Edge 8000

Documentation Suite

Software Release: 24.1
Document Revision: 03.01
Published: 31 August 2024

Contents

Edge 8000 24.1 Documentation

Product Introduction

- Edge 8000 Series Product Overview
- Performance
- High Availability
- Contact and Support

Initial Setup

- Workflow for Initial Setup
- Installing Edge 8000 Hardware
- Running Setup Wizard
- Activating High Availability

Operations and Maintenance

- Backup and Restore Operations
- License Management
- Software Management
- System Security and Administration
- Troubleshooting, Repairs, and System Status

Hardware Guide

Configuration Examples

- FXS Configuration for IP PBX Deployment
- SIP Trunk Configuration for IP PBX Deployment
- Ribbon Product Interoperability Testing

Configuration Guides

- Configuration of SIP to SIP Calls

Gateway Reference

- SIP-User-Agent
- SIP-Gateway
- PRI-Setting

Related Documents

- 6WIND Router Documentation
- RAMP Documentation
- SBC Edge Documentation

Edge 8000 Releases

- Edge 8000 Series Hardware Specifications
- Edge 8000 Shipping Contents
- Front and Back Panels

- Edge 8000 24.1 Release Notes

Product Introduction

Contents

Edge 8000 Series Product Overview

The Ribbon Edge 8000 Series provides a highly scalable 10GB multi-tenant Ethernet router with rich layer 3 routing, tunneling, and switching features, plus full-featured Session Border Controller functionality.

Contents

About the Ribbon Edge 8000 Series

Formerly, a Session Border Controller (SBC) served as a network element deployed to protect SIP-based Voice over Internet Protocol (VoIP) networks. Early deployments of SBCs were focused on the borders between two service provider networks in a peering environment. This role has now expanded to include significant deployments between a service provider's access network and a backbone network to provide service to residential and/or enterprise customers.

The Edge 8000 product is the newest, high-performance member of Ribbon's services gateway routers that combines security, routing, switching, and 10 Gbps WAN interfaces with next-generation voice and data services where the combination of broadband connectivity and advanced threat mitigation capabilities are required. By consolidating fast, highly available routing, security, and next-generation SBC capabilities in a single Multi-Service Edge (MSE) device, enterprises can remove network complexity, protect and prioritize resources, and improve user and application experience while lowering the total cost of ownership.

Available Models and Features

The Edge 8000 Series consists of two models:

- Edge 8100, a highly scalable Ethernet SBC and data router.
- Edge 8300, a high-capacity mixed SBC, analog, and data router.

The Edge 8000 Series supports the Ribbon SBC SWe Edge function as an onboard VNF application. By consolidating fast, highly available routing, security, and next-generation VNF capabilities in a single device, enterprises can remove network complexity and protect network resources.

With the SBC SWe Edge VNF, the Edge 8000 product qualifies as a Microsoft Teams Direct Routing Virtual Survivable Branch Appliance (vSBA). The vSBA function allows users inside a branch office to make and receive Public Switched Telephone Network (PSTN) calls when there is an external outage. Refer to Working with the Virtual Survivable Branch Appliance for more information.

All Ribbon Edge 8000 devices integrate with Ribbon RAMP. RAMP offers the convenience of a single interface from which to launch the GUIs of your RAMP-registered Edge 8000 devices, and the display of all SBC SWe Edge traps from those devices.

For an application of SIP to SIP calls only (no analog calls), a pair of Edge 8000 devices can be deployed for High Availability (HA) call protection. Refer to Overview of High Availability.

The Edge 8300 model includes all the capabilities of the 8100, plus integrates analog endpoints – FXS, FXO, and T1/E1 PRI – to accommodate analog phones and access to the Public Switched Telephone Network (PSTN). The 8300 provides any-to-any connectivity between analog and SIP devices, enabling branch offices to migrate analog phones to SIP-based networks and to communicate seamlessly with Ribbon Session Border Controllers. For additional features and capabilities of the Edge 8000 product, refer to Edge 8000 Series Hardware Specifications.

Architecture

Operating Systems

Ribbon offers two host operating systems:

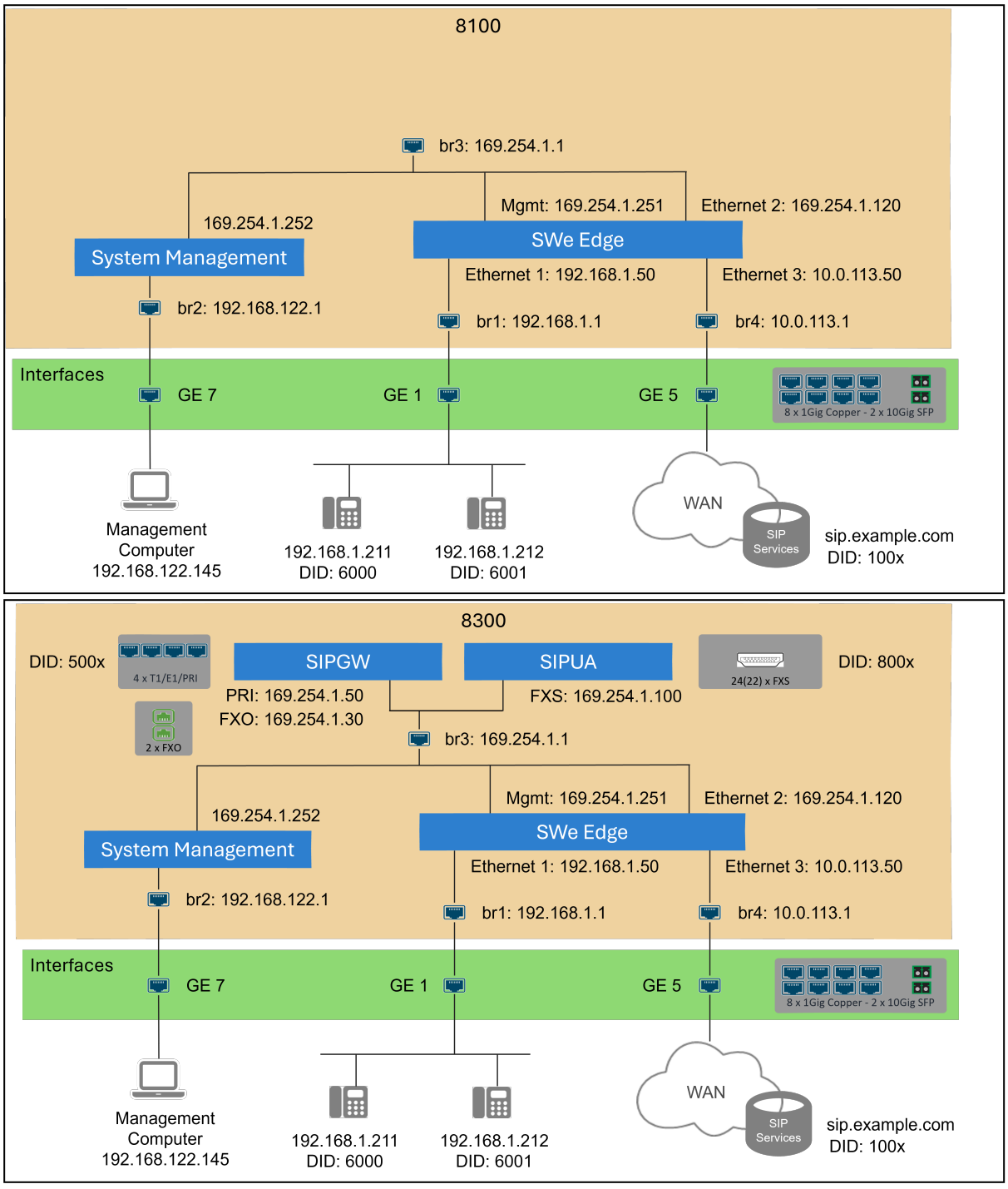
- Alma Linux
- Red Hat Enterprise Linux (RHEL)

Alma Linux is a standard, open-source operating system. Red Hat Linux is a commonly used, proprietary, licenseable operating system that features Federal Information Processing Standard (FIPS) Publication 140-1 compliance. FIPS 140-1 is a computer security standard developed by the U.S. Government and an industry working group to validate the quality of cryptographic modules. Red Hat Linux appeals to Federal agencies and to enterprises such as financial and healthcare operators that require tightly integrated security features. Whichever operating system you select, Ribbon ships installed on your Edge 8000 device.

Internal Bridges and Interfaces

The following diagrams and tables illustrate the bridges and interfaces at the heart of an Edge 8000 device. Note that the VNF SBC SWe Edge, as a virtual machine (VM), connects internally to the other components of the Edge 8000 device through an internal bridge, Bridge 3. Bridge 2 provides a single system management access point for all the major Edge 8000 functions, including the Gateway function (SIPGW and SIPUA) for the 8300 model, the Router function for both models, and the SBC SWe Edge function for both models. Bridge 1 typically connects the Edge 8000 device to a corporate or building LAN. Bridge 4 typically connects to an external WAN. Bridge 5 typically connects two devices in a High Availability system. (Refer to Overview of High Availability.)

Edge 8100 and 8300 Device Addressing – Typical Deployment



Bridges and Available Ports

Interface	Typical Purpose	Available Ports
Bridge 1	LAN connection	GE1-4

Interface	Typical Purpose	Available Ports
Bridge 2	Device management	GE7 (typical)
Bridge 3	Internal addressing	Not configurable
Bridge 4	WAN connection	GE5-8, SFP9-10
Bridge 5	High Availability connection	GE5-8, SFP9-10

Bridge 3 IP Addressing (Not Configurable)

IP Addresses	Purpose
169.254.1.254	allocated to db-manager for internal communication between host and daughter boards.
169.254.1.252	allocated to the config container for communication with SWe Edge on the management VLAN of BR3
169.254.1.251	allocated to the SWe Edge mgt port for communication with Config Container
169.254.1.120	allocated to the packet port on SWe Edge for internal SIP communication with PRI/FXS/FXO
169.254.1.110	DSP IP used in the analog board to communicate to DSP (internal messaging)
169.254.1.100	allocated to FXS for SIP signaling to SWe Edge
169.254.1.50	allocated to PRI for SIP signaling to SWe Edge
169.254.1.30	allocated to FXO for SIP signaling to SWe Edge

User Interfaces

The Edge 8000 device offers two primary user interfaces, a command line interace (CLI) and a web-based user interface (webUI).

Edge 8000 User Interfaces

User Interface	Access Method and Primary User	Primary Purpose	Main Program or User Interface Tabs	Related Edge 8000 Documentation
Edge 8000 CLI	From a Telnet session through the front panel serial console port, either directly or through a terminal server, as user System Administrator (*sysadm*). After platform setup, from a secure shell (SSH) login to the system management interface as user *sysadm*.	Platform setup. This includes assigning the system management IP address (Bridge 2).	Main program: Setup Wizard	• Running Setup Wizard - Standalone • Running Setup Wizard - High Availability • Password Management
Edge 8000 webUI	From an Internet web browser, using the system management IP address assigned during platform setup, as user Administrator (*admin*).	System operations, administration, maintenance, and provisioning.	Main user interface tabs: • Monitor • Tasks • Settings • Diagnostics • System	• Operations and Maintenance ◦ License Management ◦ Password Management • Configuration Guides • Configuration Examples

The webUI organizes device management across five major tabs at the top of the user interface. Customers familiar with the SBC SWe Edge webUI will recognize many of the same menus within the five tabs. Overall, the extensive SBC Edge Portfolio Documentation still applies to the folders and menus seen in the Edge 8000 webUI.

WebUI Tabs

Tab	Available Folders
Monitor	SBC Edge folders for Real-Time Monitor and Alarm View
Tasks	SBC Edge folders for System, Direct Routing SBA, Import/Export Configuration, SBC Easy Setup, IP/Protocols
Settings	Edge 8000 folders for System, Gateway, Routing, and SBC Edge Configuration
Diagnostics	SBC Edge folders for Logs, SBC Logs, SBC Tools, Teams Direct Routing, and Ribbon Service Troubleshooting

Tab	Available Folders
System	SBC Edge folder Statistics Edge 8000 folder About Edge 8000

What's different in the Edge 8000 webUI is that within the **Settings** tab, the menus for the SBC SWe Edge are now located within an SBC folder. In this way, the **Settings** tab accommodates all the components of the Edge 8000 device: Gateway, Router, and SBC SWe Edge. Refer to Differences Between the SBC Edge and Edge 8000 WebUIs for illustrations of the webUI differences within the Settings tab.

Folders Within the Settings Tab

Folder	Purpose
Home	Displays a system-level status of the Edge 8000 device and its call communication channels. Refer to System Status.
System	Provides system operational menus such as node-level settings for host information and time management, as well as menus for licensing, DNS settings, security settings including user account management, certificates, and logging. These settings apply to all the Edge 8000 components: Analog, Routing, SBC SWe Edge. (The Setup Wizard does not configure Time Zone, Time Server, RAMP Server, or DNS settings. The System **folder** provides menus for these settings.)
Gateway	Provides provisioning and operational menus for the device's analog (FXS/FXO) and PRI settings.
Routing	Provides provisioning and operational menus for the device's 6WIND router features, such as firewall settings.
SBC	Provides provisioning and operational menus for the SBC SWe Edge function, including call routing, signaling groups, networking interfaces, tone tables, and other SIP-related parameters and definitions. (Some system-level SWe Edge settings are located at the System level folder within the Settings tab.)

System Status

For a quick view of the system status showing the platform, licensing, and call channel status of the device, a System Status window is available from the Ribbon webUI. Refer to System Status.

Licensing

Receiving the Unit

Based on the selections you make when you place your order, Ribbon authorizes up to three product licenses – Analog, Router, and SBC SWe Edge – as described in the following table:

License Types

Type	Purpose	Edge 8000 Models
Analog	Supports TDM calls through FXS, FXO, and PRI (T1, E1) ports, collectively known as analog ports.	8300
Router	Supports data routing through the 1G and 10G Ethernet ports, including all Layer 2 and Layer 3 switching. Supports bandwidths of 2.5, 5, or 10 Gbps bi-directional throughput.	8100 and 8300
SBC SWe Edge	Supports SIP calls through the 1G and 10G Ethernet ports. Supports High Availability for SIP to SIP calls. (High Availability is not supported for calls involving analog ports.) Supports concurrent call sessions in packages of 100, 25, 10, and 5. Example: order a 100 service pack and a 25 service pack for a total of 125 concurrent sessions. Supports SWe Edge software feature packs offering different levels of DSP media processing, including transcoding, encryption, in-band media services, and RTP media manipulation. Supports Gateway Only option: calls originating and terminating through analog ports pass through the SWe Edge function with no DSP media processing and no requirement for concurrent SIP to SIP call sessions.	8100 and 8300

Ribbon ships your Edge 8000 unit with the appropriate Analog and Router licenses installed and activated. No additional action is required for these licenses.

The SWe Edge license requires additional steps to install the license, based on a license key you obtain from Ribbon after you place an order. Refer to License Management for license ordering and installation instructions.

Later Upgrading

You can later scale your device with an upgrade order based on the MAC address of the device. An upgrade order allows you to increase the data throughput of your router function, enhance your SWe Edge software features, and add concurrent call sessions to match the changing needs of an expanding network. Refer to License Management for license ordering and installation instructions.

In summary, the three types of Edge 8000 product licenses – Analog, Router, and SBC SWe Edge – can be initially ordered and later upgraded as follows:

License Ordering and Upgrading Options

License Type	Options Available When Ordering the Product or When Later Upgrading	License Status When Initially Shipped	License Can Be Upgraded Later?	Edge 8000 Models
Analog	No options offered (the complete Analog function is always shipped with the product)	Already installed	No	8300
Router	Data throughput choices: • initial levels of 2.5, 5, and 10 Gbps bi-directional performance • later upgrade choices to increase from 2.5 to 5 Gbps, and from 5 to 10 Gbps	Already installed	Yes; requires manual license installation	8100 and 8300
SBC SWe Edge	Feature and capacity choices: • Feature packs: different levels of transcoding, encryption, in-band media services, and RTP media manipulation • Concurrent call sessions: packages of 100, 25, 10, and 5 concurrent sessions • High Availability: requires a pair of Edge 8000 devices (for SIP to SIP calls only; no HA support for analog calls)	Requires manual license installation	Yes; requires manual license installation	8100 and 8300

Customer Documentation

The Edge 8000 Series product reuses Ribbon SBC SWe Edge and 6WIND software. Therefore, at times you will be directed to the customer documentation of the other product where a complete documentation suite describes all the features and functions of that software.

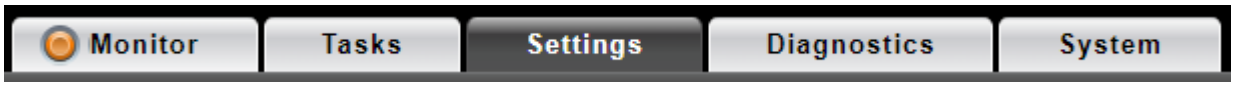
Refer to Related Documents for links to the documentation suites applicable to the Edge 8000 Series product.

Differences Between the SBC Edge and Edge 8000 WebUIs

Contents

The Edge 8000 and SBC SWe Edge webUIs share the same layout of five primary tabs across the top of the user interface.

Five Tabs at the Top of the User Interface

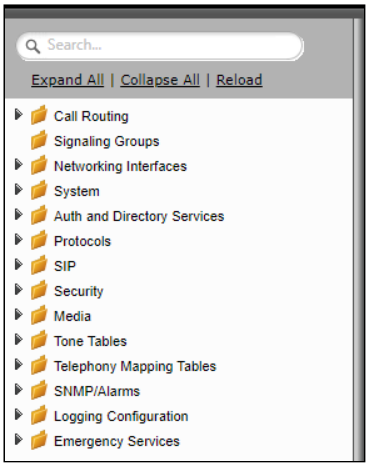


Within the **Settings** tab, the Edge 8000 webUI differs significantly from the SBC SWe Edge webUI in two important ways:

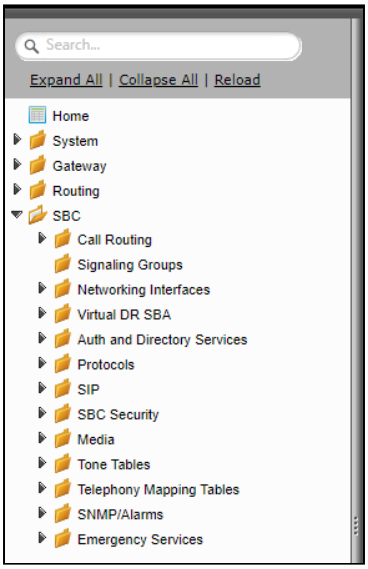
- Call routing and provisioning menus for the SBC SWe Edge function are located in folder **SBC** in the Edge 8000 webUI.
- Host-level management and administration menus are located in folder **System** in the Edge 8000 webUI.

Call Routing and Provisioning Menus in the Settings Tab

SBC Edge WebUI



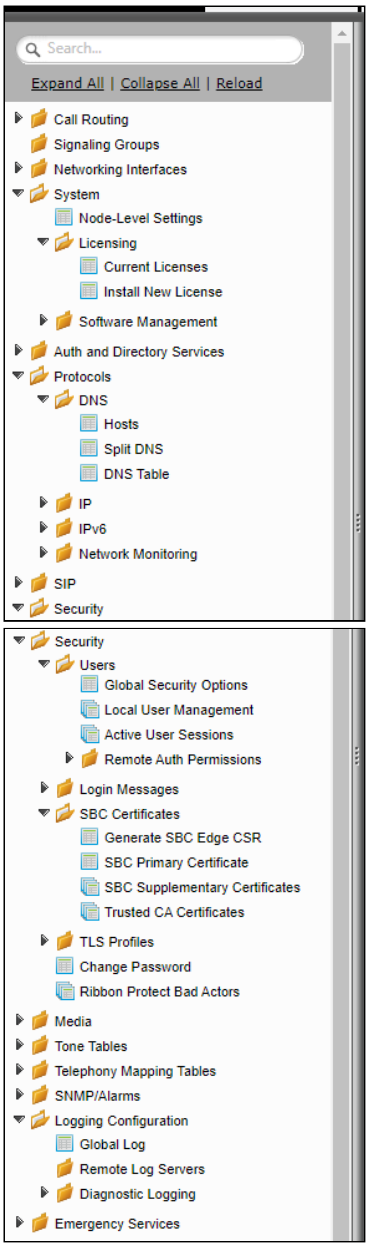
Edge 8000 WebUI

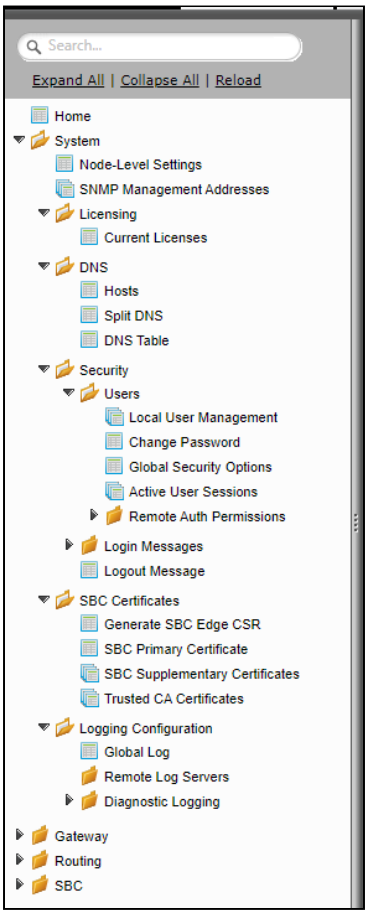


Host-Level Management and Administration Menus in the Settings Tab

SBC Edge WebUI

Edge 8000 WebUI





Performance

Contents

Introduction

The following performance data applies equally to Edge 8100 and Edge 8300 models using the Alma Linux and RHEL operating systems.

Legend:

- CPS - Calls Per Second
- CHT - Call Hold Time
- RPS - Registrations Per Second

Edge 8000 Performance Numbers

The following performance numbers have been recorded for proxy and DSP transcoding call modes.

> **Note**
>
> A maximum of 25 calls per second (CPS) and 10 registrations per second (RPS) are allowed.

Voice Pass-through (Proxy Mode) Performance

This is the performance measured using multiple calls in media pass-through mode.

	Scenario	vCPU	Memory (GB)	CPS	CHT (seconds)	Sessions
1	G711U [TLS] [SRTP] to G711U [TLS] [SRTP]	2	2	10	96	960
2	G711U [TLS] [SRTP] to G711U [TLS] [SRTP]	4 (HA)	4	25	38	950

Voice Transcoding (DSP Mode) Performance

This is the performance measured using multiple calls with voice transcoding involved.

	Scenario	vCPU	Memory (GB)	CPS	CHT (seconds)	Sessions
1	G711U UDP/RTP to G711U UDP/RTP	2	2	10	20	200
2	G711U TLS/SRTP to G711U TLS/SRTP	2	2	10	20	200
3	G711U TLS/SRTP to G711U TLS/SRTP	4 (HA)	4	10	40	400

SIP Registration Performance

	Scenario	RPS	Concurrent Call Sessions
1	Registration Load	10	5000

Voice Transcoding Interworking Performance

	Scenario	Max Lines	ISDN Trunk Switch Type	ISDN Codec	SIP Codec	SWe Edge Audio Mode	Call Rate (CPS)	Call Hold Duration (secs)	Max Concurrent Calls
1	PRI-T1 to SIP	4 x T1	NI2	G711U	G729A	DSP	4	100	92
2	PRI-T1 to SIP	4 x T1	NI2	G711U	G729A	DDSP	4	100	92

High Availability

Contents

Overview of High Availability

Contents

Introduction

You can optionally deploy a pair of Edge 8000 devices for High Availability. High Availability (HA) protects SIP to SIP calls using SBC SWe Edge HA functionality. HA functionality enhances resiliency by offering Active and Standby SWe Edge instances. When the Active instance fails during a call, the Standby instance takes over the call management to maintain the call.

The Active and Standby SWe Edge instances operate using a single HA license. At the time of initial setup, you install the HA license on the Active instance. Once accepted, the HA system replicates the information to the Standby instance.

