Table of Contents

Audience ....................................................................................................................................................... 4
1 Introduction ............................................................................................................................................... 4
2 Network Topology ...................................................................................................................................... 5
3 System Components ............................................................................................................................... 6
  3.1 Hardware Components ....................................................................................................................... 6
  3.2 Software Requirements ..................................................................................................................... 7
4 Features ..................................................................................................................................................... 7
  4.1 Supported Features ............................................................................................................................ 7
  4.2 Unsupported Features ......................................................................................................................... 7
5 Caveats and Limitations ......................................................................................................................... 7
6 Configuration ............................................................................................................................................. 8
  6.1 ShoreTel PBX Configuration ............................................................................................................... 8
  6.2 Test Lab Notes .................................................................................................................................. 8
  6.3 Phone Number Assignments ............................................................................................................ 9
  6.4 Initial IP PBX web user interface (UI) welcome screen ................................................................. 9
  6.5 Support welcome screen for advanced customization .................................................................. 9
  6.6 SIP Trunk Configuration ................................................................................................................... 10
  6.7 PBX SIP Users & Extension Management ..................................................................................... 15
  6.8 Administration>Call Control>Account Codes ............................................................................... 20
  6.9 Administration>Call Control>Hunt Groups ..................................................................................... 20
  6.10 Administration>Call Control>Hunt Groups ................................................................................... 22
  6.11 Administration>Call Control>Codec Lists .................................................................................... 24
  6.12 Administration>Call Control>Options .......................................................................................... 26
  6.13 Administration>Auto-Attendant Menu ......................................................................................... 27
  6.14 Analog Fax/Modem ......................................................................................................................... 28
7 Ingate SIParator Configuration .............................................................................................................. 30
  7.1 Web User Interface .......................................................................................................................... 30
  7.2 Authentication and Accounting ...................................................................................................... 36
  7.3 SIParator Configuration File ............................................................................................................ 41
8 Troubleshooting ..................................................................................................................................... 59
  8.1 ShoreTel Trunk Test Tool ............................................................................................................... 59
  8.2 InGate Logging and Tools .............................................................................................................. 60
9 SIP Messaging examples, taken from inside of E-SBC ...................................................................... 63
  9.1 Basic outbound on-net and off-net calls ......................................................................................... 63

Table of Figures

Figure 1 – Cox Fiber Network .................................................................................................................. 4
Figure 2 – Reference Network Architecture .......................................................................................... 5
Figure 3 – ShoreTel UCP SIP Trunk Lab Network .................................................................................. 6
Figure 4 – ShoreWare Director: Trunk Groups ....................................................................................... 10
Figure 5 – ShoreWare Director: Trunk Groups (continued) .................................................................. 11
Figure 6 – ShoreWare Director: Trunk Groups (continued) .................................................................. 12
Figure 7 – DID Range ............................................................................................................................. 13
Figure 8 – Area Codes ............................................................................................................................. 13
Figure 9 – Trunk Groups Dialing Rules .................................................................................................. 14
Figure 10 – Edit Trunks ........................................................................................................................... 14
1 Introduction

This Configuration Guide describes configuration steps for Cox SIP trunking to a ShoreTel Unified Communications Platform (UCP) PBX. Cox SIP Trunking is a scalable and efficient IP trunking telecommunication solution for your business that provides all the traditional services such as Direct Inward Dialing, Hunting, Calling Name, Calling Number, Local/Long Distance and Business Continuity options, including:

- Burstable Trunk Capacity – Dynamically increases call capacity during peak busy periods so your customers never receive a busy signal.
- Call Forward Always – On the trunk group pilot number for all calls in case of an outage (i.e., flood, fire, loss of power, etc.).
- Call Forward Not Reachable – On the trunk group pilot number that operates on a per-call contingency basis to forward the call to any PSTN number (i.e., call center or alternate office location) during temporary call completion impairments.
- Route Exhaustion – Automatic reroute of trunk group calls to any PSTN phone number (i.e., a call center) if calls can’t be completed to the PBX.
- Support for geo-redundant PBX deployments and automatic reroute of SIP trunks to the backup customer data center.

All calls are routed over Cox’s national fiber network with guaranteed Quality of Service (QoS); calls never traverse the Internet.

Figure 1 – Cox Fiber Network
2 Network Topology

The high-level Cox SIP trunk network architecture is depicted below. The key network elements are:

- IP PBX – Customer PBX for terminating SIP trunks.
- Cox Enterprise Session Border Controller (E-SBC) – The E-SBC is a smart service demarcation device and SIP Application Layer Gateway (ALG) installed and managed by Cox.
- Core Session Border Controllers and Broadsoft SIP Call Server for maximum survivability and reliability.
- PSTN Gateway for connections to the Public Switched Telephone Network (PSTN).

![Reference Network Architecture Diagram]

This SIP trunk network architecture is replicated across the Cox operating regions for scalability and operational autonomy.

Cox will deploy one or more Enterprise Session Border Controllers (E-SBCs) to meet call capacity, customer data center geo-redundancy and trunk group requirements. The E-SBC is owned and managed by Cox and is the service demarcation point. The E-SBC performs SIP ALG, SIP normalization, NAT, security, traffic shaping/prioritization, performance reporting and remote diagnostic functions.
3 System Components

The lab network consists of the following components:

- ShoreTel ShoreGear 50 PBX for voice features, call control and phone management.
- InGate SIParator for SIP trunk registration and message authentication with the Cox Business SIP Trunk service. The InGate SIParator is packaged with the ShoreTel PBX.
- Various SIP phones on the local LAN.
- The Cox E-SBC is the Edgewater Networks (www.edgewaternetworks.com) EdgeMarc 4550. The EdgeMarc is the service demarcation point between customer’s LAN network and Cox’s WAN network and provides firewall/NAT traversal, B2BUA and SIP Application-level gateway. The EdgeMarc has diverse routes to a primary and secondary Acme SBC.
- Acme Packet Net-Net 9200 Session Border Controllers (SBC).

3.1 Hardware Components

- Windows 2003 Server with 4 GB RAM and multi-core Intel i3 3.07 GHz CPU’s
- ShoreTel ShoreGear 50 Switch (IP PBX)
- Three ShoreTel IP Phones, model IP 230
- InGate SIParator 19
- Analog Fax Machine
- EdgeMarc 4550 E-SBC
3.2 Software Requirements

- ShoreTel ShoreWare Director release 10.2 (build 15.41.9301.0)
- InGate SIParator 19 release 4.8.4
- EdgeMarc 4550 9.12.5 release

4 Features

4.1 Supported Features

- Basic Calls using G.711ulaw CODEC
- Calling Party Number Presentation and Restriction
- Call Transfer
- Call Forwarding
- RFC2833 transcoding
- Fax and modem inband G.711

4.2 Unsupported Features

- Codec negotiation of G.729, G.726, and others
- T.38 Fax relay

5 Caveats and Limitations

All configurations were performed using the ShoreTel ShoreWare Director Web based Administration GUI unless exclusively stated in this document.

- Three-way calling fails when a PBX Phone calls an off-net PSTN number and a PBX extension. All the other Three-way call scenarios work.
- Unable to complete call transfer of a call on hold using the Cox Personal Call Manager web GUI. User should be able to put the call on hold and retrieve the call and transfer the call using Personal Call Manager, but we found that while retrieving the call we ran into a media flows issue with the Acme 9200 SBC.
6 Configuration

6.1 ShoreTel PBX Configuration

The ShoreWare Director component is a web-based configuration and management software solution that is best run on a dedicated Windows-based server meeting the hardware specifications outlined in the release notes. It also functions as the applications server for features such as voicemail.

ShoreGear switches act as media gateways and call agents for the IP phones; they are optionally fault-tolerant.

ShoreTel IP 230 phones are 3-line MGCP endpoints with PoE support and built-in switchports. The ShoreTel PBX does not register as a SIP trunk, but uses static SIP trunking instead.

The InGate SIParator is required to meet the requirements of the test scenario. A SIParator 19 is an enterprise small office/home office model supporting up to 40 concurrent sessions.

6.2 Test Lab Notes

The default LAN gateway and DHCP server was an Edgewater Networks EdgeMarc 450 series (E-SBC) running 9.12.5 code. It handled firewall and NAT functions for the ShoreTel PBX network under test. As tested, the ShoreTel IP 230 phones used DHCP from the E-SBC and the other PBX components were statically addressed as follows:

- **Ingate SIParator 19:** 192.168.1.250
- **ShoreWare Director Server:** 192.168.1.35
- **ShoreGear 50 Switch:** 192.168.1.10
- **Edgewater EdgeMarc 4550:** 192.168.1.1

The PBX was configured with five static SIP trunks to the SIParator. The SIParator was set-up to register a single pilot number as the SIP trunk to/through the E-SBC. All SIP traffic between the Cox ITSP system and the IP PBX passed through the E-SBC and SIParator.

The ShoreWare Director ran release 10.2 (build 15.41.9301.0) on a Windows 2003 R2 enterprise SP2 server with 4 GB RAM and multi-core Intel i3 3.07 GHz CPU’s. The following licenses keys were present:

- 10 SIP Trunks Licenses
- 3 Extension and Mailbox Licenses
- 1 Enterprise Edition System License

The SIParator ran release 4.8.4 software, was licensed for 5 SIP traversals and 10 SIP user registrations, and had the following modules installed:

- Standard SIP features
- SIP Trunking
- Advanced SIP Routing
- Failover – not tested
- VPN (IPsec and PPTP) – not tested
- QoS – trial copy
6.3 Phone Number Assignments

678-239-1120  Registering PBX Pilot Number
678-239-1121  Test Phone #1 (IP 230)
678-239-1122  Test Phone #2 (IP 230)
678-239-1123  Test Phone #3 (IP 230)
678-239-1124  Hunt Group (ShoreTel)
678-239-1125  Auto Attendant (Broadsoft)
678-239-1126  Analog FXS interface/channel #1 (FAX/modem)
678-239-1127  Voice Portal (Broadsoft)
678-239-1128  Hunt Group (Broadsoft)
678-239-1129  Auto Attendant & Voicemail Portal (ShoreTel)

6.4 Initial IP PBX web user interface (UI) welcome screen

- Install ShoreWare Director software on the server.
- Open an Internet Explorer browser window to [http://localhost/ShoreWareDirector](http://localhost/ShoreWareDirector)
- Login with default username/password of admin/changeme.

6.5 Support welcome screen for advanced customization

* Advanced support login access is achieved by clicking on the underlined letter U in "User ID" while holding down Ctrl and Shift keys, before entering the same username/password. This method is required when making certain customizations to the PBX. See image below for subsequent welcome screen:
### 6.6 SIP Trunk Configuration

After registering and setting up global configurations details per the Administration Guide (i.e. site, voice switch, and application server, etc.) on the ShoreTel PBX system, the static SIP trunks were created from the primary ShoreGear voice switch to the SIParator appliance. Within ShoreWare Director, a new trunk group was added (Trunks>Trunk Groups>Add…of type…SIP) with the following settings, many of which were default.

NOTE: Dialing a trunk access code (e.g. 9) is required by the PBX; this field may not be left blank.

