



## Sbc Service User Guide

Dgw v2.0

May 1, 2015

# Table of Contents

- Copyright Notice..... 4**
  
- Mediatrix Sentinel.....5**
  - Dual Trunk Survivability..... 5
  - PSTN Survivability..... 6
  - Remote Users - Mediatrix Unit Located in the LAN or on the Edge.....7
  
- Configuration notes..... 9**
  - Sbc Service Configuration Notes.....9
  
- Call Agents..... 10**
  - phone\_lines\_ca** Call Agent..... 13
  - trunk\_lines\_ca** Call Agent..... 14
  - local\_users\_ca** Call Agent..... 15
  - remote\_users\_ca** Call Agent..... 15
  - lan\_ip\_pbx\_ca** Call Agent..... 16
  - wan\_ip\_trunk\_ca** Call Agent..... 16
  - secondary\_ip\_trunk\_ca** Call Agent..... 17
  - registration\_ca** Call Agent..... 17
  - Configuring a Call Agent..... 18
  
- Signaling and Media Interfaces..... 19**
  - Creating a Media Interface..... 19
  - Creating a Signaling Interface..... 20
  
- Rulesets.....21**
  - Creating a New Ruleset..... 21
  - Cloning a Ruleset..... 22
  - Modifying a Ruleset..... 23

---

Adding Rules to a Ruleset.....	23
Changing the Name and Description of a Ruleset.....	24
Deleting a Ruleset.....	24
Changing the Execution Priority Level of a Call Agent Ruleset.....	25
Changing the Execution Priority Level of a Routing Ruleset.....	25
Changing the Execution Priority Level of a Ruleset Rule.....	26
Changing the Execution Priority Level of a Rule Action.....	26
Changing the Execution Priority Level of a Rule Condition.....	27
Importing Rulesets.....	27
Call Agent Rulesets.....	28
Associating Call Agent Rulesets to a Call Agent.....	28
Routing Rulesets.....	29
Associating Routing Rulesets to Your Configuration.....	29
<b>Monitoring.....</b>	<b>31</b>
Penalty Box.....	31
Configuring the Call Agent Penalty Box.....	31
Keep-Alive.....	31
Setting the Keep-Alive Interval.....	32
Registration Agent.....	32
Configuring a Registration Agent.....	32
<b>Parameters.....</b>	<b>34</b>
SBC > Status Parameters.....	34
SBC > Configuration Parameters.....	34
<b>Glossary.....</b>	<b>35</b>
<b>Acronyms.....</b>	<b>50</b>

## Copyright Notice

Copyright © 2015 Media5 Corporation.

This document contains information that is confidential and proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.

## Mediatrix Sentinel

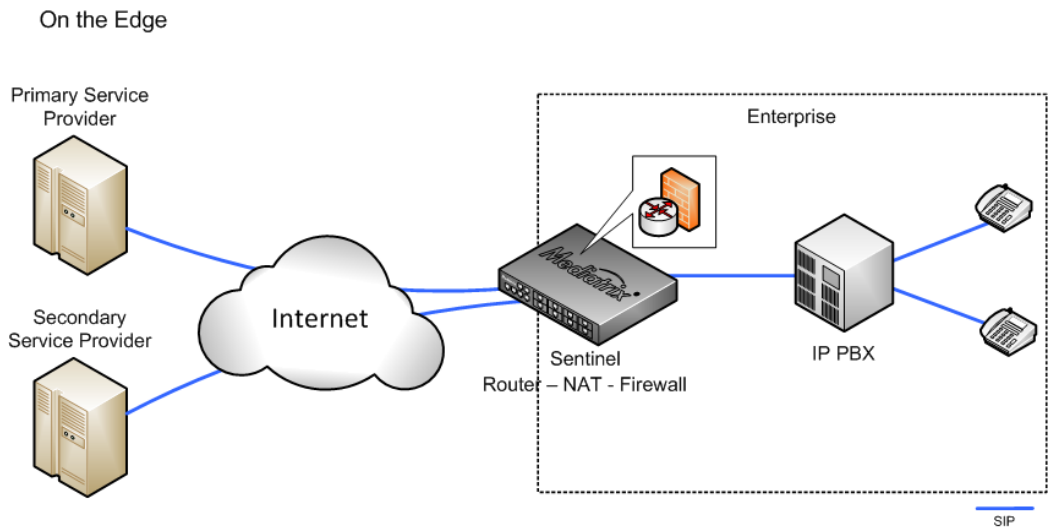
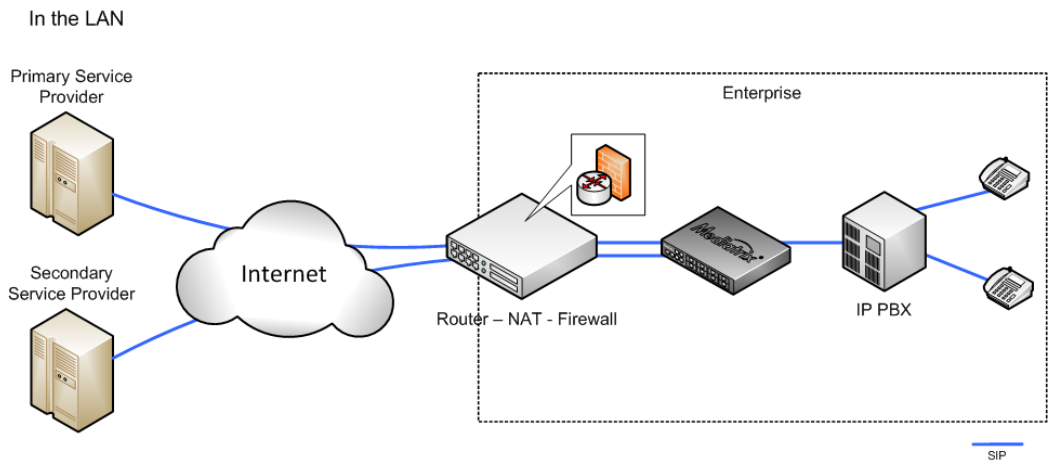
Sentinel bundles the capabilities of a Session Border Controller and a Media Gateway. Robust and field - upgradable, this multi-service business platform is designed for medium and large enterprises. Sentinel is ideally targeted for applications ranging from 30 to 600 simultaneous sessions. Sentinel delivers a flexible architecture designed to address a variety of applications including security, demarcation point, SIP normalisation and survivability.

Module	Interfaces
Base Unit	<ul style="list-style-type: none"> <li>• 1 WAN + 4 LAN Gigabit Ethernet</li> <li>• 8 slots for telephony cards</li> <li>• 3 SBC session licenses</li> </ul>
Telephony Cards (optional)	<ul style="list-style-type: none"> <li>• PRI Port card (004-00096-00)</li> <li>• 4 x FXS Ports card (004-00085-00)</li> <li>• 4 x FXO Ports card (004-00087-00)</li> <li>• DSP card (needed when using FXS, FXO or BRI)</li> <li>• 2 x BRI card (available soon)</li> </ul>
SBC Licenses	<ul style="list-style-type: none"> <li>• Individual sessions</li> <li>• 10 session package</li> <li>• 100 session package</li> <li>• Transcoding (available soon)</li> <li>• Voice Recording (available soon)</li> <li>• WebRTC gateway (available soon)</li> </ul>

## Dual Trunk Survivability

When Dual Trunk survivability is configured it implies that:

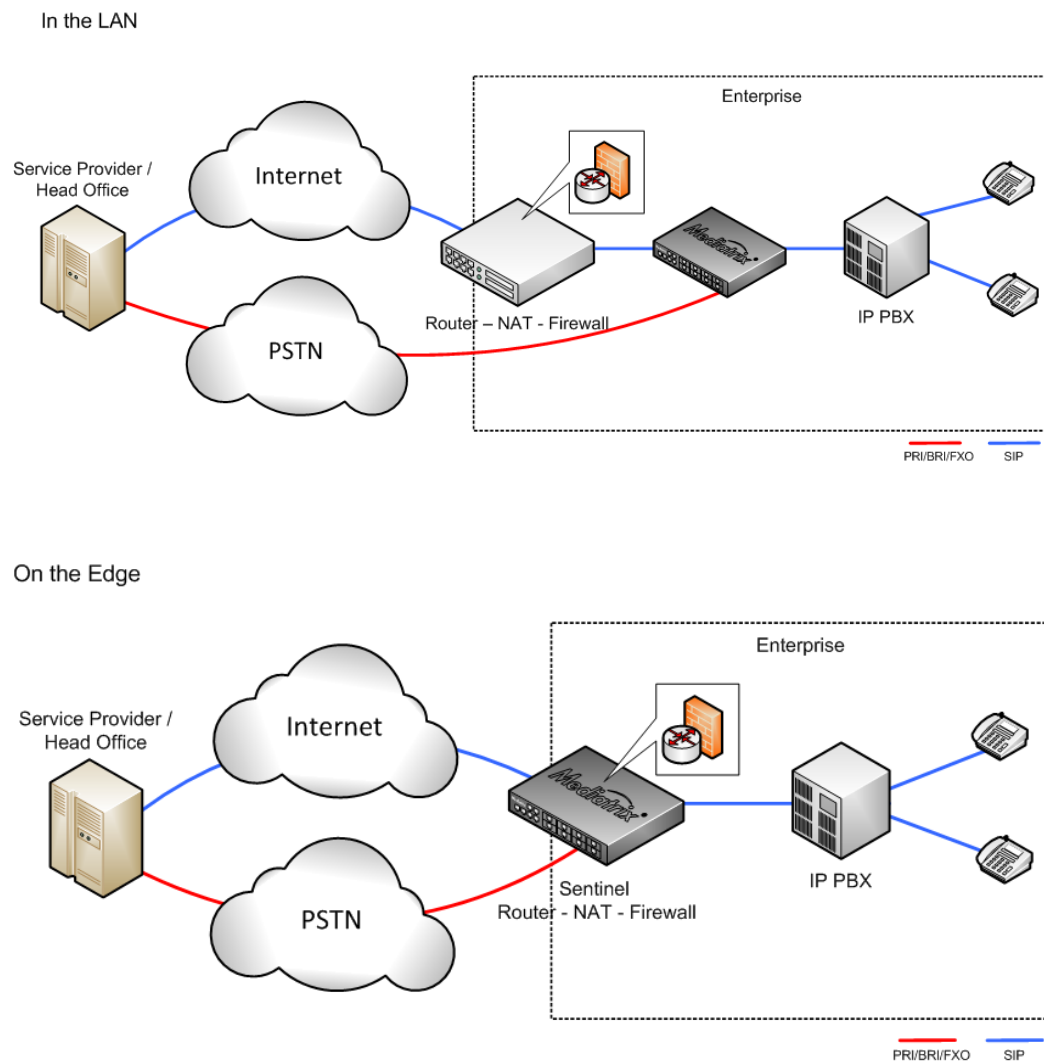
- The Mediatrix unit is setup as a Demarcation point
- When the primary SIP trunk fails, calls go through the secondary SIP trunk.
- The Mediatrix unit may or may not register to the SIP trunk.
- In fallback situations, when the primary trunk comes back online, the Mediatrix unit must wait for a REGISTER to go through before sending the calls to the primary trunk.
- The Mediatrix unit is located on the edge of the Internet with one interface in the LAN and one on the Internet or in the LAN, behind a Near-End NAT.



## PSTN Survivability

When PSTN survivability is configured it implies that:

- The Mediatrix unit is setup as a demarcation point.
- When SIP trunk fails, calls go through the unit's PRI or FXO port.
- The Mediatrix unit may or may not register to the SIP trunk.
- The PBX may or may not register to the Mediatrix unit.
- The Mediatrix unit is located on the edge of the Internet with one interface in the LAN and one on the Internet or in the LAN, behind a Near-End NAT.