Provisioning for HA can only be done at the time of initial installation and only for a pair of Edge 8000 devices that solely support SIP to SIP calls. Additional limitations apply. See Limitations.

For installation and HA activation instructions, refer to Workflow for Initial Setup - High Availability.

Architecture

In an Edge 8000 High Availability setup, two Edge 8000 devices share the responsibility of the HA function. Each device is assigned with corresponding Ethernet interfaces to serve the requirements of the deployment, as shown in the following table:

HA Interface Assignments: Typical Deployment

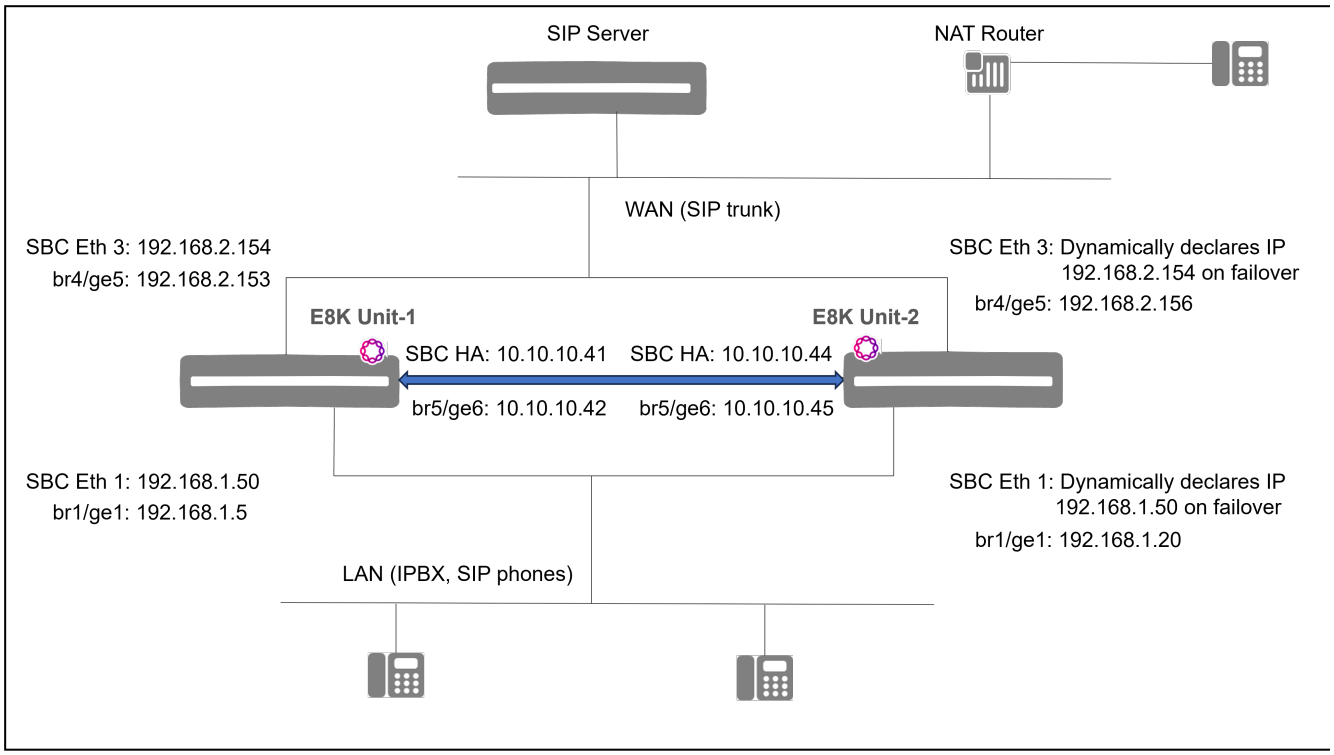
Ethernet Interface Requirement	Edge 8000 Physical Port	Internal Bridge	SWe Edge Logical Interface
LAN side of the network	ge1	br1	Ethernet 1
WAN side of the network	ge5	br4	Ethernet 3
HA monitoring between the two devices	ge6	br5	High Availability

Once HA is enabled, the Standby instance monitors the Active instance through the High Availability interface. When a failover occurs, the HA function "floats" (assigns) the Ethernet 1 and Ethernet 3 addresses from the (former) Active instance to the Standby instance, which acts as the new Active instance. To the outside world, no change of the Edge 8000 device is discernible other than a change in the MAC address of the (new) Active device.

The following diagram depicts the topology of a typical HA deployment. Note that:

- Your network administrator will provide unique IP addresses for the bridge interfaces (br4, br5, and br1) and the SBC SWe Edge logical interfaces (SBC Eth 3, SBC HA, and SBC Eth1).
- The physical port assignments for the LAN and WAN services can be any of the available Gigabit Ethernet ports, ge1-8, or SFP+ ports, SFP9 or SFP10, exclusive of the port used for the High Availability interface. (Note that the ports do not receive IP addresses. Rather, you simply assign a port to be a member of a bridge.)

HA Deployment Example



Limitations

The following limitations apply to Edge 8000 HA functionality:

- **Deployment**
  - HA can only be provisioned at the time of initial installation. Ribbon does not offer a path for stand-alone (SA) to HA conversion.
  - HA only applies to SIP to SIP calls. Analog calls are excluded.
  - HA supports only static IP addressing on the Ethernet Media (packet) and High Availability ports, not DHCP.
  - The HA interface IP addresses must be static IPv4 addresses on the same subnet at least three addresses apart. Example: 10.10.10.41 and 10.10.10.44.
  - HA supports floating IP addresses only on the Ethernet Media (packet) interfaces, not on the High Availability interface. (The HA function automatically assigns, or "floats," the media interfaces of the Active device to the Standby device when a failover occurs.)
  - HA does not support Geo Redundancy. The two HA devices must be on the same subnet.
  - Edge 8000 devices do not support redundancy at the card or port level.
- **Data Replication**
  - The Standby instance does not replicate Alarms, Counters, and CDR details.
  - The Standby instance does not replicate caches.
  - The Active and the Standby instances do not store backup CDR and VQ files in the database.
  - The Active and the Standby instances do not share a Debug Facility, Monitor View, or Logging details. Each instance only shows its details.
- **Call Features**
  - SIP recording, Video calls, and Music On Hold do not support switchover scenarios.
- **Others**
  - SNMP Proxy from the Standby instance to the Active instance, so that SNMP requests always get a response regardless of which instance receives the request, is not supported.
  - Using Service Discovery to find a RAMP instance when RAMP is configured for HA is not supported.

Licenses

You must purchase an HA SKU to deploy HA on your system. Once you place an order through the Ribbon Partner Portal for HA functionality, Ribbon sends you an email that contains information on where to obtain the license associated with your system. You will receive one license for the HA pair.

SWe Edge User Interface Changes for HA

Contents

Once you have configured a pair of Edge 8000 devices for High Availability (HA) and installed an HA license, you can select HA-related configuration options from the web-based Edge 8000 user interface. The following sections describe user interface changes related to HA that appear within the five general tabs of the SWe Edge WebUI.

Settings Tab

> **Note**
>
> For Edge 8000 users, all SBC SWe Edge menus in the **Settings** tab are located under the main folder **SBC**. This means to find menus for Signaling Groups, for example, navigate to **SBC** > **Signaling Groups**.

By default, in the Settings tab, you can only configure the settings of your SBC SWe Edge through the Active instance. The Standby instance is mainly in a view-only permissions mode unless otherwise specified.

Folder	Subfolder/Task	WebUI Path	WebUI Changes
Signaling Groups	**Add SIP SG**	Settings > Signaling Groups > Signaling Group Table	• **Add SIP SG, which** is available on the Active instance only. ◦ The HA interface is removed from the **Signaling/Media Source IP** dropdown menu in the **SIP IP Details section**. ◦ The **SIP Recording** section is removed for HA.

<table>
<tr><th>Folder</th><th>Subfolder/Task</th><th>WebUI Path</th><th>WebUI Changes</th></tr>
<tr><td>Networking Interfaces</td><td>Logical Interfaces</td><td>Settings > Networking Interfaces > Logical Interfaces</td><td>

The High Availability interface is added. The HA interface supports only static IPv4 and includes the following fields:

Local IP Address
Local IP Netmask
Remote IP Address

HA Interface Field Descriptions
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Local IP Address</td><td>The HA IP address of the instance you are currently in.</td></tr>
<tr><td>Local IP Netmask</td><td>The netmask for the local IP address.</td></tr>
<tr><td>Remote IP Address</td><td>The HA IP address of the other instance.</td></tr>
</table>
Note
You can configure all the interfaces on the Active instance but you can only configure the Admin IP and High Availability interfaces on the Standby instance.

The IPv6 option is removed from the IP Addressing Mode dropdown menu for all packet interfaces, as the interfaces only support IPv4 addresses in release SBC 12.1.

</td></tr>
</table>

<table>
<tr><th>Folder</th><th>Subfolder/Task</th><th>WebUI Path</th><th>WebUI Changes</th></tr>
<tr><td rowspan="2">System</td><td>Node-Level Settings</td><td>Settings > System > Node-Level Settings</td><td>

The Enable HA button is added.
The Enable HA button opens the Create HA Interface window, which includes the following fields:

Local IP Address
Local IP Netmask
Remote IP Address

HA Interface Field Descriptions
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Local IP Address</td><td>The HA IP address of the instance you are currently in.</td></tr>
<tr><td>Local IP Netmask</td><td>The netmask for the local IP address.</td></tr>
<tr><td>Remote IP Address</td><td>The HA IP address of the other instance.</td></tr>
</table>
Note
The Active and Standby instances reboot after you enable HA and change the local or remote IP addresses.
</td></tr>
<tr><td>Install New License</td><td>Settings > System > Licensing</td><td>

Install New License is removed from the Standby instance.

</td></tr>
</table>

Folder	Subfolder/Task	WebUI Path	WebUI Changes
	Application Partitions	Settings > System > Software Management	• The Active instance lists the details of the partitions of both the Active and the Standby instances. • The Standby instance only lists the details of its partitions. • A column for **HA Role** is added to the **Partitions Table** pane on the Active instance. • You can perform **Upload Software** and **Backup Configuration** on the Active instance only.
SIP	**SIP Recording**	Settings > SIP	• The **SIP Recording** folder is removed from the Active and the Standby instances.

<table>
<tr><th>Folder</th><th>Subfolder/Task</th><th>WebUI Path</th><th>WebUI Changes</th></tr>
<tr><td>Logging Configuration</td><td>Global Log Date/ Time Format</td><td>Settings > Logging Configuration > Global Log</td><td>

The Global Date/Time Format configuration field is added to the Global Log Configuration pane. The Global Date/Time Format configuration field has two options: Default and RFC 5424.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Global Date/ Time Format</td><td>The Global Date/Time Format shows the date/time format used in the log lines. This configuration field has two options:
Default: The existing date and time format currently used, for example, 2023-05-12 12:04:00,621.
RFC 5424: The date and time format in RFC 5424, for example, 2023-05-12T12:05:03Z,948.</td></tr>
</table>
</td></tr>
</table>

Folder	Subfolder/Task	WebUI Path	WebUI Changes
			• The Standby instance only allows you to view the configuration for **Global Date/Time Format**.

Tasks Tab

By default, in the Tasks tab, you can only configure the settings of your SBC SWe Edge through the Active instance. The Standby instance is mainly in a view-only permissions mode unless otherwise specified.

Task	Subtask	WebUI Path	WebUI Changes
System	**HA Software Upgrade**	Tasks > System > HA Software Upgrade	• **HA Software Upgrade** is available on the Active instance only. • **HA Software Upgrade Warning Message** A warning message for HA Software Upgrade is added.
	Backup/Restore Config	Tasks > System > Backup/ Restore Config	
	Reboot SBC Edge	Tasks > System > Reboot SBC Edge	• **Reboot SBC Edge** is available on both the Active and the Standby instances. • The warning message, "This operation will stop all the calls and reboot the system." is removed from the Active and the Standby instances.
	SBC Edge Factory Default - Factory Default	Tasks > System > SBC Edge Factory Default	• The Active and the Standby instances both support the **Factory Default** option.
	Import Partial Configuration	Tasks > System > Import Partial Configuration	

Task	Subtask	WebUI Path	WebUI Changes
Import/Export Configuration Items	**Import Local/ Passthrough Auth Table**	Tasks > Import/Export Configuration Items > Import Local/Passthrough Auth Table	• The task of **Import/ Export Configuration Items** and its subtasks are removed from the Standby instance.
	Transformation Tables	Tasks > Import/Export Configuration Items > Transformation Tables	
	SIP Message Rule	Tasks > Import/Export Configuration Items > SIP Message Rule	
SBC Easy Setup	**Easy Configuration Wizard**	Tasks > SBC Easy Setup	• **Easy Configuration Wizard** is supported on the Active instance only.
	Media System Configuration	Tasks > SBC Easy Setup	
	Certificates	Tasks > SBC Easy Setup	
IP/Protocols	**Modify Ethernet IP Address**	Tasks > IP/Protocols	
BroadSoft Provisioning	**Auto Configuration**	Tasks > BroadSoft Provisioning	

Diagnostics Tab

In the Diagnostics tab, you can perform the tasks and subtasks on both the Active and the Standby instances unless otherwise specified.

Task	Subtask	WebUI Path	WebUI Changes
Logs	**Restart Report**	Diagnostics > Logs	• The Standby instance only allows you to view **Core Files** in **Restart Report**.
Tools	**Test a Call**	Diagnostics > Tools	• The Standby instance only allows you to view the configuration for **Test a Call**.

Task	Subtask	WebUI Path	WebUI Changes
	Debug Call	Diagnostics > Tools	• The Standby instance only allows you to view **Configure Subsystem** in **Debug Call**.
	Query AD Cache	Diagnostics > Tools	• You must configure Active Directory on the Active instance to see **Active Directory Cache Query**. • The Standby instance only allows you to view **Active Directory Cache Query**.
	Ping Destination	Diagnostics > Tools	• The Active instance lists all the interfaces. • The Standby instance only lists the management interface (Admin IP).
	Traceroute to Destination	Diagnostics > Tools	• The Standby instance only allows you to view the configuration for **Traceroute to Destination**.
	ARP Cache	Diagnostics > Tools	• The Standby instance only allows you to view **ARP Cache**.

Task	Subtask	WebUI Path	WebUI Changes
High Availability	**HA Status Details**	Diagnostics High Availability > HA Status Details	• Both the Active and the Standby instances display the HA status details. • Both the Active and the Standby instances display the peer instance's WebUI link. **Note** When you configure an HA pair, web servers run on both the Active and the Standby instances. These servers are configured so that if you navigate to the Standby instance on standard web ports: 80 and 443, you are automatically redirected to the Active instance to facilitate changing HA configurations. You can view the peer instance's WebUI link on both the Active and the Standby instances. Note that you can use non-standard web ports to view the link for the Standby instance on the Active instance.
	HA Tracking Table	Diagnostics High Availability > HA Tracking Table	• Both the Active and the Standby instances support the **HA Tracking Table**. • The **HA Tracking Table** provides information on what time an instance assumes a role (Active or Standby). • The **HA Tracking Table** only tracks the changes of the instance that you are in.

Task	Subtask	WebUI Path	WebUI Changes
Teams Direct Routing	**Connectivity Checks**	Diagnostics > Tools	• The Standby instance only allows you to view the configuration for **Connectivity Checks**.
	SBA Logs	Diagnostics > Tools	• **SBA Logs** is removed for HA.
Ribbon Service Troubleshooting	**Software Upgrade**	Diagnostics > Ribbon Service Troubleshooting	• **Software Upgrade** is added under **Diagnostics** for HA. **Note** **Software Upgrade** only upgrades the HA instance that you are currently in. Ribbon does not encourage upgrading HA instances individually. If you need to upgrade an HA instance individually, contact Ribbon Support.
	Packet Capture	Diagnostics > Ribbon Service Troubleshooting	• **Packet Capture** is available on both the Active and the Standby instances.

System Tab

Task	Subtask	WebUI Path	WebUI Changes
Overview	**System Overview**	System > Overview	• **System Mode** is added in **Overview** on both the Active and Standby instances.

Monitor Tab

By default, in the Monitor tab you can only configure the settings of your SBC SWe Edge through the Active instance. The Standby instance is mainly in a view-only permissions mode unless otherwise specified.

Task	WebUI Path	WebUI Changes
SBC Edge Real-Time Monitor	System > SBC Edge Real-Time Monitor	• The Standby instance only allows you to view **SBC Edge Real-Time Monitor**.
Alarm View	System > Alarm View	• The Standby instance only allows you to view **Alarm View**.

Contact and Support

Access to the Ribbon support portals and technical assistance centers is available to customers who have purchased maintenance and technical support services.

Customer Support

To contact the Ribbon Customer Portal, refer to Ribbon Support.

For immediate assistance, please call: +1 833 742 2661

Customer Documentation

For customer documenation, refer to Ribbon Product Documentation Home.

Initial Setup

Follow the instructions given in Workflow for Initial Setup to configure your device for a stand-alone or high-availability deployment. The instructions cite procedures for installing the hardware and configuring the platform for the Edge 8000 Series device.

Contents

Workflow for Initial Setup

Ribbon offers two options for the initial installation of the Edge 8000 product: standalone for a single device, and High Availability for a pair of devices.

Contents

Workflow for Initial Setup - Standalone

Use the following workflow to configure standalone service on a single new Edge 8000 device. (Refer to Workflow for Initial Setup - High Availability to configure High Availability on a pair of Edge 8000 devices.)

Prerequisites

- Login access to the following user interfaces:
  - Edge 8000 CLI, as user *sysadm*
  - Edge 8000 webUI, as user *admin*
  - RAMP CLI, as users *insight* and *admin*

Refer to Password Defaults for the initial (default) passwords.

Workflow

Step	Action	User Interface Required
1	Physically install the device. Install the device and its cabling. Power on the system. Refer to Installing Edge 8000 Hardware.	
2	Configure the initial platform settings.[1] Refer to Running Setup Wizard - Standalone.	Edge 8000 CLI via the front panel serial console port
3	Generate and install the SWe Edge license.[2] Refer to: • Ordering a License and Generating a Key • Install an SBC SWe Edge License	Edge 8000 GUI via web browser
4	Configure the SWe Edge application.[1] Refer to Configuration Guides and Configuration Examples.	Edge 8000 GUI via web browser
5	Configure dynamic RAMP registration.[3] Refer to Register an Edge 8000 Device.	RAMP CLI via ssh client

Notes:

1. Upon initial login, the system instructs you to change the password. Refer to Password Defaults for the initial (default) passwords.
2. Each Edge 8000 device comes factory-installed with an on-premise, virtual machine (VM) version of SBC SWe Edge. Follow the procedures to order a node-locked production license, generate a license key, and install the license.
3. This step references the Ribbon Application Management Platform (RAMP) documentation.

Workflow for Initial Setup - High Availability

Use the following workflow to configure High Availability on a pair of new Edge 8000 devices. For an overview of the High Availability architecture and the associated user interface menus, refer to High Availability. (Refer to Workflow for Initial Setup - Standalone for configuring standalone service on a single Edge 8000 device.)

Prerequisites

- Login access to the following user interfaces:
  - Edge 8000 CLI, as user *sysadm*
  - Edge 8000 webUI, as user *admin*
  - RAMP CLI, as users *insight* and *admin*

Refer to Password Defaults for the initial (default) passwords.

Workflow

Step	Action	User Interface Required
1	Physically install the two Edge 8000 devices. Install the devices and their cabling. For High Availability, this includes connecting the HA cable between the devices. Power on the systems. Refer to Installing Edge 8000 Hardware.	
2	Configure the initial platform settings on the devices.[1] For High Availability, this includes: • changing the default CPU assignments to decrease the number of 6WIND Fast Path router cores to 2 and increase the SWe Edge call management cores to 4 • increasing the default SWe Edge memory to 4096 MB • utilizing Bridge 5 as the HA bridge Refer to Running Setup Wizard - High Availability. Perform this procedure on one and then on the other Edge 8000 device.	Edge 8000 CLI via the front panel serial console port
3	Activate High Availability on the two devices.[1,2] This includes: • setting each device's local and remote HA interface addresses so the Standby SWe Edge instance can monitor the Active SWe Edge instance • allowing the devices to reboot • installing a single HA license that applies to both devices Note that the first Edge 8000 device you enable for High Availability becomes the Active device; the other becomes the Standby. You install the HA License only on the Active Edge 8000 device. Once the Active instance accepts the licensing data, the HA feature automatically replicates the licensing information to the Standby. Refer to Activating High Availability.	Edge 8000 GUI via web browser

Step	Action	User Interface Required
4	Configure the SWe Edge application on the Active device.[1] On the Active device, complete all the provisioning required for the desired deployment. For the Standby device, manual provisioning is not required. The HA feature automatically replicates the SWe Edge configuration from the Active device to the Standby device in real-time. Refer to Configuration Guides and Configuration Examples.	Edge 8000 GUI via web browser
5	Configure dynamic RAMP registration on the Active device.[3] Refer to Register an Edge 8000 Device.	RAMP CLI via ssh client

Notes:

1. Upon initial login, the system instructs you to change the password. Refer to Password Defaults for the initial (default) passwords.
2. Each Edge 8000 device comes factory-installed with an on-premise, virtual machine (VM) version of SBC SWe Edge. Follow the procedures to order a node-locked production license, generate a license key, and install the license.
3. This step references the Ribbon Application Management Platform (RAMP) documentation.

Installing Edge 8000 Hardware

Use the following workflow to install an Edge 8000 Series device. For a High Availability (HA) system, this includes connecting the HA cable between two Edge 8000 devices.

Caution

Observe the following guidelines when installing an Edge 8000 system:

- Always verify that the device power cord is disconnected from any power source prior to installation.
- Ensure that the installation site has adequate air circulation and meets the minimum operating conditions for the system as specified in Edge 8000 Series Hardware Specifications.

Prerequisites

Gather the following items before starting. Refer to Edge 8000 Shipping Contents for the list of items included in shipping.

Installation items required:

- For rack mounting the unit:

    - Phillips-head screwdriver
    - Chassis bracket and chassis bracket screws — To attach brackets to the chassis
    - Rack mount screws — To attach the chassis by its mounting brackets to the rack
- SFP+ modules — To interface between the SFP ports of the unit to the public (WAN) network.
- Analog telephony cables — To connect the analog (FXS, FXO, and PRI (T1/E1)) ports of the unit to TDM-based telephone devices and services. (Does not apply to the Edge 8100 model).
- Ethernet cables — To connect the gigabit Ethernet ports of the unit to private (LAN) switches, individual VoIP devices, and public (WAN) devices; and to connect one HA port to another port between two High Availability Edge 8000 devices.
- RS232 serial console cable — To provide administrative access to the unit from a laptop computer through the serial console port.

Attention

Ribbon designs all Edge 8000 models with an internal surge protection system. For more effective protection, Ribbon recommends connecting the Edge 8000 device to an external surge protector or UPS.

Workflow

Step	Action
1	Place or Mount the Edge 8000 Device
2	Connect the Network Cables
3	Connect the Power Cables and Power on the Device

Place or Mount the Edge 8000 Device

For a High Availability deployment, perform this procedure for both Edge 8000 devices.

Start

1. Remove the device and accessories from the shipping container.
2. Place the device on a flat, dry surface such as a desktop, shelf, or tray.
3. For a rack mounted deployment, install the device on the rack.
    a. Attach the rack mount brackets to both sides of the Edge 8000 chassis with the chassis bracket screws supplied by Ribbon.
    b. Install the chassis in the rack with rack mount screws (not supplied by Ribbon).

Connect the Network Cables

Connect all SFP+ modules and all cables supplied by your system administrator or network planning team. This includes the HA Ethernet cable between two Edge 8000 devices for a High Availability (HA) deployment.

Start

1. Install the SFP+ modules.
2. Connect the routing cables per your network design:
    a. Cables to the two SFP+ ports
    b. Cables to the eight Gigabit Ethernet (GE) RJ-45 ports
3. For the Edge 8300 device, connect the telephony cables:

   a. T1/E1 cables to the T1/E1 ports
   b. FXS phone lines to the Amphenol connector
   c. FXO lines to the RJ-11 ports (for devices equipped with FXO ports)
4. For a High Availability system, connect an Ethernet cable between the HA ports of the two Edge 8000 devices.
   Example: connect an Ethernet cable between port GE 6 (ge6) of the first unit to the same port, GE 6 (ge6), of the other unit.
5. Connect the console cable from your System Administrator (laptop) computer to the Console RJ-45 port, or from a network terminal server to the Console RJ-45 port.