![Figure 4 – ShoreWare Director: Trunk Groups](image)

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name:</strong></td>
<td>SIPtrunk-BroadCorp</td>
</tr>
<tr>
<td><strong>Site:</strong></td>
<td>CoxLab</td>
</tr>
<tr>
<td><strong>Language:</strong></td>
<td>English (US)</td>
</tr>
<tr>
<td><strong>Teleworkers:</strong></td>
<td>Off</td>
</tr>
<tr>
<td><strong>Enable SIP Info for 0,711 DTMF Signaling:</strong></td>
<td>Off</td>
</tr>
<tr>
<td><strong>Profile:</strong></td>
<td>_SystemTrunk</td>
</tr>
<tr>
<td><strong>Digest Authentication:</strong></td>
<td>None (default)</td>
</tr>
<tr>
<td><strong>User ID:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Password:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Inbound:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Number of Digits from CO:</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>DNIS</strong></td>
<td></td>
</tr>
<tr>
<td><strong>DID</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Extension:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Translation Table:</strong></td>
<td>None (default)</td>
</tr>
<tr>
<td><strong>Prepend Dial in Prefix</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Use Site Extension Prefix</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Tandem Trunking</strong></td>
<td>Off</td>
</tr>
<tr>
<td><strong>User Group:</strong></td>
<td>Executives</td>
</tr>
</tbody>
</table>
Figure 5 – ShoreWare Director: Trunk Groups (continued)
Figure 6 – ShoreWare Director: Trunk Groups (continued)
The “Edit DID Range” was set for the ten test numbers:

![DID Range Siptrunk-Broadsoft](image)

**Figure 7 – DID Range**

The other Atlanta NPA’s were also manually specified by clicking the “Edit” button next to “Additional Local Area Codes.”

![Additional Local Area Codes – Webpage Dialog](image)

**Figure 8 – Area Codes**

Tips:
- Modifying the “Trunk Group Dialing Rules” requires logging in through the advanced/support welcome screen.
- To allow certain star feature codes to pass transparently through the PBX, the strings shown below were added—the first line is a sample of code only, the others permit code+dialstring, and finally there is a “10E” appended to force the preferred number format (no prepended “+1”) in the SIP URI.
After creating the trunk group, individual trunks are added with the quantity determining the maximum number of simultaneous calls into/out of the PBX. The far end of each of the SIP trunks is the LAN IP address of the Siparator.

### Trunks

**Edit Trunk**

![Edit Trunk](image)

**Figure 10 – Edit Trunks**
6.7 PBX SIP Users & Extension Management

It is important to consider the user group, class of service, and personal options that are associated when provisioning a PBX SIP user extension. For most of the testing, premium user group (Executives) and class of service (Fully Featured, No Restrictions, Large Mail Box) were used.

The exception was the testing of account codes for certain call types.

Before users are created, the IP phones and voice switches should be configured. One or more ShoreGear voice switches manage phones in the PBX system.

For MGCP endpoint like the ShoreTel IP 230, only is the MAC address of the phone needs to be entered. SIP telephone/endpoint registration was not tested and hence not included in this document.

The voice switches are set-up manually with port configurations. We used the ShoreGear 50 as the T1k model did not support SIP trunking. SIP proxy features were configured but not tested. At least three switch ports need to be configured for "Conference" type to demonstrate the 3-way calling feature on the PBX. Additionally, each port can be configured for up to 5 SIP trunks or an analog extension (FXO or FXS).
Figure 14 – Primary Switches

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Site</th>
<th>Server</th>
<th>Type</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Serial Number</th>
<th>IP Phones In Use</th>
<th>IP Phones Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShoreGear50</td>
<td>VoIP Gateway/PBX</td>
<td>CoxLab</td>
<td>Headquarters</td>
<td>50-50</td>
<td>192.168.1.10</td>
<td>00-10-48-16-15-74</td>
<td>S500017161074</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>ShoreGear51</td>
<td></td>
<td>CoxLab</td>
<td>Headquarters</td>
<td>SO-11</td>
<td>192.168.1.11</td>
<td>00-10-48-16-16-1A</td>
<td>T1K201216161A</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SoftSwitch</td>
<td></td>
<td>CoxLab</td>
<td>Headquarters</td>
<td>SKY</td>
<td>192.168.1.65</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>3</strong></td>
<td><strong>5</strong></td>
</tr>
</tbody>
</table>

Figure 15 – Switches: Edit ShoreGear 50 Switch

Figure 16 – ShoreGear 50 Switch Port Assignments
A user's Call Handling mode determines most of the incoming call features. To access most of these, choose Personal Options under the Users  Individual Users screen.

![Users Window](image)

**Figure 17 – Edit User: Personal Options**

- **User Name**: Bob Cobb
- **Extension**: 1122
- **Call Control Options**:
  - **Current Call Stack Size**: 4
  - **Ring Type**: Standard
  - **Automatic Off-Hook Preference**: Speaker
  - **Handsfree Mode**: Unchecked
  - **Call Waiting Tone Enabled**: Checked
  - **Trunk Group Access Code**: Analog Loop Start
  - **Mailbox for Recorded Calls**: 

**Call Handling Mode Options**:

- **Current Call Handling Mode**: Standard
- **Outlook Automated Call Handling**: Checked

**Edit Call Handling Modes**:

- Standard
- In a Meeting
- Out of Office
- Extended Absence
- Custom

**Mailbox Options**:

- Find Me

**Figure 18 – Edit Call Handling Modes**
A custom call handling mode or one of the four other default ones can be selected in the Personal Options screen to adjust call forwarding behavior.

![Edit User: Call Forwarding Options](image)

**Figure 19 – Edit User: Call Forwarding Options**
By clicking on "External Assignment and Additional Phones" on the Personal Options screen, the find-me, follow-me functions may be set.
6.8 Administration>Call Control>Account Codes

Figure 21 – Account Codes

6.9 Administration>Call Control>Hunt Groups

Figure 22 – Hunt Groups
Figure 23 – Edit Hunt Group
6.10 Administration>Call Control>Hunt Groups
In this section you can setup the Hunt groups and the associated extensions.

Figure 24 – Edit Hunt Group (continued)

Figure 25 – Pickup Group List
Figure 26 – Pickup Group

Pickup Groups
Edit Pickup Group

Edit this record

Refresh this page

Name: PU2
Extension: 1125
Switch: ShoreGear50
Extension List: ListLowest

Edit this extension list

Figure 27 – Pickup Group Extension List

Users
Edit Extension List

Edit this record

Refresh this page

Name: ListLowest

Filter Users By:
First Name: Last Name: Extension:
Sort By: Extension

Choose Members:
Show Page: 1: 1126 - 1126

Extension List Members:
1122: Bob Cobb
1123: PHONE_1123

Add >>
<< Remove

Figure 27 – Pickup Group Extension List
6.11 Administration>Call Control>Codec Lists

A custom media codec list was created for the testing that included only the G.711 codec.
And for Fax /Modem calls:

**Figure 30 – CODEC List for Fax/Modem Calls**

<table>
<thead>
<tr>
<th>Choose Codecs</th>
<th>Codec List Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVl4/8000</td>
<td>L16/3000</td>
</tr>
<tr>
<td>G729/8000</td>
<td>PCMU/8000</td>
</tr>
<tr>
<td>L16/16000</td>
<td></td>
</tr>
<tr>
<td>AAC_LC/32000</td>
<td></td>
</tr>
<tr>
<td>PCMA/8000</td>
<td></td>
</tr>
<tr>
<td>G722/8000</td>
<td></td>
</tr>
<tr>
<td>BV32/16000</td>
<td></td>
</tr>
<tr>
<td>BV16/8000</td>
<td></td>
</tr>
<tr>
<td>T.38</td>
<td></td>
</tr>
<tr>
<td>Add &gt;&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;&lt; Remove</td>
<td></td>
</tr>
<tr>
<td>Move Up ^</td>
<td></td>
</tr>
<tr>
<td>Move Down v</td>
<td></td>
</tr>
</tbody>
</table>
6.12 Administration>Call Control>Options

The Options section of the Call Control screen was used to provision the DTMF Payload Type to 101, from the default of 102, for better interoperability with telephone events.

**Figure 31 – Call Control: DTMF Payload**
6.13 Administration>Auto-Attendant Menu

Figure 32 – Auto-Attendant Menu

Figure 33 – Auto-Attendant Configuration
6.14 Analog Fax/Modem

For the analog line tests, a user was created and assigned to the FXS port of the primary voice switch. The Fax Support parameter was set to prevent incoming fax calls to be re-directed to the applications server for handling.

![Image of ShoreWareTel](image)

**Figure 34 – FXS Port for Fax Testing**

![Image of Fax Support](image)

**Figure 35 – Fax Support – No Redirect**
Fax and modem calls were set to only use G.711 by specifying the appropriate codec list in the configuration of the site (Administration>Sites)—see also above.

**Figure 36 – Fax and Modem Calls CODEC**

<table>
<thead>
<tr>
<th>Bandwidth:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admission Control Bandwidth:</td>
</tr>
<tr>
<td>Intra-Site Calls:</td>
</tr>
<tr>
<td>Inter-Site Calls:</td>
</tr>
<tr>
<td>FAX and Modern Calls:</td>
</tr>
</tbody>
</table>
7 Ingate SIParator Configuration

The principal purpose of the SIParator is to register the SIP trunk to the ITSP and handle authentication of other SIP messaging like SIP INVITES. In the lab setup, VoIP media was not handled by the SIParator.

7.1 Web User Interface

The Ingate SIParator appliance is typically set-up using the company’s Startup Tool (available for downloading from their website http://www.ingate.com). This application was used for initial set-up in the lab, but subsequent customization was required using the web user interface (http or https). The default username/password of admin/changeme was maintained in the lab.

The product also supports Ingate’s CLI via SSH, but it was not the primary method of configuration employed for the ShoreTel testing. Backups of the saved running can be stored and/or loaded from both compressed and human-readable files.

In Software could not maintain the correct date and time. However, this was not essential critical issue for the PBX certification.

The SIParator has three Fast Ethernet interfaces enabling it to support several possible scenarios where it may be placed in front, behind, or in parallel with an enterprise firewall. Because the test plan called for the E-SBC to be the LAN firewall without DMZ and the ITSP’s SIP proxy and demarcation device, it was most appropriate to use the SIParator as in a modified “LAN SIParator mode” (identified as “DMZ type” in the running config). This required only one physical network interface with a single IP address assigned to it. Because of the mode, the IP interface was assigned with the same static address, default gateway and DNS settings as the PBX components in the LAN.
Begin by logging into the Ingate SIParator and opening the web menu:

- **Administration**
  - Save/Load Configuration
  - Show Configuration
  - User Administration
  - Upgrade
  - Table Look
  - Date and Time
  - Restart
  - Change Language

- **Basic Configuration**
  - Basic Configuration
  - Access Control
  - RADIUS
  - SNMP
  - Dynamic DNS Update
  - Certificates
  - Advanced Settings
  - SIParator Type

- **Network Configuration**
  - Networks and Computers
  - Default Gateways
  - All Interfaces
  - VLAN
  - Fih0
  - Fih1
  - Fih2
  - Interface Status
  - PPPoE
  - Topology

- **SIP Services**
  - Basic Settings
  - Signaling Encryption
  - Media Encryption
  - Interoperability
  - Sessions and Media
  - Remote SIP Connectivity
  - VoIP Survival

- **SIP Traffic and Users**
  - SIP Methods
  - Filtering
  - Local Registrar
  - Authentication and Accounting
  - SIP Accounts
  - Dial Plan
  - Routing
  - Time Classes
  - SIP Status
  - SIP Test
  - SIP Test Status

- **Virtual Private Networks**
  - IPsec Peers
  - IPsec Tunnels
  - IPsec Crypto
  - IPsec Key
  - IPsec Settings
  - IPsec Status
  - PPTP
  - PPTP Status

- **Quality of Service**
  - QoS Information

- **Failover**
  - Failover Settings
  - Reference Hosts
  - Failover Status

- **Logging and Tools**
  - Display Log
  - Packet Capture
  - Check Network
  - Logging Configuration
  - Log Classes
  - Log Sending

![Figure 37 – Ingate SIParator: Main Menu](image)

The VPN and Failover modules were not required for testing. However, the DSCP value for outbound SIP traffic was set to 24 (CS3) with the QoS module.

The SIParator type was “DMZ” with the optional data firewall turned off.