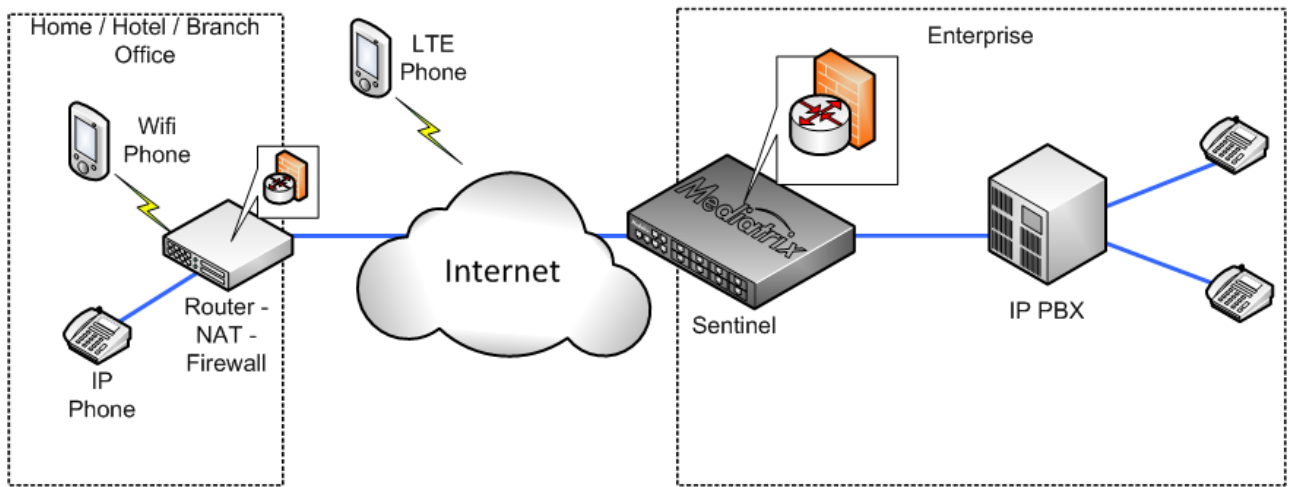


## Remote Users - Mediatrix Unit Located in the LAN or on the Edge

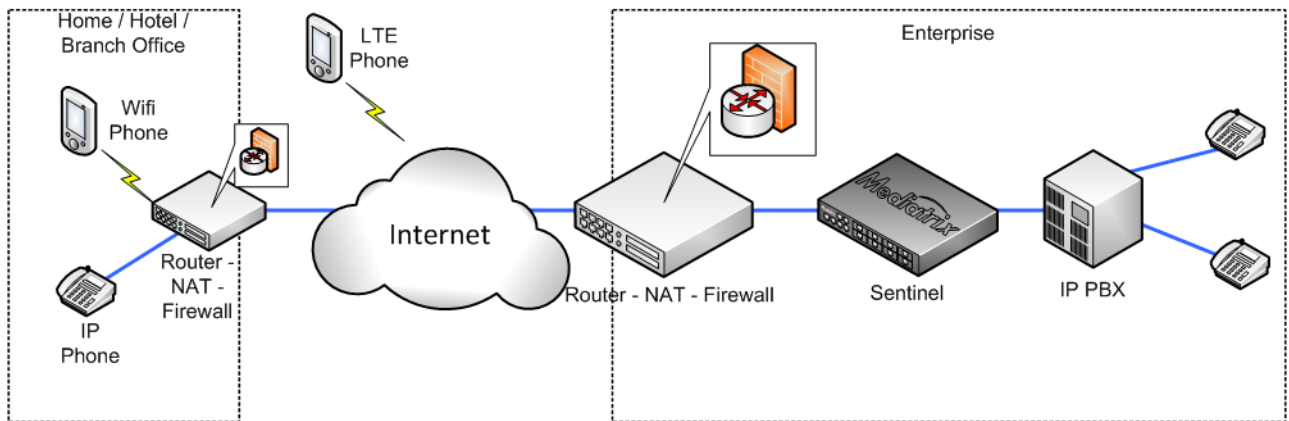
When the Mediatrix unit is located in the LAN or on the Edge, it implies that:

- The remote users are using SIP endpoints on the public Internet or behind a NAT on the public Internet.
- The SIP endpoints register on a PBX located in the LAN of the office, using the Mediatrix unit as an outbound proxy.
- The Mediatrix unit generates enough traffic from the SIP endpoints to maintain the firewall open.
- The Mediatrix unit protects the local PBX from Internet threats.
- The Mediatrix unit is in the LAN, behind the enterprise NAT or The Mediatrix unit is located on the Edge of the internet with one interface in the LAN and one on the Internet.

On the Edge



In the LAN





## 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.

### Sbc Service Configuration Notes

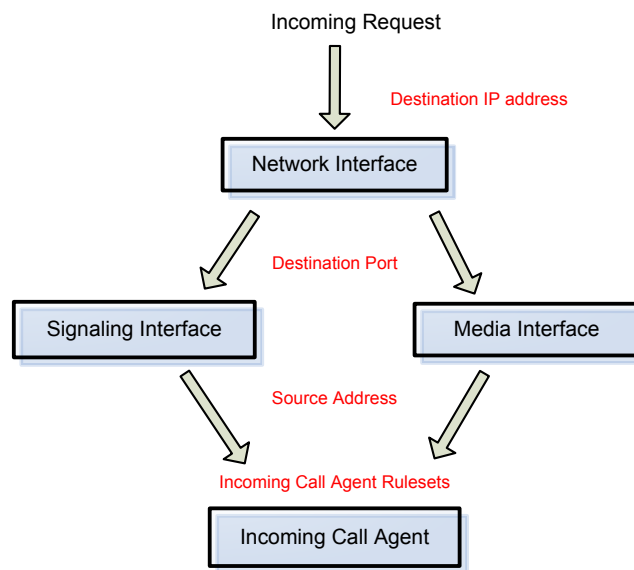
- Dual Trunk Survivability - Sentinel in the LAN with Static PBX IP Address
- Dual Trunk Survivability - Sentinel in the LAN with PBX Registering to SBC
- Dual Trunk Survivability - Sentinel on the Edge with PBX Registering to SBC
- Dual Trunk Survivability - Sentinel on the Edge with Static PBX IP Address
- PSTN Survivability - Sentinel in the LAN with PBX Registering to SBC
- PSTN Survivability - Sentinel in the LAN with Static PBX IP Address
- PSTN Survivability - Sentinel on the Edge with PBX Registering to SBC
- PSTN Survivability - Sentinel on the Edge with Static PBX IP Address
- Remote User - Sentinel in the LAN
- Remote User - Sentinel on the Edge

## Call Agents

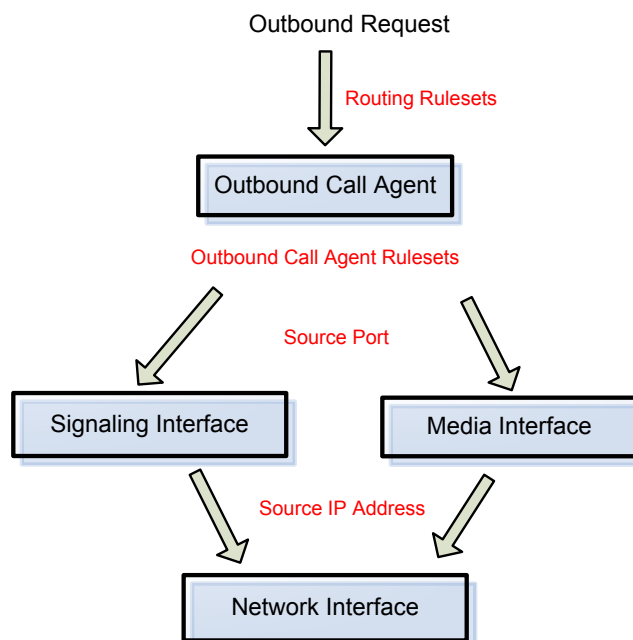
Call Agents represent logical end-points that connect the Mediatrix unit to peers.

For security reasons, the Mediatrix unit communicates by default only with well-known and defined peers. When a request cannot be associated with a Call Agent, it is rejected. The same Call Agent can be used for inbound and outbound requests. However, in most cases, the inbound request will go through one Call Agent and the outbound request will use another Call Agent. Call Agents are then identified as the inbound Call Agent and the outbound Call Agent, indicating if the Call Agent is managing an inbound or an outbound request.

Call Agents can be associated with one or several Rulesets which can be applied to the inbound or the outbound requests. A Call Agent can be assigned to Signaling and Media Interfaces which are associated with Network Interfaces. To determine the Call Agent an incoming request will go through, the Mediatrix unit uses the destination IP address to choose the Network interface. Then the destination port of the inbound request will determine the Signaling Interface used. Finally, the source address and the source port, will allow the Mediatrix unit to direct the request to the appropriate Call Agent. At this point any Rulesets associated with the Call Agent will be applied in order of priority.



When a request is sent out, the Routing Rulesets will determine which Call Agent will be used. Then the Call Agent Rulesets will be applied to the outbound request, in reverse priority order. The request will then be sent to the Signaling Interface associated with the Call Agent. The outbound request will be sent to the Network Interface associated with the Signaling Interface. If the public IP address is used, then the SIP request will use this address as the source IP address. The outbound request will then be sent to the peer address of the Call Agent or according to the routing Ruleset if the peer is a Network.



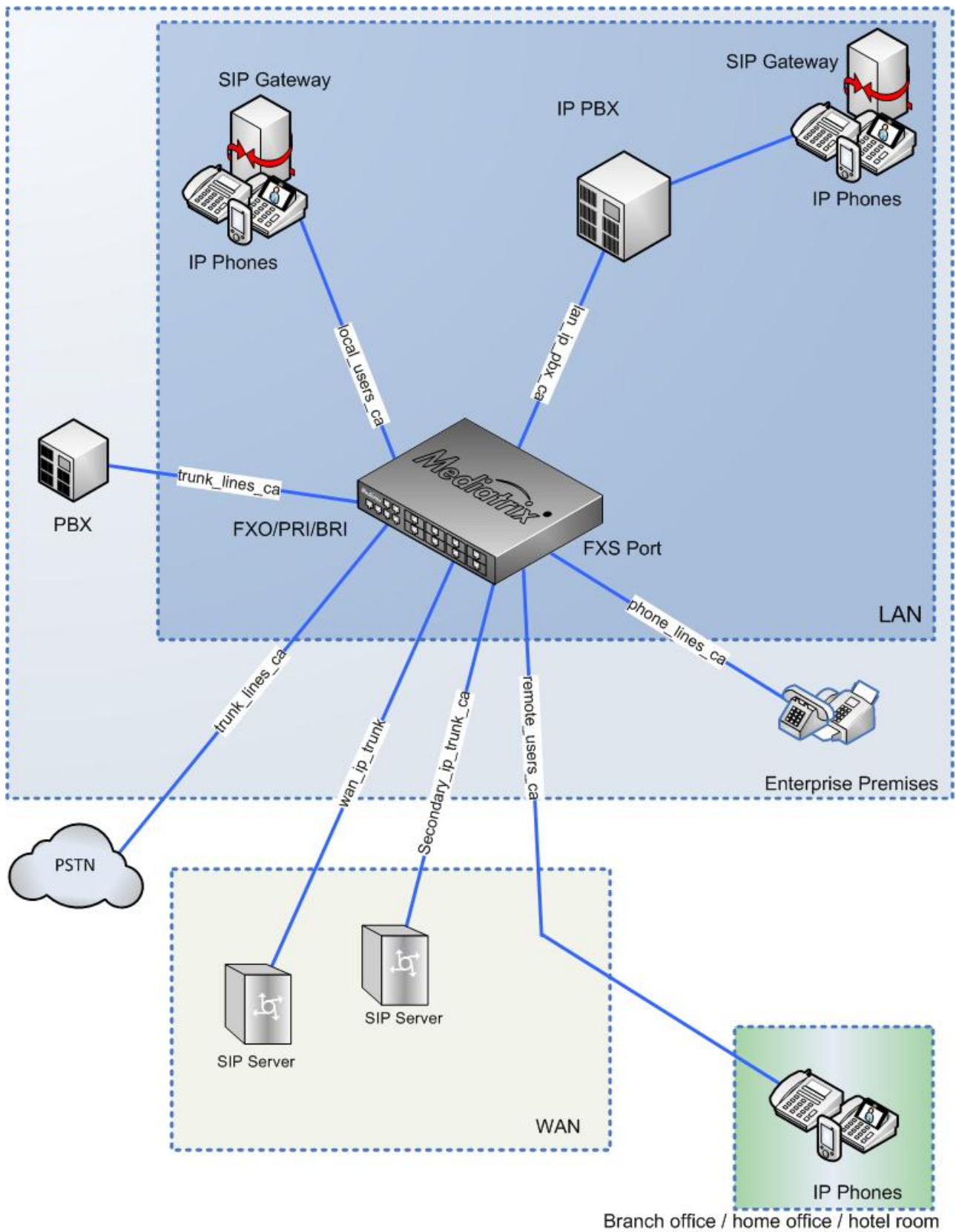
In addition, a Call Agent can initiate REGISTER requests or monitor the peer host using SIP options. When these features are activated, the Call Agent registration state and monitoring state are updated allowing a Routing Ruleset to select another Call Agent based on the state of a primary Call Agent.