Connect the Power Cables and Power on the Device

The Edge 8000 Series devices include single AC, redundant AC, and redundant DC models.

Connect the device to the power source and power on the system.

Caution

1. Always connect the power cord(s) to a power source suitable for the power required of the unit being installed. Refer to Specifications and Certifications.
2. Secure the power cord to a cable management system using a fastener or tie wrap.

Warning

The equipment has a separate protective earthing terminal on the chassis that must be permanently connected to earth ground to adequately ground the chassis and protect the operator from electrical hazards.

Start

1. Connect the AC or DC power.
   a. If the unit is equipped for AC power, connect the AC power cable from the AC outlet or outlets to the unit.
   b. If the unit is equipped for DC power, connect the DC power source to the power lugs on the device.
2. Press the Power Switch on.
   a. If the unit is equipped with a single AC power supply, press the Power Switch to the On position to start the device.
   b. If the unit is equipped with redundant AC or DC power supplies, press the Power Switch for 4 - 5 seconds to start the device.
3. Make sure the power LED on the front panel is a solid green after the device powers on.

Running Setup Wizard

Run the Edge 8000 Setup Wizard to configure the device for standalone service or High Availability (HA), depending on if the deployment is for a single device or a pair of Edge 8000 devices.

Contents

Running Setup Wizard - Standalone

Use the following workflow to set up the basic platform characteristics of a single Edge 8000 device.

For the complete configuration instructions for standalone service, refer to Workflow for Initial Setup - Standalone.

Attention

Remember these important considerations when running Setup Wizard:

1. Plan to run the Setup Wizard only once, since you can only define the IP addresses and host name of the internal configuration container and SBC SWe Edge VM once when they are initially created. To update the settings later, you must perform a factory reset of the device and then rerun the Setup Wizard. A few specific cases may warrant rerunning the Setup Wizard:
   a. Changing the memory assigned to the SBC SWe Edge VM, such as when the intent is to change an existing setup to use 30 cps vs 10 cps
   b. Changing the vCPU assigned to the SBC SWe Edge VM
   c. Adding extra interfaces to the SBC SWe Edge VM
2. The Setup Wizard "save" option is only allowed when the user is running Setup Wizard from a telnet or console session and not via an SSH session. Attempting to save while connected from an SSH session results in an error message. This is to ensure that the user has access to the device in case the user incorrectly configures the network and the device becomes isolated.

Prerequisites

- Login access to the Edge 8000 CLI as user system administrator (*sysadm*).

  Note that initially, the serial console port of the front panel provides the login access, either directly from a physically connected laptop or remotely via a terminal server. Refer to Edge 8000 Front and Back Panels for the location and description of the console port. Once the setup is complete, you can access the CLI remotely through a secure shell (ssh) connection using port 22 and the management interface IP address established with Bridge 2. See Complete the BR1, 2, 4, and 5 Menus of this workflow.

Workflow

Step	Action
1	Log in and Start the Setup Wizard
2	Complete the System Menu
3	Complete the BR1, 2, 4, and 5 Menus
4	Complete the GE1-8 Menus
5	Complete the SFP9-10 Menus
6	Complete the Default Gateway Menu
7	Complete the SWe-Edge Settings Menu

Step	Action
8	Exit the Setup Wizard

Job Aid: Navigating Within the Setup Wizard

The Setup Wizard is a text user interface (TUI). To move between elements and activate selections, use the following keys from the keyboard.

Key	Movement or Action
Up-arrow, down-arrow	moves the selection up or down one element in the same area
Tab	moves the selection between areas
Enter	activates a selection
Space bar	toggles a selection between enabled [*] and not enabled [ ]

Log In and Start the Setup Wizard

1. From the Edge 8000 CLI, log in as user system administrator (*sysadm*).
2. Follow the prompts to change the password, and then log in again.
   Refer to Password Management for the initial (default) passwords.
3. Change to root user. Enter the new password you chose in the previous step.

```
$ sudo -i
password for sysadm:
```

4. Start the Setup Wizard.

```
# setupwizard
```

   The System Startup Configuration window appears.

Complete the System Menu

1. From the System Startup Configuration window, select **System** and press **Enter**.
2. The System Configuration window appears, showing available elements to configure: Hostname, PRI type, and 6WIND fast path cores.
3. Press the down-arrow key to select an element in the System Configuration window.
   For example,
   a. Select **Hostname** and press **Enter**.
      The Host Configuration window appears.
   b. Configure the Hostname settings.

c. Click **OK** to save the settings.
The System Configuration window appears again, enabling you to select another element for configuration.

4. Modify the system settings per the field definitions given in the following table.
5. Click **OK** to save the settings.

System Configuration - Field Definitions

Field	Descriptions
Hostname	Enter the hostname of your system. Default: e8000
PRI type	Select the PRI interface type from one of the following options: • T1Net • T1User • E1Net • E1User Additional notes: Network-side PRI (T1Net or E1Net) enables the Edge 8000's SIP User Agent (SIP_UA) to provide a standard ISDN PRI network-side interface to a legacy TDM PBX and mimic the behavior of legacy phone switches. The SIP_UA receives calls from a TDM PBX and connects the calls to the IP network using SIP and vice versa. User-side PRI (T1User or E1User) enables the Edge 8000's SIP gateway (SIP_GW) to provide a standard PRI client-side interface to the PSTN. The SIP_GW receives calls from the IP network and connects them through PRI to the PSTN and vice versa. Whichever PRI type you choose here determines the menu choices available later in the Analog PRI-Setting folder of the Edge 8000 webUI.
6WIND fast path cores	Enter the number of CPU cores to use for the 6WIND fast path. Default: 4 Available values: 2, 4, and 6 Supported values for the 6WIND application in the Edge 8000 device: 2 and 4 Additional notes: This field enables the 6WIND router to access more or fewer CPU cores in the host operating system. Consult Ribbon Technical Support before modifying the fast path cores setting, as Ribbon has optimized the default settings (4 CPU cores for 6WIND fast path, 2 for SBC SWe Edge) for overall Edge 8000 performance.

Complete the BR1, 2, 4, and 5 Menus

1. From the System Startup Configuration window, select a bridge and press **Enter**.
   A Bridge Configuration window appears, for example, the BR1 Configuration window.
2. Modify the bridge settings per the field definitions given in the following table.

> **Note**
>
> BR3 is an internal bridge with no provisionable fields.

3. Click **OK** to save the settings.

BR1, 2, 4, and 5 Configuration - Field Definitions

Field	Descriptions
Interface Name	Required field for all bridges. Default names: BR1 VNF Private: br1 BR2 VNF Management: br2 BR4 VNF Public: br4 BR5 VNF Additional: br5 Additional notes: BR1 and BR4 are associated with SBC SWe Edge. BR1 typically serves as the LAN side of an Edge 8000 device, and BR4 typically serves as the WAN side of the device. BR2 provides administrative access to all of the Edge 8000 components, including the SBC SWe Edge VNF.
IPv4 Address	Required field for all bridges. Default addresses: BR1 Configuration: 192.168.1.1 BR2 Configuration: 192.168.122.1 BR4 Configuration: 0.0.0.0 BR5 Configuration: 0.0.0.0
Netmask Length	Required field for all bridges. Default: 24 Additional Notes: The allowed range for netmask is 16-28 for BR1 and BR2. For BR4 and BR5, it can be any value.

Field	Descriptions
Members	Optional field, available for BR1, BR2, BR4, and BR5. Default members: BR1: ge1 ge2 ge3 ge4 BR2: ge7 (BR4 and BR5 do not have defaults.) Possible values: ge1-ge8, sfp9, sfp10 Additional Notes: The physical port you assign as a member of Bridge 2 will be the access point for the CLI and webUI management of the device.
DHCP server	Optional field, available for BR1, BR2. Default: enabled [*] Additional Notes: The DHCP server serves external DHCP clients assigned to the bridge. The default DHCP start range is based on the network IP (IP address intersected with the netmask) plus the value 2. The end range is the network IP plus the value 12.
Enable DHCP Client	Optional field, available for BR4, BR5. Default: enabled [*] **Note** If you specify an interface in the Members field and leave DHCP client enabled [*], you must keep the IPv4 address at the default value of 0.0.0.0 and manually configure a gateway and DNS. If you specify an interface in the Members field and disable DHCP client [ ], you must enter a static IPv4 address.

Complete the GE1-8 Menus

1. From the System Startup Configuration window, select a Gigabit Ethernet (GE) port and press **Enter**. A GE Configuration window appears, for example the GE1 Configuration window.
2. Modify the Gigabit Ethernet settings per the field definitions given in the following table.

> **Note**
>
> If the interface is a member of a bridge, do not enter values in the IPv4 Address and Netmask Length fields. Leave the default values in place.

3. Click **OK** to save the settings.

GE1-8 Configuration - Field Definitions

Field	Descriptions
Interface Name	Default names for interfaces GE1-8: ge1 ge2 ge3 ge4 ge5 ge6 ge7 ge8
IPv4 Address	Default: 0.0.0.0
Netmask Length	Default: 0

Complete the SFP9-10 Menus

1. From the System Startup Configuration window, select an SFP port and press **Enter**.
   An SFP window appears, for example, the SFP9 Configuration window.
2. Modify the SFP settings per the field definitions given in the following table.

> **Note**
>
> If the interface is a member of a bridge interface, do not enter IPv4 Address and Netmask Length values. Leave the default values in place.

3. Click **OK** to save the settings.

SFP9-10 Configuration - Field Definitions

Field	Description
Interface Name	Default names: sfp9 sfp10
IPv4 Address	Enter the IP address. Default: 0.0.0.0 **Note** To assign a static IP address in the IPv4 Address field, you must disable the DHCP client. (Press the space bar in the Enable DHCP Client field to toggle between enabled [*] and disabled [ ].)

Field	Description
Netmask Length	Default: 0
Enable DHCP Client	Default: disabled [ ] **Note** To activate a DHCP client, change the DHCP Client field to enabled [*], keep the IPv4 address at the default value of 0.0.0.0, and manually configure a gateway and DNS.

Complete the Default Gateway Menu

1. From the System Startup Configuration window, select **Default Gateway** and press **Enter**.
   The Default Gateway window appears.
2. Modify the default gateway settings per the field definitions given in the following table.
3. Click **OK** to save the settings.

Default Gateway Configuration - Field Definitions

Field	Description
IPv4 Address	Enter the IP address. Default: 0.0.0.0 Additional notes: The IPv4 address must be within a subnet on an interface.

Complete the SWe-Edge Settings Menu

1. From the System Startup Configuration window, select **SWe-Edge Settings** and press **Enter**.
   The Swe-Edge Configuration window appears.
2. Modify the SWe Edge settings per the field definitions given in the following table.
3. Click **OK** to save the settings.

SWe Edge Configuration - Field Definitions

Field	Description
CPUs (1 2 4)	Default: 2 Additional notes: This field enables the 6WIND router to access more or fewer CPU cores in the host operating system. Consult Ribbon Technical Support before modifying the fast path cores setting, as Ribbon has optimized the default settings for overall Edge 8000 performance.
Memory in MBs (1536-4096)	Default: 2048
Extra Interface 1, 2	The Extra Interface values must be one of the VNF bridge interface names (BR4 or BR5). Default: not assigned Additional notes: BR4 is the VNF Public bridge. BR5 is the VNF Additional bridge.

Exit the Setup Wizard

Exiting the Setup Wizard saves the configuration settings and applies the changes. This will cause a service interruption for approximately 3 minutes, during which time the system will be unreachable.

1. From the System Startup Configuration window, select **SAVE** and press **Enter**.
2. From the Confirm Screen window, select **OK** and press **Enter**.

> **Caution**
>
> This operation causes a service disruption. Perform this procedure only during a maintenance window.

Running Setup Wizard - High Availability

Use the following workflow to set up the basic platform characteristics of a pair of Edge 8000 devices.

For the complete configuration instructions for High Availability, refer to Workflow for Initial Setup - High Availability.

Attention

Remember these important considerations when running Setup Wizard:

1. Plan to run the Setup Wizard only once, since you can only define the IP addresses and host name of the internal configuration container and SBC SWe Edge VM once when they are initially created. To update the settings later, you must perform a factory reset of the device and then rerun the Setup Wizard. A few specific cases may warrant rerunning the Setup Wizard:
   a. Changing the memory assigned to the SBC SWe Edge VM, such as when the intent is to change an existing setup to use 30 cps vs 10 cps
   b. Changing the vCPU assigned to the SBC SWe Edge VM
   c. Adding extra interfaces to the SBC SWe Edge VM
2. The Setup Wizard "save" option is only allowed when the user is running Setup Wizard from a telnet or console session and not via an SSH session. Attempting to save while connected from an SSH session results in an error message. This is to ensure that the user has access to the device in case the user incorrectly configures the network and the device becomes isolated.

Note that the actions performed in this workflow mirror those found in Running Setup Wizard - Standalone. Where differences exist, Attention boxes highlight actions that are unique to High Availability. For example:

Attention

For High Availability, set the **6WIND fast path cores** to 2. Decreasing the 6WIND cores to 2 allows you to increase the SBC SWe Edge CPUs to 4 later in this procedure.

Use this workflow twice, once for each Edge 8000 device. Then return to Workflow for Initial Setup - High Availability.

Prerequisites

- Login access to the Edge 8000 CLI as user system administrator (*sysadm*).

  Note that initially, the serial console port of the front panel provides the login access, either directly from a physically connected laptop or remotely via a terminal server. Refer to Edge 8000 Front and Back Panels for the location and description of the console port. Once the setup is complete, you can access the CLI remotely through a secure shell (ssh) connection using port 22 and the management interface IP address established with Bridge 2. See Complete the BR1, 2, 4, and 5 Menus of this workflow.

Workflow

Step	Action
1	Log in and Start the Setup Wizard
2	Complete the System Menu[1]
3	Complete the BR1, 2, 4, and 5 Menus[1]
4	Complete the GE1-8 Menus
5	Complete the SFP9-10 Menus

Step	Action
6	Complete the Default Gateway Menu
7	Complete the SWe-Edge Settings Menu[1]
8	Exit the Setup Wizard

[1] This procedure contains an Attention box highlighting actions that are unique to High Availability.

Job Aid: Navigating Within the Setup Wizard

The Setup Wizard is a text user interface (TUI). To move between elements and activate selections, use the following keys from the keyboard.

Key	Movement or Action
Up-arrow, down-arrow	moves the selection up or down one element in the same area
Tab	moves the selection between areas
Enter	activates a selection
Space bar	toggles a selection between enabled [*] and not enabled [ ]

Log In and Start the Setup Wizard

1. From the Edge 8000 CLI, log in as user system administrator (*sysadm*).
2. Follow the prompts to change the password, and then log in again.
   Refer to Password Management for the initial (default) passwords.
3. Change to root user. Enter the new password you chose in the previous step.

```
$ sudo -i
password for sysadm:
```

4. Start the Setup Wizard.

```
# setupwizard
```

   The System Startup Configuration window appears.

Complete the System Menu

1. From the System Startup Configuration window, select **System** and press **Enter**.

2. The System Configuration window appears, showing available elements to configure: Hostname, PRI type, and 6WIND fast path cores.
3. Press the down-arrow key to select an element in the System Configuration window. For example,
   a. Select **Hostname** and press **Enter**.
      The Host Configuration window appears.
   b. Configure the Hostname settings.
   c. Click **OK** to save the settings.
      The System Configuration window appears again, enabling you to select another element for configuration.
4. Modify the system settings per the field definitions given in the following table.

> **Attention**
>
> For High Availability, set the **6WIND fast path cores** to 2. Decreasing the 6WIND cores to 2 allows you to increase the SBC SWe Edge CPUs to 4 later in this procedure in Complete the SWe-Edge Settings Menu.

5. Click **OK** to save the settings.

System Configuration - Field Definitions

Field	Descriptions
Hostname	Enter the hostname of your system. Default: e8000
PRI type	Select the PRI interface from one of the following options: • T1Net • T1User • E1Net • E1User Additional notes: Network-side PRI (T1Net or E1Net) enables the Edge 8000's SIP User Agent (SIP_UA) to provide a standard ISDN PRI network-side interface to a legacy TDM PBX and mimic the behavior of legacy phone switches. The SIP_UA receives calls from a TDM PBX and connects the calls to the IP network using SIP and vice versa. User-side PRI (T1User or E1User) enables the Edge 8000's SIP gateway (SIP_GW) to provide a standard PRI client-side interface to the PSTN. The SIP_GW receives calls from the IP network and connects them through PRI to the PSTN and vice versa. Whichever PRI type you choose here determines the menu choices available later in the Analog PRI-Setting folder of the Edge 8000 webUI.

Field	Descriptions
6WIND fast path cores	Enter the number of CPU cores to use for the 6WIND fast path. Default: 4 Available values: 2, 4, and 6 Supported values for the 6WIND application in the Edge 8000 device: 2 and 4 Additional notes: For High Availability, enter 2.

Complete the BR1, 2, 4, and 5 Menus

1. From the System Startup Configuration window, select a bridge and press **Enter**.
   A Bridge Configuration window appears, for example, the BR1 Configuration window.
2. Modify the bridge settings per the field definitions given in the following table.

Attention

For High Availability, configure Bridge 5 as the HA interface bridge:

- Enter an **IPv4 Address** that is:
  - unique to the device being configured but on the same subnet as Bridge 5 of the other HA device
  - one address higher than the HA base IP address you will enter when you enable HA for the device in the Edge 8000 webUI, per procedure Activating High Availability (Example: if you plan to enter 10.10.10.41 for the local IP address when you enable HA on the device, then enter 10.10.10.42 here for the Bridge 5 IP address)
- In the bridge **Members** field, enter the name of the port you used for HA cabling when you physically installed the device. (Refer to Connect the Network Cables.) Example: ge6.
- Disable **DHCP Client** (press the space bar to change the field to [ ]).

Note

BR3 is an internal bridge with no provisionable fields.

3. Click **OK** to save the settings.

BR1, 2, 4, and 5 Configuration - Field Definitions

Field	Descriptions
Interface Name	Required field for all bridges. Default names: BR1 VNF Private: br1 BR2 VNF Management: br2 BR4 VNF Public: br4 BR5 VNF Additional: br5 Additional notes: BR1 and BR4 are associated with SBC SWe Edge. BR1 typically serves as the LAN side of an Edge 8000 device, and BR4 typically serves as the WAN side of the device. BR2 provides administrative access to all of the Edge 8000 components, including the SBC SWe Edge VNF. BR5 serves as an HA interface bridge. Enter an **IPv4 Address** that is: • unique to the device being configured but on the same subnet as Bridge 5 of the other HA device • one address higher than the HA base IP address you will enter when you enable HA for the device in the Edge 8000 webUI, per procedure Activating High Availability
IPv4 Address	Required field for all bridges. Default addresses: BR1 Configuration: 192.168.1.1 BR2 Configuration: 192.168.122.1 BR4 Configuration: 0.0.0.0 BR5 Configuration: 0.0.0.0 Additional Notes: For High Availability, enter an IPv4 address for BR5 that is unique to the device being configured but on the same subnet as BR5 of the other HA device.
Netmask Length	Required field for all bridges. Default: 24 Additional Notes: The allowed range for netmask is 16-28 for BR1 and BR2. For BR4 and BR5, it can be any value.

Field	Descriptions
Members	Optional field, available for BR1, BR2, BR4, and BR5. Default members: BR1: ge1 ge2 ge3 ge4 BR2: ge7 (BR4 and BR5 do not have defaults.) Possible values: ge1-ge8, sfp9, sfp10 Additional Notes: The physical port you assign as a member of Bridge 2 will be the access point for the CLI and webUI management of the device. For High Availability, enter as a member of Bridge 5 the name of the port, such as ge6, that you used for HA cabling when you physically installed the device.
DHCP server	Optional field, available for BR1, BR2. Default: enabled [*] Additional Notes: The DHCP server serves external DHCP clients assigned to the bridge. The default DHCP start range is based on the network IP (IP address intersected with the netmask) plus the value 2. The end range is the network IP plus the value 12.
Enable DHCP Client	Optional field, available for BR4, BR5. Default: enabled [*] Additional Notes: For High Availability, disable DHCP Client. **Note** If you specify an interface in the Members field and leave DHCP client enabled [*], you must keep the IPv4 address at the default value of 0.0.0.0 and manually configure a gateway and DNS. If you specify an interface in the Members field and disable DHCP client [ ], you must enter a static IPv4 address.

Complete the GE1-8 Menus

1. From the System Startup Configuration window, select a Gigabit Ethernet (GE) port and press **Enter**. A GE Configuration window appears, for example the GE1 Configuration window.
2. Modify the Gigabit Ethernet settings per the field definitions given in the following table.

> **Note**
>
> If the interface is a member of a bridge, do not enter values in the IPv4 Address and Netmask Length fields. Leave the default values in place.

3. Click **OK** to save the settings.

GE1-8 Configuration - Field Definitions

Field	Descriptions
Interface Name	Default names for interfaces GE1-8: ge1 ge2 ge3 ge4 ge5 ge6 ge7 ge8
IPv4 Address	Default: 0.0.0.0
Netmask Length	Default: 0

Complete the SFP9-10 Menus

1. From the System Startup Configuration window, select an SFP port and press **Enter**. An SFP window appears, for example, the SFP9 Configuration window.
2. Modify the SFP settings per the field definitions given in the following table.

> **Note**
>
> If the interface is a member of a bridge interface, do not enter IPv4 Address and Netmask Length values. Leave the default values in place.

3. Click **OK** to save the settings.

SFP9-10 Configuration - Field Definitions

Field	Description
Interface Name	Default names: sfp9 sfp10

Field	Description
IPv4 Address	Enter the IP address. Default: 0.0.0.0 **Note** To assign a static IP address in the IPv4 Address field, you must disable the DHCP client. (Press the space bar in the Enable DHCP Client field to toggle between enabled [*] and disabled [ ].)
Netmask Length	Default: 0
Enable DHCP Client	Default: disabled [ ] **Note** To activate a DHCP client, change the DHCP Client field to enabled [*], keep the IPv4 address at the default value of 0.0.0.0, and manually configure a gateway and DNS.

Complete the Default Gateway Menu

1. From the System Startup Configuration window, select **Default Gateway** and press **Enter**.
   The Default Gateway window appears.
2. Modify the default gateway settings per the field definitions given in the following table.
3. Click **OK** to save the settings.

Default Gateway Configuration - Field Definitions

Field	Description
IPv4 Address	Enter the IP address. Default: 0.0.0.0 Additional notes: The IPv4 address must be within a subnet on an interface.

Complete the SWe-Edge Settings Menu

1. From the System Startup Configuration window, select **SWe-Edge Settings** and press **Enter**.
   The Swe-Edge Configuration window appears.
2. Modify the SWe Edge settings per the field definitions given in the following table.

Attention

For High Availability:

- Set the **CPUs** value to 4. This increases the CPUs assigned to SWe Edge processing, as required for High Availability. (Earlier, in Complete the System Menu, you decreased the number of CPUs assigned for 6WIND fast path CPU cores to 2 to maintain the correct balance of CPU assignments.)
- Enter 4096 for the **Memory**.
- Enter Bridge 5 (br5) for the value of **Extra Interface 2**. This is the interface you configured in Complete the BR1-4 Menus for the HA interface between the two devices.

3. Click **OK** to save the settings.

SWe Edge Configuration - Field Definitions

Field	Description
CPUs (1 2 4)	Default: 2 Additional Notes: For High Availability, enter 4.
Memory in MBs (1536-4096)	Default: 2048 Additional Notes: For High Availability, enter 4096.
Extra Interface 1, 2	The Extra Interface values must be one of the VNF bridge interface names (BR4 or BR5). Default: not assigned Additional notes: BR4 is the VNF Public bridge. BR5 is the VNF Additional bridge. For High Availability, enter BR5 for the value of Extra Interface 2.