![Figure 38 – Ingate SIParator Type: DMZ](image)
While appearing trivial in the selected mode, networks were defined to help describe the flow of the SIP traffic through the SIParator.

![Networks and Computers](https://example.com/networks.png)

**Figure 39 – Ingate SIParator: Networks**

The surrounding part of the topology tab specifies the DMZ sub-type as simply LAN:

![Surroundings](https://example.com/surroundings.png)

**Figure 40 – Ingate SIParator: Surrounding Network Topology**
The SIP Services section includes an Interoperability tab that gives great flexibility. Minor changes to the default for the ShoreTel PBX testing were to allow large UDP packets and send response before forwarding re-INVITES. In addition, RTP codecs were limited to G.711 and telephone events.

Figure 41 – Ingate SIParator: Interoperability
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept RTP/AVP With sdescriptions</td>
<td>Recommended setting: Accept RTP/AVP with sdescriptions offer</td>
</tr>
<tr>
<td></td>
<td>- Accept RTP/AVP with sdescriptions offer</td>
</tr>
<tr>
<td></td>
<td>- Only accept RTP/AVP with sdescriptions offer</td>
</tr>
<tr>
<td>Force Record-Route for Outbound Requests</td>
<td>Recommended setting: No</td>
</tr>
<tr>
<td></td>
<td>- Force Record-Route for outbound requests: Yes, No</td>
</tr>
<tr>
<td>Force Remote TLS Connection Reuse</td>
<td>Recommended setting:</td>
</tr>
<tr>
<td></td>
<td>- DNS Name or IP Address</td>
</tr>
<tr>
<td></td>
<td>- IP Address</td>
</tr>
<tr>
<td></td>
<td>- Delete Row</td>
</tr>
<tr>
<td>Allow Large UDP Packets</td>
<td>Recommended setting:   Use TCP for large packets</td>
</tr>
<tr>
<td></td>
<td>- Allow large UDP packets</td>
</tr>
<tr>
<td>Forward CANCEL Body</td>
<td>Recommended setting: Send CANCEL without body</td>
</tr>
<tr>
<td></td>
<td>- Send CANCEL without body</td>
</tr>
<tr>
<td></td>
<td>- Forward CANCEL body</td>
</tr>
<tr>
<td>Preserve RFC 2543 Hold</td>
<td>Recommended setting: Use RFC 3264 Hold for all SDPs</td>
</tr>
<tr>
<td></td>
<td>- Use RFC 3264 Hold for all SDPs</td>
</tr>
<tr>
<td></td>
<td>- Preserve RFC 2543 Hold</td>
</tr>
<tr>
<td>Inhibit Hold</td>
<td>Recommended setting: Allow hold</td>
</tr>
<tr>
<td></td>
<td>- Allow hold</td>
</tr>
<tr>
<td></td>
<td>- Inhibit hold</td>
</tr>
<tr>
<td>Transmit RTP/AVP With sdescriptions</td>
<td>Recommended setting: Transmit RTP/SAVP with sdescriptions offer</td>
</tr>
<tr>
<td></td>
<td>- Transmit RTP/SAVP with sdescriptions offer</td>
</tr>
<tr>
<td>Force Record-Route for All Requests</td>
<td>Recommended setting: No</td>
</tr>
<tr>
<td></td>
<td>- Force Record-Route for All Requests: Yes, No</td>
</tr>
<tr>
<td>Accept TCP Marked As TLS</td>
<td>Recommended setting: Only accept TLS transport for TLS marked signaling</td>
</tr>
<tr>
<td></td>
<td>- Only accept TLS transport for TLS marked signaling</td>
</tr>
<tr>
<td></td>
<td>- Accept TCP marked as TLS</td>
</tr>
<tr>
<td>Remove Headers in 180 Responses</td>
<td>Recommended setting: Keep Record-Route and Contact headers in 180 responses</td>
</tr>
<tr>
<td></td>
<td>- Remove Record-Route and Contact headers in 180 responses</td>
</tr>
<tr>
<td>Use CANCEL Body in ACK</td>
<td>Recommended setting: Send ACK without CANCEL body</td>
</tr>
<tr>
<td></td>
<td>- Send ACK without CANCEL body</td>
</tr>
<tr>
<td></td>
<td>- Use CANCEL body in ACK</td>
</tr>
<tr>
<td>Force RFC 3264 Hold Compliance</td>
<td>Recommended setting: Preserve RFC 3264 hold type</td>
</tr>
<tr>
<td></td>
<td>- Preserve RFC 3264 hold type</td>
</tr>
<tr>
<td></td>
<td>- Force RFC 3264 hold compliance</td>
</tr>
<tr>
<td>Convert Escaped Whitespace in URIs</td>
<td>Recommended setting: Preserve “%20” in URIs</td>
</tr>
<tr>
<td></td>
<td>- Convert “%20” into whitespace in URIs</td>
</tr>
</tbody>
</table>

**Figure 42 – Ingate SIParator: Interoperability (continued)**
### Figure 43 – Ingate SIParator: Interoperability (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inhibit Hold</strong></td>
<td>Recommended setting: Allow hold</td>
</tr>
<tr>
<td>Allow hold</td>
<td></td>
</tr>
<tr>
<td>Inhibit hold</td>
<td></td>
</tr>
<tr>
<td><strong>Strip ICE Attributes</strong></td>
<td>Recommended setting: Keep ICE attributes in SDPs</td>
</tr>
<tr>
<td>Keep ICE attributes in SDPs</td>
<td></td>
</tr>
<tr>
<td>Strip ICE attributes in SDPs</td>
<td></td>
</tr>
<tr>
<td><strong>Keep User-Agent Header When Acting as B2BUA</strong></td>
<td>Recommended setting: Use Ingate SIParator as User-Agent header</td>
</tr>
<tr>
<td>Use Ingate SIParator as User-Agent header</td>
<td></td>
</tr>
<tr>
<td>Keep existing User-Agent header</td>
<td></td>
</tr>
<tr>
<td><strong>Use RTCP Attribute in SDP</strong></td>
<td>Recommended setting: Always receive RTCP one port number above RTP media</td>
</tr>
<tr>
<td>Always receive RTCP one port number above RTP media</td>
<td></td>
</tr>
<tr>
<td>Use RTCP attribute in SDP</td>
<td></td>
</tr>
<tr>
<td><strong>Media Stream Reuse Time</strong></td>
<td>Recommended setting: 0 seconds</td>
</tr>
<tr>
<td>Remember media streams after use:</td>
<td></td>
</tr>
<tr>
<td><strong>DNS Override When Redirecting on 3xx</strong></td>
<td>Recommended setting: Use DNS Override</td>
</tr>
<tr>
<td>Use DNS Override</td>
<td></td>
</tr>
<tr>
<td>Skip DNS Override</td>
<td></td>
</tr>
<tr>
<td><strong>Allow RFC 2069 Authentication</strong></td>
<td>Recommended setting: No</td>
</tr>
<tr>
<td>Allow RFC 2069 Digest authentication:</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
<tr>
<td><strong>Convert Escaped Whitespaces in URLs</strong></td>
<td>Preserve &quot;%20&quot; in URIs</td>
</tr>
<tr>
<td>Convert &quot;%20&quot; into whitespace in URIs</td>
<td></td>
</tr>
<tr>
<td><strong>Ports and the maddr Attribute</strong></td>
<td>Use original URI port when using the maddr attribute</td>
</tr>
<tr>
<td>Ignore original URI port when using the maddr attribute</td>
<td></td>
</tr>
<tr>
<td><strong>SDP Offer in re-INVITE</strong></td>
<td>Re-use old answer for SDP offer in re-INVITE</td>
</tr>
<tr>
<td>Add codes to new SDP offer in re-INVITE</td>
<td></td>
</tr>
<tr>
<td><strong>Keep To Header in Forwarded Requests</strong></td>
<td>Change To header into the forwarding target</td>
</tr>
<tr>
<td>Keep the To header when forwarding requests</td>
<td></td>
</tr>
<tr>
<td><strong>Wildcard Server Domain Certificate Match</strong></td>
<td>Recommended setting: Don't allow wildcard in server certificates</td>
</tr>
<tr>
<td>Don't allow wildcard in server certificates</td>
<td></td>
</tr>
<tr>
<td>Allow wildcard in server certificates</td>
<td></td>
</tr>
<tr>
<td><strong>Open Port 6891 for File Transfer</strong></td>
<td>Recommended setting: Do not open port 6891 unless negotiated</td>
</tr>
<tr>
<td>Do not open port 6891 unless negotiated</td>
<td></td>
</tr>
<tr>
<td>Open port 6891 at File transfer</td>
<td></td>
</tr>
<tr>
<td><strong>Pretend to Support &quot;privacy&quot; Option Tag in Proxy</strong></td>
<td>Recommended setting: Don't pretend to support &quot;privacy&quot; option tag</td>
</tr>
<tr>
<td>Don't pretend to support &quot;privacy&quot; option tag</td>
<td></td>
</tr>
<tr>
<td>Pretend to support &quot;privacy&quot; option tag</td>
<td></td>
</tr>
</tbody>
</table>
7.2 Authentication and Accounting

The SIP Traffic and Users section defined the SIP trunk authentication parameters. The IP address of the E-SBC was identified as a trusted domain with the pilot number as the registration account. Aliases were also built in the Routing tab and tied to a second “Cox” domain account for authenticating re-INVITES properly.

![Figure 44 – Ingate SiParator: SIP Authentication](image-url)
## Figure 45 – Ingate SIParator: SIP Accounts

<table>
<thead>
<tr>
<th>Username</th>
<th>Domain</th>
<th>Authentication Name</th>
<th>Display Name</th>
<th>P-Asserted-Identity</th>
<th>Password</th>
<th>Account Type</th>
<th>Delete Row</th>
</tr>
</thead>
<tbody>
<tr>
<td>6782391120</td>
<td>192.168.1.1</td>
<td>6782391120</td>
<td></td>
<td>6782391120</td>
<td></td>
<td>Register</td>
<td></td>
</tr>
<tr>
<td>Cox</td>
<td>192.168.1.1</td>
<td>6782391120</td>
<td></td>
<td></td>
<td></td>
<td>Domain</td>
<td></td>
</tr>
</tbody>
</table>

Registration Parameters

- Registration interval: 60 seconds
- Retry registration after: 300 seconds
Figure 46 – Ingate SIParator: Dial Plan
### Dial Plan (Help)

<table>
<thead>
<tr>
<th>No.</th>
<th>From Header</th>
<th>Request-URI</th>
<th>Action</th>
<th>Forward To</th>
<th>Add Prefix</th>
<th>ENUM Root</th>
<th>Time Class</th>
<th>Comment</th>
<th>Delete Row</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ShortTel</td>
<td>Outbound</td>
<td>forward</td>
<td>ShortTel-FWD</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Generic ITSP</td>
<td>-</td>
<td>forward</td>
<td>ShortTel-FWO</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add new rows: 1 row(s).

### Methods in Dial Plan (Help)

The ACK, PRACK, CANCEL, BYE, UPDATE and INFO methods cannot be handled by the Dial Plan.

**REGISTER in Dial Plan (Help)**
- Keep To headers for REGISTER requests passed through the Dial Plan
- Rewrite To headers for REGISTER requests passed through the Dial Plan

### ENUM Root (Help)

<table>
<thead>
<tr>
<th>Name</th>
<th>Subsno.</th>
<th>ENUM Root</th>
<th>Delete Row</th>
</tr>
</thead>
<tbody>
<tr>
<td>c124</td>
<td>1</td>
<td>c124.cox</td>
<td></td>
</tr>
<tr>
<td>c124</td>
<td>1</td>
<td>c124.cox</td>
<td></td>
</tr>
</tbody>
</table>

Add new rows: 1 row(s) groups with: 1 rows per group.