Eight default types of Call Agents were created for Mediatrix unit. This should be enough to cover all your needs. However, for advanced users, it is possible to create new Call Agents.

Seven default Call Agents allow the Mediatrix unit to communicate with eight different types of end-points.

Call Agent Name	Endpoint Type
<b>wan_ip_trunk_ca</b>	SIP server located on the WAN.
<b>trunk_lines_ca</b>	Public Switch Telephony Network (PSTN), through PRI, BRI or FXO ports.
<b>phone_lines_ca</b>	Telephones, through FXS ports.
<b>lan_ip_pbx_ca</b>	IP Private branch exchange (PBX) located on the LAN.
<b>local_users_ca</b>	Users via SIP telephony located on the LAN.
<b>remote_users_ca</b>	Users using SIP telephony located on the WAN.
<b>registration_ca</b>	Used to manage all SBC registrations.
<b>secondary_ip_trunk_ca</b>	SIP server if the <b>wan_ip_trunk_ca</b> Call Agent is not available.

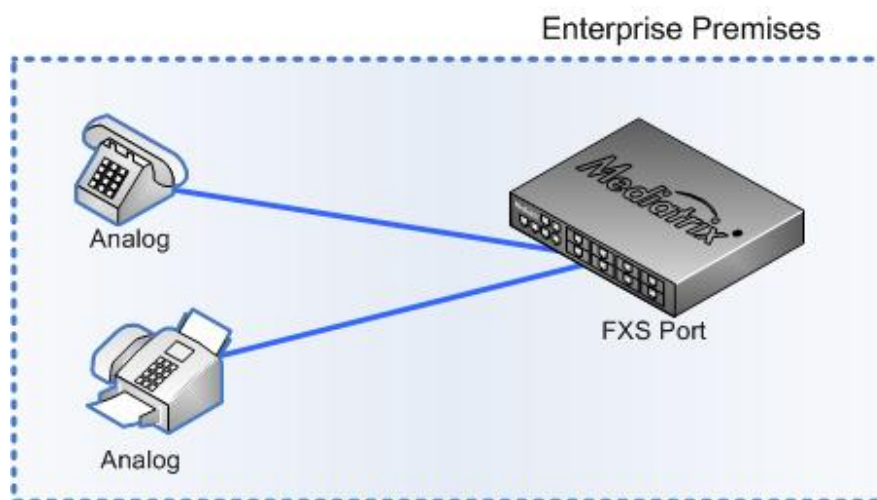
For more details on Rulesets, refer to [Rulesets \(p. 21\)](#).



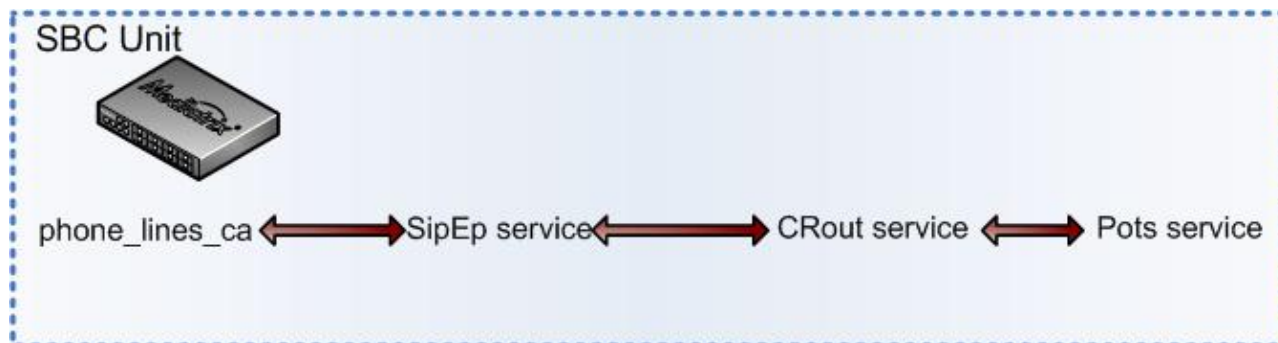
## phone\_lines\_ca Call Agent

The **phone\_lines\_ca** Call Agent is used to route calls via an FXS port of the Mediatrix unit.

Typically it will route calls to and from analog phones and faxes within the enterprise premises. This Call Agent will be used for example when a call is routed from one colleague to another using analog phones connected on the FXS ports of the Mediatrix unit. In such a scenario, the call does not go through the LAN network nor the Internet. Since by default this Call Agent uses the loop network to route the media, the **media\_relay** Ruleset is usually associated with this Call Agent.



The **phone\_lines\_ca** Call Agent is associated with the **phone\_lines\_gw** gateway of the SipEp service. By default, each FXS port sends a REGISTER by the **phone\_lines\_ca** Call Agent. Therefore, the administrator must make sure to route these REGISTERS to a server, or to disable them in the SipEp service. If needed, FXS ports can be configured in the Pots service.

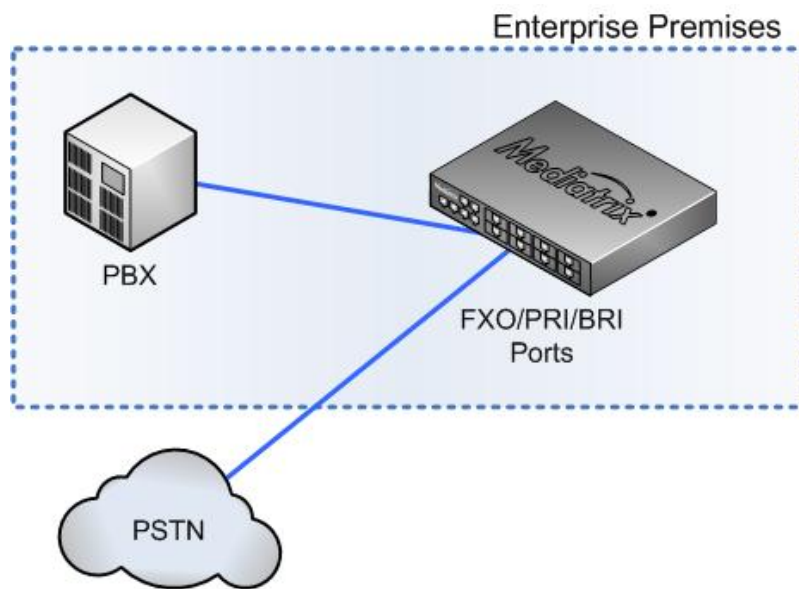


## trunk\_lines\_ca Call Agent

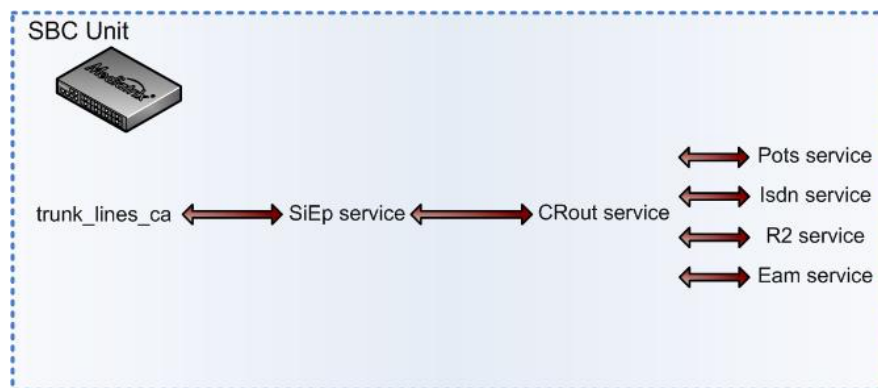
The **trunk\_lines\_ca** Call Agent is used to route calls to the Public Switch Telephony Network (PSTN) or a enterprise's existent PBX through the PRI, BRI or FXO ports of the unit.

Calls made outside the enterprise premises to telecommunication service providers or calls made within the enterprise through a PBX will typically be routed through this Call Agent. Since by default this Call Agent uses the loop network to route the media, the **media\_relay** Ruleset is usually associated with this Call Agent.

If there are no PRI, BRI or FXO card on the unit, calls through trunk lines can also be routed by the **wan\_ip\_trunk\_ca** or **secondary\_ip\_trunk\_ca** Call Agent, provided there is an analog or digital gateway to convert the VoIP call to an analog or digital call, or vice versa.



Further more, the **trunk\_lines\_ca** Call Agent is associated with the **trunk\_lines\_gw** of the SipEp service. FXO/PRI/BRI ports will need to be configured in either the Pots, Isdn, R2 or Eam services for the calls to be routed properly.

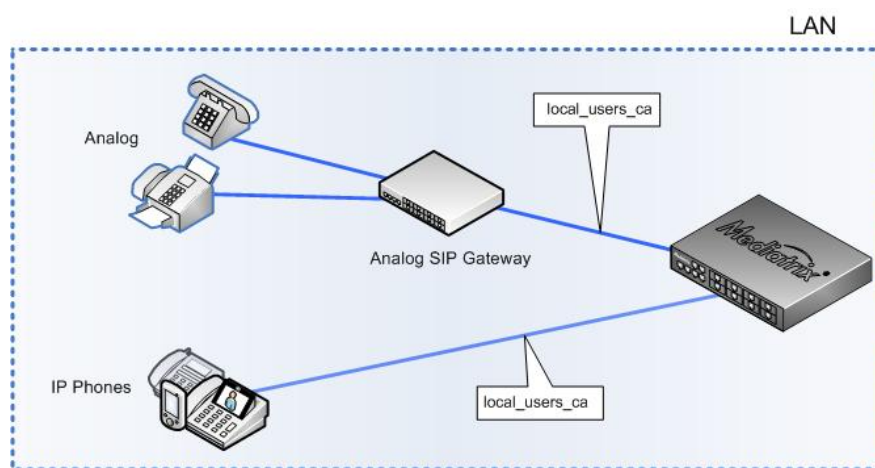




## local\_users\_ca Call Agent

The **local\_users\_ca** Call Agent is used to route calls from and to local users, i.e. located in the LAN, via VoIP calls.

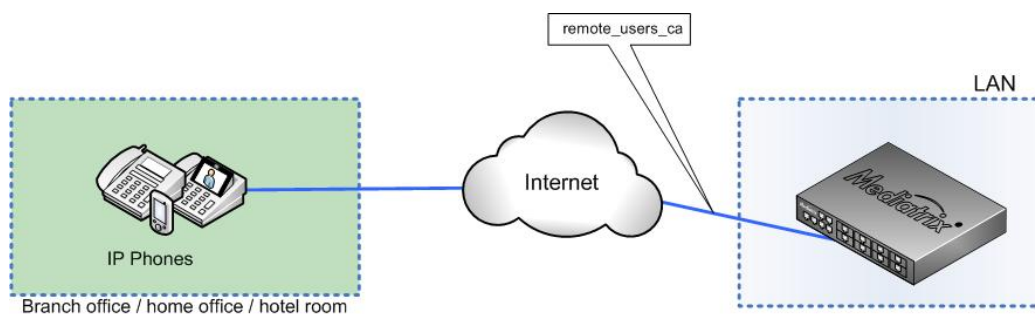
For the call to use this Call Agent, the endpoint must belong to the company and use the company's system. This Call Agent is often used as a regrouping point of all local endpoints to be routed to a PBX or Trunk lines. For instance, if you are a Media5 corporation employee, with a cell phone using the Media5 fone application and the enterprise IP-PBX, then your call will be routed through the **local\_users\_ca** Call Agent. If an internal employee is using an analog phone, the call can also be routed through this Call Agent provided the call goes first through a gateway to convert the analog call into a VoIP call.



## remote\_users\_ca Call Agent

The **remote\_users\_ca** Call Agent is used to route calls from users working out the office and using VoIP calls through an external network or Internet.