Exit the Setup Wizard

Exiting the Setup Wizard saves the configuration settings and applies the changes. This will cause a service interruption for approximately 3 minutes, during which time the system will be unreachable.

1. From the System Startup Configuration window, select **SAVE** and press **Enter**.
2. From the Confirm Screen window, select **OK** and press **Enter**.

Caution

This operation causes a service disruption. Perform this procedure only during a maintenance window.

Activating High Availability

Use the following workflow to activate High Availability on a pair of newly installed Edge 8000 devices. The workflow includes setting each device's local and remote HA interface addresses and installing the single HA license that applies to both devices.

Refer to High Availability for an overview of the feature and a summary of the corresponding HA user interface changes. Refer to Workflow for Initial Setup - High Availability for the complete installation and configuration instructions.

Prerequisites

- Login access at each device to the Edge 8000 webUI as user administrator (*admin*).
- Completion of the Workflow for Initial Setup - High Availability up to this point in the workflow.
- A Node-Locked License (NLL) for Edge 8000 HA deployment uploaded to the Active device. Note that generating the license file in Salesforce requires the SBC SWe Edge IDs of both devices. Refer to Obtaining and Installing an SBC SWe Edge Production Node-Locked License.
- Ethernet interfaces defined or reserved for the SBC SWe Edge function, as follows:

<table>
<tr><th>SBC Ethernet Interface Type</th><th>Characteristics</th><th></th></tr>
<tr><td>High Availability</td><td>Each device has a dedicated SBC SWe Edge HA interface, High Availability.

When you enable HA for a device, you assign a local IP address that serves as the device's base HA IP address. From that, the system automatically assigns three IP addresses to support the device's HA interface.

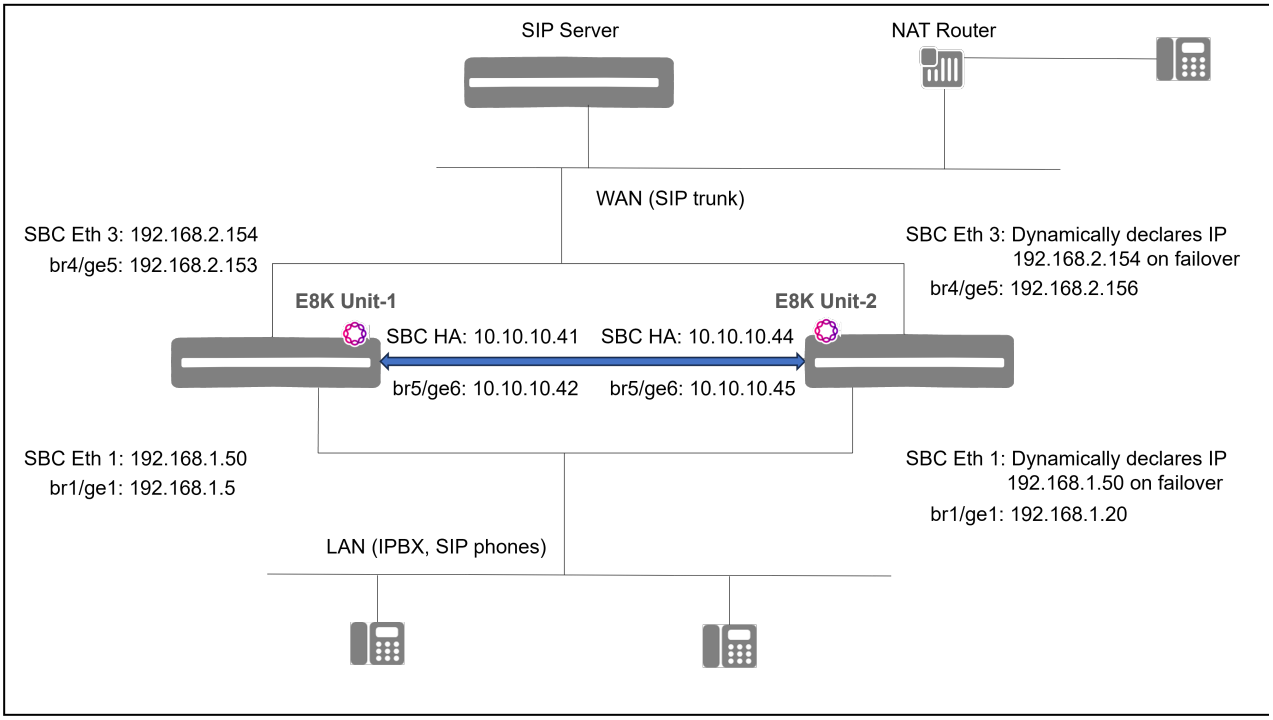
Note
The base HA IP addresses of the two devices must be static IPv4 addresses on the same subnet and at least three addresses apart. Example: 10.10.10.41 and 10.10.10.44.

Here is an example of the IP address assignments for a pair of Edge 8000 devices after HA has been enabled on both devices:

<table>
<tr><th rowspan="2">IP Address</th><th rowspan="2">Purpose</th><th colspan="2">Example:</th></tr>
<tr><th>Active Device</th><th>Standby Device</th></tr>
<tr><td>base IP address</td><td>HA interface</td><td>10.10.10.41</td><td>10.10.10.44</td></tr>
<tr><td>base IP address +1</td><td>Bridge 5[1]</td><td>10.10.10.42</td><td>10.10.10.45</td></tr>
<tr><td>base IP address +2</td><td>Configuration sync[2]</td><td>10.10.10.43</td><td>10.10.10.46</td></tr>
</table>
[1] Overrides any assignment made in the Setup Wizard.
[2] Not viewable or configurable to the user from the webUI.</td><td></td></tr>
</table>

SBC Ethernet Interface Type	Characteristics	
Media (packet)	Each device has SWe Edge media (packet) interfaces, **Ethernet 1** and **Ethernet 3**. You will assign unique, static IP addresses to the media interfaces later, after you have enabled HA on the two devices. Refer to Workflow for Initial Setup - High Availability. (The SWe Edge settings replicate automatically to the Standby device in real-time when you configure the Active device.)	

HA Deployment Example



Workflow

Step	Action
1	Enable High Availability on Active and Standby Devices
2	Verify High Availability Status
3	Install an HA License

Enable High Availability on Active and Standby Devices

Enter the local and remote HA interface IP addresses of the first High Availability device, then allow the device to reboot. Repeat the steps for the other device.

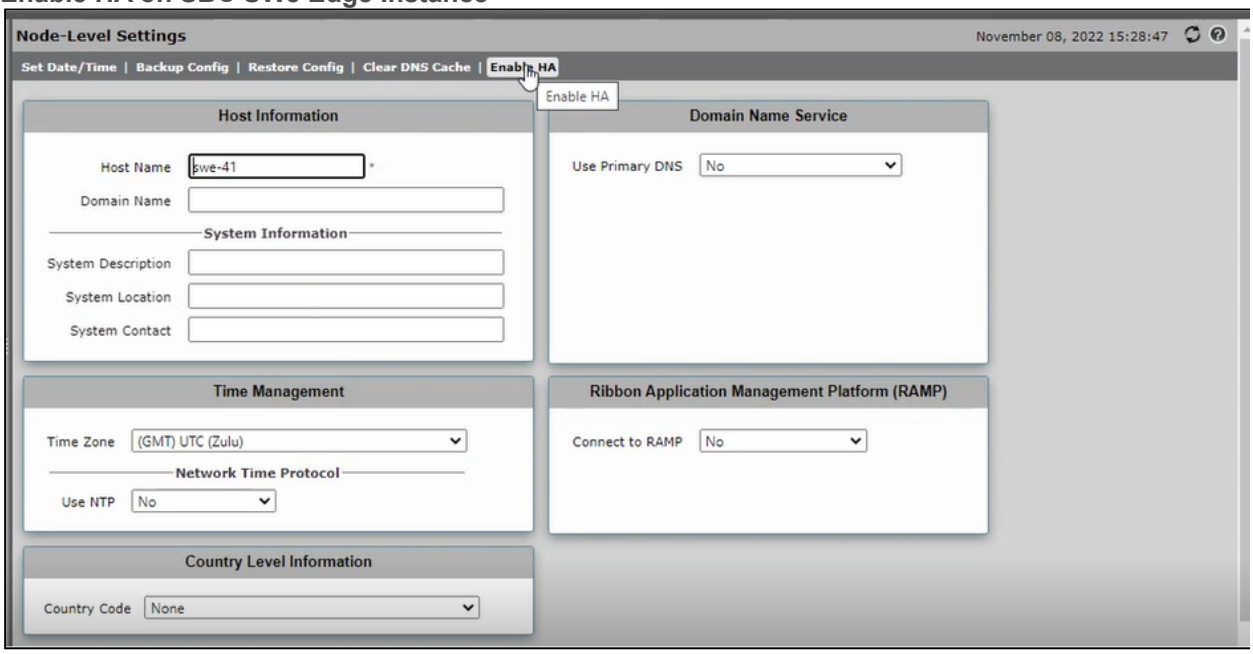
> **Note**
>
> In the following procedure, to "Log in to your SBC SWe Edge instance" means to log in to the Edge 8000 webUI.

> **Attention**
>
> When assigning local and remote IP addresses, they must be static IPv4 addresses on the same subnet and at least three addresses apart. Example: 10.10.10.41 and 10.10.10.44.

Start

1. Log in to your SBC SWe Edge instance.
2. Click the **Settings** tab at the top of the WebUI.
3. In the left navigation pane, go to **System** > **Node-level Settings.**
4. Click **Enable HA.**

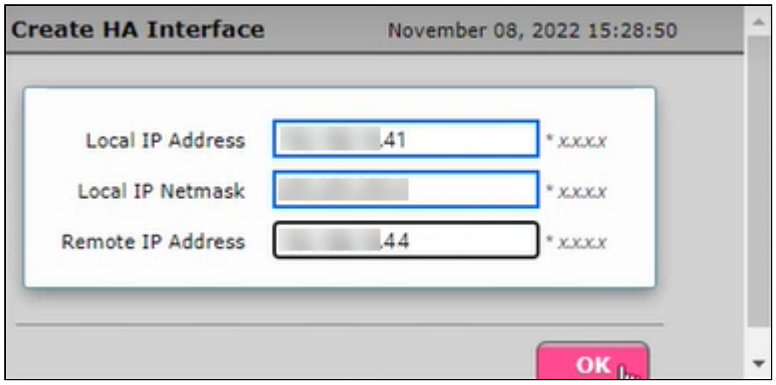
Enable HA on SBC SWe Edge Instance



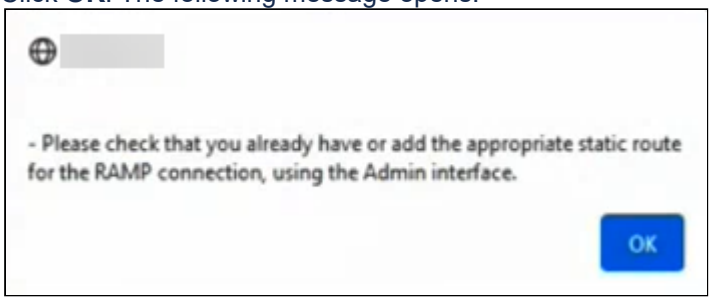
5. Enter the Local IP Address, Local IP Netmask, and Remote IP Address in the Create HA Interface pop-up window.

> **Note**
>
> The Local IP is the HA IP address of the instance you are currently logged in. The Remote IP is the other HA IP address of the other instance, as mentioned in the the Prerequisites section.

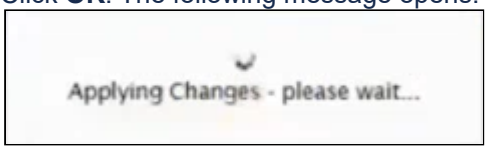
Create HA Interface on the Instance



6. Click **OK**. The following message opens.



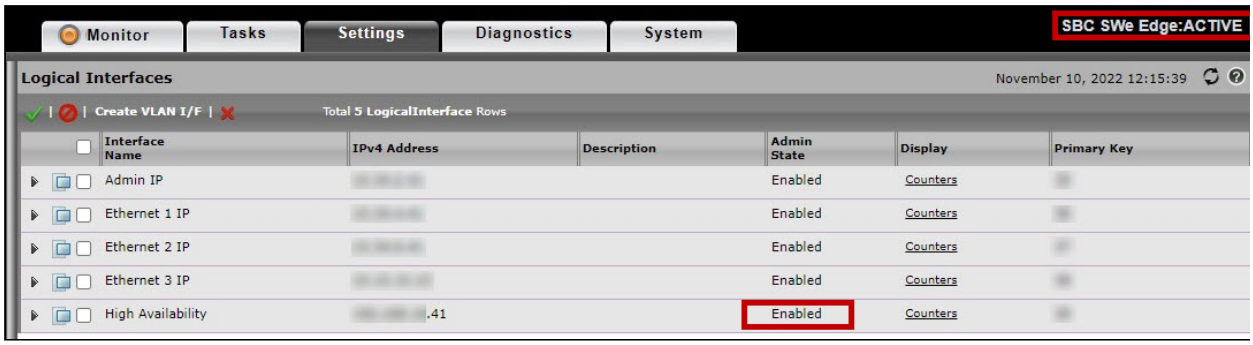
7. Click **OK**. The following message opens.



> **Note**
>
> It takes about 2 minutes for the instance to reboot. The system takes you back to the log in page once the reboot is complete.

8. Log in to your SBC SWe Edge instance.
9. Click the **Settings** tab at the top of the WebUI.
10. In the left navigation pane, go to **Networking Interfaces** > **Logical Interfaces**.
    (In the Edge 8000 webUI, go to **SBC** > **Networking Interfaces** > **Logical Interfaces**.)

HA Interface on the Active Instance



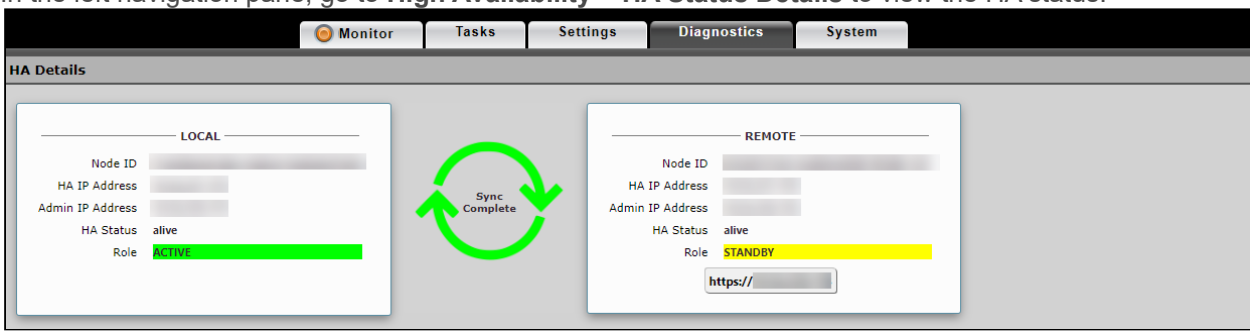
11. Confirm that HA is enabled on this instance. The HA role of the instance is seen at the top right hand corner of the WebUI.
12. Repeat steps 1 to 11 in the second instance, which will become the Standby.

Verify High Availability Status

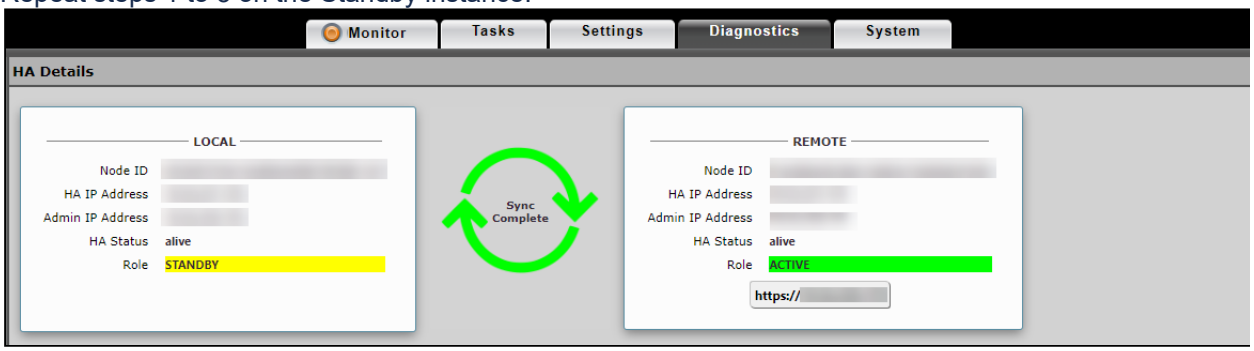
Check the High Availability status to ensure that both devices, referred to as the the Active and Standby instances, are properly enabled.

Start

1. Log in to the Active instance.
2. Click the **Diagnostics** tab at the top of the WebUI.
3. In the left navigation pane, go to **High Availability > HA Status Details** to view the HA status.



4. Repeat steps 1 to 3 on the Standby instance.



Install an HA License

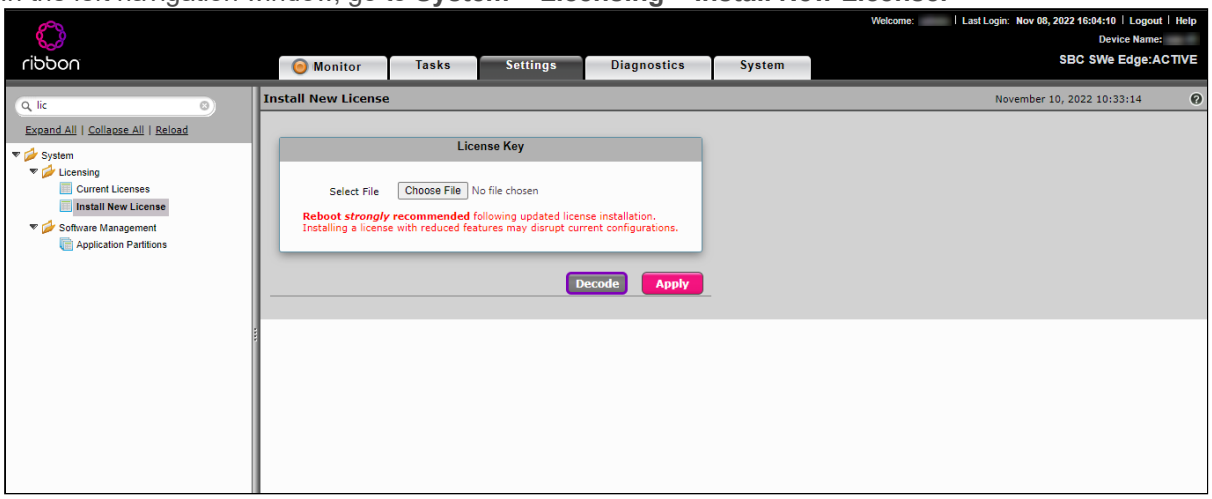
Install the HA license that applies to both devices.

> **Note**
>
> In step 3 of the following procedure, select SWe Edge from the **Version** dropdown list.

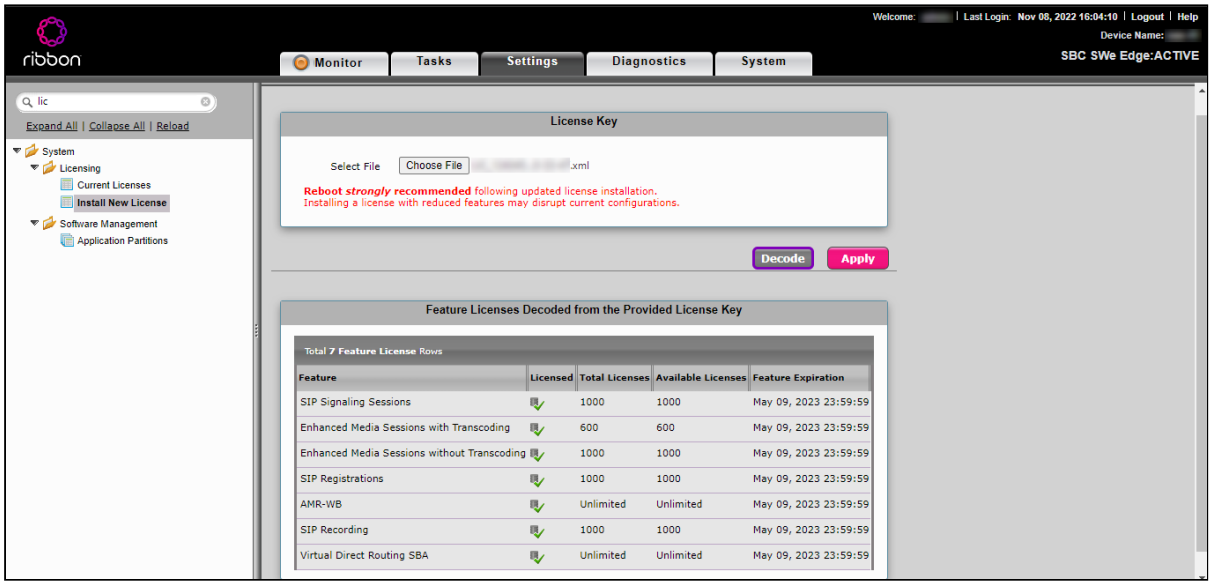
> **Attention**
>
> When you apply the HA license to the Active device, allow approximately 10 minutes for the license to appear and sync with the standby device.

Start

1. Log in to the Active instance.
2. Click the **Settings** tab at the top of the WebUI.
3. In the left navigation window, go to **System > Licensing > Install New License.**

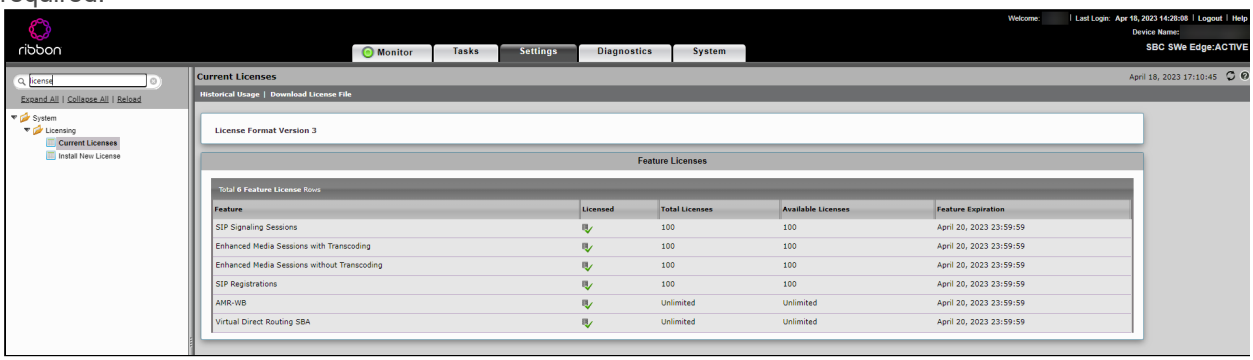


4. Click **Choose File** and upload your license key.
5. Click **Decode** to see the details of the license.



6. Click **Apply**.
7. In the left navigation pane, select **System** > **Licensing > Current Licenses**. The **Current Licenses** pane opens on the right.

8. In the **Feature Licenses** section, verify the license count that is currently available on the system is as required.



Hardware Guide

Contents

Edge 8000 Series Hardware Specifications

Contents

Specifications and Certifications

Contents

Device Characteristics

Edge 8000 Series devices provide data and voice connectivity toward a service provider network. Each unit has 10 Ethernet interfaces, 8 x 1GB RJ-45 and 2 x 10GB SFP+, and each interface can be configured for LAN (private) or WAN (public) use.

Data and voice services can be configured to use any interface on the system. When data service requires up to 10GB of data throughput, the SFP+ interfaces are used.

Voice services that require T1/E1 PRI support for SIP trunk replacement or for PSTN connectivity can be configured using the 4 x T1/E1 interfaces on the system, in a NET (PSTN) or USER (TDM PBX) orientation.