Figure 47 – Ingate SIParator: Dial Plan (continued)
### Figure 48 – Ingate SIParator: Routing

#### DNS Override For SIP Requests

<table>
<thead>
<tr>
<th>Domain</th>
<th>Relay To</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Name or IP Address</td>
<td>DNS Name or IP Address</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address</td>
</tr>
<tr>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td>Transport</td>
<td>Transport</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight</td>
</tr>
</tbody>
</table>

Add new rows: 1

Groups with: 1 rows per group.

#### SIP Routing Order

<table>
<thead>
<tr>
<th>No.</th>
<th>Routing Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DNS Override</td>
</tr>
<tr>
<td>2</td>
<td>Local Registrar</td>
</tr>
<tr>
<td>3</td>
<td>Dial Plan</td>
</tr>
</tbody>
</table>

Class 3xx Message Processing

- Forward all
- Follow redirects

#### Static Registrations

Requests To User | Also Forward To | Delete Row
--- | --- | ---
User | User |

Add new rows: 1

Groups with: 1 rows per group.

#### Local REFER Handling

- Always handle REFER locally
  - For clients not supporting REFER
  - For clients not supporting replaces
  - For dialogs with specified From URI
  - For dialogs with specified User-Agent

From URIs For Which REFER is Handled Locally | User-Agent Headers For Which REFER is Handled Locally
--- | ---

Add new rows: 1

### Figure 49 – Ingate SIParator: Routing (continued)

#### User Routing

<table>
<thead>
<tr>
<th>User</th>
<th>Alias</th>
<th>Restrict Incoming Callers</th>
<th>Forward Action</th>
<th>Forward To</th>
<th>Send To Voice Mail</th>
<th>Time Class</th>
<th>Comment</th>
<th>Delete Row</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cox@192.168.1.1</td>
<td>6782391211,678</td>
<td>No</td>
<td>Forward</td>
<td>$in user@192</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7.3 SIParator Configuration File

The following is the SIParator configuration proven in the Cox certification lab.

```
# coding: utf-8
#
# Unitname: CoxLab-ShoreTel
# Product: Ingate SIParator 19
# Version: 4.8.4
# Product-type: S
# Product-subtype: DMZ
# Serial: IG-092-022-6031-2
# Interfaces: eth0 eth1 eth2
# Modules: failover vpn sip qos siptrunk sipswitch
# Timestamp: 2010-11-11 19:48:05

load-factory --all

# cert.cas
clear-table cert.cas

# cert.own_certs
clear-table cert.own_certs

# config.allow_config
clear-table config.allow_config
add-row config.allow_config {id 1} client_network=192.168.1.0/255.255.255.0 \   
   from_tunnel=- http=on https=off logclass=Local number=1 ssh=off
add-row config.allow_config {id 2} client_network=10.0.0.0/255.0.0.0 \   
   from_tunnel=- http=on https=off logclass=Local number=2 ssh=off

# config.allow_via_interface
modify-row config.allow_via_interface 1 config_on=on interface=eth0
modify-row config.allow_via_interface 2 config_on=off interface=eth1
modify-row config.allow_via_interface 3 config_on=off interface=eth2

# config.auth_logclass
modify-row config.auth_logclass 1 logclass=Local

# config.authentication
modify-row config.authentication 1 auth_type=local

# config.http_servers
modify-row config.http_servers 1 ip=inside port=80

# config.https_servers
modify-row config.https_servers 1 cert=- ip=- port=443

# config.mgmt_logclass
modify-row config.mgmt_logclass 1 logclass=Local

# config.ssh_servers
modify-row config.ssh_servers 1 ip=- port=22

# failover.iface_ref_hosts
clear-table failover.iface_ref_hosts

# firewall.blind_route_policy
modify-row firewall.blind_route_policy 1 action=discard
```
# firewall.broadcast_logclass
modify-row firewall.broadcast_logclass 1 logclass=Local

# firewall.default_policy
modify-row firewall.default_policy 1 action=discard

# firewall.dhcp_logclass
modify-row firewall.dhcp_logclass 1 logclass=Local

# firewall.network_groups
clear-table firewall.network_groups
add-row firewall.network_groups {id 1} interface=- lower_ip=192.168.1.0
   name=LAN subgroup=- upper_ip=192.168.1.255
add-row firewall.network_groups {id 3} interface=- lower_ip=192.168.1.1
   name=ITSP_IP subgroup=- upper_ip=192.168.1.1
add-row firewall.network_groups {id 4} interface=- lower_ip=192.168.1.10
   name=ShoreTel subgroup=- upper_ip=""

# firewall.own_logclass
modify-row firewall.own_logclass 1 logclass=Local

# firewall.ping_policy
modify-row firewall.ping_policy 1 policy=always

# firewall.policy_logclass
modify-row firewall.policy_logclass 1 logclass=Local

# firewall.services
clear-table firewall.services
add-row firewall.services {id 1} client_ports="" fwtype=static ixmptype=""
   name=ah protocol=AH server_ports="" subgroup=-
add-row firewall.services {id 2} client_ports=1024-65535 fwtype=dynamic
   name=daytime protocol=TCP server_ports=13 subgroup=-
add-row firewall.services {id 3} client_ports=68 fwtype=static ixmptype=""
   name=dhcp protocol=UDP server_ports=67 subgroup=-
add-row firewall.services {id 4} client_ports="" fwtype=static ixmptype=""
   name=dns protocol=UDP server_ports=53 subgroup=-
add-row firewall.services {id 5} client_ports=53 fwtype=static ixmptype=""
   name=dns-reply protocol=UDP server_ports=""53,1024-65535" subgroup=-
add-row firewall.services {id 6} client_ports="" fwtype=dynamic ixmptype=""
   name=dns-tcp protocol=TCP server_ports=53 subgroup=-
add-row firewall.services {id 7} client_ports="" fwtype=static ixmptype=0
   name=echo-reply protocol=ICMP server_ports="" subgroup=-
add-row firewall.services {id 8} client_ports="" fwtype=static ixmptype=8
   name=echo-request protocol=ICMP server_ports="" subgroup=-
add-row firewall.services {id 9} client_ports="" fwtype=static ixmptype=""
   name=esp protocol=ESP server_ports="" subgroup=-
add-row firewall.services {id 10} client_ports=1024-65535 fwtype=dynamic
   name=finger protocol=TCP server_ports=79 subgroup=-
add-row firewall.services {id 11} client_ports=1024-65535 fwtype=ftp
   name=ftp protocol=TCP server_ports=21 subgroup=-
add-row firewall.services {id 12} client_ports=1024-65535 fwtype=dynamic
   name=high-high protocol=TCP server_ports=""1024-65535" subgroup=-
add-row firewall.services {id 13} client_ports=1024-65535 fwtype=dynamic
   name=http protocol=TCP server_ports=80 subgroup=-
add-row firewall.services {id 14} client_ports=1024-65535 fwtype=dynamic
   name=https protocol=TCP server_ports=443 subgroup=-
ixmptype='"' name=https protocol=TCP server_ports=443 subgroup=-
add-row firewall.services {id 15} client_ports='"' fwtype=static  
ximptype=0-120 name=icmp protocol=ICMP server_ports='"' subgroup=-
add-row firewall.services {id 16} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=ident protocol=TCP server_ports=113 subgroup=-
add-row firewall.services {id 17} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=imap protocol=TCP server_ports=143 subgroup=-
add-row firewall.services {id 18} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=imaps protocol=TCP server_ports=993 subgroup=-
add-row firewall.services {id 19} client_ports='"' fwtype=static ixmptype='"'  
name=ipv6to4 protocol=IPv6 server_ports='"' subgroup=-
add-row firewall.services {id 20} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=nfs-tcp protocol=TCP server_ports=2049 subgroup=-
add-row firewall.services {id 21} client_ports=1024-65535 fwtype=static  
ximptype='"' name=nfs-udp protocol=UDP server_ports=2049 subgroup=-
add-row firewall.services {id 22} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=nntp protocol=TCP server_ports=119 subgroup=-
add-row firewall.services {id 23} client_ports=123 fwtype=static ixmptype='"'  
name=ntp protocol=UDP server_ports=123 subgroup=-
add-row firewall.services {id 24} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=pop3 protocol=TCP server_ports=110 subgroup=-
add-row firewall.services {id 25} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=pop3s protocol=TCP server_ports=995 subgroup=-
add-row firewall.services {id 26} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=smtp protocol=TCP server_ports=25 subgroup=-
add-row firewall.services {id 27} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=ssh protocol=TCP server_ports=22 subgroup=-
add-row firewall.services {id 28} client_ports=0-65535 fwtype=dynamic  
ximptype='"' name=tcp protocol=TCP server_ports=0-65535 subgroup=-
add-row firewall.services {id 29} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=telnet protocol=TCP server_ports=23 subgroup=-
add-row firewall.services {id 30} client_ports='"' fwtype=static ixmptype=11  
name=time-exceeded protocol=ICMP server_ports='"' subgroup=-
add-row firewall.services {id 31} client_ports=1024-65535 fwtype=static  
ximptype='"' name=traceroute protocol=UDP server_ports=33434-33690  
subgroup=-
add-row firewall.services {id 32} client_ports='"' fwtype=static  
ximptype='3,11' name=traceroute-reply protocol=ICMP server_ports='"'  
subgroup=-
add-row firewall.services {id 33} client_ports=0-65535 fwtype=static  
ximptype='"' name=udp protocol=UDP server_ports=0-65535 subgroup=-
add-row firewall.services {id 34} client_ports='"' fwtype=-- ixmptype='"'  
name=www protocol=-- server_ports='"' subgroup=http
add-row firewall.services {id 35} client_ports='"' fwtype=-- ixmptype='"'  
name=www protocol=-- server_ports='"' subgroup=https
add-row firewall.services {id 36} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=x11-display0 protocol=TCP server_ports=6000  
subgroup=-
add-row firewall.services {id 37} client_ports='"' fwtype=-- ixmptype='"'  
name=icmp/udp/tcp protocol=-- server_ports='"' subgroup=icmp
add-row firewall.services {id 38} client_ports='"' fwtype=-- ixmptype='"'  
name=icmp/udp/tcp protocol=-- server_ports='"' subgroup=udp
add-row firewall.services {id 39} client_ports='"' fwtype=-- ixmptype='"'  
name=icmp/udp/tcp protocol=-- server_ports='"' subgroup=tcp
add-row firewall.services {id 40} client_ports=1024-65535 fwtype=dynamic  
ximptype='"' name=kerberos-udp protocol=UDP server_ports=88  
subgroup=-
add-row firewall.services {id 41} client_ports=1024-65535 fwtype=dynamic  
name=www protocol=https server_ports=80 subgroup=https
ixmptype="" name=kerberos-tcp protocol=TCP server_ports=88 \
subgroup=-
add-row firewall.services {id 42} client_ports="" fwtype=-- ixmptype="" \
name=kerberos protocol=- server_ports="" subgroup=kerberos-udp
add-row firewall.services {id 43} client_ports="" fwtype=-- ixmptype="" \
name=kerberos protocol=- server_ports="" subgroup=kerberos-tcp
add-row firewall.services {id 44} client_ports=1024-65535 fwtype=dynamic \
ixmptype="" name=ldap-udp protocol=UDP server_ports=389 subgroup=-
add-row firewall.services {id 45} client_ports=1024-65535 fwtype=dynamic \
ixmptype="" name=ldap-tcp protocol=TCP server_ports=389 subgroup=-
add-row firewall.services {id 46} client_ports="" fwtype=-- ixmptype="" \
name=ldap protocol=- server_ports="" subgroup=ldap-udp
add-row firewall.services {id 47} client_ports="" fwtype=-- ixmptype="" \
name=ldap protocol=- server_ports="" subgroup=ldap-tcp
add-row firewall.services {id 48} client_ports=1024-65535 fwtype=dynamic \
ixmptype="" name=ms-rpc protocol=TCP server_ports=135 subgroup=-
add-row firewall.services {id 49} client_ports=1024-65535 fwtype=pptp \
ixmptype="" name=pptp protocol=TCP server_ports=1723 subgroup=-
add-row firewall.services {id 50} client_ports=1024-65535 fwtype=dynamic \
ixmptype="" name=rsp protocol=TCP server_ports=1723 subgroup=-
add-row firewall.services {id 51} client_ports=1024-65535 fwtype=dynamic \
ixmptype="" name=smb protocol=TCP server_ports=445 subgroup=-
add-row firewall.services {id 52} client_ports="" fwtype=-- ixmptype="" \
name=www/dns protocol=-- server_ports="" subgroup=www
add-row firewall.services {id 53} client_ports="" fwtype=-- ixmptype="" \
name=www/dns protocol=-- server_ports="" subgroup=dns
add-row firewall.services {id 54} client_ports="" fwtype=-- ixmptype="" \
name=www/dns protocol=-- server_ports="" subgroup=dns-tcp
add-row firewall.services {id 55} client_ports=1024-65535 fwtype=tftp \
ixmptype="" name=tftp protocol=TCP server_ports=554 subgroup=-
add-row firewall.services {id 56} client_ports=1024-65535 fwtype=tftp \
ixmptype="" name=tftp protocol=UDP server_ports=69 subgroup=-