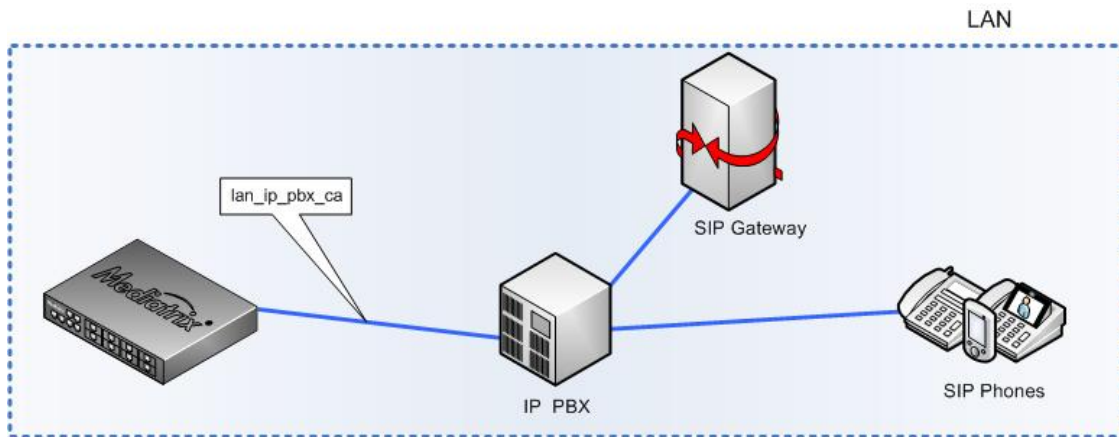
Calls are routed through a WAN then to the Mediatix unit via the **remote\_users\_ca** Call Agent.



## lan\_ip\_pbx\_ca Call Agent

The **lan\_ip\_pbx\_ca** Call Agent routes calls to and from an IP PBX located in the LAN. The IP PBX manages all internal communications between different SIP clients (soft phones or SIP gateways).

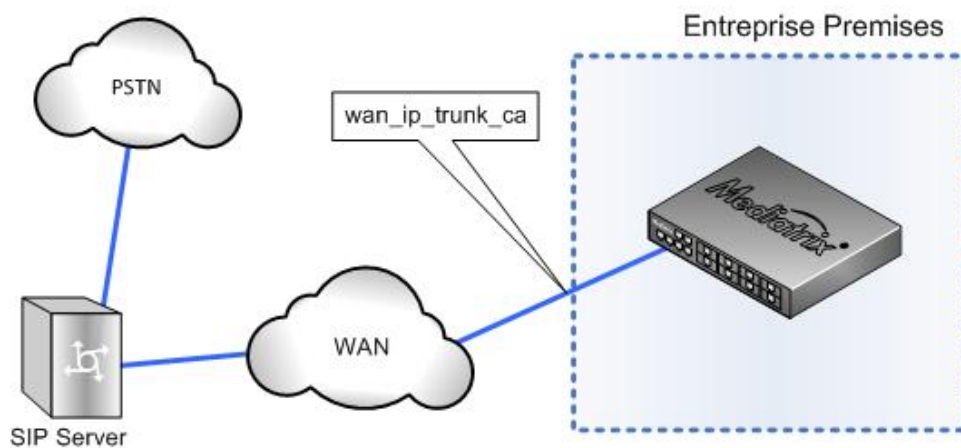
This Call Agent is usually used to link a local PBX with an external trunk (IP or PSTN).



## wan\_ip\_trunk\_ca Call Agent

The **wan\_ip\_trunk\_ca** Call Agent is used to route VoIP calls.

Calls are routed from or to the main SIP server or provider located in the WAN. Typical peers for this Call Agent are the head office of the enterprise, an Internet telephony service provider (ITSP) or an IP Multimedia Core Network Subsystem (IMS).

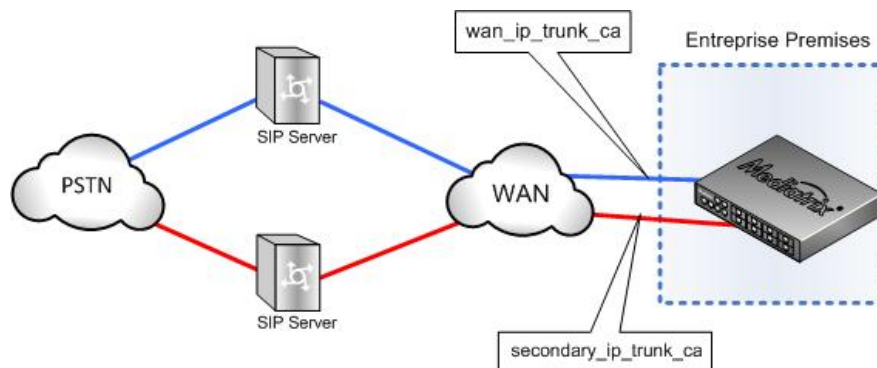




## secondary\_ip\_trunk\_ca Call Agent

The **secondary\_ip\_trunk\_ca** Call Agent is used to route VoIP calls.

This Call Agent is identical to the **wan\_ip\_trunk\_ca** Call Agent. The **secondary\_ip\_trunk\_ca** can be used for different purposes. The most common use for this Call Agent, is to route calls to and from the backup server in the event the primary server does not respond. However, this Call Agent can also be used, for example, to route calls directly to and from a Branch Office or route a specific type of call such as international calls. Typical peers for this Call Agent are the head office of the enterprise, an Internet telephony service provider (ITSP) or an IP Multimedia Core Network Subsystem (IMS).

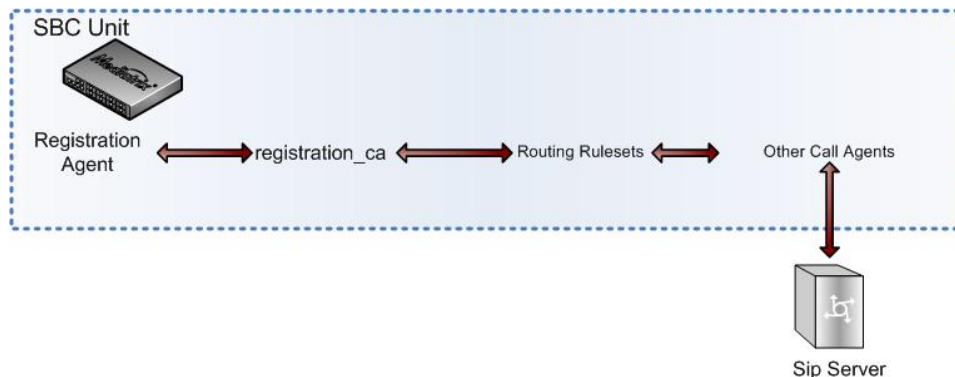


## registration\_ca Call Agent

The **registration\_ca** Call Agent is used to route the registrations issued by the Registration Agent.

The **registration\_ca** Call Agent should not be used for other purposes. The registrations issued by the Registration Agent must be routed from the **registration\_ca** to the Call Agent facing the destination Sip registrar (typically **wan\_ip\_trunk\_ca\_ca** or **secondary\_ip\_trunk\_ca**).

The registration is routed using the User Name, Password and Domain to build the AOR and the R-URI . The Contact is the contact header of the registration, it should contain the IP-address or FQDN of the Mediatrax unit.





## Configuring a Call Agent

### Information

If you are not familiar with the meaning of the fields, click **Show Help**, located at the upper right corner of the Web page, to display field description when mousing over the field name.

### Steps

- 1) Go to **SBC > Configuration**.
- 2) In the **Call Agent Configuration** table, click **Edit** located on the row of the Call Agent you wish to configure.
- 3) In the **Configure Call Agent** table, complete the fields as required and make sure the **Enable** check box is selected.
  -  **Monitoring Parameters** are not mandatory.
- 4) Complete the fields of the **Call Agent Configuration** as required.
- 5) Click **Save**.
  -  The changes are saved, but not all applied to the configuration.
- 6) Click **Apply** to apply all changes to the configuration.

### Result

**No** will be displayed in the **Config. Modified** field, indicating that the configuration that was modified is now applied to the system. When the Mediatrix unit will use the selected Call Agent for a communication, the selected parameters will be applied.

### What to do next

[Associating a Ruleset to a Call Agent](#)

## Signaling and Media Interfaces

The Signaling Interface is used for SIP signaling and the Media Interface is used for media ( RTP, UDPTL ) processing.

When configuring a Call Agent, you must select a Signaling Interface and a Media Interface. These interfaces are used whenever SIP signaling or media packets are sent to or received by the Call Agent.

It is possible to create several Signaling and Media Interfaces on the same Network Interface but for different purposes. For example, one set of Signaling and Media Interfaces for a WAN SIP Trunk and another set of Signaling and Media Interfaces for remote user calls. This means, for instance, that two Signaling Interfaces will be created on the same Network Interface, using the same IP address, but with a port range that will differ according to their intended use and to avoid conflicts.

A Media or Signaling Interface can be used by more than one Call Agent, but a specific Signaling or Media Interface can be created for a specific Call Agent. This provides the liberty to define non conflicting range of contactable interfaces on any physical network interfaces of the units for your network structure needs (such as Vlans, PPPoE interfaces, multiple Ethernet ports or multiple addresses on a link).

The following Signaling and Media Interfaces are supplied by default:

- **lan1\_m**
- **lan1\_s**
- **Loop\_m**
- **Loop\_s**
- **uplink\_s**
- **uplink\_m**

**Loop\_m** and **Loop\_s** interfaces are used to communicate with the internal services of the unit. For example, the loop interfaces can be used to communicate with the SipEp service to access phone ports.

## Creating a Media Interface



### Before you start


[Creating a Network Interface](#) must be completed.

### Information

If you are not familiar with the meaning of the fields, click **Show Help**, located at the upper right corner of the Web page, to display field description when mousing over the field name.

### Steps

- 1) Go to **SBC > Configuration**.
- 2) In the **Media Interface Configuration** table, click **+**.
  -  A new line of empty fields is added to the **Media Interface Configuration** table. An error message will be displayed indicating that the configuration of the row is invalid. This is normal as the Media Interface is not yet configured.
- 3) In the **Media Interface Configuration** table, complete the fields as required.
  -  The Network Interfaces displayed in the **Network** column, are created under **Network > Interfaces** tab.

- 4) Click **Save**.  
 The changes are saved, but not all applied to the configuration.
- 5) Click **Apply** to apply all changes to the configuration.
- 6) Click **Restart required services**, located at the top of the page.

**Result**

The Media Interface will be available when configuring a Call Agent, in the **Media Interface** selection list of the **Configure Call Agent** page.

## Creating a Signaling Interface





**Before you start**

[Configuring a Network Interface](#) must be completed.

**Information**

If you are not familiar with the meaning of the fields, click **Show Help**, located at the upper right corner of the Web page, to display field description when mousing over the field name.

**Steps**

- 1) Go to **SBC > Configuration**.
- 2) In the **Signaling Interface Configuration** table, click .  
 A line is added to the **Signaling Interface Configuration** table. An error message will be displayed indicating that the configuration of the row is invalid. This is normal as the Signaling Interface is not yet configured.
- 3) In the **Signaling Interface Configuration** table, complete the fields as required.  
 The Network Interfaces displayed in the **Network** column, are created under **Network > Interfaces** page.
- 4) Click **Save**.  
 The changes are saved, but not all applied to the configuration.
- 5) Click **Apply** to apply all changes to the configuration.
- 6) Click **Restart required services**, located at the top of the page.

**Result**

The Signaling Interface will be available when configuring a Call Agent, in the **Signaling Interface** selection list of the **Configure Call Agent** page.

---

## Rulesets

Rulesets define one or several rules used to filter, manipulate or route inbound or outbound requests.

There are two types of Rulesets:

- **Call Agent Rulesets** : they describe how inbound or outbound requests are handled by a specific Call Agent. They can also implement services or collect data.
- **Routing Rulesets**: they are used to globally route outbound requests, i.e. that they apply to all Call Agents.

When a request arrives at a Call Agent from a peer, the inbound rules of the Rulesets associated with the Call Agent are executed. Then, Routing Rulesets are executed until a Call Agent is selected for the destination. Last, the outbound rules of the Rulesets associated with the destination Call Agent are executed before sending the request to the peer.