Voice services that require FXS support for analog devices, including T.38 for FAX devices, can be configured in one of two ways, depending on the model ordered:

- 24 x FXS ports
- 22 x FXS ports with 2 x FXO ports

Notes

1. The Edge 8000 model with 24 x FXS ports cannot be configured for FXO ports. Only the model with 22 x FXS ports and 2 x FXO ports offers FXO voice service for PSTN connectivity.
2. ISDN NFAS is not supported.

The Ribbon Edge 8000 Series is a family of platforms, 8100 and 8300.

Edge 8100 Vs Edge 8300

	EDGE-8100	EDGE-8300
CPU	C3758, 8-core	C3758, 8-core
System Memory	16GB DDR4 (2400MT)	16GB DDR4 (2400MT)
Storage	64GB SATA DOM	64GB SATA DOM
Boot Flash	16MB Flash for UEFI BIOS	16MB Flash for UEFI BIOS
Fiber Optic 10G	2 x SFP+ interface	2 x SFP+ interface
Copper 1GB	8 x RJ-45 interface	8 x RJ-45 interface
PCI-E Gen 3 x4 Connector	x4 PCIe bus bandwidth	x4 PCIe bus bandwidth
USB	2x USB 2.0 Front Type-A 1x USB 3.0 Type-A	2x USB 2.0 Front Type-A 1x USB 3.0 Type-A
Real Time Clock	Yes	Yes
Console Port	RJ45	RJ45
BIOS	UEFI 2.1	UEFI 2.1
T1 Support	N/A	4 T1/E1 ports
Phone/Line	N/A	22 FXS + 2 FXO
	N/A	24 FXS

	EDGE-8100	EDGE-8300
Reset Button	Yes	Yes
Fan Speed Control	Yes	Yes
Fan Air Flow	12.8 CFM (0.36 m3/min)	12.8 CFM (0.36 m3/min)
Number of Fans Used	3	3
Power Supply	1U Single AC PSU, Watts: 250W	1U Single AC PSU, Watts: 250W
	1U Redundant AC PSU, Watts: 300W	1U Redundant AC PSU, Watts: 300W
	1U Redundant DC PSU, Watts: 300W	1U Redundant DC PSU, Watts: 300W
Chassis	44mm (1.73”, 1U)H 445mm (17.5”)W 437.8mm (17.23”)D	44mm (1.73”, 1U)H 445mm (17.5”)W 437.8mm (17.23”)D

Environment and Hardware Specifications

Specifications

Characteristics	Specifications
Chassis dimensions	44mm (1.73”, 1U) H 445mm (17.5”) W 437.8mm (17.23”) D
Weight	4.1 kg (9 lbs) - Single power supply unit
Mounting options	Shelf or rack mountable
Operating temperature	0°C to 40°C
Operating relative humidity	4% to 90% (non-condensing)
Chassis power	ATX PSU 250W 110-240 VAC, 50-60 Hz Optional dual 300W AC or dual 300W 48V DC Power Supply
Processor	C3758 at 2.2 GHz

Characteristics	Specifications
Compliance	RoHS 2.0, UL/cUL, CB, FCC-15, FCC-68, ISED, IC, CE, RCM, VCCI

Capabilities Summary

Edge 8000 Series devices have the following capabilities:

- Functionality
  - SBC with or without transcoding
  - Support for legacy Analog interfaces (Edge 8300 only)
  - Routing and Security
- Throughput
  - Supports up to 10Gbps of system throughput for data and voice services
- Platform
  - Intel Atom 8 core processor
  - Alma Linux or Redhat Linux
  - KVM Hypervisior
  - VNF support - Support for third party vendor VFNs (future). Currently, SWe Edge is the supported VNF in the system.
- Management
  - RAMP support - FCAPS support for Edge 8000 on the high availability, geo-redundant, multi-tenanted RAMP platform
  - Yang modeling
  - REST API
  - Web GUI
  - SNMP

Additional capabilities include:

- Robust routing with data rates of up to 10 Gbps
- Multi-homing with BGP for resilient/diverse links
- Large Scale NAT support for multi-tenant use
- SBC capacity of up to 1000 concurrent calls
- All network interfaces (10 ports) can be provisioned as public or private (no fixed function for interfaces)
- Centrally managed by the Ribbon Application Management Platform (RAMP) for single sign-on to all Edge 8000 Series device GUIs and common display of all Edge 8000 Series SBC SWe Edge trap messages
- Microsoft Teams, Zoom Phone, Google Workspace SIP Link & Webex Local Gateway Certified

Detailed Features

Features

Features and Capabilities	Specifications
Performance	
Maximum data Throughout	10 Gbps
Maximum number of registered devices	5000

Features and Capabilities	Specifications
Maximum concurrent voice sessions	1000
Telecom Ports	
FXO/FXS Ports	8100 model – none 8300 model – two configuration options, mutually exclusive: ◦ 2 FXO and 22 FXS ports ◦ 0 FXO and 24 FXS ports (FXS 1000 ft maximum loop length, 5 REN)
T1/E1 PRI ports	8100 model – none 8300 model – 4
Security	
Encryption and Authentication	TLS, SRTP, HTTPS, SSH
Encryption protocol supported	3DES, AES, SHA-256, MD-5

Additional Features

Features and Capabilities	Specifications
Routing Services	
Network Throughput Options (Bidirectional)	• 1G (base configuration, which gives 2.5 Gbps burst throughput) • 5G (optional upgrade) • 10G (optional upgrade)

Features and Capabilities	Specifications
Routing Protocol Support	•BGP4, BGP4+, BGP L3VPN, BGP RPKI •OSPFv2, OSPFv3 •RIPv1, RIPv2, RIPng •Static Routes •Path Monitoring for Static Routes •ECMP •PBR •MPLS •BFD •NHRP •VXLAN EVPN
L2 and Encapsulation	•VLAN (802.1Q, QinQ) •VXLAN •LAG (802.3ad, LACP) •Ethernet Bridge
IP Networking	•IPv6 Autoconfiguration •VRF •NAT •Multicast
Management and Monitoring Options	•SSHv2 •CLI •YANG •REST •SNMP •Syslog •802.1ab LLDP
Security	•ACLs
IP Services	•DHCP Server / Client / Relay •DNS Client / Proxy •NTP

Features and Capabilities	Specifications
Traffic prioritization and QoS	•Rate Limiting per Interface •Rate Limiting per VRF •Class-based QoS •Classification: ToS / IP / DSCP / CoS •Shaping and Policing •Scheduling: PQ, PB-DWRR, HTB
Logging Options	•Port batching •Syslog
System Management	
Local Device Management	CLI (SSH)
Remote upgrades, back-up, restore	FTP, HTTP, and HTTPS
Central Management via Ribbon Application Management Platform (RAMP)	•Single sign-on for access to device GUIs and device REST APIs •Collection of device SBC SWe Edge traps for display in RAMP Fault Manager
Firmware	Local firmware image for upgrade
Network Management	SNMPv1-3
Message Analytics	System monitoring
Debug tools	Packet capture (tcpdump), traceroute, ping, syslog
SBC Services (optional)	

Features and Capabilities	Specifications
Security	•TLS (Transaction Layer Security) for signaling encryption - TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446) •Secure Real-time Transport Protocol (SRTP) and Control Protocol (SRTCP) for media and media control encryption (RFC 3711) •Multiple unique X.509 public key certificates/PKCS #12 files (up to 11) •Wildcard certificate support •Topology hiding; user privacy •Prevention of Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks •Traffic separation (VLAN interface separation) •Malformed packet protection •Access Control Lists (ACLs) •IPsec VPN tunnel •NAT/NAPT and port forwarding; NAT traversal
Protocol Support	•SIP (RFC 3261) over UDP, TCP, TLS •RTP/RTCP/RTCP-XR (RFC 3550, 3551, 3611) •RTP/RTCP multiplexing over single UDP port (RFC 5761) •IPv4, IPv6, and IPv4/IPv6 interworking •DHCP server & client (RFC 2131) •Network Address Translation – NAT (RFC 2663) •SNMPv2c, SNMPv3 •HTTPS
Media Services	•G.711, G.722, G.722.2 (AMR-WB), G.723.1, G.726 (32 kbps), G.729A/B (8 kbps), T.38, SILK-NB/WB media encoding •Video interworking •Session Recording Protocol support - SIPREC (RFC 7866) •DTMF support: RFC 4733, inband DTMF, SIP INFO (RFC 2833) •Voice Activity Detection (VAD) •G.168 Echo cancellation with standard 128 ms tail length •Comfort noise generation and packet loss concealment •Music on hold •RTP inactivity monitoring (inactive call detection)

Features and Capabilities	Specifications
Quality of Service (QoS)	•Bandwidth management •Call Admission Control (CAC) to deny inappropriate calls •P-time mediation for rate limiting •Per-call statistics •Diffserv/DSCP marking
Routing and Policy	•Interactive Connectivity Establishment (ICE), lite support (RFC 8445) •Active Directory®/LDAP-based call routing •Least cost, time of day and quality-based routing •On-board call forking (up to eight end points) •Supplementary services: call hold, call transfer (blind & assisted) and call forward •SIP routing based on source and destination IP address or Fully Qualified Domain Name (FQDN) •ITSP E911 support; 911 call preemption
Management Capabilities	•Single, secure, web-based GUI with real-time port monitoring •Easy Configuration Wizard, for quick provisioning between SIP trunks, SIP phones, SIP PBXs (e.g. Avaya® Aura® or Cisco® Unified Communications Manager) • Microsoft Direct Routing •Centralized management from Ribbon Application Management Platform (RAMP) •REST-based programmatic interface to remotely manage multiple SBCs •SNMP v2c/v3 for comprehensive network management using third-party management systems •Configuration backup and restore; upload from one site to another •CDR reporting and local logging for troubleshooting •Free Ribbon LX syslog server and log parser tool available •Authentication: local user (username/password), Active Directory®, RADIUS

Features and Capabilities	Specifications
Certified SBC for Microsoft Phone System & Direct Routing (Teams)	•SILK-NB, SILK-WB codec support for improved Microsoft Teams user experience •Enhanced 911 (E911) and Emergency Location Identification Number (ELIN) Gateway Support •Media Bypass and Local Media Optimization support •Simplified migration from on-premises Skype for Business Server to Microsoft Teams •Support for multiple tenant-related Direct Routing deployments with Microsoft partners and PSTN carriers
Site Survivability	•IP route redundancy to UC provider, in case of ISP or router failure •PSTN fallback in case of public side failure •Built-in SIP registrar for site survivability for SIP clients including Yealink® Teams and Poly® UC phones and conference bridges •Multiple Spanning Tree Protocol, to prevent routing loops

Standards Compliance

All Edge 8000 devices comply with the required criteria levels of Generic or Basic standards of EMC Directive 2014/30/EU:

- EN 55032:2015+A11:2020 Class A
- BS EN 55032:2015+A11:2020 Class A
- AS/NZS CISPR 32:2015 Class A
- EN IEC 61000-3-2:2019+A1:2021 Class A
- BS EN IEC 61000-3-2:2019+A1:2021 Class A
- EN 61000-3-3:2013+A1:2019
- BS EN 61000-3-3:2013+A1:2019
- EN 55035:2017+A11:2020
- BS EN 55035:2017+A11:2020

All Edge 8300 models comply with telephony standards:

- AS/ACIF S016:2001
  Requirements for customer equipment for connection to hierarchical digital interfaces.
- AS/CA S002:2011
  Analogue interworking and non-interference requirements for customer equipment for connection to the public switched telephone network.
- AS/CA S003.1:2010
  Requirements for customer access equipment for connection to a telecommunications network-Part 1:General.
- AS/CA S003.3:2010
  Requirements for customer access equipment for connection to a telecommunications network-Part 3: Packet and cell based technologies.

All Edge 8000 devices are RoHS compliant, which means Ribbon has eliminated or brought to within acceptable limits: Lead, Mercury, Cadmium, Hexavalent Chromium, Polybrominated Biphenyls, and Polybrominated Diphenylethers. For more information please contact: www.ribboncommunications.com/global-services.

Console Settings and Pin Assignments

This page provides the settings and cable pinouts for the console port of an Edge 8000 Series device.

Console Settings

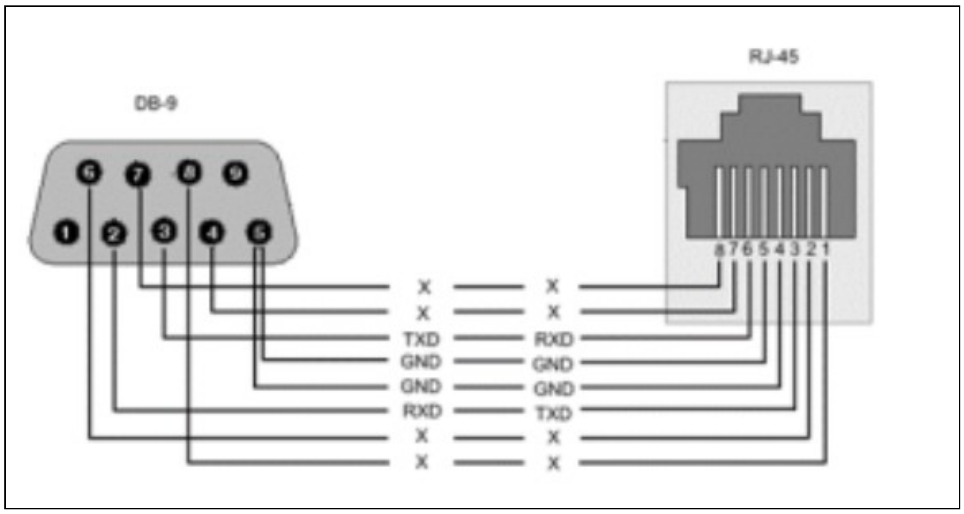
The RJ-45 port is configured as an RS232 serial console output port with the following settings:

- Baud rate: 115200 baud
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: None

Pin Assignments

Here are the pin assignments for the RJ-45 console.

Pin Assignments for the Console Cable



Pinout for the Console Cable

Signal	DB9 Pin	RJ45 Pin	Signal
-	1 - NC	NC	-
RXD	2	3	TXD
TXD	3	6	RXD
-	4 - NC	NC	-

Signal	DB9 Pin	RJ45 Pin	Signal
GND	5	4	GND
-	6 - NC	NC	-
-	7 - NC	NC	-
-	8 - NC	NC	-
-	9 - NC	-	-

Legend

NC: Not Connected

TXD: Transmit Data

RXD: Receive Data

GND: Ground

Supported SFP+ Modules

The following table lists the SFP+ modules supported by Ribbon for the 10GB ports of the Edge 8000 Series devices.

> **Note**
>
> SFP+ modules must be ordered separately.

SFP+ Fiber Optic Modules Supported by Ribbon

8100 and 8300	Vendor	Vendor PN	Full description
YES	Finisar	FTLX1475D3BCL	10.3GB/S, SINGLE MODE, FIBER OPTIC XCVR, LC, SFP, 10KM 1310NM, DMI
YES	Finisar	FTLX8574D3BCL	10.3GB/S, MULTI-MODE, FIBER OPTIC XCVR, LC, SFP, 300M 850NM, DMI
YES	Finisar	FTLF1318P3BTL	1GB/S SINGLE MODE, FIBER OPTIC XCVR, LC, SFP, 10KM 1310NM, STD
YES	Finisar	FTLF8519P3BNL	1GB/S, MULTI MODE, FIBER OPTIC XCVR, LC, SFP, 300M 850NM, DMI (-20 to 85C)

Edge 8000 Shipping Contents

The following table describes the shipping contents of an Edge 8000 Series device.

Item	Description
1	Edge 8000 device
2	For units with AC power supplies: AC power cord (two cords if dual AC power supply)
3	Two rack-mount brackets with screws, for attachment to the chassis of the device
4	Console cable
5	Safety Instructions

Not included with the shipping box:

- Rack mounting screws to mount the chassis by its brackets to the rack
- SFP+ modules

Front and Back Panels

Contents

This section describes all the ports, buttons and LEDs accessible from the front and back panels of the Edge 8000 Series devices.

Edge 8100 Front Panel

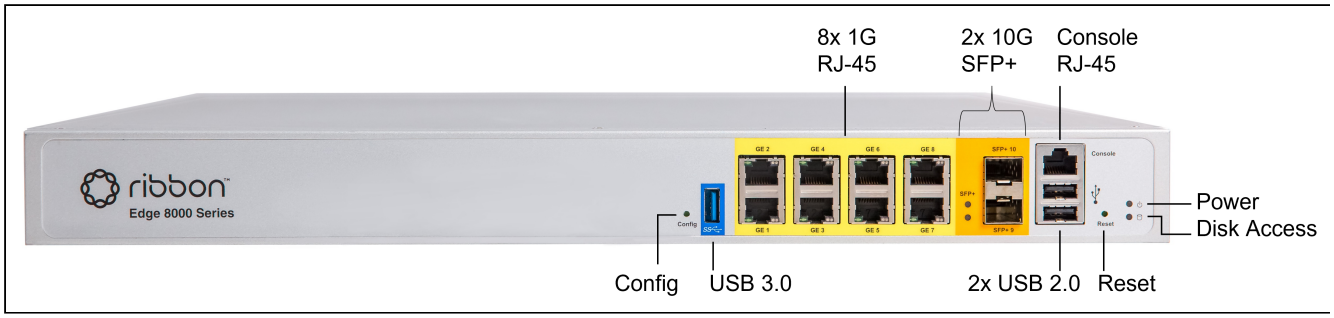
Contents

The Ribbon Edge 8100 device supports 10 Ethernet interfaces on the front panel.

- 2 x 10Gbps SFP+ Ethernet interfaces
- 8 x 1Gbps RJ-45 Ethernet interfaces

The following diagram shows the Edge 8100 front panel:

Edge 8100 Front Panel



Config Button

The Config button on the front panel is a recessed, pinhole button used to reset the CLI password or reset the entire router configuration (including the CLI password) to its original Factory settings. Press and hold the button for 3 seconds to reset the CLI password. (Refer to procedure Restore the CLI Password to Its Factory Default.) Press and hold the button for 10 seconds to reset the entire router configuration.

> **ATTENTION**
>
> Resetting the router configuration causes a service outage. In addition, all customized settings are lost and must be reconfigured after resetting the router configuration.

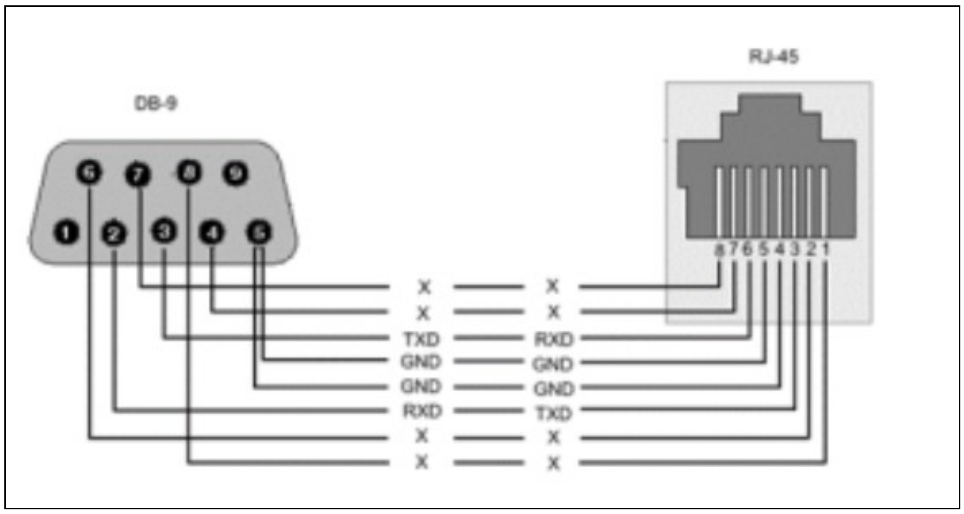
USB Ports

The Edge 8100 device contains 2 x USB 2.0 ports located on the front panel on the combined USB + serial console connector. The USB 3.0 port is located as a stand-alone port with a blue internal tab. The transfer rates offered by USB 2.0 is 480 Mbps and that offered by USB 3.0 is 4.8 Gbps. The USB 3.0 port supports USB 2.0 but at the lower data rate.

Serial Console Port

The RJ-45 port is configured as an RS232 serial console output port, configured at 115200 Baud rate, 8 data bit, 1 stop bit, no parity, and no hardware flow control. It is denoted as 115200 8N1.

RJ-45 Console Pin Assignment



10G Ethernet SFP+ Ports

The Edge 8000 device offers 2 x 10Gbps SFP+ interfaces, allowing different connections such as fiber and copper to be used for the interface.

> **Note**
>
> The SFP+ interface is not compatible with SFP modules.

1G Ethernet Ports

The device has 8 x 1Gbps Gigabit Ethernet (GE) ports for copper connections. Each port has a unique MAC address.

PRI Ports

The 8100 system has no T1/E1 PRI ports.

Reset Button

The Reset button on the front panel is a recessed, pinhole button used to restart the system. It has the same effect as operating the Power Switch on the back panel. It does not alter the system configuration. Press the button quickly to restart the system.

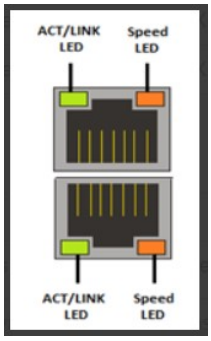
> **Caution**
>
> Restarting the system causes a service outage.

LEDs

When lit, the Power LED indicates power is supplied to the system.

LAN Status LEDs change to indicate the current state of the connection.

LAN Port LED

10/100/1000 Ethernet Port LEDs	ACT/LINK LED		
		Off	The device is not powered, no cable is connected, or no powered device is connected to the associated port.
		Solid Green	A powered device is connected to the associated port.
		Flickering Green	Activity is seen from the device associated with the port. (There is traffic in the inbound or outbound direction on the associated port.) Note: The flickering of the light synchronizes to the actual data traffic.
	Speed LED		
		Off	The device is not powered, no cable is connected, or the port speed is set to 10 Mbps.
		Solid Green	A powered device is connected, and the port speed is set to 100 Mbps.
		Solid Amber	A powered device is connected, and the port speed is set to 1000 Mbps.

The following table describes the function, Activity LED color, and behavior of the LEDs.

LED Indications

Function	Activity LED color	LED color and behavior
Power LED	Solid Green	Green color LED when the system is powered.
SATA device access LED	Red blinking	Red color LED blinking when SATA storage devices are read/write accessed; off when there is no data accessing activity.
SFP+ port access LED	Blue blinking	Blue color LED, blinking when the port is at data transmitting/receiving activity; lights up when the port is linked.

Edge 8300 Front Panel

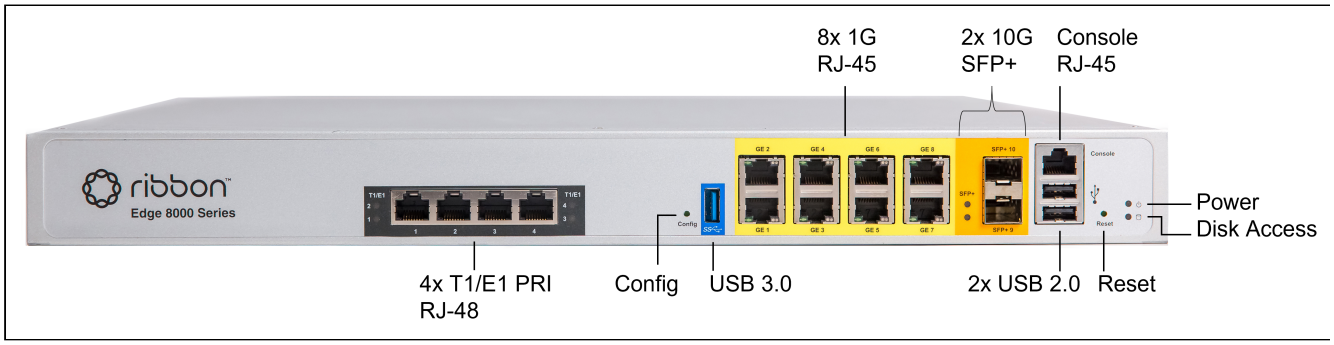
Contents

The Ribbon Edge 8300 device supports 10 Ethernet interfaces and 4 PRI interfaces on the front panel.