# firewall.spoofing_logclass
modify-row firewall.spoofing_logclass 1 logclass=Local

# firewall.timeclasses
clear-table firewall.timeclasses
add-row firewall.timeclasses {id 1} from_day=monday from_time=00:00 \
name=24/7 to_day=sunday to_time=24:00

# ipsec.crypto_def
clear-table ipsec.crypto_def
add-row ipsec.crypto_def {id 1} auth=md5 encryption=3des name=3DES-MD5
add-row ipsec.crypto_def {id 2} auth=sha1 encryption=3des name=3DES-SHA1
add-row ipsec.crypto_def {id 3} auth=md5 encryption=aes128 name=AES128-MD5
add-row ipsec.crypto_def {id 4} auth=sha1 encryption=aes128 name=AES128-SHA1
add-row ipsec.crypto_def {id 5} auth=md5 encryption=aes256 name=AES256-MD5
add-row ipsec.crypto_def {id 6} auth=sha1 encryption=aes256 name=AES256-SHA1
add-row ipsec.crypto_def {id 7} auth=md5 encryption=null name=NULL-MD5
add-row ipsec.crypto_def {id 8} auth=sha1 encryption=null name=NULL-SHA1

# ipsec.esp_proposals
clear-table ipsec.esp_proposals
add-row ipsec.esp_proposals {id 1} crypto=AES128-SHA1 name=AES/3DES number=1
add-row ipsec.esp_proposals {id 2} crypto=AES128-MD5 name=AES/3DES number=2
add-row ipsec.esp_proposals {id 3} crypto=3DES-SHA1 name=AES/3DES number=3
add-row ipsec.esp_proposals {id 4} crypto=3DES-MD5 name=AES/3DES number=4
add-row ipsec.esp_proposals {id 5} crypto=NULL-MD5 name=NULL number=1
add-row ipsec.esp_proposals {id 6} crypto=NULL-SHA1 name=NULL number=2

# ipsec.espah_logclass
modify-row ipsec.espah_logclass 1 logclass=-

# ipsec.ike_logclass
modify-row ipsec.ike_logclass 1 logclass=Local

# ipsec.ike_proposals
clear-table ipsec.ike_proposals
add-row ipsec.ike_proposals {id 1} crypto=AES128-SHA1 group=modp1536 
  name=AES/3DES number=1
add-row ipsec.ike_proposals {id 2} crypto=AES128-SHA1 group=modp1024 
  name=AES/3DES number=2
add-row ipsec.ike_proposals {id 3} crypto=AES128-MD5 group=modp1536 
  name=AES/3DES number=3
add-row ipsec.ike_proposals {id 4} crypto=AES128-MD5 group=modp1024 
  name=AES/3DES number=4
add-row ipsec.ike_proposals {id 5} crypto=3DES-SHA1 group=modp1536 
  name=AES/3DES number=5
add-row ipsec.ike_proposals {id 6} crypto=3DES-SHA1 group=modp1024 
  name=AES/3DES number=6
add-row ipsec.ike_proposals {id 7} crypto=3DES-MD5 group=modp1536 
  name=AES/3DES number=7
add-row ipsec.ike_proposals {id 8} crypto=3DES-MD5 group=modp1024 
  name=AES/3DES number=8

# ipsec.ipsec_nets
clear-table ipsec.ipsec_nets

# ipsec.nat_t_keepalive
modify-row ipsec.nat_t_keepalive 1 force=on interval=60

# ipsec.peers
clear-table ipsec.peers

# ipsec.pluto_logclass
modify-row ipsec.pluto_logclass 1 logclass=Local

# ipsec.plutoverbose_logclass
modify-row ipsec.plutoverbose_logclass 1 logclass=-

# ipsec.radiusauth_server
modify-row ipsec.radiusauth_server 1 cert=- ip=- port=443

# ipsec.tunneled_nets
clear-table ipsec.tunneled_nets

# ipsec.userauth_logclass
modify-row ipsec.userauth_logclass 1 logclass=Local

# ipsec.x509_cacerts
clear-table ipsec.x509_cacerts

# ipsec.x509_cert
modify-row ipsec.x509_cert 1 cert=-
# misc.conntrack_timeouts
modify-row misc.conntrack_timeouts 1 icmp=30 tcp_established=432000 udp=10 \ 
    udp_stream=180

# misc.default_domain
modify-row misc.default_domain 1 domain=""

# misc.dns_servers
clear-table misc.dns_servers
add-row misc.dns_servers {id 1} number=1 server=68.0.3.2

# misc.dyndns
modify-row misc.dyndns 1 backup=off enabled=off ip=- mx="" offline=off \ 
    password="" service=- user="" wildcard=off

# misc.dyndns_name
clear-table misc.dyndns_name

# misc.fversion
modify-row misc.fversion 1 enabled=on

# misc.ntp_servers
clear-table misc.ntp_servers
add-row misc.ntp_servers {id 1} server="time.nist.gov|192.43.244.18|

# misc.unitname
modify-row misc.unitname 1 unitname=CoxLab-ShoreTel

# misc.use_ntp
modify-row misc.use_ntp 1 enabled=on

# monitor.cpuload_level_alarm
modify-row monitor.cpuload_level_alarm 1 max_cpuload="" ok_cpuload=""

# monitor.email_alert_logclass
modify-row monitor.email_alert_logclass 1 logclass=Local

# monitor.email_server
modify-row monitor.email_server 1 server=""

# monitor.hardware_logclass
modify-row monitor.hardware_logclass 1 logclass=Local

# monitor.logclasses
clear-table monitor.logclasses
add-row monitor.logclasses {id 1} email="" facility=- level=- local=on \ 
    name=Local
add-row monitor.logclasses {id 2} email="" facility=Auth level=Notice \ 
    local=on name="Local+Syslog"
add-row monitor.logclasses {id 3} email="" facility=Auth level=Notice \ 
    local=off name=Syslog

# monitor.memory_level_alarm
modify-row monitor.memory_level_alarm 1 max_memory="" ok_memory=""

# monitor.radius_errors_logclass
modify-row monitor.radius_errors_logclass 1 logclass=Local
# monitor.sip_level_alarms
modify-row monitor.sip_level_alarms 1 max_registered_users="" \ 
 max_sessions="" ok_registered_users="" ok_sessions=""

# monitor.snmp_agent_address
modify-row monitor.snmp_agent_address 1 snmpagentip=-

# monitor.snmp_agent_logclass
modify-row monitor.snmp_agent_logclass 1 logclass=Local

# monitor.snmp_contact_person
modify-row monitor.snmp_contact_person 1 snmp_contact_person=""

# monitor.snmp_management_stations
modify-row monitor.snmp_management_stations 1 client_netgroup=-

# monitor.snmp_node_location
modify-row monitor.snmp_node_location 1 snmp_node_location=""

# monitor.snmp_packet_logclass
modify-row monitor.snmp_packet_logclass 1 logclass=Local

# monitor.snmp_trap_receivers
clear-table monitor.snmp_trap_receivers

# monitor.snmp_trap_sending
modify-row monitor.snmp_trap_sending 1 enabled=off

# monitor.snmp_v1v2c_access
modify-row monitor.snmp_v1v2c_access 1 enabled=off

# monitor.snmp_v1v2c_auth
clear-table monitor.snmp_v1v2c_auth

# monitor.snmp_v3_access
modify-row monitor.snmp_v3_access 1 enabled=off

# monitor.snmp_v3_auth
clear-table monitor.snmp_v3_auth

# monitor.syslog_servers
clear-table monitor.syslog_servers

# monitor.watchdogs
modify-row monitor.watchdogs 1 enabled=off service=sipfw

# network.alias_addresses
clear-table network.alias_addresses

# network.discard_weird.fragments
modify network.discard_weird_fragments 1 enabled=on

# network.extra_default_gateways
clear-network extra_default_gateways

# network.interfaces
modify-network interfaces 1 autoneg=auto enabled=on interface=eth0 \ 
 name=inside
modify-row network.interfaces 2 autoneg=auto enabled=off interface=eth1 \ name=Ethernet1
modify-row network.interfaces 3 autoneg=auto enabled=off interface=eth2 \ name=Ethernet2

# network.local_nets
clear-table network.local_nets
add-row network.local_nets {id 1} address=192.168.1.250/255.255.255.0 \ interface=eth0 name=inside vlanid=""

# network.pppoe
modify-row network.pppoe 1 lcp_echo_interval=10 logclass=Local password="" \ service="" user=""

# network.proxy_arp
clear-table network.proxy_arp

# network.route_test_servers
clear-table network.route_test_servers

# network.routes
clear-table network.routes
add-row network.routes {id 1} destination=default/ gateway=192.168.1.1 \ interface=eth0 priority=""

# network.vlans
clear-table network.vlans

# pptp.gre_logclass
modify-row pptp.gre_logclass 1 logclass=-

# pptp.pptp_enable
modify-row pptp.pptp_enable 1 enabled=off

# pptp.pptp_logclass
modify-row pptp.pptp_logclass 1 logclass=Local

# pptp.pptp_nets
modify-row pptp.pptp_nets 1 client_netgroup=- dns1="" dns2="" \ lcp_echo_interval="" local_addr=- wins1="" wins2=""

# pptp.pptp_serverip
modify-row pptp.pptp_serverip 1 ip=-

# pptp.pptp_users
clear-table pptp.pptp_users

# pptp.pptpneg_logclass
modify-row pptp.pptpneg_logclass 1 logclass=Local

# qos.bandwidths
modify-row qos.bandwidths 1 egress_bandwidth=1000 egress_enabled=off \ egress_reserve_sip_media="" egress_reserve_sip_media_emergency="" \ ingress_bandwidth="" ingress_enabled=off \ ingress_reserve_sip_media="" ingress_reserve_sip_media_emergency="" \ interface=eth0
modify-row qos.bandwidths 2 egress_bandwidth="" egress_enabled=off \ egress_reserve_sip_media="" egress_reserve_sip_media_emergency="" \
ingress_bandwidth="" ingress_enabled=off \ 
ingress_reserve_sip_media="" ingress_reserve_sip_media_emergency="" \ interface=eth1
modify-row qos.bandwidths 3 egress_bandwidth="" egress_enabled=off \ 
egress_reserve_sip_media="" egress_reserve_sip_media_emergency="" \ interface=eth2

# qos.classes
clear-table qos.classes
add-row qos.classes {id 1} client_netgroup=- dscp="" max_packet_size="" \ 
min_packet_size="" name="SIP Signaling" number=1 server_netgroup=- \ 
service=- sip=signaling tos=-