Inbound rules of the Ruleset are executed in ascending Ruleset priority order. Outbound rules are executed in descending Ruleset priority order.

The Mediatrix unit is fundamentally rule driven. This means that almost all features can be activated based on certain conditions evaluated at run-time, based on parts of the signaling messages or media payload. All rules are constructed using the same pattern. They consist of a set of one or more conditions. If all conditions apply (logical conjunction), a set of one or more actions is executed. It is important to understand that rules are generally applied only on incoming or outbound requests. However, some rules have a scope that goes beyond these incoming or outbound requests. For example, header filters apply to all requests exchanged, including incoming requests.

Call Agent Rulesets have an \*.crs extension and Routing Rulesets use the \*.rrs extension. For more details on Ruleset conditions and descriptions, refer to the [Reference Guide](#).




## Creating a New Ruleset




### Information

This procedure applies to Call Agent and Routing Rulesets.

 To save time, consider [Cloning a Ruleset](#) (p. 22).

### Steps

- 1) Go to **SBC > Rulesets**.
- 2) In the **Rulesets** page, enter a name in the empty field of either the **Call Agent Rulesets** or **Routing Rulesets** table.
- 3) Click **+**.  
 The name of the Ruleset will be added at the end of the table.
- 4) In the **Rulesets** page, click  located on the row of the Ruleset you have just created.
- 5) In the **Ruleset Edit** page, in either the **Outbound Rules** or **Inbound Rules**, click **Insert new Rule**.
- 6) In the **Conditions** and **Actions** section, complete the fields as required.  
 For more details on Actions and Conditions, refer to the [Reference Guide](#).
- 7) If necessary, click **Add condition** to add another condition.

- 8) If necessary, click **Add** to add another action.
- 9) Click **Save**.
  -  The new rule is saved but the modified configuration is not yet applied to the system.
  -  Rules are executed from top to bottom. Consider [Changing the Execution Priority Level of a Ruleset Rule \(p. 26\)](#).
- 10) Go to **SBC > Configuration**.
- 11) Click **Apply**.
  -  The modified configuration is applied to the system.

### Result








The new Ruleset is available to be associated with a Call Agent.

## Cloning a Ruleset

### Information

This procedure applies to Call Agent and Routing Rulesets

### Steps

- 1) Go to **SBC > Rulesets**.
- 2) In the **Rulesets** page, click  next to the Ruleset you wish to clone.
- 3) Click **OK**.
  -  The cloned Ruleset will be added at the end of the table. The name of the cloned Ruleset will include a numerical suffix to distinguish it from the original Ruleset.
- 4) In the **Rulesets** page, click  located on the row of the Ruleset you have just cloned.
- 5) Click **Edit** next to the rules you wish to modify.
- 6) In the **Conditions** and **Actions** section, modify the fields as required.
  -  For more details on Actions and Conditions, refer to the [Reference Guide](#).
- 7) If necessary, click **Add condition** to add another condition.
- 8) If necessary, click **Add** to add another action.
- 9) Click **Save**.
- 10) Click **Change Name /description** to change the name and the description of the Ruleset.
- 11) Click **Save**.
  -  The new cloned rule is saved but the modified configuration is not yet applied to the system.
  -  Rules are executed from top to bottom. Consider [Changing the Execution Priority Level of a Ruleset Rule \(p. 26\)](#).
- 12) Go to **SBC > Configuration**.
- 13) Click **Apply**.
  -  The modified configuration is now applied to the system.

**Result**






The new Ruleset is available to be associated with a Call Agent.

## Modifying a Ruleset

**Information**

This procedure applies to Call Agent and Routing Rulesets

**Steps**

- 1) Go to **SBC > Rulesets**.
- 2) In the **Rulesets** page, click  located on the row of the Ruleset you wish to modify.
- 3) In the **Ruleset Edit** page, click **Edit** located on the row of the rule you wish to modify.
- 4) In the **Conditions** and **Actions** section, modify the fields as required.
  -  For more details on Actions and Conditions, refer to the [Reference Guide](#).
- 5) If necessary, click **Add condition** to add another condition.
- 6) If necessary, click **Add** to add another action.
- 7) Click **Save**.
  -  The modified rule is saved but the modified configuration is not yet applied to the system.
  -  Rules are executed from top to bottom. Consider [Changing the Execution Priority Level of a Ruleset Rule \(p. 26\)](#).
- 8) Go to **SBC > Configuration**.
- 9) Click **Apply**.
  -  The modified configuration is now applied to the system.

**Result**



The Ruleset will be applied with the new changes.

## Adding Rules to a Ruleset

**Information**

This procedure applies to Call Agent and Routing Rulesets

**Steps**

- 1) Go to **SBC > Rulesets**.
- 2) In the **Rulesets** page, click  located on the row of the Ruleset for which you wish to add a rule.
- 3) In the **Ruleset Edit** page,
  - click **Insert new Rule** to add a rule at the top of the list of rules
  - click **Append new rule** to add a rule at the bottom of the list of rules.
- 4) In the **Conditions** and **Actions** sections, complete the fields as required.
  -  For more details on Actions and Conditions, refer to the [Reference Guide](#).

- 5) If necessary, click **Add condition** to add another condition.
- 6) If necessary, click **Add** to add another action.
- 7) Click **Save**.

 The new rule is added to the Ruleset and saved, but the modified configuration is not yet applied to the system.

- 8) Go to **SBC > Configuration**.
- 9) Click **Apply**.

 The modified configuration is now applied to the system.

#### Result


The rule will be executed the next time the Ruleset is used.

## Changing the Name and Description of a Ruleset

#### Information

This procedure applies to Call Agent and Routing Rulesets.

#### Steps

- 1) Go to **SBC > Rulesets**.
- 2) In the **Rulesets** page, click  located on the row of the Ruleset you wish to modify.
- 3) In the **Ruleset Edit** page, click **Change Name/description** located next to the name of the Ruleset.
- 4) In the **Ruleset Change Name/Description** page, modify the fields as required.
- 5) Click **Save**.

 The new name is saved but the modified configuration is not yet applied to the system.

- 6) Go to **SBC > Configuration**.
- 7) Click **Apply**.

 The modified configuration is now applied to the system.

#### Result


If you change the name of the Ruleset, you will need to re-associate the Ruleset to the Call Agent it is associated with otherwise, the configuration will be considered invalid.

## Deleting a Ruleset

#### Information

This procedure applies to Call Agent and Routing Rulesets.

#### Steps

- 1) Go to **SBC > Rulesets**.
- 2) In the **Rulesets** page, click  next to the Ruleset you wish to delete.
- 3) Click **OK**.
- 4) Go to **SBC > Configuration**.



- 5) Click **Apply**.




The modified configuration is now applied to the system.

**Result**

The Ruleset will no longer be available in the **Rulesets** page to be associated with a Ruleset. If the Ruleset was associated with a Call Agent, it will need to be removed manually from the list of Rulesets associated with the Call Agent otherwise, the configuration will be considered invalid.

## Changing the Execution Priority Level of a Call Agent Ruleset

**Steps**


- 1) Go to **SBC > Configuration**.
- 2) In the **Call Agent Configuration** table, click  next to the Call Agent for which you wish to modify the Ruleset priority level.
- 3) Use the arrows of the **Call Agent Rulesets** table to move a Ruleset up or down.
- 4) Click **Save**.  
The changes will be applied to the configuration, but the modified configuration is not yet applied to the system.
- 5) Click **Apply** to apply the modified configuration to the system.

**Result**

Inbound rules of the Ruleset will be executed in ascending Ruleset priority order but Outbound rules will be executed in descending Ruleset priority order.

## Changing the Execution Priority Level of a Routing Ruleset

**Steps**

- 1) Go to **SBC > Configuration**.
- 2) Use the arrows of the **Routing Rulesets** table to move a Ruleset up or down.
- 3) Click **Save**.  
 The changes will be applied to the configuration, but the modified configuration is not yet applied to the system.
- 4) Click **Apply** to apply the modified configuration to the system.

### Result


Inbound rules of the Ruleset will be executed in ascending Ruleset priority order but Outbound rules will be executed in descending Ruleset priority order.

## Changing the Execution Priority Level of a Ruleset Rule

### Information

This procedure applies to Call Agent and Routing Rulesets.

### Steps

- 1) Go to **SBC > Rulesets**.
- 2) Click  next to the Ruleset for which you wish to change the priority level of rules.
- 3) Use the **Up** and **Down** buttons to move the rules.
- 4) Go to **SBC > Configuration**.
- 5) Click **Apply**.



The changes are saved to the configuration and the modified configuration is now applied to the system.

### Result




Inbound rules of the Ruleset are executed in ascending Ruleset priority order but Outbound rules are executed in descending Ruleset priority order.

## Changing the Execution Priority Level of a Rule Action

### Information

This procedure applies to Call Agent and Routing Rulesets

### Steps

- 1) Go to **SBC > Rulesets**.
- 2) Click  next to the Ruleset for which you wish to change the priority level of rule actions.
- 3) Click **Edit** next to the rule for which you wish to change the actions order.
- 4) Click  or  to move actions.
- 5) Click **Save**.



The new priority level is saved but the modified configuration is not yet applied to the system.

- 6) Go to **SBC > Configuration**.
- 7) Click **Apply**.



The modified configuration is now applied to the system.

**Result**






When the Ruleset is used, the actions of a rule are always executed in the ascending priority order.

## Changing the Execution Priority Level of a Rule Condition

**Information**

This procedure applies to Call Agent and Routing Rulesets

**Steps**

- 1) Go to **SBC > Rulesets**.
- 2) Click  next to the Ruleset for which you wish to change the priority level of rule conditions.
- 3) Click **Edit** next to the rule for which you wish to change the conditions order.
- 4) Click  or  to move conditions.
- 5) Click **Save**.
  -  The new priority level is saved but the modified configuration is not yet applied to the system.
- 6) Go to **SBC > Configuration**.
- 7) Click **Apply**.
  -  The modified configuration is now applied to the system.

**Result**

When the Ruleset is used, the conditions of the rule are always executed in the ascending priority order.

## Importing Rulesets



**Before you start**

Rulesets must be created.

**Information**

This procedure is valid for Call Agent and Routing Rulesets.

**Steps**

- 1) Go to **Management > File**.
  -  Step 2 is only required when importing the first Ruleset and if you are not using a secure connexion to access the Management Interface (http://).
- 2) Click **Activate unsecure file transfer through web browser**.
- 3) From the **Path** field, select sbc/rulesets/.
- 4) Click **Browse**, and navigate to the Ruleset you wish to import.
  -  Ruleset file extension must be \*.crs for Call Agent Rulesets or \*.rrs for Routing Rulesets.
- 5) Click **Import**.

**Result**

The imported Ruleset will appear in the **Internal Files** table, with the selected path in front of the name. The Ruleset will be available in the tables of the **SBC > Rulesets** page.

## Call Agent Rulesets

Name	Description
automatic_media_relay	Media goes through the SBC except for users in the same network.
drop_common_scanners_in	Drop requests from known SIP scanners.
drop_register_in	Drop all inbound registration requests.
drop_unregistered_users_in	Drop inbound requests from unregistered users.
media_relay	Force Media to go through the SBC.
rate_limit_invite_per_source_in	Limit call attempts per second per source IP address.
rate_limit_register_per_source_in	Limit registration attempts per minute per source IP address.
register_cache_out	Create alias in cache for outbound registrations and restore the contact from the cache for inbound requests.
registrar_in	Store contact locally and reply to inbound registration requests.
registration_throttling_in	Use different expiration for UA and registrar.
reject_unregistered_users_in	Reject inbound requests from unregistered users.
remote_users_behind_nat	Handle Far-End NAT for registrations and calls.
topology_hiding_out	Remove user-agent or server header on outbound requests.
uac_authentication_out	Provide authentication credentials for outbound requests.

### Associating Call Agent Rulesets to a Call Agent

**Before you start**

- The Call Agents must be configured.
- [Importing Rulesets \(p. 27\)](#) must be completed.

**Steps**

- 1) Go to **SBC > Configuration**.
- 2) From the **Call Agent Configuration** table, click  located on the same row as the Call Agent to which you wish to associate a Ruleset.
- 3) In the **Call Agent Rulesets** table, click .

- 4) From the **Name** selection list, select a Ruleset.
- 5) To add other Rulesets, click **+**.
- 6) Click **Save**.
- 7) In the **Configure Call Agent** page, click **Save**.
- 8) Click **Apply** to apply all changes to the configuration.