- 2 x 10Gbps SFP+ Ethernet interfaces
- 8 x 1Gbps RJ-45 Ethernet interfaces
- 4 x T1/E1 RJ-48 PRI interfaces

The following diagram shows the Edge 8300 front panel:

Edge 8300 Front Panel



Config Button

The Config button on the front panel is a recessed, pinhole button used to reset the CLI password or reset the entire router configuration (including the CLI password) to its original Factory settings. Press and hold the button for 3 seconds to reset the CLI password. (Refer to procedure Restore the CLI Password to Its Factory Default.) Press and hold the button for 10 seconds to reset the entire router configuration.

ATTENTION

Resetting the router configuration causes a service outage. In addition, all customized settings are lost and must be reconfigured after resetting the router configuration.

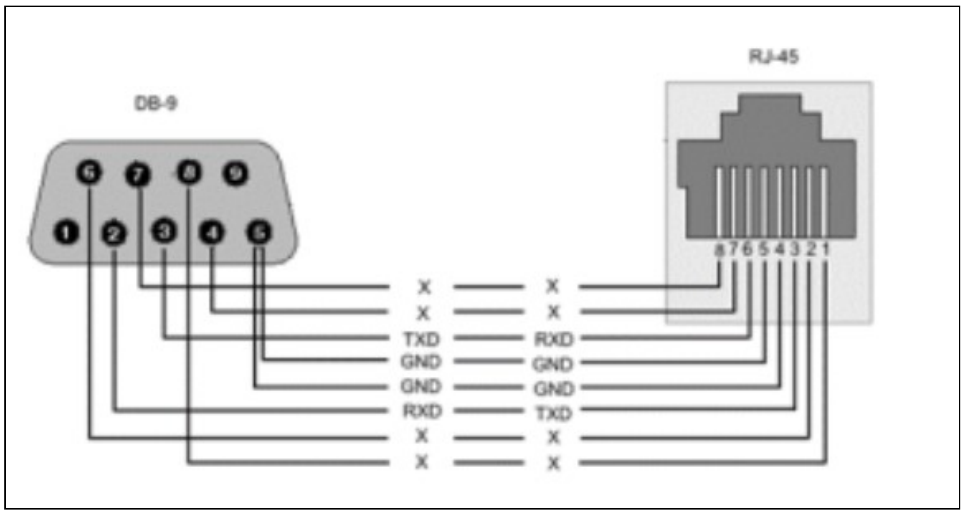
USB Ports

The Edge 8300 device contains 2 x USB 2.0 ports located on the front panel on the combined USB + serial console connector. The USB 3.0 port is located as a stand-alone port with a blue internal tab. The transfer rates offered by USB 2.0 is 480 Mbps and that offered by USB 3.0 is 4.8 Gbps. The USB 3.0 port supports USB 2.0 but at the lower data rate.

Serial Console Port

The RJ-45 port is configured as an RS232 serial console output port, configured at 115200 Baud rate, 8 data bit, 1 stop bit, no parity, and no hardware flow control. It is denoted as 115200 8N1.

RJ-45 Console Pin Assignment



10G Ethernet SFP+ Ports

The Edge 8000 device offers 2 x 10Gbps SFP+ interfaces, allowing different connections such as:

- Copper module
- Single mode Fiber (SMF) module
- Multi-mode Fiber (MMF) module

> **Note**
>
> The SFP+ interface is not compatible with SFP modules.

1G Ethernet Ports

The device has 8 x 1Gbps Gigabit Ethernet (GE) ports for copper connections. Each port has a unique MAC address.

PRI Ports

The 8300 system supports 4 x T1/E1 PRI ports. The ports are connected to the public network using 4-wire shielded 26 AWG or larger twisted pair telecommunication line cords with RJ-48C connector type.

T1/E1 Connector Pinouts

Pin Number	Description
1	Receive Ring

Pin Number	Description
2	Receive Tip
3	no connection
4	Transmit Ring
5	Transmit Tip
6	no connection
7	no connection
8	no connection

Reset Button

The Reset button on the front panel is a recessed, pinhole button used to restart the system. It has the same effect as operating the Power Switch on the back panel. It does not alter the system configuration. Press the button quickly to restart the system.

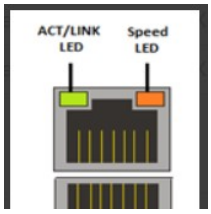
> **Caution**
>
> Restarting the system causes a service outage.

LEDs

When lit, the Power LED indicates power is supplied to the system.

LAN Status LEDs change to indicate the current state of the connection.

LAN Port LED

10/100/1000 Ethernet Ports LEDs	ACT/LINK LED		
		Off	The device is not powered, no cable is connected, or no powered device is connected to the associated port.
		Solid Green	A powered device is connected to the associated port

10/100/1000 Ethernet Ports LEDs	ACT/LINK LED		
		Flickering Green	Activity is seen from the device associated with the port. (There is traffic in the inbound or outbound direction on the associated port.) Note: The flickering of the light synchronizes to the actual data traffic.
	Speed LED		
		Off	The device is not powered, no cable is connected, or the port speed is set to 10 Mbps.
		Solid Green	A powered device is connected, and the port speed is set to 100 Mbps.
		Solid Amber	A powered device is connected, and the port speed is set to 1000 Mbps.

The following table describes the function, Activity LED color, and behavior of the LEDs.

LED Indications

Function	Activity LED color	LED Color and Behaviour
Power LED	Solid Green	Green color LED when the system is powered.
SATA device access LED	Red blinking	Red color LED blinking when when SATA storage devices are read/write accessed; off when there is no data accessing activity.
SFP+ port access LED	Blue blinking	Blue color LED, blinking when port is at data transmitting/receiving activity; lights up when the port is linked.
T1/E1 port LED	Solid Green	Indicates that the T1/E1 link is in the up, green state and has achieved T1 frame synchronization.
T1/E1 port LED	Solid amber	Indicates that the T1/E1 is in the down, yellow alarm state. The remote end is not able to synchronize to the T1 link.

Function	Activity LED color	LED Color and Behaviour
T1/E1 port LED	Solid Red	Indicates that the T1/E1 is in the down, red alarm state. It is not receiving framing from the remote end.

Edge 8100 Back Panel

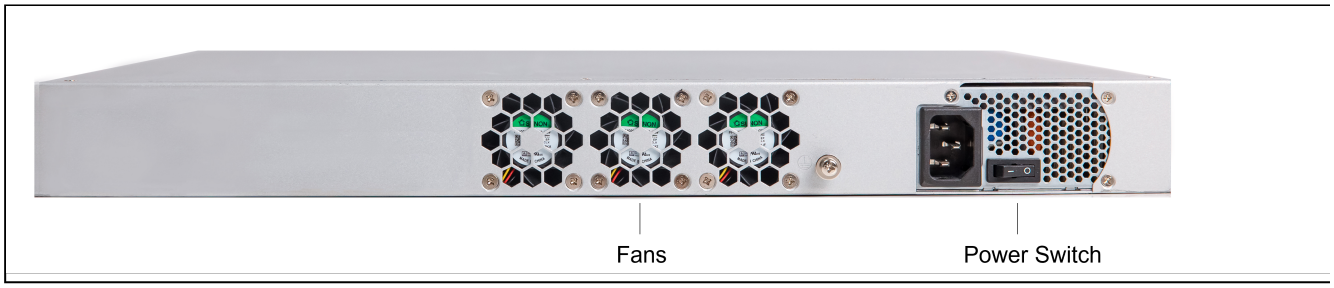
Contents

The Ribbon Edge 8100 device offers three types of power supplies: single power supply and redundant AC or DC power supply.

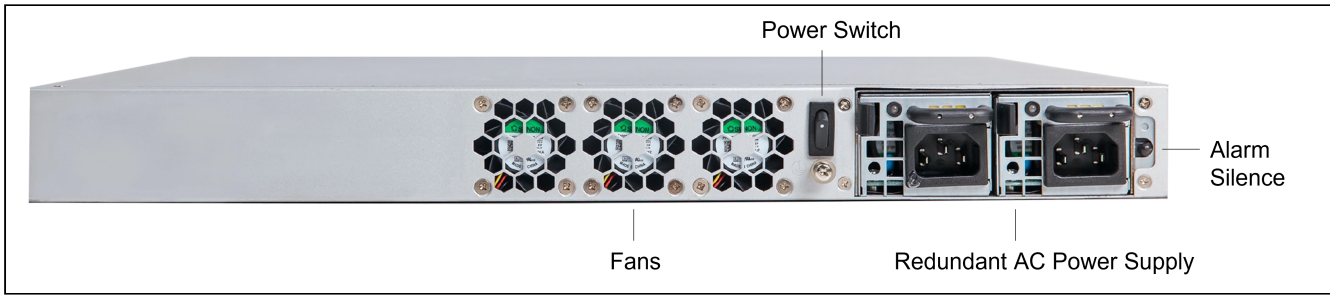
Back Panel Images

The following images show the back panel of the 8100 with single power supply, redundant AC power supply and redundant DC power supply.

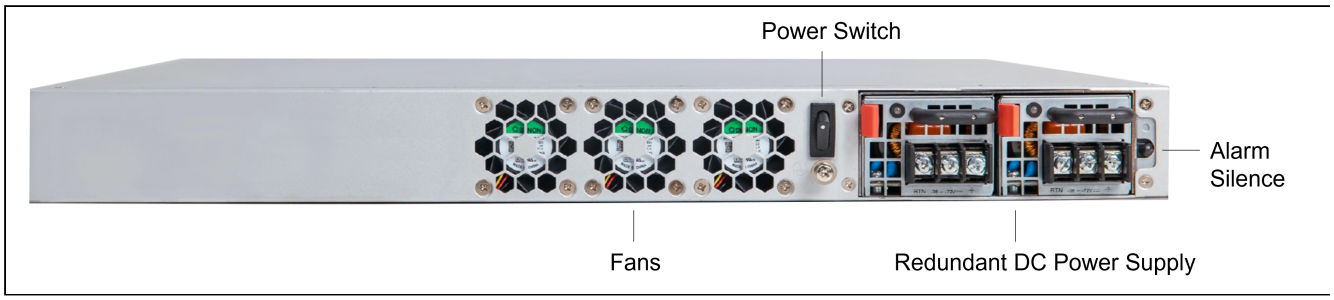
Edge 8100 Back Panel



Edge 8100-R Back Panel



Edge 8100-R-DC Back Panel



Fans

The fans help the device stay cool. To avoid the device overheating, place the device in an area that allows free airflow in front of the fan vents.

Power Switch

The power switch is used to switch on or off the device or to reset the device. The power and status LEDs on the front panel turn solid green after the device powers on.

The power switch operates in two modes, depending on the device configuration:

Power Supply Type	Power Switch Operation
Single AC power supply	Power On-Off: Press the switch to turn on or turn off the hardware. (The power switch is a toggle on, toggle off switch.)
Redundant AC or DC power supply	Power Reset: Press the switch for 4 - 5 seconds to perform a hardware reset. (The power switch is a spring-loaded reset switch.)

Redundant AC Power Supply

The redundant AC power supplies are hot swappable and can be removed and replaced without shutting down the device, provided that one of the power supplies is online and working.

An audio alarm sounds if a power supply fails or is missing. Press the black button on the right side of the PSU cage to silence the alarm.

Redundant AC Power Supply - LED Status

Power Supply Condition	Power Supply LED
Output ON and OK	Green
No AC power to all PSU	OFF
AC present/only standby output on	1Hz Flashing Green

Power Supply Condition	Power Supply LED
AC cord unplugged or AC power lost; with a second power supply in parallel still with AC input power.	1Hz Flashing Red
Power supply warning events where the power supply continues to operate; high temp, high power, high current, slow fan.	1Hz Flashing Red/Green
Power supply critical event causing a shutdown; failure, OCP, OVP, UVP	Red

Redundant DC Power Supply

The redundant DC power supplies are hot swappable and can be removed and replaced without shutting down the device, provided that one of the power supplies is online and working.

An audio alarm sounds if a power supply fails or is missing. Press the black button on the right side of the PSU cage to silence the alarm.

Redundant DC Power Supply - LED Status

Power Supply Condition	Power Supply LED
Output ON and OK	Blue
No DC power to all PSU	OFF
DC present/only standby output on	1Hz Flashing Blue
DC cord unplugged or DC power lost; with a second power supply in parallel still with DC input power.	1Hz Flashing Red
Power supply warning events where the power supply continues to operate; high temp, high power, high current, slow fan.	1Hz Flashing Red/ Blue
Power supply critical event causing a shutdown; failure, OCP, OVP, UVP	Red

Analog Ports

The 8100 has no analog ports on the back panel.

Edge 8300 Back Panel

Contents

The Ribbon Edge 8300 device features interfaces for analog telephony access:

- On the front panel, each of the 4 x T1/E1 ISDN PRI interfaces can be enabled or disabled by configuration.
- On the back panel, each of the 24 FXS/FXO interfaces can be enabled or disabled by configuration.

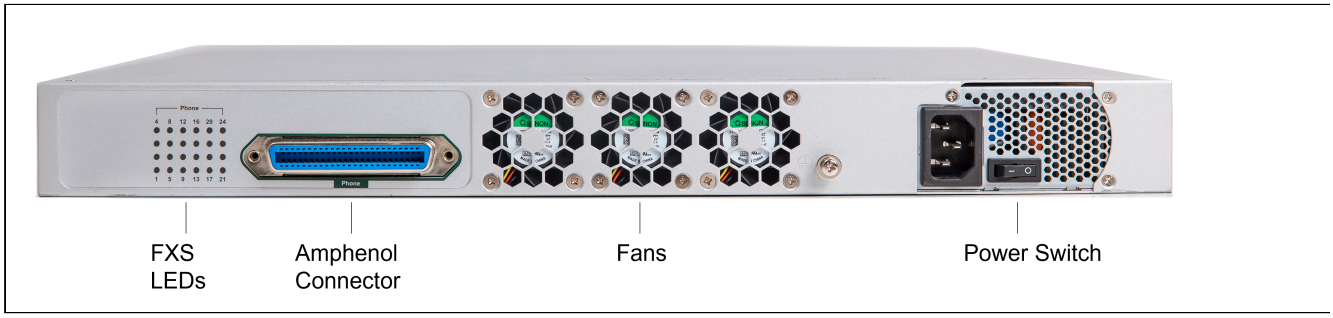
The FXS/FXO interfaces on the back panel are available in two configurations: either 24 FXS ports, or 22 FXS ports and 2 FXO ports. The ports are not interchangeable: FXS ports cannot be configured as FXO ports or vice-versa. An Amphenol connector (also known as a telco connector) on the back panel provides access to the FXS interfaces. Two RJ-11 ports provide access to the FXO interfaces.

For power, the Ribbon Edge 8300 device offers three types of power supplies: single power supply and redundant AC or DC power supply.

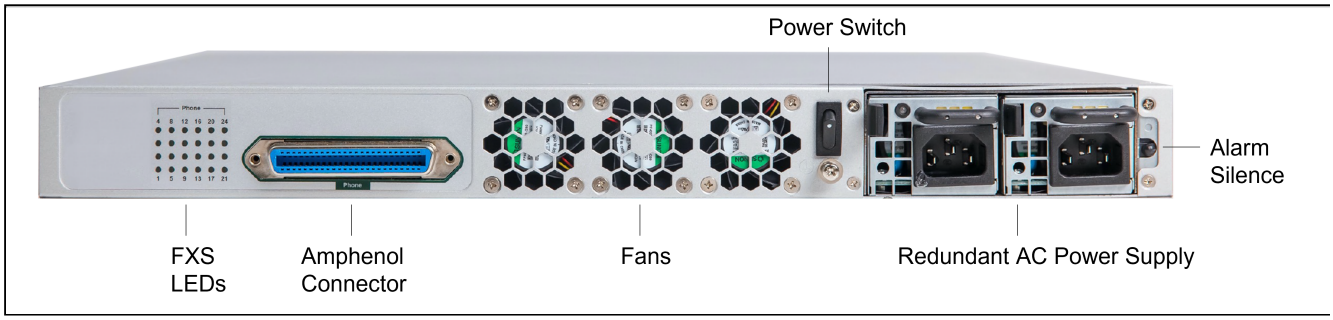
Back Panel Images

The following images show the back panel of the 8300 with single power supply, redundant AC power supply and redundant DC power supply for each of the two FXS/FXO configurations, for a total of six options.

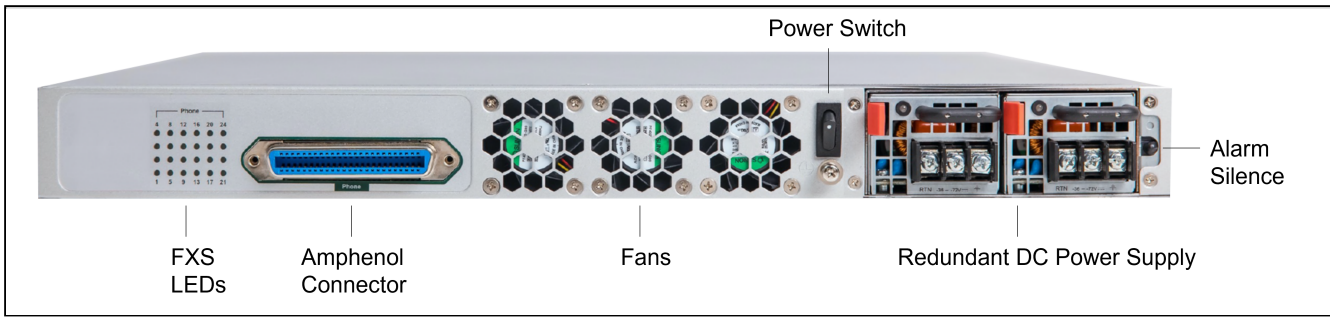
Edge 8300-24S Back Panel



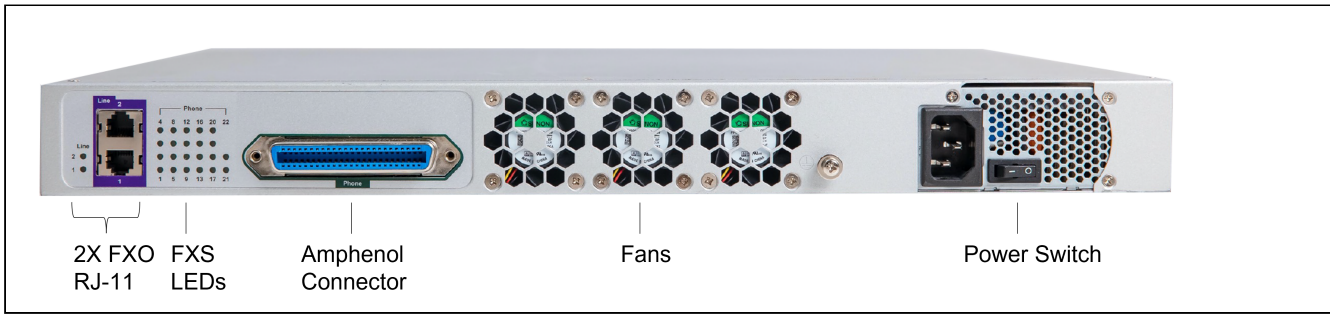
Edge 8300-24S-R Back Panel



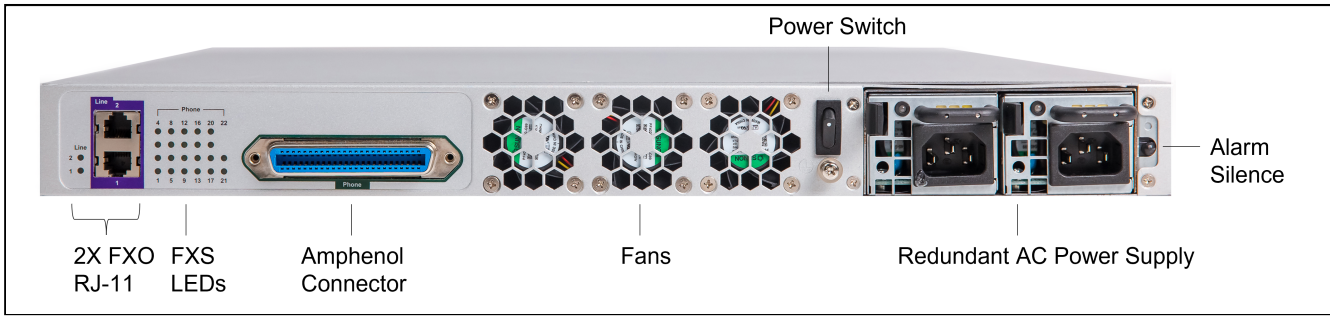
Edge 8300-24S-R-DC Back Panel



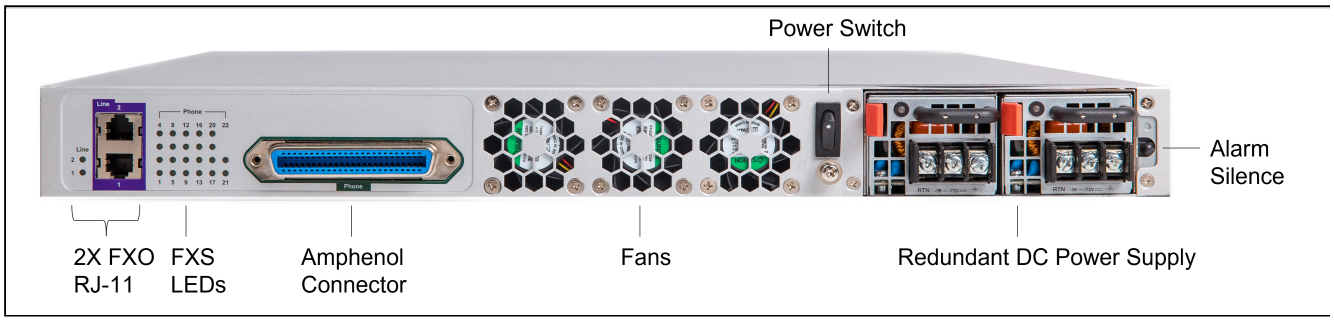
Edge 8300 22S-2X Back Panel



Edge 8300 22S-2X-R Back Panel



Edge 8300 22S-2X-R-DC Back Panel



Fans

The fans help the device stay cool. To avoid the device overheating, place the device in an area that allows free airflow in front of the fan vents.

Power Switch

The power switch is used to switch on or off the device or to reset the device. The power and status LEDs on the front panel turn solid green after the device powers on.

The power switch operates in two modes, depending on the device configuration:

Power Supply Type	Power Switch Operation
Single AC power supply	Power On-Off: Press the switch to turn on or turn off the hardware. (The power switch is a toggle on, toggle off switch.)
Redundant AC or DC power supply	Power Reset: Press the switch for 4 - 5 seconds to perform a hardware reset. (The power switch is a spring-loaded reset switch.)

Redundant AC Power Supply

The redundant AC power supplies are hot swappable and can be removed and replaced without shutting down the device, provided that one of the power supplies is online and working.

An audio alarm sounds if a power supply fails or is missing. Press the black button on the right side of the PSU cage to silence the alarm.

Redundant AC Power Supply - LED Status

Power Supply Condition	Power Supply LED
Output ON and OK	Green
No AC power to all PSU	OFF
AC present/only standby output on	1Hz Flashing Green
AC cord unplugged or AC power lost; with a second power supply in parallel still with AC input power.	1Hz Flashing Red
Power supply warning events where the power supply continues to operate; high temp, high power, high current, slow fan.	1Hz Flashing Red/Green
Power supply critical event causing a shutdown; failure, OCP, OVP, UVP	Red

Redundant DC Power Supply

The redundant DC power supplies are hot swappable and can be removed and replaced without shutting down the device, provided that one of the power supplies is online and working.

An audio alarm sounds if a power supply fails or is missing. Press the black button on the right side of the PSU cage to silence the alarm.

Redundant DC Power Supply - LED Status

Power Supply Condition	Power Supply LED
Output ON and OK	Blue
No DC power to all PSU	OFF
DC present/only standby output on	1Hz Flashing Blue
DC cord unplugged or DC power lost; with a second power supply in parallel still with DC input power.	1Hz Flashing Red
Power supply warning events where the power supply continues to operate; high temp, high power, high current, slow fan.	1Hz Flashing Red/ Blue
Power supply critical event causing a shutdown; failure, OCP, OVP, UVP	Red

Analog Ports

The 8300 supports two analog port configurations on the back of the chassis:

- 8300-24S: 24 FXS ports
- 8300-22S-2X: 22 FXS ports and 2 FXO ports

When present, the FXO interfaces appear as a pair of RJ-11 ports.