# qos.egress_default_queueing
modify-row qos.egress_default_queueing 1 interface=eth0 limit="" queue=prio8 \ 
rates=""
modify-row qos.egress_default_queueing 2 interface=eth1 limit="" queue=prio8 \ 
rates=""
modify-row qos.egress_default_queueing 3 interface=eth2 limit="" queue=prio8 \ 
rates=""

# qos.egress_queueing
clear-table qos.egress_queueing
add-row qos.egress_queueing {id 1} cname="SIP Signaling" interface=eth0 \ 
limit="" queue=prio1 rate=""

# qos.ingress_default_queueing
modify-row qos.ingress_default_queueing 1 interface=eth0 limit="" queue=prio8 rate=""
modify-row qos.ingress_default_queueing 2 interface=eth1 limit="" queue=prio8 rate=""
modify-row qos.ingress_default_queueing 3 interface=eth2 limit="" queue=prio8 rate=""

# qos.ingress_queueing
clear-table qos.ingress_queueing

# qos.sip_cac
modify-row qos.sip_cac 1 enabled=off

# qos.status
modify-row qos.status 1 prio_save=0 type=priority

# qos.tagging
clear-table qos.tagging
add-row qos.tagging {id 1} cname="SIP Signaling" dscp=24 tos=-

# sip.accelerated_tls
modify-row sip.accelerated_tls 1 enabled=off

# sip.active
modify-row sip.active 1 enabled=on

# sip.add_expire_header
modify-row sip.add_expire_header 1 action=never
# sip.allowed_codecs

```bash
clear-table sip.allowed_codecs
add-row sip.allowed_codecs {id 15} allow=on bandwidth="" name=PCMU \type=audio
add-row sip.allowed_codecs {id 17} allow=on bandwidth="" \name=telephone-event type=audio
```

# sip.asserted_identity

```bash
modify-row sip.asserted_identity 1 enabled=on
```

# sip.auth_methods

```bash
clear-table sip.auth_methods
add-row sip.auth_methods {id 1} allow=on auth=off method=BYE traffic_to=both
add-row sip.auth_methods {id 2} allow=on auth=off method=FEATURE \traffic_to=both
add-row sip.auth_methods {id 3} allow=on auth=off method=INFO \traffic_to=both
add-row sip.auth_methods {id 4} allow=on auth=off method=INVITE \traffic_to=both
add-row sip.auth_methods {id 5} allow=on auth=off method=MESSAGE \traffic_to=both
add-row sip.auth_methods {id 6} allow=on auth=off method=NOTIFY \traffic_to=both
add-row sip.auth_methods {id 7} allow=on auth=off method=OPTIONS \traffic_to=both
add-row sip.auth_methods {id 8} allow=on auth=off method=PRACK \traffic_to=both
add-row sip.auth_methods {id 9} allow=on auth=off method=PUBLISH \traffic_to=both
add-row sip.auth_methods {id 10} allow=on auth=off method=REFER \traffic_to=both
add-row sip.auth_methods {id 11} allow=on auth=off method=REGISTER \traffic_to=both
add-row sip.auth_methods {id 12} allow=on auth=off method=SERVICE \traffic_to=both
add-row sip.auth_methods {id 13} allow=on auth=off method=SUBSCRIBE \traffic_to=both
add-row sip.auth_methods {id 14} allow=on auth=off method=UPDATE \traffic_to=both
```

# sip.b2bua_offer_from_template

```bash
modify-row sip.b2bua_offer_from_template 1 enabled=off
```

# sip.b2bua_pending_timeout

```bash
modify-row sip.b2bua_pending_timeout 1 timeout=2
```

# sip.b2bua_reinvites_end_to_end

```bash
modify-row sip.b2bua_reinvites_end_to_end 1 enabled=off
```

# sip.codec_filtering

```bash
modify-row sip.codec_filtering 1 enabled=on
```

# sip.default_gateway

```bash
clear-table sip.data_interfaces
```

# sip.data_interfaces

```bash
modify-row sip.default_gateway 1 gateway=-
```
# sip.dialing_domains
clear-table sip.dialing_domains

# sip.dns_override_on_recursion
modify-row sip.dns_override_on_recursion 1 enabled=on

# sip.emergency
modify-row sip.emergency 1 emergency=911

# sip.extern_radius_db
modify-row sip.extern_radius_db 1 client_netgroup=- db_type=local

# sip.external_relay
clear-table sip.external_relay

# sip.fake_proxy_supported_privacy
modify-row sip.fake_proxy_supported_privacy 1 enabled=off

# sip.fix_file_transfer_port
modify-row sip.fix_file_transfer_port 1 enabled=off

# sip.force_3264_hold
modify-row sip.force_3264_hold 1 enabled=off

# sip.force_modify
clear-table sip.force_modify

# sip.forward_cancel_body
modify-row sip.forward_cancel_body 1 enabled=off

# sip.forward_to_header
modify-row sip.forward_to_header 1 enabled=off

# sip.forward_user_agent
modify-row sip.forward_user_agent 1 enabled=off

# sip.global_policies
modify-row sip.global_policies 1 sip_policy=proxy sipauth_allow_rfc2069=off \ sipauth_enabled=on sipauth_realm=BroadWorks

# sip.header_filter_default
modify-row sip.header_filter_default 1 action=process

# sip.header_filter_rules
clear-table sip.header_filter_rules

# sip.ignore_uri_port_when_maddr
modify-row sip.ignore_uri_port_when_maddr 1 enabled=off

# sip.inhibit_hold
modify-row sip.inhibit_hold 1 enabled=off

# sip.large_udp
modify-row sip.large_udp 1 enabled=on

# sip.listen
clear-table sip.listen
# sip.local_domains
clear-table sip.local_domains
add-row sip.local_domains {id 1} domain=192.168.1.250

# sip.loose_refer_to
modify-row sip.loose_refer_to 1 enabled=off

# sip.loose_user_name_check
modify-row sip.loose_user_name_check 1 enabled=off

# sip.lr_true
modify-row sip.lr_true 1 enabled=off

# sip.media_encryption_policy
modify-row sip.media_encryption_policy 1 allowed_suites=-

# sip.media_encryption_rules
clear-table sip.media_encryption_rules

# sip.media_encryption_settings
modify-row sip.media_encryption_settings 1 accept_avp_sdescriptions=on \ enabled=off prefer_rtp_savp=off transmit_avp_sdescriptions=off

# sip.media_encryption_suite
clear-table sip.media_encryption_suite
add-row sip.media_encryption_suite {id 1} name=Cleartext suite=cleartext
add-row sip.media_encryption_suite {id 2} name="Encrypted (transcodable)" \ suite=sdescriptions-AES_CM_128_HMAC_SHA1_32
add-row sip.media_encryption_suite {id 3} name="Encrypted (transcodable)" \ suite=sdescriptions-AES_CM_128_HMAC_SHA1_80
add-row sip.media_encryption_suite {id 4} name=SRTP \ suite=sdescriptions-AES_CM_128_HMAC_SHA1_32
add-row sip.media_encryption_suite {id 5} name=SRTP \ suite=sdescriptions-AES_CM_128_HMAC_SHA1_80
add-row sip.media_encryption_suite {id 6} name=SRTP \ suite=sdescriptions-F8_128_HMAC_SHA1_80
add-row sip.media_encryption_suite {id 7} name="Any (transcodable)" \ suite=cleartext
add-row sip.media_encryption_suite {id 8} name="Any (transcodable)" \ suite=sdescriptions-AES_CM_128_HMAC_SHA1_32
add-row sip.media_encryption_suite {id 9} name="Any (transcodable)" \ suite=sdescriptions-AES_CM_128_HMAC_SHA1_80

# sip.media_ports
modify-row sip.media_ports 1 ports_lower=58024 ports_upper=60999

# sip.media_restriction
modify-row sip.media_restriction 1 medialock=lock

# sip.media_stream_linger
modify-row sip.media_stream_linger 1 time=0

# sip.media_timeouts
modify-row sip.media_timeouts 1 oneway="" rtcp="" rtp="" tear_down=off

# sip.message
modify-row sip.message 1 max_message_size=131072
# sip.mfull
modify-row sip.mfull 1 enabled=on

# sip.mimetypes
clear-table sip.mimetypes
add-row sip.mimetypes {id 1} allowed=off mimetype="application/SOAP+xml"
add-row sip.mimetypes {id 2} allowed=off mimetype="application/pidf+xml"
add-row sip.mimetypes {id 3} allowed=off \  mimetype="application/vnd-microsoft-roaming-acls+xml"
add-row sip.mimetypes {id 4} allowed=off \  mimetype="application/vnd-microsoft-roaming-contacts+xml"
add-row sip.mimetypes {id 5} allowed=off \  mimetype="application/vnd-microsoft-roaming-provisioning+xml"
add-row sip.mimetypes {id 6} allowed=off mimetype=application/xml
add-row sip.mimetypes {id 7} allowed=off mimetype=image/jpeg
add-row sip.mimetypes {id 8} allowed=off mimetype=text/html
add-row sip.mimetypes {id 9} allowed=off mimetype=text/lpidf
add-row sip.mimetypes {id 10} allowed=off mimetype=text/plain
add-row sip.mimetypes {id 11} allowed=off mimetype=text/xml
add-row sip.mimetypes {id 12} allowed=off mimetype="text/xml+msrtc.pidf"
add-row sip.mimetypes {id 13} allowed=off mimetype="text/xml+msrtc.wpended"
add-row sip.mimetypes {id 14} allowed=off mimetype="application/adr1+xml"
add-row sip.mimetypes {id 15} allowed=off mimetype=message/sipfrag
add-row sip.mimetypes {id 16} allowed=on mimetype=*
add-row sip.mimetypes {id 17} allowed=on mimetype=*

# sip.monitor_server
clear-table sip.monitor_server

# sip.music_on_hold
modify-row sip.music_on_hold 1 enabled=off

# sip.music_on_hold_servers
modify-row sip.music_on_hold_servers 1 port="" transport=- userdomain=""

# sip.option_timeout
modify-row sip.option_timeout 1 timeout=41

# sip.outbound_proxy
clear-table sip.outbound_proxy

# sip.pai_use_from
modify-row sip.pai_use_from 1 enabled=off

# sip.percent20_to_whitespace
modify-row sip.percent20_to_whitespace 1 enabled=on

# sip.preserve_2543_hold
modify-row sip.preserve_2543_hold 1 enabled=off

# sip.public_ip
modify-row sip.public_ip 1 ip=""

# sip.radius_acct
modify-row sip.radius_acct 1 diversion=off enabled=off media=off \  p_asserted_identity=off remote_party_id=off

# sip.recurse_on_3xx_in_b2bua
modify-row sip.recurse_on_3xx_in_b2bua 1 enabled=off

# sip.redirect_server
modify-row sip.redirect_server 1 server=

# sip.referto_replacement
modify-row sip.referto_replacement 1 domain="" type=never

# sip.registrar_limits
modify-row sip.registrar_limits 1 maxRegistrations=5 maxUsers="" registrationTimeout=3600

# sip.relay_rules
clear-table sip.relay_rules

# sip.remove_via
clear-table sip.remove_via

# sip.reply_config
modify-row sip.reply_config 1 class3=all

# sip.rewrite_to_for_register_in_dp
modify-row sip.rewrite_to_for_register_in_dp 1 enabled=off

# sip.ringback
modify-row sip.ringback 1 action=if_transferee_hangs_up tone_type=us

# sip.route180
modify-row sip.route180 1 enabled=off

# sip.route_use_sport
clear-table sip.route_use_sport

# sip.routing_order
modify-row sip.routing_order 1 function=dns_override number=1
modify-row sip.routing_order 2 function=registrar number=2
modify-row sip.routing_order 3 function=dialplan number=3