## Routing Rulesets


Name	Description
lan_pbx_to_remote_users	Route from lan_ip_pbx_ca to remote_users_ca
lan_pbx_to_wan_ip_trunk_failover_to_second	Route from lan_ip_pbx_ca to wan_ip_trunk_ca with failover to secondary_ip_trunk_ca
lan_pbx_to_wan_ip_trunk_failover_to_second_dm	Route from lan_ip_pbx_cato wan_ip_trunk_cawith failover to secondary_ip_trunk_ca in demarcation set
lan_pbx_to_wan_ip_trunk_failover_to_trunk_dm	Route from lan_ip_pbx_ca to wan_ip_trunk_ca with failover to trunk_lines_ca in demarcation setup
local_users_to_wan_ip_trunk_failover_to_second	Route from local_users_ca to wan_ip_trunk_ca with failover to secondary_ip_trunk_ca
registration_to_wan_ip_trunk_failover_to_second	Route from registration_ca to wan_ip_trunk_ca with failover to secondary_ip_trunk_ca
registration_to_wan_ip_trunk	Route from registration_ca to wan_ip_trunk_ca
remote_users_to_lan_pbx	Route from remote_users_ca to lan_ip_pbx_ca
secondary_ip_trunk_to_lan_pbx	Route from secondary_ip_trunk_ca to lan_ip_pbx_ca
trunk_lines_to_local_pbx_dm	Route from trunk_lines_ca to lan_ip_pbx_ca in demarcation setup
wan_ip_trunk_to_lan_pbx	Route from wan_ip_trunk_ca to lan_ip_pbx_ca

### Associating Routing Rulesets to Your Configuration

#### Before you start

[Importing Rulesets \(p. 27\)](#) must be completed for Routing Rulesets to be available.

#### Steps

- 1) Go to **SBC > Rulesets**.
- 2) In the **Routing Rulesets** table, select the Routing Rulesets you wish to apply to the configuration.
- 3) Click **Attach**.
  -  The **Configuration** page is displayed.
- 4) Click **Save**.

- 5) Click **Apply** to apply all changes to the configuration.

---

## Monitoring

### Penalty Box

The penalty box feature is enabled for a specific Call Agent to temporarily avoid contacting the peer hosts (addresses) that are expected not to answer.

Without the use of the penalty box, DNS SRV failover is delayed until the SIP transaction times out. In a DNS SRV failover, without the use of the penalty box, the Call Agent will first try to communicate with the peer host on the first server, then once the SIP transaction has timed out, it will try the second and so on, always waiting for the SIP transaction timer to expire. With the penalty box, the call Agent will not try any servers that are already in the penalty box. Remember, dynamic call routing (e.g. survivability) based on server availability requires the penalty box to be enabled.

There are typically three situations that will cause a peer host to be put in the penalty box:

- If the transaction timer of a communication is expired, the peer host will be considered Down and will be put in the penalty box.
- If the transaction timer of a keep-alive communication is expired, the peer host will be considered Down and will be put in the penalty box.
- If after sending a keep-alive request or any other message to a peer host, the Call Agent receives one of the selected error codes, the peer host will be put in the penalty box. It is the error code that will indicate that the peer host cannot be used.



When configuring the Call Agent it is possible to indicate the error codes that will trigger the peer host to be sent to the penalty box. (**SBC/Configuration/Blacklisting Error Codes**)


It is possible to configure how much time a peer host will remain in the penalty box, and the delay before which a peer host is considered down. This delay starts after the expiration of the transaction timer. It is also possible to disable the penalty box feature by using the special value 0 as the duration the peer host will remain in the penalty box.

### Configuring the Call Agent Penalty Box

#### Information

If you are not familiar with the meaning of the fields, click **Show Help**, located at the upper right corner of the Web page, to display field description when mousing over the field name.

#### Steps

- 1) Go to **SBC/Configuration**.
- 2) Click  next to the Call Agent you wish to configure.
- 3) In the **Configure Call Agent** table, complete the fields as required.
- 4) Click **Save**.

### Keep-Alive

The Keep-Alive monitoring parameter allows the unit to periodically send messages to a server to make sure the server can still be reached.

The Keep-Alive parameter is set individually for each Call Agent. SIP options are sent periodically for each Call Agent to their corresponding server. Any response received from the server means that it can be reached.




No additional processing is performed on the response. If no response is received after the retransmission timer expires, the Sbc service considers the server as unreachable. In this case, any call attempt through the Call Agent is refused and the peer host will be sent to the Penalty Box. SIP options are still sent when the server cannot be reached and as soon as it can be reached again, new calls are allowed.

## Setting the Keep-Alive Interval

### Information

If you are not familiar with the meaning of the fields, click **Show Help**, located at the upper right corner of the Web page, to display field description when mousing over the field name.

### Steps

- 1) Go to **SBC/Configuration**.
- 2) From the **Call Agent Configuration** table, click  next to the Call Agent you wish to configure.
- 3) In the **Keep-Alive Interval**, indicate the interval in seconds for sending SIP options to the Call Agent Peer host.
  -  30 seconds is a good compromise between the speed at which errors are detected versus the resources used by the keep-alive signals.
  -  0 indicates that the keep-alive feature is disabled.
- 4) Click **Save**.

## Registration Agent

The Registration Agent is a module that performs REGISTERS on behalf of other users.


In some use cases, using the Registration Agent may be necessary to have a module perform the REGISTERS on behalf of users. For example:

- To register a SIP PBX to a SIP Service Provider using « SipConnect » registrations when the PBX does not support this kind of registration.
- When users cannot register themselves.
- To separate internal and external networks in Demarcation Point scenarios


The Registration Agent is only involved with the registrations it initiates. If the Registration Agent is used, its REGISTERS are routed to the Mediatrix unit via the registration\_ca Call Agent.

## Configuring a Registration Agent

### Information

-  This procedure is only necessary if your Mediatrix unit registers to the service provider.

### Steps

- 1) Go to **SBC >Registration**.
- 2) In the **Registration Agent Configuration** table, click **++**.
  -  A new line of fields is added.
- 3) Complete the **User Name**, **Friendly Name** and **Domain parameters** fields according to the service provider's requirements.



- 4) In the **Contact** field, enter **sip:user:password@WANipaddress** if your unit is on the Edge or **sip:user:password@public\_ip**, if your unit is in the LAN.
- 5) If necessary, repeat [step 2](#) to [step 4](#) if you are using more than one service provider.
- 6) Click **Apply**.

## Parameters

### SBC > Status Parameters

Although the services can be configured in great part in the web browser, some aspects of the configuration can only be completed with the MIB parameters by :

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

#### **Tcp Connect Timeout**

Refer to **Sbc.SignalingInterfaceStatus.TcpConnectTimeout** in the [Reference Guide](#).

#### **Tcp Idle Timeout**

Refer to **Sbc.SignalingInterfaceStatus.TcpIdleTimeout** in the [Reference Guide](#).

#### **Need Restart Info**

Refer to **Sbc.NeedRestartInfo** in the [Reference Guide](#).

### SBC > Configuration Parameters

Although the services can be configured in great part in the web browser, some aspects of the configuration can only be completed with the MIB parameters by :

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

#### **Tcp Connect Timeout**

Refer to **Sbc.SignalingInterface.TcpConnectTimeout** in the [Reference Guide](#).

#### **Tcp Idle Timeout**

Refer to **Sbc.SignalingInterface.TcpIdleTimeout** in the [Reference Guide](#).

#### **Registration Expiration**

Refer to **Sbc.RegistrationAgent.ExpireValue** in the [Reference Guide](#).

#### **Registration Expiration**

Refer to **Sbc.RegistrationAgent.RetryInterval** in the [Reference Guide](#).

#### **Min Severity**

Refer to **Sbc.MinSeverity** in the [Reference Guide](#).

## Glossary

### 10 Base T

An Ethernet local area network that works on twisted pair wiring. 10 indicates the transmission speed of 10 Mbps, while base refers to baseband signaling i.e. that it only carries Ethernet signals. T refers to the twisted pair of cables this technology uses.

### 100 Base T

A version of Ethernet that operates at 10 times the speed of a 10 BaseT Ethernet. 100 indicates the transmission speed of 100 Mbps, while base refers to baseband signaling i.e. that it only carries Ethernet signals. T refers to the twisted pair of cables this technology uses.

### 1000 Base T

A version of Ethernet that operates at 10 times the speed of a 100 BaseT Ethernet. 1000 indicates the transmission speed of 1,000 Mbps, while base refers to baseband signaling i.e. that it only carries Ethernet signals. T refers to the twisted pair of cables this technology uses.

## A

### Authentication, Authorization and Accounting (AAA)

System service that authenticates a user and grants rights to perform specific tasks on the system.

### Access Device

Device capable of sending or receiving data over a data communications channel.

### Accounting

Accounting measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilisation, and capacity planning activities.

### A-Law

The ITU-T companding standard used in the conversion between analog and digital signals in PCM (Pulse Code Modulation) systems. A-law is used primarily in European telephone networks and contrasts with the North American mu ( $\mu$ )-law standard. See also [mu \( \$\mu\$ \)-law](#).

### ANI (Automatic Number Identification)

In Channel Associated Signaling, the sending of the calling numbers is known as Automatic Number Identification.

### AOC

In ISDN signaling, an Advice Of Charge (AOC-D) message is sent to advise of the current charge (D)uring a call or an AOC-E message is sent to advise of the total charge at the (E)nd of a call.

### Area Code

The preliminary digits that a user must dial to be connected to a particular outgoing trunk group or line.

### **Authentication**

Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials do not match, authentication fails and network access is denied.

## **B**

### **Basic Rate Interface**

Basic Rate Interface or Basic Rate Access is an Integrated Services Digital Network (ISDN) configuration defined in the physical layer standard I.430 produced by the ITU. This configuration consists of two 64 kbit/s "bearer" channels (B channels) and one 16 kbit/s "data" channel (D channel). The B channels are used for voice or user data, and the D channel is used for any combination of: data, control/signalling and X.25 packet networking. The two B channels can be bonded together giving a total data rate of 128 kbit/s. BRI is the kind of ISDN interface most likely to be found in a residential service.

### **Basic Network Interfaces (Bni)**

User service managing the layer 3 network interfaces.

## **C**

### **Call Detail Record (Cdr)**

User service allowing the administrator to generate custom call notifications with information such as endpoints, point of origin, duration, etc.

### **Call Routing**

Calls through the unit can be routed based on a set of routing criteria.

### **Call Routing (CRout)**

User service manipulating properties and routing calls between the telephony interfaces and the SIP endpoints.

### **Certificate Management (Cert)**

System service that manages the security certificates used for the authentication of the unit and its peers before establishing a secure connection.

### **Channel Associated Signaling (CAS)**

With this method of signaling, each traffic channel has a dedicated signaling channel. In other words the signaling for a particular traffic circuit is permanently associated with that circuit. Channel-associated call control is still widely used today mostly in South America, Africa, Australia and in Europe.

**Command Line Interface (Cli)**

User service allowing the administrator to manage the unit using the SSH or TELNET protocols.

**Configuration Manager (Conf)**

System service executing configuration scripts as well as performing backup/restore of the unit's configuration.

**Country Code (CC)**

In international direct telephone dialing, a code that consists of 1-, 2-, or 3-digit numbers in which the first digit designates the region and succeeding digits, if any, designate the country.

**CPE WAN Management Protocol (Cwmp)**

User service allowing the administrator to manage the unit using the TR-069 protocol.

**D****Device Control Manager (Dcm)**

System service managing the auto-detection and identification of unit hardware components as well as the license activation keys.

**Dynamic Host Configuration Protocol Server (Dhcp)**

User service managing a DHCP server on each network interface.

**Dialed Number Identification Service (DNIS)**

DNIS is a telephone service that identifies for the receiver of a call the number that the caller dialed. It's a common feature of 800 and 900 lines. If you have multiple 800 or 900 numbers to the same destination, DNIS tells which number was called. DNIS works by passing the touch tone digits (dual tone multi frequency or MF digits) to the destination where a special facility can read and display them or make them available for call center programming.

**Digital Subscriber Lines (DSL)**

A technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL.

