specific technical action, such as performing a firmware upgrade.
- **Hardware installation guide**: They provide the detailed procedure on how to safely and adequately install the unit. It provides information on card installation, cable connections, and how to access for the first time the Management interface.
- **User guide**: The user guide explains how to customise to your needs the configuration of the unit. Although this document is task oriented, it provides conceptual information to help the user understand the purpose and impact of each task. The User Guide will provide information such as where and how TR-069 can be configured in the Management Interface, how to set firewalls, or how to use the CLI to configure parameters that are not available in the Management Interface.
- **Reference guide**: This exhaustive document has been created for advanced users. It includes a description of all the parameters used by all the services of the Mediatrix units. You will find, for example, scripts to configure a specific parameter, notification messages sent by a service, or an action description used to create Rulesets. This document includes reference information such as a dictionary, and it does not include any step-by-step procedures.

Copyright Notice

media5 corporation

media5corp.com