# sip.rroute_always
modify-row sip.rroute_always 1 enabled=off

# sip.rroute_outbound
modify-row sip.rroute_outbound 1 enabled=off

# sip.session_limits
modify-row sip.session_limits 1 maxSipSessions="" maxStreamsPerReq=6 sessionTimeout=14400

# sip.signal_address_for_destination
clear-table sip.signal_address_for_destination

# sip.sip_alias
clear-table sip.sip_alias

# sip.sip_errors_logclass
modify-row sip.sip_errors_logclass 1 logclass=Local

# sip.sip_license_logclass
modify-row sip.sip_license_logclass 1 logclass=Local
    
    # sip.sip_media_logclass
    modify-row sip.sip_media_logclass 1 logclass=Local
    
    # sip.sip_message_logclass
    modify-row sip.sip_message_logclass 1 logclass=Local
    
    # sip.sip_signaling_logclass
    modify-row sip.sip_signaling_logclass 1 logclass=Local
    
    # sip.sip_verbose_logclass
    modify-row sip.sip_verbose_logclass 1 logclass=Local
    
    # sip.st_type
    modify-row sip.st_type 1 st_type=DMZ
    
    # sip.strip_ice_attributes
    modify-row sip.strip_ice_attributes 1 enabled=off
    
    # sip.surroundings
    clear-table sip.surroundings
    add-row sip.surroundings {id 1} negotiator_netgroup=- surrounding_netgroup=LAN
    
    # sip.tcp_timeout
    modify-row sip.tcp_timeout 1 tcp_timeout=90
    
    # sip.tel_to_outbound_proxy
    modify-row sip.tel_to_outbound_proxy 1 enabled=off
    
    # sip.testua
    modify-row sip.testua 1 display_name="" uri=sip:testagent@anonymous.invalid
    
    # sip.testua_acl
    clear-table sip.testua_acl
    
    # sip.testua_active
    modify-row sip.testua_active 1 enabled=off
    
    # sip.testua_client
    modify-row sip.testua_client 1 call_duration=30 call_interval=3600 \ call_preferred_pt=pcmu call_ptime=20 call_to=""
    
    # sip.testua_client_active
    modify-row sip.testua_client_active 1 enabled=off
    
    # sip.testua_server_active
    modify-row sip.testua_server_active 1 enabled=off
    
    # sip.tls_cacerts
    clear-table sip.tls_cacerts
    
    # sip.tls_client_cfg
    modify-row sip.tls_client_cfg 1 client_methods="SSLv2:SSLv3,TLSv1" \ default_cert=-
    
    # sip.tls_server_cfg
clear-table sip.tls_server_cfg

# sip.tls_settings
modify-row sip.tls_settings 1 check_x509_server_subject=on \ 
        check_x509_server_wildcard=off

# sip.transaction_config
modify-row sip.transaction_config 1 default_timeout=40 inv_rt=6 \ 
        max_timeout=60 ninv_rt=10 timer_a=0.5

# sip.trusted_domain
clear-table sip.trusted_domain
add-row sip.trusted_domain {id 1} transport=any trusted_netgroup=ITSP_IP

# sip.ua_register
modify-row sip.ua_register 1 expires=60 retry_time=300

# sip.uri_encoding
modify-row sip.uri_encoding 1 type=db

# sip.use_cancel_body_in_ack
modify-row sip.use_cancel_body_in_ack 1 enabled=off

# sip.use_rtcp_attribute
modify-row sip.use_rtcp_attribute 1 enabled=off

# sip.use_tls
modify-row sip.use_tls 1 tlsconf=no_tls

# sipswitch.accounts
clear-table sipswitch.accounts
add-row sipswitch.accounts {id 1} auth_name=6782391120 display_name="" \ 
        domain=192.168.1.1 p_asserted_id=6782391120 password=password \ 
        type=reg user=6782391120
add-row sipswitch.accounts {id 12} auth_name=6782391120 display_name="" \ 
        domain=192.168.1.1 p_asserted_id="" password=password type=domain \ 
        user=Cox

# sipswitch.b2bua_transfer_enable
modify-row sipswitch.b2bua_transfer_enable 1 always=on \ 
        clients_lack_refer=off clients_lack_replace=off use_from_uri=off \ 
        use_user_agent=off

# sipswitch.b2bua_transfer_for_client
clear-table sipswitch.b2bua_transfer_for_client

# sipswitch.b2bua_transfer_from_user
clear-table sipswitch.b2bua_transfer_from_user

# sipswitch.dial_plan
clear-table sipswitch.dial_plan
add-row sipswitch.dial_plan {id 1} action=fwd comment="" enum_prefix="" \ 
        enum_root=- forward_prefix="" forward_to="Generic ITSP-FWD" number=1 \ 
        reqfrom=ShoreTel ruri=Outbound timeclass=-
add-row sipswitch.dial_plan {id 13} action=fwd comment="" enum_prefix="" \ 
        enum_root=- forward_prefix="" forward_to=ShoreTel-FWD number=2 \ 
        reqfrom="Generic ITSP" ruri=- timeclass=-
# sipswitch.dial_plan_enable
modify-row sipswitch.dial_plan_enable 1 enabled=on

# sipswitch.dial_plan_methods
clear-table sipswitch.dial_plan_methods
add-row sipswitch.dial_plan_methods {id 1} method=INVITE
add-row sipswitch.dial_plan_methods {id 2} method=OPTIONS
add-row sipswitch.dial_plan_methods {id 3} method=SUBSCRIBE
add-row sipswitch.dial_plan_methods {id 4} method=MESSAGE
add-row sipswitch.dial_plan_methods {id 5} method=REFER

# sipswitch.enum_root
clear-table sipswitch.enum_root
add-row sipswitch.enum_root {id 1} name=e164.arpa. number=1 root=e164.arpa.
add-row sipswitch.enum_root {id 2} name=e164.org. number=1 root=e164.org.

# sipswitch.forward_to
clear-table sipswitch.forward_to
add-row sipswitch.forward_to {id 1} account=6782391120@192.168.1.1 domain="" 
   name="Generic ITSP-FWD" number=1 port="" regexp="" transport=-
add-row sipswitch.forward_to {id 11} account=- domain="" name=ShoreTel-FWD 
   number=1 port="" regexp="sip:(.*)@192.168.1.10;b2bua" transport=-

# sipswitch.incoming_unauth
clear-table sipswitch.incoming_unauth

# sipswitch.request_from
clear-table sipswitch.request_from
add-row sipswitch.request_from {id 2} client_netgroup=ShoreTel domain="" 
   name=ShoreTel regexp="" transport=any username=""
add-row sipswitch.request_from {id 3} client_netgroup=ITSP_IP 
   domain=192.168.1.1 name="Generic ITSP" regexp="" transport=any 
   username=""

# sipswitch.request_to
clear-table sipswitch.request_to
add-row sipswitch.request_to {id 1} domain="" head="" min_tail_length="" 
   name=Outbound prefix="" regexp="sip:\+?(.*)@192.168.1.250" tail=-

# sipswitch.user_routing
clear-table sipswitch.user_routing
add-row sipswitch.user_routing {id 1} action=forward 
   aliases="6782391121,6782391122,6782391123,6782391124,6782391125,6782391126,6782 
   391127,6782391128,6782391129" 
   comment="" forward_to="$\{ruri.user\}@192.168.1.10" 
   restrict_incoming=off timeclass=- user=Cox@192.168.1.1 voice_mail=-

# sipswitch.users
clear-table sipswitch.users

# sipswitch.voicemail
clear-table sipswitch.voicemail

# userdb.radius_local_endpoint
modify-row userdb.radius_local_endpoint 1 nas_identifier="" 
   radius_local_ip=- use_nas_ip_address=on

# userdb.radius_servers
clear-table userdb.radius_servers

# End of configuration file
8 Troubleshooting

Troubleshooting techniques are the same as other IP PBX’s with regard to the E-SBC Edgemarc 4550. In addition, debugging is facilitated by two other tools: the ShoreTel “Trunk Test Tool” and the Ingate SIParator’s web user interface’s “Logging and Tools” section.

8.1 ShoreTel Trunk Test Tool

This is a utility accompanying the ShoreWare Director software and installs automatically. It provides a diagnostic window where you can generate test calls and view the status of voice switch trunks.

![ShoreTel Trunk Test Tool]

Figure 50 – ShoreTel Trunk Test Tool
8.2 **InGate Logging and Tools**

This section of the SIParator web interface provides extensive logging options and packet capture ability. The logs can be easily viewed and exported. A “tech support report” including configuration details is easy to obtain with a click of the “Export Support Report” button on the Display Log tab.

![Figure 51 – InGate Logs and Tools](image_url)
Figure 52 – Figure 53 – InGate Logs and Tools (continued)
The SIParator’s Packet Capture tab is similarly intuitive with Start, Stop, Download and Delete buttons at the bottom of the page. It supports the ability to filter by interface, layer 3 and layer 4 characteristics.

Ingate SIParator has a built-in packet capture function which produces pcap trace files. You can select to capture traffic on one specific interface or on all interfaces.

For contacts with the Ingate Support Team, a packet capture is not what is usually expected (sometimes it is even not useful). For these purposes, please always send a Support Report.

You can also select the type of IP packets to capture, based on IP address, protocol and port.