The FXS ports connect using a 50-pin Amphenol connector (also known as a telco connector), which can be wired to a breakout panel. Order the optional breakout panel and cable from Ribbon using the following codes:

Breakout (Patch Panel) Ordering Codes

Part Number	Description
EDGE-8300-22-PTCH PNL-S	EDGE 8300 22 PORT ANALOG PATCH PANEL, AMPHENOL CABLE
EDGE-8300-24-PTCH PNL-S	EDGE 8300 24 PORT ANALOG PATCH PANEL, AMPHENOL CABLE

LED Indications for FXS/FXO Ports

Function	Activity LED color	LED color and behavior

FXS port LED	Solid Green	Solid Green color LED, when FXS port is off hook.
FXO port LED	Solid Green	Solid Green color LED, when FXO port is off hook.

Configuration Guides

Contents

For specific Edge 8000 deployment examples, refer to Configuration Examples.

Configuration of SIP to SIP Calls

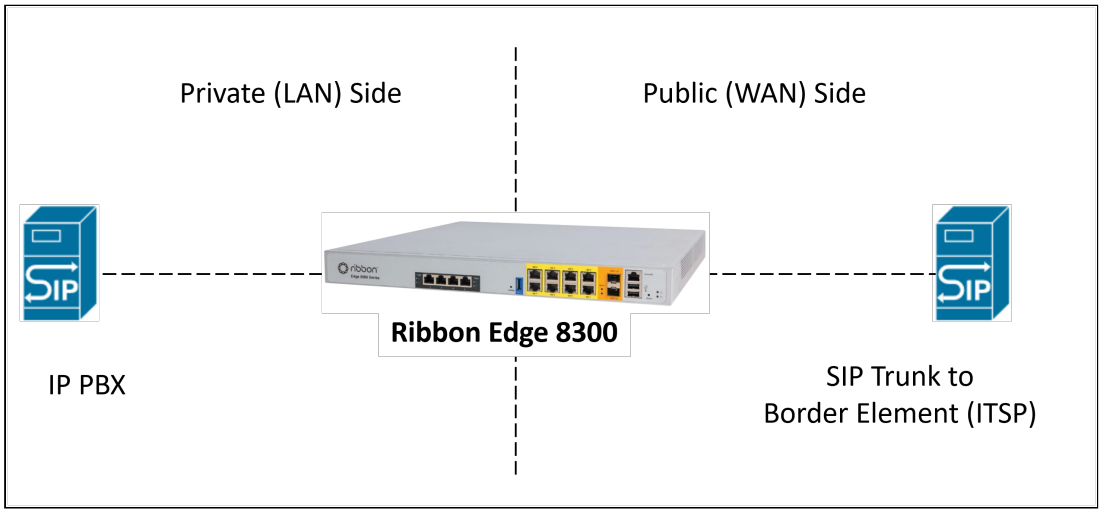
Contents

Configuring SIP Trunk to SIP IP PBX Calls

Perform the procedures in the following workflow to configure the Edge 8000 device for a basic SIP Trunk to SIP IP PBX application. The resulting configuration connects an existing LAN-side IP PBX host to a WAN-side Border Element host, such that internal callers can reach an outside Internet Telephony Service Provider (ITSP) and vice-versa. (Provisioning for a specific dial plan is beyond the scope of this workflow.)

For a complete illustration of the entire provisioning process, including sample outputs of the Setup Wizard, Network Interface provisioning, Static Route provisioning, and the Easy Configuration Wizard, refer to SIP Trunk Configuration for IP PBX Deployment.

Basic SIP Trunk to SIP IP PBX Application



> **Note**
>
> Throughout the procedures, links to SBC Edge customer documentation provide SBC SWe Edge topics helpful in configuring your Edge 8000 device.

> **ATTENTION**
>
> The IP addresses shown in the examples may conflict with an existing or planned production network. Consult with your network administrator for the specific IP addresses required for your deployment.

Prerequisites

- Completion of the initial setup procedures per the Workflow for Initial Setup. This includes physically installing the device, configuring the initial platform settings (Setup Wizard), and installing the SBC SWe Edge license.
- Login access to the SBC SWe Edge WebUI as user administrator (*admin)*

Workflow

Step	Action
1	Configure Network Interfaces
2	Configure Static Routes
3	Run the Easy Config Wizard

Configure Network Interfaces

Use this procedure to manage the way the SBC SWe Edge within the Edge 8000 device interfaces with the external network.

The SBC SWe Edge supports:

- four system-created logical interfaces: the Administrative IP, Ethernet 1 IP, Ethernet 2 IP, and Ethernet 3 IP interfaces
- user-created VLAN logical sub-interfaces

> **Tip**
>
> Refer to Managing Logical Interfaces within the SBC Edge documentation for additional SBC SWe Edge information

The following table explains the nature of each of the logical interfaces.

Logical Interfaces for a SIP to SIP IP PBX Application

Logical Interface	When and How Configured	Purpose
Admin IP	Set during the execution of the Setup Wizard[1].	Provides access to the Edge 8000 WebUI
Ethernet 1 IP	Configured manually.	Provides access to the LAN-side IP PBX
Ethernet 1.2626 IP	Configured manually.	Provides a VLAN logical sub-interface to the LAN-side IP PBX
Ethernet 2 IP	Configured manually.	Not used in this SIP to SIP IP PBX application
Ethernet 3 IP	Configured manually.	Provides access to the WAN-side Border Element (Internet Telephony Service Provider, ITSP)

[1] References to the Setup Wizard refer to the procedures in Running Setup Wizard, either for the Edge 8000 stand-alone or Edge 8000 High Availability deployment.

Start

1. In the Web UI, click the **Settings** tab.
2. Navigate to **SBC** > **Networking Interfaces** > **Logical Interfaces**.
3. Configure each of the logical interfaces per your network plan.
   For field definitions, refer to Configuring and Modifying Logical Interfaces in the SBC Edge documentation.

Configure Static Routes

Use this procedure to configure static routes required by your Edge 8000 device to communicate with remote networks.

In a production environment, static routes are mainly configured for routing from a specific network to another network that can only be accessed through a gateway (for a single path access or default route). When planning your network, consider these factors:

- For smaller networks with just one or two routes, configuring static routing is preferable. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- For networks that have a LAN-side gateway on Voice VLAN or Multi-Switch Edge Devices (MSEs) with voice VLAN towards the SBC Edge, static routing configurations are not required.

> **Tip**
>
> Refer to Managing Static IP Route Tables within the SBC Edge documentation for additional SBC SWe Edge information.

In the following example, two static routes are defined:

- The first static route gives access to the SWe Edge WebUI through a VPN subnet.
- The second static route gives access to SIPP servers on the WAN side of the Edge 8000 device.

Start

1. In the Web UI, click the **Settings** tab.
2. Navigate to **SBC** > **Protocols** > **IP** > **Static Routes**.
3. Configure each of the static routes per your network plan.
   For field definitions, refer to Creating Entries in a Static IP Route Table in the SBC Edge documentation.

Run the Easy Config Wizard

Use this procedure to configure the basic call routing framework for a SIP Trunk to SIP IP PBX application.

The Edge 8000 WebUI includes an Easy Configuration Wizard, which enables end-users to quickly configure settings for different deployment scenarios. Based on a template, you can configure items including:

- an endpoint, with a defined user and provider
- a routing scheme, with a routing configuration applied to the scenario
- a country, with tone table parameters and emergency numbers for the chosen country

> **Note**
>
> Once you complete the Easy Config Wizard, you must apply additional provisioning before making calls. This includes changing entries to the Transformation Tables, Signaling Groups and Routing Tables according to the network topology and dialing plan unique to your particular deployment.

> **Tip**
>
> Refer to Working with SBC Easy Configuration within the SBC Edge documentation for additional SBC SWe Edge information.

Start

1. In the Web UI, click the **Tasks** tab.
2. Navigate to **SBC Easy Setup** > **Easy Config Wizard**.
3. From the **Step 1** menu, complete the fields for **Scenario Parameters**, **SIP Trunk** and **IP PBX**.
   For the **SIP Sessions** parameter, enter a value based on the license allocation for concurrent call sessions you ordered when you placed your Edge 8000 order.
   For field definitions, refer to Configure a SIP Trunk With IP PBX in the SBC Edge documentation.

   > **Note**
   >
   > The value entered for Scenario Description will be prefixed to all SBC configuration elements that the Easy Config Wizard creates.
   >
   > Example: If you enter SIP to SIP for the description, then the Call Routing tables for this deployment will be SIP to SIP: From IP PBX and SIP to SIP: From SIP Trunk.

   Example:

Panel	Area	Field	Value
Scenario Parameters		Application	SIP Trunk ↔ IP PBX
		Scenario Description	SIP to SIP

Panel	Area	Field	Value
		Telephone Country	United States
		Emergency Services	None
	SIP Properties	SIP Sessions	100 (*or whatever number you have licensed*)
SIP Trunk		Name	Other SIP Trunk
IP PBX		Type	Other IP PBX

4. Click **Next**.
5. From the **Step 2** menu, complete the fields for **SIP Trunk** and **IP PBX**.
   For field definitions, refer to Configure a SIP Trunk With IP PBX in the SBC Edge documentation.
   Example:

Panel	Field	Value
SIP Trunk: Other SIP Trunk	Border Element Server	10.230.98.141
	Protocol	UDP
	Port Number	5060
	Use Secondary Border Element Server	Disabled
IP PBX: Other IP PBX	Host	10.230.98.142
	Protocol	UDP
	Port Number	5060
	Use Secondary Server	Disabled

6. Click **Next**.
7. From the **Step 3** menu, examine the **SBC Setup Configuration Summary**.
   Click **Previous** to make a change in a previous step.
   Click **Finish** when you are satisfied with the entries.
8. After clicking **Finish**, click **OK** when you are ready to continue.
   Note that after clicking **Finish**, a confirmation message appears stating that a standard configuration is being applied and that you will need to configure additional parameters (especially for Transformation Tables, Signaling Groups and Routing Tables) before making calls. Click **OK** when you are ready to complete the Easy Configuration process.

Operations and Maintenance

Contents

Backup and Restore Operations

Contents

Overview of Backup and Restore Operations

Use the Backup and Restore from Backup procedures to:

- Capture deployment-specific configuration settings of an Edge 8000 device.
  The `backup` and `restore` commands save and restore all the configuration settings of the device components, including the settings for Gateway, Router, and SBC SWe Edge functions.
- Restore the configuration settings as part of the Performing Software Upgrades and Performing Disaster Recovery.
  Use the Disaster Recovery procedures when an Edge 8000 device suffers a partial or complete failure and must be replaced as a whole unit.

Attention

Ribbon highly recommends storing the backups at an off-site location to ensure the recovery of the backups in the event of an on-site disaster.

Tip

When executing commands for a backup or recovery, remember you can always enter the CLI `sys-tools help` command. The response gives a list of available commands with the proper syntax and a brief explanation of each command.

```
[sysadm@8000 ~]$ sudo -i
[sudo] password for sysadm:
[root@8000 ~]# sys-tools help
Help:
app reinstall [ pkg_name ] - reinstall package
config backup [ ConfigName | default ] - configuration backup
config restore [ ConfigName | default ] - configuration restore
config ls - list saved configurations
debug - show some status and logs
image ls - show iso images on disk
image download [ http://path_to_get_file ] - download iso file
image active filename.iso - activate local repo from iso image
image install filename.iso - reboot and install using filename.iso
image delete filename.iso - delete image filename.iso
license [analog|router] license_key_string - update analog|router licnese key
license sweedge license_file.xml - update sweedge licnese file
linkstatus InterfaceName - show interface link status
report  [ name ] - report status/config to name
help - show help
[root@8000 ~]#
```

Back Up the Configuration Settings

Overview

Use this procedure to save the configuration settings of your Edge 8000 device to a backup file. The `sys-tools config backup` command saves the running configuration settings and all components active in the device, including

- Analog Manager - All settings are saved, including SIP User Agent, SIP Gateway, and PRI settings (Does not apply to the Edge 8100 model.)
- 6Wind Router - All settings are saved
- SBC SWe Edge VNF—This is a pre-installed KVM virtual machine (VM), so the complete VM, including the complete running configuration, is saved

> **Note**
>
> You can also save and download the SBC SWe Edge running configuration using the SWe Edge GUI interface.

- User Management - Users and Passwords

The backup filename of the command can be prefixed with Alpha, Numeric, and these special characters:

!$%^&*()_-+=

The system appends the filename with c*fg_<host-name>_<Edge-8000-sw-version>_*<year-month-day-hour.min.sec>.

For example, if

hostname = 8300-EAST-01

Edge 8000 software version = v24.1.0RCbuild.106e640

date = 17 June, 2024

time = 1:08 am and 50 second

then the backup filename is appended with cfg_8300-EAST-01_v24.1.0RCbuild.106e640_2024_2024-06-17-01.08.50

This procedure applies to all Edge 8000 Series devices.

> **Attention**
>
> Ribbon highly recommends storing the backups at an off-site location to ensure the recovery of the backups in the event of an on-site disaster.

Prerequisites

- System Administrator login access to the Edge 8000 CLI
- Physical access to the port associated with the BR2 management bridge (example: port GE 7)

Start

1. Connect the management computer to the port associated with the BR2 management bridge (example: port GE 7) at the front of the Edge 8000 device.
   The computer will receive a DHCP IPv4 address on the Edge 8000's management subnet, 192.168.122.0/24.
   (If the system's management network is reachable from the remote management computer, then SSH directly to the Edge 8000's management address.)
2. Open a secure shell (ssh) session to the system's management IPv4 address. The default IP address is 192.168.122.1.
3. Log in to the Edge 8000 CLI as System Administrator (*sysadm*) and enter the password.
4. Change permission to root user by entering the command `sudo -i.` Then enter the *sysadm* user password.
5. Execute the system tools (`sys-tools`) command to back up the device.
   Syntax:
   `sys-tools config backup <backup_file_name>`

The backup file path is /E8000/backup_config/.
The following example gives the name RL-bkup as the prefix of the backup filename.

Example

```
# sys-tools config backup RL-bkup
...
extract file from SBCSWeEdge  success
backup file is /E8000/backup_config/RL-bkup_cfg_8300-EAST-01_v24.1.0RCbuild.106e640_2024-06-17-01.08.50.tgz
#
```

6. Exit the CLI session and remove the physical connection from the front panel.

Restore the Configuration Settings from Backup

Overview

Use this procedure to restore from backup the configuration settings of your Edge 8000 device. The `sys-tools config restore` command restores the system to a previous backup configuration. This includes the configuration of all the components that were active in the device at the time of the backup, including

- Analog Manager (not applicable for the Edge 8100 model)
- 6Wind Router
- SBC SWe Edge VNF
- User Management - Users and Passwords

This procedure applies to all Edge 8000 Series devices.

Note

You can also save and restore the SBC SWe Edge configuration separately using the SWe Edge GUI interface.

Attention

For a full recovery of all the system software of the Edge 8000 device, including the operating system software, refer to Performing Disaster Recovery.

Prerequisites

- Access to the backup file (Refer to Back Up the Configuration Settings.)
- System Administrator login access to the Edge 8000 CLI
- Physical access to the port associated with the BR2 management bridge (example: port GE 7)

Start

1. Connect the management computer to the port associated with the BR2 management bridge (example: port GE 7) at the front of the Edge 8000 device.
   The computer will receive a DHCP IPv4 address on the Edge 8000's management subnet, 192.168.122.0/24.

(If the system's management network is reachable from the remote management computer, then SSH directly to the Edge 8000's management address.)
2. Open a secure shell (ssh) session to the system's management IPv4 address. The default IP address is 192.168.122.1.
3. Log in to the Edge 8000 CLI as System Administrator (*sysadm*) and enter the password.
4. Change permission to root user by entering `sudo -i`. Then enter the *sysadm* user password.
5. Execute the system tools (`sys-tools`) command to restore the configuration settings from backup.
   Syntax:
   `sys-tools config restore <backup_file_name>`

   Example

   ```
   # sys-tools config restore RL-bkup_cfg_8300-EAST-01_v24.1.0RCbuild.106e640_2024-06-17-01.08.50.tgz
   ...
   virsh start SBCSWeEdge  ====> Success.
   systemctl stop evagent.service  ====> Success.
   systemctl stop emtunnel.service  ====> Success.
   #
   ```
6. Exit the CLI session and remove the physical connection from the GE 7 port.

Performing Disaster Recovery

A disaster results in the partial or complete loss of an Edge 8000 Series device.

Use this workflow to replace the device and to apply the appropriate software, including configuration settings. This workflow applies to all Edge 8000 Series devices.

Prerequisites

- System Administrator login access to the web-based Edge 8000 user interface
- System Administrator login access to the web-based SBC SWe Edge user interface
- The software image file of the last software release installed on the device
- The last backup of the configuration settings

Workflow

Step	Action
1	Position or mount the replacement unit. Attach the network and power cables, and power on the unit. Refer to Installing Edge 8000 Hardware.
2	Install an Edge 8000 Software Image File on the replacement unit using the last known software image that was installed on the damaged unit.
3	Restore the Configuration Settings from Backup.

License Management

The following workflows and procedures explain how to obtain, view and install licenses for the Edge 8000 Series product.

Contents

For additional information, refer to:

- Edge 8000 Series Product Overview: Licensing for an explanation of available options when placing an Edge 8000 order.
- Returning a Defective Unit (RMA Process) for instructions on ordering and installing a replacement unit for a defective product.
- Obtaining and Installing an SBC SWe Edge Production Node-Locked License in the SBC Edge documentation for general background information on SBC SWe Edge licensing.

Ordering a License and Generating a Key

Use this workflow to order a license for your Edge 8000 device, and to generate a SWe Edge license key.

Prerequisites

- Administrator (*admin*) login access to the Edge 8000 WebUI

Workflow

Step	Action
1	Order a License
2	Generate a SWe Edge License Key

Order a License

Start

1. A software license or licenses must be purchased from Ribbon Sales. To purchase a license, contact Ribbon as follows:
   a. Contact a Ribbon Partner.
   b. Contact Sales and Support: 1-833-742-2661.
   c. Fill out the Contact Form (go to https://ribboncommunications.com and click **Contact**).
2. Once you complete the order, Ribbon sends you further instructions via email.
   a. For SBC SWe Edge licensing, the instructions explain how to access the self-service portal which you then use to generate a SWe Edge license key. You later use the key to install the SBC SWe Edge license.
   b. For Router licensing, Ribbon ships the product with the appropriate Router license installed if this is a new installation. For an upgrade or an RMA action, Ribbon sends the Router license, which must be installed.

c. For Analog licensing, Ribbon always ships the product with the appropriate Analog license installed. No additional action is required for Analog licensing.

Generate a SWe Edge License Key

Start

1. Locate and record the SBC SWe Edge ID from your device.
   a. From the **Settings** tab of the Edge 8000 WebUI, click the **Home** tab.
   b. From the **SWeEdge** panel, record the **SWe Edge ID** number. This serves as the SBC SWe Edge ID.
2. Access the Ribbon Self-Service Licensing and Download Portal and enter credentials.
3. Click **Generate License Key**.
4. Click **Configuration**.
5. Enter the **SBC SWe Edge ID** in the **UUID#1** field and click **Generate**.
   Within 24 hours, you will receive an email (check spam folder) with an attachment.
6. Save the file attachment, which is the license key in .XML format.
   This is the license key you will need for the license installation.

Installing and Viewing Licenses

Use the following procedures to install and view Edge 8000 licenses.

Note that Ribbon ships the Edge 8000 device fully licensed for the Analog function. Refer to Licensing for a discussion of Ribbon's policies for Router, Analog and SBC SWe Edge licensing.

Workflow

Step	Action
1	Install a Router License
2	Install an SBC SWe Edge License
3	View all Licenses

Install a Router License

Prerequisites

- Administrator (*admin*) login access to the Edge 8000 WebUI

Start

1. Log in to the Edge 8000 web-based user interface as user administrator (*admin*).
2. Click the **Settings** tab.
3. In the navigation pane, select **System > Licensing > Install New License**.
4. From the **Version** dropdown list, select **Routing**.
5. Copy the license information you received from Ribbon into the empty **License Key** box.
6. Click **Apply**.
7. In the navigation pane, select **System > Licensing > Current Licenses**.
8. Verify that the license features displayed match the license features you ordered.

Install an SBC SWe Edge License

Prerequisites

- Administrator (*admin*) login access to the Edge 8000 WebUI
- A license key file you obtained from the Ribbon Self-Service Licensing and Download Portal. Refer to Ordering a License and Generating a Key.

Start

1. Log in to the Edge 8000 web-based user interface as user administrator (*admin*).
2. Click the **Settings** tab.
3. In the navigation pane, select **System > Licensing > Install New License**.
4. From the **Version** dropdown list, select **SWeEdge**.
5. Select **Choose File**.
   Navigate to and select the license key file you obtained from the Ribbon Self-Service Licensing and Download Portal.
6. Click **Decode** to view the license details. Verify that the license features you see match the features you ordered.
7. Click **Apply**.
8. In the navigation pane, select **System > Licensing > Current Licenses**.
9. Verify that the license features displayed match the license features you ordered.

View all Licenses

Prerequisites

- Administrator (*admin*) login access to the Edge 8000 WebUI

Start

1. Log in to the Edge 8000 web-based user interface as user administrator (*admin*).
2. Click the **Settings** tab.
3. In the navigation pane, select **System > Licensing > Current Licenses**.
4. Scroll through to see all the Analog, Routing and SBC SWe Edge licenses installed on the device.

Software Management

Contents

Performing Software Upgrades

Upgrades for Edge 8000 software releases, whether for a patch, minor release, or major software release, all work the same way: Ribbon provides a new image to install. The image file contains all the application and operating system software needed to support the release.

Use this workflow to perform a software upgrade. This workflow applies to all Edge 8000 Series devices.

> **Caution**
>
> This operation causes a service disruption. Perform this procedure only during a maintenance window.

Prerequisites

- System Administrator login access to the Edge 8000 Command Line Interface (CLI)
- The ISO image file supplied by Ribbon or available in Ribbon Global Service Center (GSC)

Workflow

Step	Action
1	View the current software versions of your device. Refer to View Current Software Versions.
2	Back Up the Configuration Settings.[1]
3	Install an Edge 8000 Software Image File.
4	Confirm the new software versions. Refer to View Current Software Versions.

[1]The utility for installing an image file includes an automatic backup of the site-specific configuration before the installation. When the installation finishes, the system automatically restores the configuration from the backup. Perform a backup first in case an error occurs during the upgrade and the configuration must be restored from backup.

Install an Edge 8000 Software Image File

Overview

Use this procedure to install an Edge 8000 software image file. This procedure applies to all Edge 8000 Series devices.

Ribbon ships the Edge 8000 device with preinstalled firmware. For version control or solution reasons, Ribbon Support may recommend the system be upgraded to a newer or specific version of firmware.

Ribbon Support provides a link to the image to be downloaded to the local management computer. The management computer must have IPv4 access to the Edge 8000 system to perform the image transfer and then perform the upgrade. When upgrading more than one system on the network it may be desired to place the image files on a HTTP server to allow multiple systems to pull the image files.

SCP is the preferred method to transfer the file from the management computer to the system. Use SCP as a command line option or use an SCP application utility like WinSCP. The image file and the associated md5sum file must be placed in the /e8k-data directory on the system, with a maximum of 2 versions in the directory.

Connecting to the serial console port gives access to the system, allowing the user to view the installation process on the management computer. This console interface provides an option to keep the existing configuration or select a factory default option. The default is to keep the existing configuration.

> **Caution**
> This operation causes a service disruption. Perform this procedure only during a maintenance window.