**Distinguished Encoding Rules (DER)**

DER for ASN.1, as defined in ITU-T Recommendation X.509, is a more restrictive encoding standard than the alternative BER (Basic Encoding Rules) for ASN.1, as defined in ITU-T Recommendation X.209, upon which DER is based. Both BER and DER provide a platform-independent method of encoding objects such as certificates and messages for transmission between devices and applications

**Domain Name Server (DNS)**

Internet service that translates domain names into IP addresses. For instance, the domain name www.example.com might translate to 198.105.232.4.

**Dual-Tone Multi-Frequency (DTMF)**

In telephone systems, multi-frequency signaling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol “#” or “\*”, the “\*” being reserved for special purposes.

#### **Dynamic Host Configuration Protocol (DHCP)**

TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.

## **E**

#### **Echo Cancellation**

Technique that allows for the isolation and filtering of unwanted signals caused by echoes from the main transmitted signal.

#### **E&M Channel Associated Signaling (Eam)**

Service managing the E&M CAS telephony interfaces.

#### **Endpoint Administration (EpAdm)**

User service allowing for high-level management of telephony endpoints.

#### **Endpoint Services (EpServ)**

User service managing the telephony services of each endpoint.

#### **Ethernet Manager (Eth)**

System service managing the unit's Ethernet link interfaces.

## **F**

#### **Far End Disconnect**

Refers to methods for detecting that a remote party has hung up. This is also known as Hangup Supervision. There are several methods that may be used by a PBX/ACD/CO to signal that the remote party has hung up, including clear down tone, or a wink.

#### **Federal Communications Commission (FCC)**

U.S. Government regulatory body for radio, television, interstate telecommunications services, and international services originating in the United States.

#### **File Manager (File)**

System service allowing the administrator to manage the files stored on the unit.

#### **Firewall**

A firewall in a networked environment blocks some communications forbidden by the security policy. It has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust).

### **Foreign Exchange Office (FXO)**

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., “foreign”, exchange, rather than the local exchange area’s central office. This is the office end of an FX circuit (frequently a PBX).

### **Foreign Exchange Service/Station (FXS)**

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., “foreign”, exchange, rather than the local exchange area’s central office. This is the station (telephone) end of an FX circuit. An FXS port will provide dial tone and ring voltage.

### **Firmware Pack Updater (Fpu)**

System service managing firmware upgrade, downgrade and rollback operations.

### **Full-Duplex Connection**

Refers to a transmission using two separate channels for transmission and reception and that can transmit in both ways at the same time. See also [Half Duplex Connection](#).

## **G**

### **G.703**

ITU-T recommendation for the physical and electrical characteristics of hierarchical digital interfaces at rates up to 140Mbit/s.

### **G.704**

ITU-T recommendation for synchronous frame structures on G.703 interfaces up to 45Mbit/s. The conventional use of G.704 on a 2Mbit/s primary rate circuit provides 30 discrete 64kbit/s channels, with a further 64kbit/s channel available for common channel signaling

### **G.711**

Algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48 kbps, 56 kbps, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

### **G.723.1**

A codec that provides the greatest compression, 5.3 kbps or 6.3 kbps; typically specified for multimedia applications such as H.323 videoconferencing.

### **G.726**

An implementation of ITU-T G.726 standard for conversion linear or A-law or  $\mu$ -law PCM to and from a 40, 32, 24 or 16 kbit/s channel.

### **G.729**

A codec that provides near toll quality at a low delay which uses compression to 8 kbps (8:1 compression rate).

### **Gateway**

A device linking two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

## **H**

### **Half-Duplex Connection**

Refers to a transmission using the same channel for both transmission and reception therefore it can't transmit and receive at the same time. See also [Full Duplex Connection](#).

### **Host Configuration (Hoc)**

System service managing the IP host parameters and other system settings.

### **Hunt Group**

The hunt group hunts an incoming call to multiple interfaces. It accepts a call routed to it by a routing table or directly from an interface and creates another call that is offered to one of the configured destination interfaces. If this destination cannot be reached, the hunt group tries another destination until one of the configured destinations accepts the call. When an interface accepts a call, the interface hunting is complete and the hunt group service merges the original call with the new call to the interface that accepted the call.

## **I**

### **Impedance**

Impedance is the apparent resistance, in an electric circuit, to the flow of an alternating current, analogous to the actual electrical resistance to a direct current, being the ratio of electromotive force to the current.

### **Information Transfer Capability (ITC)**

A request to the network exchange equipment to ask if a particular type of encoding is allowed. It is also called ISDN bearer capability or ISDN service.

### **Integrated Services Digital Network (ISDN)**

A set of digital transmission protocols defined by the international standards body for telecommunications, the ITU-T (formerly called the CCITT). These protocols are accepted as standards by virtually every telecommunications carrier all over the world. ISDN complements the traditional telephone system so that a single pair of telephone wires is capable of carrying voice and data simultaneously. It is a fully digital network where all devices and applications present themselves in a digital form.

### **Integrated Services Digital Network (Isdn)**



User service managing the ISDN parameters for BRI and PRI telephony interfaces.

**International Telecommunication Union (ITU)**

Organization based in Geneva, Switzerland, that is the most important telecom standards-setting body in the world.

**Internet-Drafts**

Internet-Drafts are working documents of the IETF, its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

**Internet Protocol (IP)**

A standard describing software that keeps track of the Internet's addresses for different nodes, routes outgoing messages, and recognizes incoming messages.

**IP Forwarding**

Allows the packet to be forwarded to a specific network based on the packet's criteria (source IP address and source Ethernet link).

**IP Routing (IpRouting)**

User service managing the unit's IP routing table.

**IP Synchronisation (IpSync)**

User service controlling the IP media synchronization using clock reference signals sent over IP.

**Internet Protocol version 4 (IPv4)**

IPv4 (Internet Protocol version 4) is a 32-bit address internet protocol.

**Internet Protocol version 6 (IPv6)**

IPv6 (Internet Protocol version 6) is the successor to the common Internet Protocol (IPv4). IPv6's is a 128-bit address Internet protocol.

**J****Jitter**

A distortion caused by the variation of a signal from its references which can cause data transmission errors, particularly at high speeds.

**L****Light Emitting Diode (LED)**

A semiconductor diode that emits light when a current is passed through it.

**Link Layer Discovery Protocol (Lldp)**

User service managing the IEEE 802.1ab protocol used for advertising the unit's capabilities on the network.

### **Local Area Network (LAN)**

Data-only communications network confined to a limited geographic area, with moderate to high data rates. See also [WAN](#).

### **Local Firewall**

Allows you to dynamically create and configure rules to filter incoming packets with the unit as destination. The traffic is analysed and filtered by all the configured rules.

### **Local Firewall (Lfw)**

User service allowing the administrator to filter incoming packets with the unit as final destination.

### **Local Quality Of Service (LQos)**

System service managing the QOS parameters applicable to the unit.

## **M**

### **Management Information Base (MIB)**

Specifications containing definitions of management information so that networked systems can be remotely monitored, configured and controlled.

### **Media Access Control (MAC) Address**

A layer 2 address, 6 bytes long, associated with a particular network device; used to identify devices in a network; also called hardware or physical address.

### **Media Interface**

The Media Interface is used for media ( RTP, UDPTL) processing.

### **Media IP Transport (Mipt)**

User service managing the voice and data encodings over the IP network.

### **Mu ( $\mu$ )-Law**

The PCM (Pulse Code Modulation) voice coding and companding standard used in Japan and North America. See also [A-Law](#).

### **Music on Hold (MoH)**

User service managing the option to play an audio file when a telephony endpoint is on hold.

## **N**

### **Network**

A group of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances. A network can consist of any combination of local area networks (LAN) or wide area networks (WAN).

### **Network Address Translation (NAT)**

NAT, also known as network masquerading or IP masquerading, rewrites the source and/or destination addresses/ports of IP packets as they pass through a router or firewall. It is most commonly used to connect multiple computers to the Internet (or any other IP network) by using one IP address. This allows home users and small businesses to cheaply and efficiently connect their network to the Internet. The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address. There are two types of NAT rules:

- Source rules: They are applied on the source address of outgoing packets.
- Destination rules: They are applied on the destination address of incoming packets.

### **Network Address Translation (Nat)**

User service allowing the administrator to change the source or the destination IP address of a packet.

### **Network Firewall**

Allows dynamically creating and configuring rules to filter packets forwarded by the unit. Since this is a network firewall, rules only apply to packets forwarded by the unit. The traffic is analyzed and filtered by all the rules configured.

### **Network Firewall (Nfw)**

User service allowing the administrator to filter traffic that is routed between networks.

### **Network Traffic Control (Ntc)**

User service allowing the administrator to perform traffic shaping on the network interfaces.

### **Notification and Logging Manager (Nlm)**

User service managing the routing and filtering of the unit's event notification messages.

## **O**

### **Off-hook**

A line condition caused when a telephone handset is removed from its cradle.

### **On-hook**

A line condition caused when a telephone handset is resting in its cradle.

## **P**

### **Packet**

Includes three principal elements: control information (such as destination, origin, length of packet), data to be transmitted, and error detection. The structure of a packet depends on the protocol.

### **Plain Old Telephone System (POTS)**

Standard telephone service used by most residential locations; basic service supplying standard single line telephones, telephone lines, and access to the public switched network.

### **Plain Old Telephone System Line (Pots)**

User service managing the FXS and FXO analog telephony interfaces.

### **Point to Point Protocol over Ethernet (PPPoE)**

A proposal specifying how a host personal computer interacts with a broadband modem (i.e., DSL, cable, wireless, etc.) to access the growing number of Highspeed data networks. Relying on two widely accepted standards, Ethernet and the point-to-point protocol (PPP), the PPPoE implementation requires virtually no more knowledge on the part of the end user other than that required for standard Dial up Internet access. In addition, PPPoE requires no major changes in the operational model for Internet Service Providers (ISPs) and carriers. The base protocol is defined in RFC 2516.

### **Port**

Network access point, the identifier used to distinguish among multiple simultaneous connections to a host.

### **Portable Operating System Interface (POSIX)**

POSIX is a set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to be able to develop programs that could be moved among different manufacturer's computer systems without having to be recoded.

### **Primary Rate Interface (PRI)**

A telecommunications standard for carrying multiple DS0 voice and data transmissions between two physical locations. All data and voice channels are (ISDN) and operate at 64 kbit/s. North America and Japan use a T1 of 23 B channels and one D channel which corresponds to a T1 line. Europe, Australia and most of the rest of the world use the slightly higher capacity E1, which is composed of 31 B channels and one D channel. Fewer active B channels (also called user channels) can be used for a fractional T1. More channels can be used with more T1's, or with a fractional or full T3 or E3.

### **Presentation Indicator (PI)**

An information element (IE) field that determines whether a caller's CLI can be displayed on a Caller ID device or otherwise presented to the called party.

### **Private Branch Exchange (PBX)**

A small to medium sized telephone system and switch that provides communications between onsite telephones and exterior communications networks.

### **Process Control Manager (PCM)**

System service managing the start-up and shutdown sequences of the system.

### **Protocol**

A formal set of rules developed by international standards bodies, LAN equipment vendors, or groups governing the format, control, and timing of network communications. A set of conventions dealing with transmissions between two systems. Typically defines how to implement a group of services in one

or two layers of the OSI reference model. Protocols can describe low-level details of machine-to-machine interfaces or high-level exchanges between allocation programs.

### **Proxy Server**

An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.

### **Public Switched Telephone Network (PSTN)**

The local telephone company network that carries voice data over analog telephone lines.

## **Q**

### **QSIG**

QSIG is an ISDN based signaling protocol for signaling between private branch exchanges (PBXs) in a Private Integrated Services Network (PISN). It makes use of the connection-level Q.931 protocol and the application level ROSE protocol. ISDN "proper" functions as the physical link layer.

### **Quality of Service (QoS)**

Measure of the telephone service quality provided to a subscriber. This could be, for example, the longest time someone should wait after picking up the handset before they receive dial tone (three seconds in most U.S. states).

## **R**

### **R2 Channel Associated Signaling (R2)**

User service managing the E1 CAS telephony interfaces.

### **Real Time Control Protocol (RTCP)**

RTCP is the control protocol designed to work in conjunction with RTP. It is standardised in RFC 1889 and 1890. In an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership.

### **Realtime Transport Protocol (RTP)**

An IETF standard for streaming real-time multimedia over IP in packets. Supports transport of real-time data like interactive voice and video over packet switched networks.