---

**Figure 54 – SIPerator Packet Capture**
9 SIP Messaging examples, taken from inside of E-SBC:

9.1 Basic outbound on-net and off-net calls.

```
17:23:37.230552 192.168.1.250.5060 > 192.168.1.1.5060:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
INVITE sip:6782351004@sipgt-2c162.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK03add7a864bc5f5b59adc6a7e144ff.0
Session-Expires: 14400
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKe27de756ad35ed6af1f4b7ee2f30.13xmmeU0JyKmctR8JZ9FA__
To: <sip:6782351004@sipgt-2c162.1.1>
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=15934451
Call-ID: 6b759fad-4c993dcb699af-293f12ee@sipgt-2c133adf
CSeq: 61447650 INVITE
User-Agent: SIParator/4.8.1
P-Asserted-Identity: sip:6782391120@127.0.0.1
Contact: <sip:EM1Rz4gbVEZBobfa@192.168.1.250>
Supported: timer, replaces
Allow: ACK, INVITE, BYE, CANCEL, OPTIONS, NOTIFY, REFER, INFO, UPDATE
Max-Forwards: 68
Content-Type: application/sdp
Content-Length: 191
Record-Route: <sip:656c941210d5e168@192.168.1.250;lr>
v=0
o=b2bua.0.1 118 718031173 IN IP4 192.168.1.52
s=IN IP4 192.168.1.52
t=0 0
m=audio 3000 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
<<<<<<<<<<<<<<<sip header stop<<<<<<<<<<<<<<<<<<<<
[tos 0xfc]
```

```
17:23:37.24535 192.168.1.1.5060 > 192.168.1.250.5060:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK03add7a864bc5f5b59adc6a7e144ff.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKe27de756ad35ed6af1f4b7ee2f30.13xmmeU0JyKmctR8JZ9FA__
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=15934451
To: <sip:6782351004@192.168.1.1.5060>
CSeq: 61447650 INVITE
WWW-Authenticate: DIGEST realm="BroadWorks", nonce="BroadWorksXged1ap55Tyh0b5hBW", algorithm=MD5, qop="auth"
Content-Length: 0
<<<<<<<<<<<<<<<sip header stop<<<<<<<<<<<<<<<<<<<<
[tos 0xb8]
```

```
17:23:37.26502 192.168.1.1.5060 > 192.168.1.250.5060:
>>>>>>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>>>>>
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK03add7a864bc5f5b59adc6a7e144ff.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKe27de756ad35ed6af1f4b7ee2f30.13xmmeU0JyKmctR8JZ9FA__
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=15934451
To: <sip:6782351004@sipgt-2c162.1.1>
Call-ID: 6b759fad-4c993dcb699af-293f12ee@sipgt-2c133adf
CSeq: 61447650 INVITE
WWW-Authenticate: DIGEST realm=""""BroadWorks", nonce="""""""" BroadWorksXged1ap55Tyh0b5hBW", algorithm=MD5, qop="auth"
Content-Length: 0
<<<<<<<<<<<<<<<sip header stop<<<<<<<<<<<<<<<<<<<<
[tos 0xb8]
```

```
17:23:37.271479 192.168.1.250.5060 > 192.168.1.1.5060:
```
```
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK04b8031804bec7577a46ae51b2ce0934.m3TM8xyCpUhSjvwG03PJyg__
Record-Route: <sip:EWGW_0@192.168.1.1;lr>
Record-Route: <sip:656c941210d5e169@192.168.1.1:5060;tag=15934451
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=15934451
To: <sip:6782351004@192.168.1.1>;tag=SD2ld4e99-13414870-1285089817409
Call-ID: 6b759fad-4c93dbc699af-293f12ee@sipgt-2c133adf
CSeq: 61447651 INVITE
Contact: <sip:192.168.1.1:5060;transport=udp>
Session: Media
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Content-Type: application/sdp
Content-Length: 184
v=0
o=BroadWorks 2897 1 IN IP4 192.168.1.1
s=-
t=0 0
m=audio 16700 RTP/AVP 0 101
c=IN IP4 192.168.1.1
a=rtpmap:0 PCMU/8000/1
a=rtpmap:101 telephone-event/8000
a=fmt:101 0-15

ACK sip:192.168.1.1:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKc835b18135376e3ca6687778e416936e.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKc835b18135376e3ca6687778e416936e.0
Route: <sip:EWGW_0@192.168.1.1;lr>
To: <sip:6782351004@192.168.1.1>;tag=SD2ld4e99-1688070869-1285089827643
Call-ID: 6b759fad-4c93dbc699af-293f12ee@sipgt-2c133adf
CSeq: 61447651 INVITE
Contact: <sip:192.168.1.1:5060;transport=udp>
Session: Media
Reason: broadworks:no-recon-on-answer
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Content-Type: application/sdp
Accept: multipart/mixed, application/media_control+xml, application/sdp
Content-Length: 206
v=0
o=BroadWorks 2894 1 IN IP4 192.168.1.1
s=-
c=IN IP4 192.168.1.1
m=audio 16700 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000/1
a=rtpmap:101 telephone-event/8000
a=fmt:101 0-15
a=sendrecv
a=ptime:20

ACK sip:192.168.1.1:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKc835b18135376e3ca6687778e416936e.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKc835b18135376e3ca6687778e416936e.0
Route: <sip:EWGW_0@192.168.1.1;lr>
To: <sip:6782351004@192.168.1.1>;tag=SD2ld4e99-1688070869-1285089827643
Call-ID: 6b759fad-4c93dbc699af-293f12ee@sipgt-2c133adf
CSeq: 61447651 INVITE
Contact: <sip:192.168.1.1:5060;transport=udp>
Session: Media
Reason: broadworks:no-recon-on-answer
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Content-Type: application/sdp
Accept: multipart/mixed, application/media_control+xml, application/sdp
Content-Length: 206
v=0
o=BroadWorks 2894 1 IN IP4 192.168.1.1
s=-
c=IN IP4 192.168.1.1
m=audio 16700 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000/1
a=rtpmap:101 telephone-event/8000
a=fmt:101 0-15
a=sendrecv
a=ptime:20

ACK sip:192.168.1.1:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKc835b18135376e3ca6687778e416936e.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKc835b18135376e3ca6687778e416936e.0
Route: <sip:EWGW_0@192.168.1.1;lr>
To: <sip:6782351004@192.168.1.1>;tag=SD2ld4e99-1688070869-1285089827643
Call-ID: 6b759fad-4c93dbc699af-293f12ee@sipgt-2c133adf
CSeq: 61447651 INVITE
Contact: <sip:192.168.1.1:5060;transport=udp>
Session: Media

Call-ID: 6b759fad-4c993dbc699af-293f12ee@sipgt-2c133adf
CSeq: 61447651 ACK
Max-Forwards: 69
User-Agent: SIParator/4.8.1
Content-Length: 0

BYE sip:192.168.1.1.1.5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKb266bc5e80f26712a66877f8e416936e.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK78ddc2001c8ddf7fc1e69511547c2519.vwRussvWwPVhqAjUfSkYew_
Route: <sip:EWGW_0@192.168.1.1;l>;tag=15934451
To: <sip:6782351004@192.168.1.1>;tag=SD2ld4e99-1688070869-1285089827643
From: <sip:+16782391122@192.168.1.10:5060>;tag=15934451
Call-ID: 6b759fad-4c993dbc699af-293f12ee@sipgt-2c133adf
CSeq: 61447652 BYE
Max-Forwards: 69
User-Agent: SIParator/4.8.1
P-Asserted-Identity: sip:6782391120@127.0.0.1
Content-Length: 0

INVITE sip:4046691360@192.168.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKb266bc5e80f26712a66877f8e416936e.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK78ddc2001c8ddf7fc1e69511547c2519.vwRussvWwPVhqAjUfSkYew_
Record-Route: <sip:EWGW_0@192.168.1.1;l>;tag=15934451
From: <sip:+16782391122@192.168.1.10:5060>;tag=15934451
To: <sip:4046691360@192.168.1.1>;tag=SD2ld4e99-1688070869-1285089827643
Call-ID: 6b759fad-4c993dbc699af-293f12ee@sipgt-2c133adf
CSeq: 1744453506 INVITE
Content-Length: 0

200 OK
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=2b2uab.014400
Session-Expires: 14400
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK18cf3755e4f49345a10f20bdebb924ab.0
Session-Expires: 14400
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK18cf3755e4f49345a10f20bdebb924ab.0
Content-Type: application/sdp
Content-Length: 191
Record-Route: <sip:656c941210d5e15f@192.168.1.250;l>

m=audio 3000 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000/1
a=rtpmap:101 telephone-event/8000
a=fmt:101 0-15
<<<<<<<<<<<sip header stop<<<<<<<<<<<
(DF) [tos 0xfc]
17:22:55.750559 192.168.1.1.5060 > 192.168.1.250.5060:
>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK18cf3755e4f49345a10f20bddebb924ab.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK1dd1fd77b518bd379e54dd586331546c.ogMyzp1+DXVonYK6pxOk9g__
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=784eb853
To: <sip:4046691360@192.168.1.1>
Call-ID: edad28d-4c993d92e205b-4a54b41a@sipgt-2c133adf
CSeq: 1744453506 INVITE
Content-Length: 0
<<<<<<<<<<<sip header stop<<<<<<<<<<<
[tos 0xb8]
17:22:55.768566 192.168.1.1.5060 > 192.168.1.250.5060:
>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>
SIP/2.0 401 Unauthorize
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK18cf3755e4f49345a10f20bddebb924ab.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK1dd1fd77b518bd379e54dd586331546c.ogMyzp1+DXVonYK6pxOk9g__
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=784eb853
To: <sip:4046691360@192.168.1.1>;tag=SDkmek299-75491763-1285089775790
Call-ID: edad28d-4c993d92e205b-4a54b41a@sipgt-2c133adf
CSeq: 1744453506 INVITE
WWW-Authenticate: DIGEST realm="BroadWorks", nonce="BroadWorksXged19t4eTu64edrBW", algorithm=MD5, qop="auth"
Content-Length: 0
<<<<<<<<<<<sip header stop<<<<<<<<<<<
[tos 0xb8]
17:22:55.771944 192.168.1.250.5060 > 192.168.1.1.5060:
>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>
ACK sip:4046691360@192.168.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bK18cf3755e4f49345a10f20bddebb924ab.0
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=784eb853
To: <sip:4046691360@192.168.1.1>;tag=SDkmek299-75491763-1285089775790
Call-ID: edad28d-4c993d92e205b-4a54b41a@sipgt-2c133adf
CSeq: 1744453506 ACK
Max-Forwards: 70
Content-Length: 0
<<<<<<<<<<<sip header stop<<<<<<<<<<<
(DF) [tos 0xfc]
17:22:55.790126 192.168.1.1.5060 > 192.168.1.250.5060:
>>>>>>>>>>>sip header start>>>>>>>>>>>>>>>
INVITE sip:4046691360@192.168.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKcb4c945a856b8c359c64145a6303ec3c.bkjm0xuim54LY1Rg3QBS5A__
Session-Expires: 14400
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKcb4c945a856b8c359c64145a6303ec3c.bkjm0xuim54LY1Rg3QBS5A__
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=784eb853
User-Agent: SIParator/4.8.1
P-Asserted-Identity: sip:6782391120@127.0.0.1
Contact: <sip:EM1Rz4gbVKEZBobfa@192.168.1.250>
Supported: timer, replaces
Allow: ACK, INVITE, BYE, CANCEL, OPTIONS, NOTIFY, REFER, INFO, UPDATE
Max-Forwards: 68
Content-Type: application/sdp
Content-Length: 191
CSeq: 1744453507 INVITE
Authorization: Digest realm="BroadWorks", nonce="BroadWorksXged19t4Tu64edrBW", username="6782391120", url="sip:4046691360@192.168.1.1.1", qop=auth, cnonce="6b71de34", nc=00000001, response="418d217756c211c87041f063c032e238", algorithm=MD5
Record-Route: <sip:656c941210d5e160@192.168.1.250;lr>

v=0
o=b2bua.0.1 116 630965660 IN IP4 192.168.1.52
s=-
c=IN IP4 192.168.1.52
t=0 0
m=audio 3000 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKcdb906e6d7067c1a2a10f20bdeebb294ab.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKcb4c945a856b8c359c64145a6303ec3c.bkj0xuim54LYRG3QBS5A__
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=784eb853
To: <sip:4046691360@192.168.1.1.1>
Call-ID: edad28d-4c993d92e205b-4a54b41a@sipgt-2c133adf
CSeq: 1744453507 INVITE
Content-Length: 0

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKcdb906e6d7067c1a2a10f20bdeebb294ab.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKcb4c945a856b8c359c64145a6303ec3c.bkj0xuim54LYRG3QBS5A__
Record-Route: <sip:EWGW_0@192.168.1.1;lr>
Record-Route: <sip:656c941210d5e160@192.168.1.250;lr>
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=784eb853
To: <sip:4046691360@192.168.1.1.1>;tag=SDkmek299-571048290-1285089775906
Call-ID: edad28d-4c993d92e205b-4a54b41a@sipgt-2c133adf
CSeq: 1744453507 INVITE
Contact: <sip:192.168.1.10:5060;transport=udp>
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKcdb906e6d7067c1a2a10f20bdeebb294ab.0
Via: SIP/2.0/UDP 192.168.1.250:5060;branch=z9hG4bKcb4c945a856b8c359c64145a6303ec3c.bkj0xuim54LYRG3QBS5A__
Record-Route: <sip:EWGW_0@192.168.1.1;lr>
Record-Route: <sip:656c941210d5e160@192.168.1.250;lr>
From: "PHONE 1122" <sip:+16782391122@192.168.1.10:5060>;tag=784eb853
To: <sip:4046691360@192.168.1.1.1>;tag=SDkmek299-571048290-1285089775906
Call-ID: edad28d-4c993d92e205b-4a54b41a@sipgt-2c133adf
CSeq: 1744453507 INVITE
Contact: <sip:192.168.1.1:5060;transport=udp>
Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
Content-Type: application/sdp
Accept: multipart/mixed, application/media_control+xml, application/sdp
Content-Length: 248
v=0
o=BroadWorks 2889 1 IN IP4 192.168.1.1