### **Registrar Server**

A server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and MAY offer location services.

### **Request for Comment (RFC)**

A formal document from the IETF that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.

## S

### **Screening Indicator (SI)**

A service provided by ISDN that can be used to test the trustworthiness of the calling party's number. This signalling-related information element is found in octet 3a of the ISDN SETUP message.

### **Service Controller Manager (Scm)**

System service allowing the administrator to enable or disable services.

### **SBC Session**

An SBC session is a SIP call established between two endpoints not including the SBC. A session usually has 2 call legs, one incoming and one outgoing of the SBC.

### **Session Border Controller (Sbc)**

User service allowing the administrator to perform SIP to SIP normalization, call routing, NAT traversal and survivability.

### **Session Border Controller (SBC)**

A Session Border Controller used in Voice over Internet Protocol (VoIP) networks to control the signaling and media streams involved in establishing, conducting and analysing telephone calls or other interactive media communications.

### **Session Description Protocol (SDP)**

Describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation. SDP communicates the existence of a session and conveys sufficient information to enable participation in the session. SDP is described in RFC 2327.

### **Session Initiation Protocol (SIP)**

A protocol for transporting call setup, routing, authentication, and other feature messages to endpoints within the IP domain, whether those messages originate from outside the IP cloud over SCN resources or within the cloud.

### **Signaling Interface**

The Signaling Interface is used for SIP signaling.

### **Simple Network Management Protocol (Snmp)**

User service allowing the administrator to manage the unit using the SNMP protocol.

### **Simple Network Management Protocol (SNMP)**

A standard of network management that uses a common software agent to manage local and wide area network equipments from different vendors; part of the Transmission Control Protocol / Internet Protocol (TCP/ IP) suite and defined in RFC 1157.

### **Simple Network Time Protocol (SNTP)**

SNTP, which is an adaptation of the Network Time Protocol (NTP), is widely used to synchronize computer clocks in the global Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and adjust the local clock in each participating subnet peer. In most places of the Internet of today, NTP provides accuracies of 1-50 ms, depending on the characteristics of the synchronisation source and network paths.

### **SIP Endpoint (SipEp)**

User service allowing the administrator to associate telephony endpoints with SIP user agents.

### **Session Traversal Utilities for NAT (STUN)**

Session Traversal Utilities for NAT is a standardized set of methods and a network protocol to allow an end host to discover its public IP address if it is located behind a Network Address Translation (NAT)

### **Subnet**

An efficient means of splitting packets into two fields to separate packets for local destinations from packets for remote destinations in TCP/IP networks.

### **Switched Circuit Network (SCN)**

A communication network, such as the public switched telephone network (PSTN), in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices.

## **T**

### **T.38**

An ITU-T Recommendation for Real-time fax over IP. T.38 addresses IP fax transmissions for IP-enabled fax devices and fax gateways, defining the translation of T.30 fax signals and Internet Fax Protocols (IFP) packets.

### **Telephony**

The science of translating sound into electrical signals, transmitting them, and then converting them back into sound.

### **Telephony Interface (Telf)**

User service managing tone generation and detection on the telephony interfaces.

### **TR-069**

The TR-069 also known as CWMP, is a Broadband Forum technical specification. This protocol can be used for monitoring and updating CPE configurations and firmware.

### **TR-104**

The TR-104 is a part of CWMP, a Broadband Forum technical specification. This specification defines the data model for provisioning a Voice over Internet Protocol (VoIP) CPE device by an Auto-Configuration Server (ACS) using the mechanism defined in TR-069.

#### **TR-106**

TR-106 specifies data model guidelines to be followed by all TR-069-enabled devices.

#### **TR-111**

This specification extends the mechanism defined in TR-069 for remote management of customer premises equipment to allow a management system to more easily access and manage devices connected via LAN through an Internet gateway.

#### **Transmission Control Protocol/Internet Protocol (TCP/IP)**

The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

#### **Trivial File Transfer Protocol (TFTP)**

A simplified version of FTP that transfers files but does not provide password protection, directory capability, or allow transmission of multiple files with one command.

## **U**

#### **User Datagram Protocol (UDP)**

An efficient but unreliable, connectionless protocol that is layered over IP, as is TCP. Application programs are needed to supplement the protocol to provide error processing and retransmission of data. UDP is an OSI layer 4 protocol.

## **V**

#### **Virtual LAN (VLAN)**

A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

#### **Virtual Private Network (VPN)**

A private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network. VPN message traffic is carried on public networking infrastructure (e.g. the Internet) using standard (often insecure) protocols, or over a service provider's network providing VPN service guarded by well defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

#### **Voice Over IP (VoIP)**



The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

## W

### **Wide Area Network (WAN)**

A large (geographically dispersed) network, usually constructed with serial lines, that covers a large geographic area. A WAN connects LANs using transmission lines provided by a common carrier.

### **Web (WEB)**

User service allowing the administrator to manage the unit using HTTP(S) web pages.

## Acronyms

### A

**Aaa**

Authentication, Authorization and Accounting

**AC**

Access Concentrator

**ACS**

Auto Configuration Server

**ADSL**

Asymmetric Digital Subscriber Line

**AES**

Advanced Encryption Standard

**ANI**

Automatic Number Identification

**AOC-E**

Advice of Charge End-of-Call

### B

**BER**

Basic Encoding Rules

**Bni**

Basic Network Interfaces

**BRI**

Basic Rate Interface

### C

**CA**

Certification Authority

**CAS**

Channel Associated Signalling

- CC**  
Country Code
- CCBS**  
Completion of Call to Subscriber
- CCNR**  
Completion of Calls on No Reply
- Cdr**  
Call Detail Record
- CDR**  
Call Detail Record
- Cert**  
Certificate Manager
- CHAP**  
Challenge Handshake Authentication
- Cli**  
Command Line Interface
- CLIP**  
Calling Line Information Presentation
- CLIR**  
Calling Line Information Restriction
- CNG**  
Comfort Noise Generator
- CNIP**  
Calling Name Identity Presentation
- COLP**  
Connected Line Identification Presentation
- COLR**  
Connected Line Identification Restriction
- Conf**  
Configuration Manager
- CRout**  
Call Routing
- CS-ACELP**  
Conjugate Structure-Algebraic Excited Linear Prediction
- Cwmp**  
CPE Wan Management Protocol

## D

**Dcm**

Device Control Manager

**DER**

Distinguished Encoding Rules

**Dhcp**

Dynamic Host Configuration Protocol Server

**DHCP**

Dynamic Host Configuration Protocol

**Dhcp**

Dynamic Host Configuration Protocol

**DNIS**

Dialed Number Identification Service

**DNS**

Domain Name Server

**DSCP**

Differentiated Services Code Point

**DSL**

Digital Subscriber Lines

**DSS1**

Digital Subscriber Signalling System No.1

**DST**

Daylight Saving Time

**DTMF**

Dual Tone Multi-Frequency

**E**

**Eam**

E&M Channel Associated Signaling

**EpAdm**

Endpoint Administration

**EpServ**

Endpoint Services

**ETH**

Ethernet Manager

**F**

**FCC**

Federal Communication Commission

**FILE**

File Manager

**Fpu**

Firmware Pack Updater

**FQDN**

Fully Qualified Domain Name

**FSK**

Frequency Shift Keying

**FXO**

Foreign Exchange Office

**FXS**

Foreign Exchange Service/Station

**G****GMT**

Greenwich Mean Time

**H****HDSL**

High-bit-rate Digital Subscriber Line

**Hoc**

Host Configuration

**HTML**

Hyper Text Markup Language

**HTTP**

Hyper Text Transfer Protocol

**HTTPS**

HTTP over the Transport Layer Security

**Hz**

Hertz

**I**

**ICMP**

Internet Control Message Protocol

**IEEE**

Institute of Electrical & Electronics Engineers

**IETF**

Internet Engineering Task Force

**IMS**

IP Multimedia Core Network Subsystem

**IP**

Internet Protocol

**IP PBX**

Internet Protocol Private Branch eXchange

**IpRouting**

IP routing

**IpSync**

IP Synchronisation

**IPv4**

Internet Protocol version 4

**IPv6**

Internet Protocol version 6

**ISDN**

Integrated Services Digital Network

**Isdn**

Integrated Services Digital Network

**ITC**

Information Transfer Capability

**ITSP**

Internet Service Provider

**ITU**

International Telecommunication Union

**K**

**kbps**

KiloBits Per Second

**L**

**LAN**

Local Area Network

**LED**

Light Emitting Diode

**Lfw**

Local Firewall

**LNP**

Local Number Portability

**LLPD-MED**

Link Layer Discovery Protocol-Media Endpoint Discovery

**LLPD**

Link Layer Discovery Protocol

**Lldp**

Link Layer Discovery Protocol

**LQos**

Local Quality of Service

**M****MAC**

Media Access Control

**MFC**

Multi-Frequency Code

**MIB**

Management Information Base

**MIKEY**

Multimedia Internet KEYing

**Mipt**

Media IP Transport

**Moh**

Music on Hold

**MSN**

Multiple Subscriber Number

**MTU**

Maximum Transmission Unit

**MWI**

Message Waiting Indicator

## N

### **NAT**

Network Address Translation

### **Nat**

Network Address Translation

### **Nfw**

Network Firewall

### **Nlm**

Notifications and Logging Manager

### **Ntc**

Network Traffic Control

### **NTP**

Network Time Protocol

## O

### **OCSP**

Online Certificate Status Protocol

## P

### **PAP**

Password Authentication Protocol

### **PBX**

Private Branch eXchange

### **PCM**

Pulse Code Modulation

### **Pcm**

Process Control Manager

### **PEM**

Privacy Enhanced Mail

### **PI**

Presentation Indicator

### **PISN**

Private Integrated Services Network

### **POSIX**



Portable Operating System Interface

**POTS**

Plain Old Telephony System

**Pots**

Plain Old Telephony System Line

**PPP**

Point-to-Point Protocol

**PPPoE**

Point-to-Point Protocol over Ethernet

**PRACK**

Provisional Response Acknowledgement

**PRI**

Primary Rate Interface

**PSTN**

Public Switched Telephony Network

## Q

**QoS**

Quality of Service

## R

**R2**

R2 Channel Associated Signaling

**Radius**

Remote Authentication Dial-In User Service

**RADSL**

Rate-adaptive Digital Subscriber Line

**RFC**

Request For Comment

**RTCP**

Realtime Control Protocol

**RTP**

Real Time Transport Protocol

## S

**Sbc**

Session Border Controller

**SBC**

Session Border Controller

**Scm**

Service Controller Manager

**SCN**

Switched Circuit Network

**SDES**

Secure Description

**SDP**

Session Description Protocol

**SHA**

Secure Hash Algorithm

**SI**

Screening Indicator

**SipEp**

SIP Endpoint

**SLA**

Service Level Agreement

**SNMP**

Simple Network Management Protocol

**Snmp**

Simple Network Management Protocol

**SNTP**

Simple Network Time Protocol

**SRTCP**

Secure Real-Time Transport Control Protocol

**SRTP**

Secure Real-Time Transport Protocol

**SSH**

Secure Socket Shell

**SSL**

Secure Socket Layer

**STD**

Standard Saving Time

**STP**

Spanning Tree Protocol

**T**

**TBRL**

Terminal Balance Return Loss

**TCP**

Transmission Control Protocol

**TCP/IP**

Transmission Control Protocol/Internet Protocol

**TE**

Terminal Equipment

**TEI**

Terminal Endpoint Identifier

**TelIf**

Telephony Interface

**TFTP**

Trivial File Transfer Protocol

**TLS**

Transport Layer Security

**TON**

Type of Number

**U****UDP**

User Datagram Protocol

**UMN**

Unit Manager Network

**UNI**

User-Network Interface

**URI**

Uniform Resource Identifier

**UTC**

Universal Time Coordinated

**V****VAD**

Voice Activity Detector

**VLAN**

Virtual Local Area Network

**VoIP**

Voice Over IP

**VPN**

Virtual Private Network

**W**

**WAN**

Wide Area Network

**Web**

Web

**WINS**

Windows Internet Name Service



4229, rue de la Garlock  
Sherbrooke (Quebec)  
J1L 2C8 Canada

Learn more at  
[www.media5corp.com](http://www.media5corp.com)