Prerequisites

- System Administrator (*sysadm*) login access to the Command Line Interface (CLI)
- The Edge 8000 ISO image file supplied by Ribbon or available in Ribbon Global Service Center (GSC)

Start

1. Log in to the Edge 8000 CLI as System Administrator (*sysadm*) and enter the password.
2. Change permission to root user by entering `sudo -i.` Then enter the *sysadm* user password.
3. Verify the integrity of the image file. Confirm that the file size from the Ribbon download server is the same size on the management computer.
4. Verify there is sufficient space to copy the new image file.
   a. List the image files.
      Syntax
      `sys-tools image ls`

      Example

      ```
      # sys-tools image ls
      CommonOs-alma.host-8.6-v1.0.0b17219-x86_64.iso
      CommonOs-alma.host-8.6-v23.6.0b18010-x86_64.iso (active)
      ```

   b. If there are two image files, remove the image that is not active to make room for the new image file.
      Syntax
      `sys-tools image delete <filename.iso>`
      Ribbon recommends deleting the non-active image file to allow the active running image to be available should a downgrade be necessary.
5. Transfer the new ISO image file and the associated md5sum file to directory /e8k-data using the CLI `scp` command.
   The sys-tools image installation tool verifies that the md5sum of the ISO file matches the value in the md5sum file before starting the installation to avoid any issues with a corrupted ISO image file.
6. Execute the command to install the new image.
   The system sets the boot option to the new ISO image, backs up all configuration settings, reboots to start the image installation, and finally restores the system configuration settings. The installation takes approximately 30 to 40 minutes.
   Syntax:
   `sys-tools image install <image_file_name.iso>`
   `sys-tools image ls`

Example

```
[root@e8000 ~]# sys-tools image install CommonOs-alma.host-8.6-v23.6.0b19919-
x86_64.iso
################Warning#############################
This action will reboot the device and enter the install Almalinux process.
All Almalinux OS data on the disk will be overwritten.
The installation will take about 30 minutes.
Continue (yes/no)?
yes
Set ventoy(0004) as next boot
...
```

7. After the system reboots, log back in to the device as System Administrator (*admin*) using the web-based user interface.
8. The current software version appears on the **Home** page of the **Settings** tab. Verify the software version is the new version.
9. As a double check, use the CLI to confirm that the system is running on the new image.
   Syntax:
   `sys-tools image ls`
   In the system response, the word "active" in parenthesis indicates which image the system is running on. Verify that the image that is active is the new image you just installed.

   Example

   ```
   # sys-tools image ls
   CommonOs-alma.host-8.6-v1.0.0b17219-x86_64.iso
   CommonOs-alma.host-8.6-v23.6.0b18010-x86_64.iso (active)
   ```

Scenarios for Software Upgrades and System Recoveries

Contents

Different scenarios require different responses, depending on the severity and urgency of the situation. This article describes different procedures available to be performed on the Edge 8000 device, depending on the scenario.

Catastrophic Recovery on Disk Failure

Create a USB flash drive with the appropriate operating system ISO file (Alma or Red Hat Linux) to apply in the recovery of a system that has experienced a hard drive failure.

Refer to Installing from a USB ISO Drive Using the Ventoy Application. Remember to Restore the Configuration Settings from Backup afterward.

Major Upgrade – Full Software Installation

When upgrading to a new major release, for example, from 24.0 to 24.1, use the `sys-tools image install` command after installing the upgraded sys-tools package for the new release. This is a full software installation.

Refer to Upgrading System Software Using the Sys-Tools Application.

Factory Reset

After resetting the device to factory default, the SBC SWe Edge VM and the internal System Management configuration container do not restart automatically. The operator must then run the Setup Wizard again to provision the correct IP network settings; then the VM and container will start. The `sys-tools image install` step is to re-install the boot partition with a clean copy of the OS files.

Prerequisites

- Login credentials as user *sysadm* to the Edge 8000 Command Line Interface (CLI).

Start

1. Remove the old configuration using one of the following three methods:
   a. Press and hold the config button for 30 seconds
   b. Execute the following CLI command:
      `setupwizard -d`
   c. Execute the following CLI command:
      `sys-tools config restore default`
2. Run the Setup Wizard to provision the correct IP network settings.
3. Re-ISO the root partition by using a `sys-tools image install` procedure. Refer to Upgrading System Software Using the Sys-Tools Application.

Installing from a USB ISO Drive Using the Ventoy Application

Use the following workflow to create a USB ISO installation flash drive and to install the operating system on an Edge 8000 unit. The operating system can be either of the following:

- Alma Linux
- Ribbon OEM Host Operating System (ROHOS), which contains the Red Hat Enterprise Linux (RHEL) operating system that Federal and other high-security deployments require

Prerequisites

- A USB data storage device, also known as a flash drive or pen drive, which is used to hold the operating system software in the form of an ISO image file. It must be 8GB or greater.
- Ventoy 1.0.98 Windows zip software, an application used to copy the ISO image file onto the USB storage device.
- PuTTY or equivalent Windows-based software, used to establish a serial or telnet connection to the Edge 8000 Console port.
- A laptop with a serial communications port. The laptop must have Windows installed.
- A serial or telnet connection to the Edge 8000 unit:

  - A serial connection requires a serial cable from your laptop to the unit's Console port on the front panel. Refer to Front and Back Panels for the location of the RJ-45 Console port. Refer to Console Settings and Pin Assignments for Console port information.
  - A telnet connection requires local area network access from your laptop to the terminal server that connects to the unit's Console port. You will need the hostname or IP address of the terminal server and the port number that connects to the unit's Console port.
- Login credentials as user *sysadm* to the Command Line Interface (CLI).
- Access to the operating system ISO file supplied by Ribbon or available in the Ribbon Global Service Center (GSC).

Workflow

Step	Action
1	Create the USB ISO Installation Drive.
2	Connect to the Edge 8000 system Console port, using either of these methods: • Connect With a Serial Cable (preferred method) • Connect With Telnet
3	Install the Software From the Installation Drive.

Create the USB ISO Installation Drive

Use this procedure to create a bootable USB installation drive containing the operating system software.

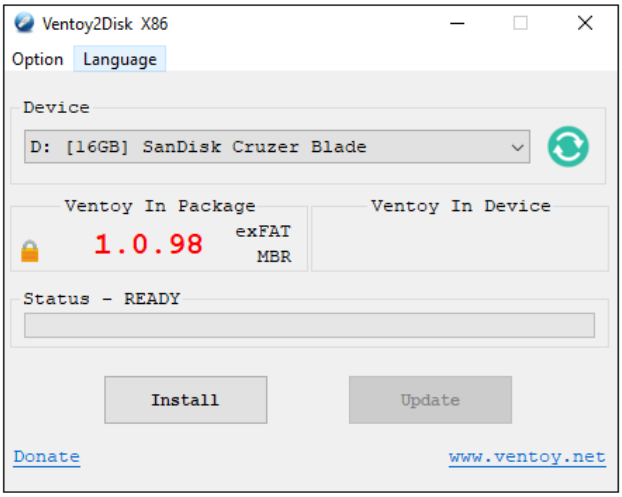
The procedure shows the use of Ventoy, a free and open-source tool.

> **Note**
>
> Ribbon recommends first backing up any files currently held on the USB storage device. In this procedure, the USB device will be formatted and all data lost.

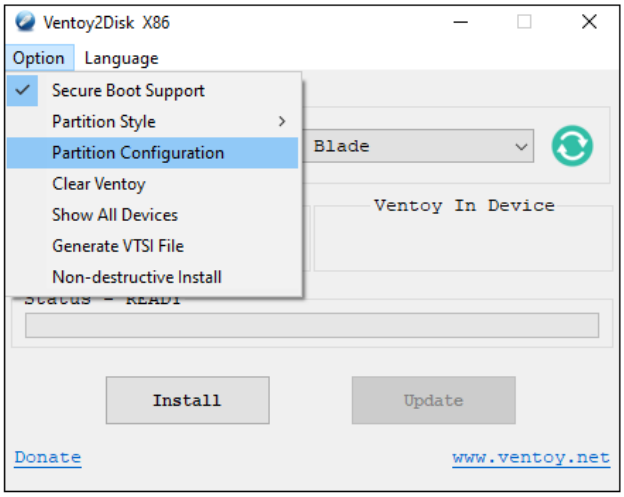
Start

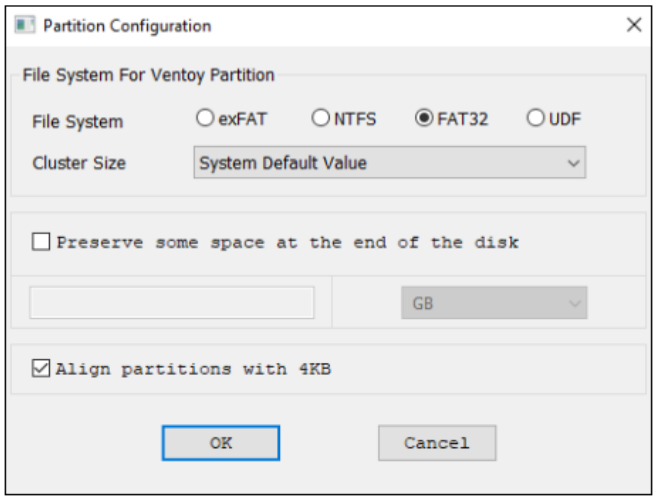
1. Download the ISO file and the ventoy.json file to your laptop.
2. Insert the USB storage device into your system.

3. Extract the Ventoy software and run the Ventoy2Disk.exe utility. The software automatically detects the USB device and displays the USB name in the **Device** field.



4. Click the Option tab and select **Partition Configuration**.





5. Select **FAT32** for File System and click **OK**.
6. Click **Install**.
7. Click **Yes** when prompted with the following warning.

Example - Warning

The device will be formatted and all the data will be lost. Continue?

Yes or No

8. Type **YES** in the text box when prompted with the following warning.

Example - Warning

Warning: Data will be lost!

Please enter YES in the text box below to confirm that you indeed want to do a fresh install instead of upgrade."

	<== YES

OK or Cancel

9. Click **OK**.
10. Click **Yes** when prompted with the following warning.

Example - Warning

The device will be formatted and all the data will be lost. Continue? (Double Check)

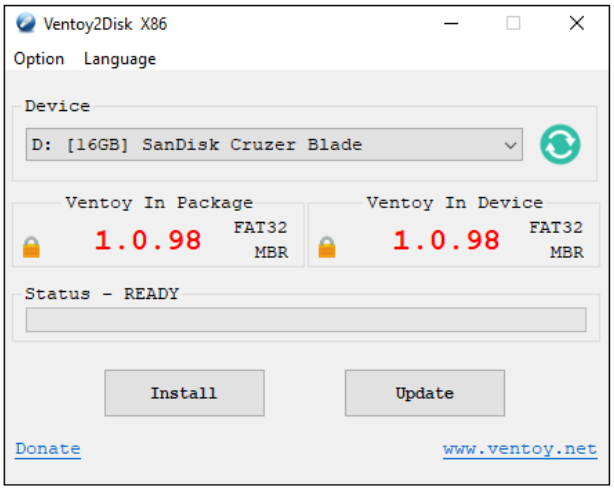
Yes or No

Clicking **Yes** erases all data, and Ventoy 1.0.98 software package is successfully installed to your USB storage device.

Attention

The ISO-burning utility (such as Ventoy) may erase all existing data from the USB device. Be sure to back up any files you wish to save before burning the ISO file onto the device.

11. Verify that **Ventoy In Package** (that you downloaded) and **Ventoy In Device** (that you installed) are identical.



12. Select the USB drive on your laptop and select **Eject**; then remove the USB storage device and reattach it to the system.
    A new partition with label VENTOY is mounted to the system.
13. In the VENTOY partition, create a new folder named ventoy and copy the ventoy.json file inside it.
14. Copy the downloaded ISO file into the VENTOY partition.
15. Close the system window and eject the USB storage device.
    You can now use the device to perform an ISO installation on the Edge 8000 hardware.

Connect With a Serial Cable

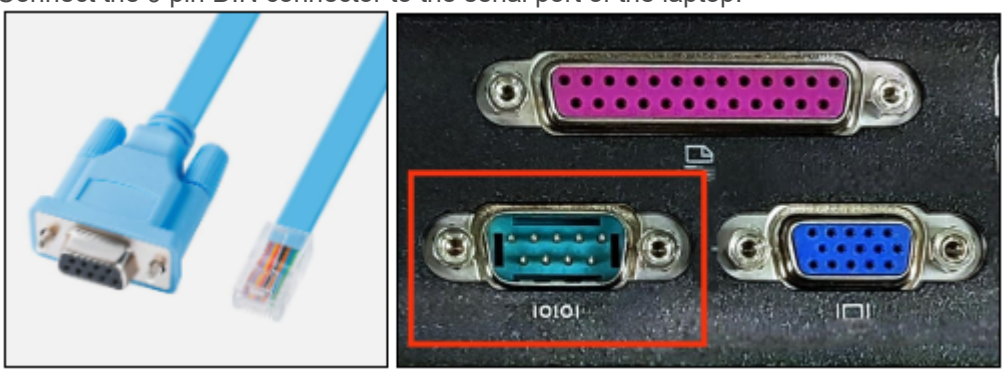
Use this procedure to connect to the Edge 8000 system console using a serial cable connected to the front panel Console port. This is the connection method Ribbon recommends.

> **Note**
> Ribbon recommends connecting to the system console through a serial cable connection as the preferred method. This is because, during the boot-up process after the ISO installation, the system redirects log messages to the serial console. This ensures that no network disruptions between the connecting computer (laptop) and the Edge 8000 device impede the view of Edge 8000 logs during the bootup sequence.

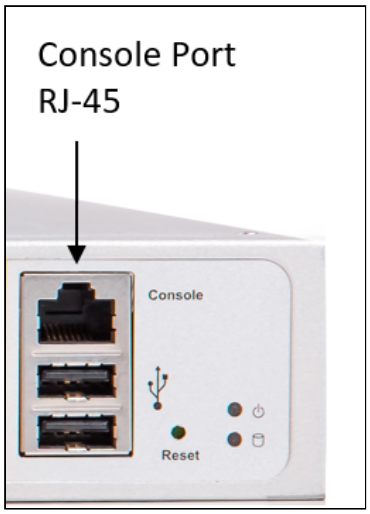
The procedure shows the use of PuTTY, a free and open-source DOS utility. However, you can connect to the unit using PuTTY or any equivalent software.

Start

1. Connect the 9 pin DIN connector to the serial port of the laptop.

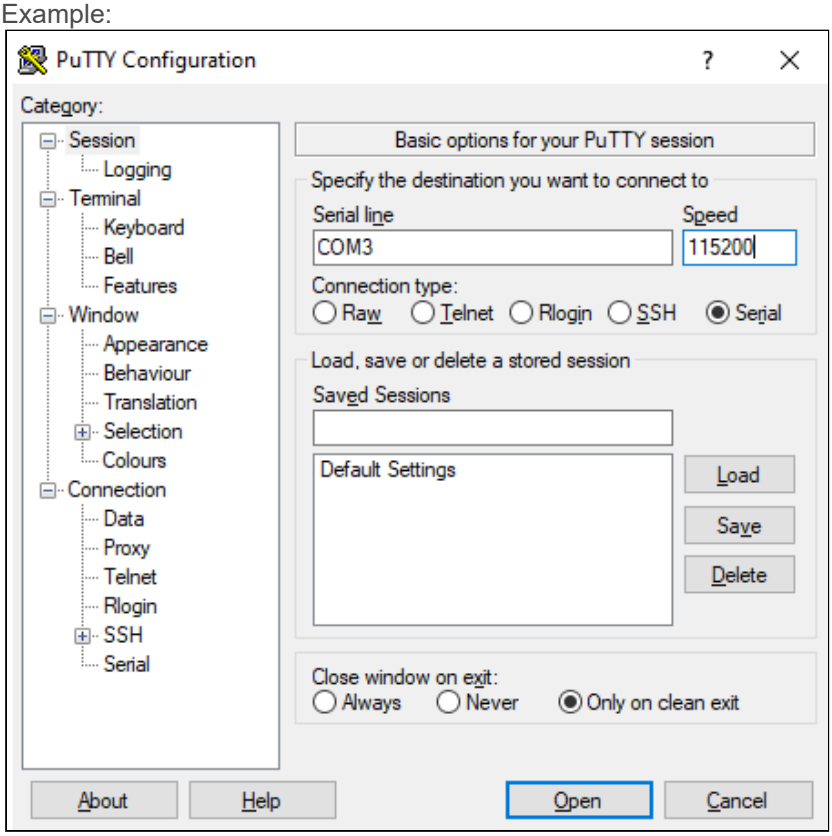


2. Connect the other end of the console cable with RJ45 connector to the Console port of your Edge 8000 device.



3. Use PuTTY or equivalent software to open a serial port connection.
   Enter the following settings:

   a. **Connection type**: Serial
   b. **Serial line**: COM3
   c. **Speed**: 115200
      Example:



2. Click **Open** to start the connection (or click an equivalent button if using other software).
   If necessary, press Enter on your keyboard to invoke the e8000 login prompt.

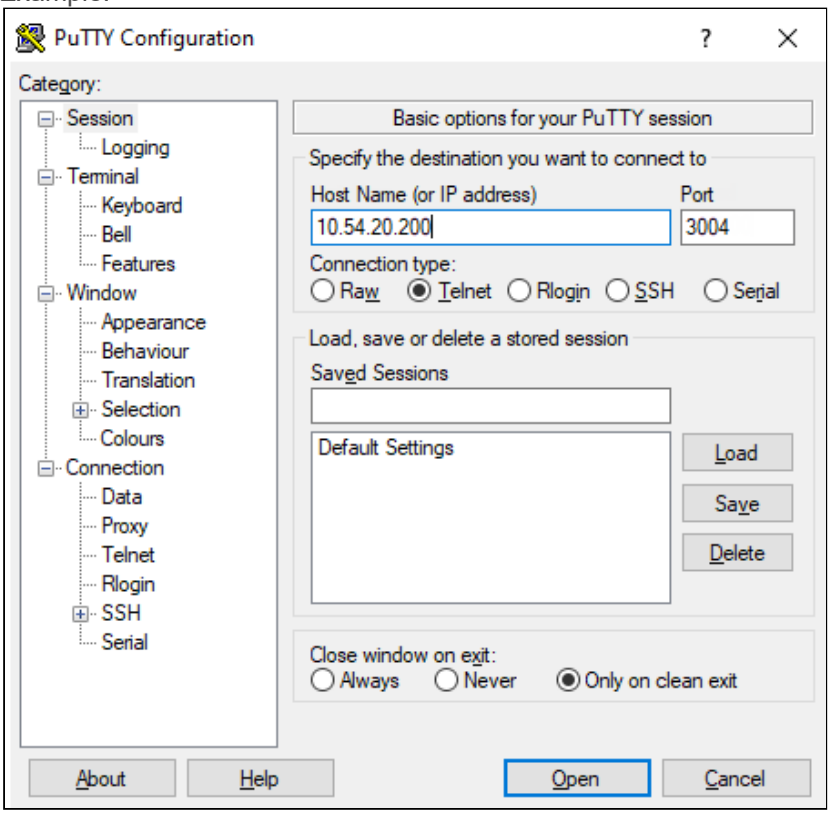
Connect With Telnet

Use this procedure to connect to the Edge 8000 system console through a telnet connection across a local area network. This is an alternate method of connecting to the device.

The procedure shows the use of PuTTY, a free and open-source DOS utility. However, you can connect to the unit using PuTTY or any equivalent software.

Start

1. Use PuTTY or equivalent software to open a telnet connection to the Edge 8000 system console. You will need the host name or IP address, and the port number, of the terminal console of the Edge 8000 device. Enter the following settings:
   a. **Connection type**: Telnet
   b. **Host Name (or IP address)**: Enter the host name or IP address of the Edge 8000 terminal console (example: 10.54.20.200).
   c. **Port:** Enter the port number of the Edge 8000 terminal console (example: 3004).
   Example:



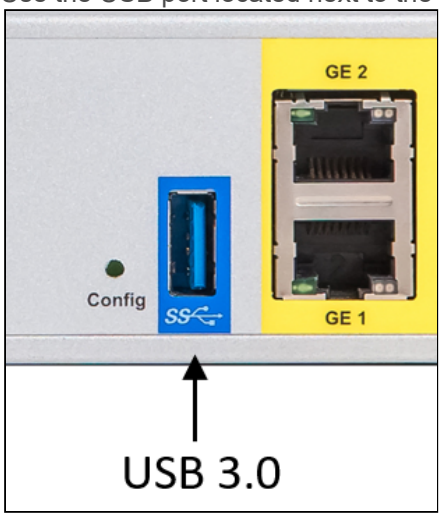
2. Click **Open** to start the connection (or click an equivalent button if using other software).
   If necessary, press Enter on your keyboard to invoke the e8000 login prompt.

Install the Software From the Installation Drive

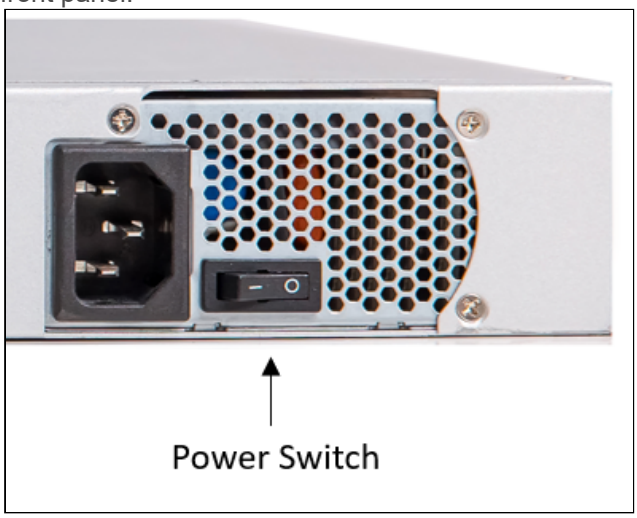
Attention

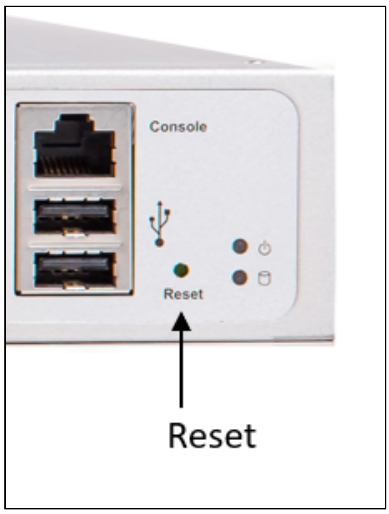
To see the status messages during the system boot-up, you must be connected to the system console.

1. Insert the USB installation drive into the USB port.
   Use the USB port located next to the Config button on the Edge 8000 front panel.



2. Verify you are connected to the serial Console port. See Connect With a Serial Cable or Connect with Telnet.
3. Power cycle the Edge 8000 unit.
   Do this by flipping the power switch on the back panel or by pressing the recessed reset button on the front panel.





4. Select the **SERIAL** option to install the ISO image.
   Selecting the serial option instructs the system to send log messages to the serial console port, where you can view them through your Console port connection.
   Use the "up" and "down" keys of your keyboard to change the selection. Press the Enter key to make the selection.

Example (showing the ROHOS RHEL operating system; Alma Linux will be similar)

```
Install RHEL SERIAL
Troubleshooting -->
```

5. Wait for the installation to complete (approximately 30 minutes).

6. Once the installation finishes, the system prompts you to proceed.
   Enter y or Y.
   Example:

   Example

   ```
   Installation is complete, press 'y/Y' to proceed: Y
   ```

7. The system finishes internal checks and starts to reboot.
8. Remove the USB installation drive. Removing the USB drive allows the system to reboot off the hard drive.
9. Once the reboot finishes, log in with the default credentials for user *sysadm*.
   Refer to Default Passwords for First-Time Logins.
10. Follow the prompts to change the default password to a new password of your choice.

Upgrading System Software Using the Sys-Tools Application

Use the following workflow to upgrade the operating system of an Edge 8000 device. These instructions use the Edge 8000 system tools (sys-tools) application to perform the upgrade.

The examples illustrate an upgrade from Alma8 to Alma9; however the same instructions apply to a ROHOS RHEL upgrade.

> **Note**
>
> The utility for installing an image file includes an automatic backup of the site-specific configuration before the installation. When the installation finishes, the system automatically restores the configuration from the backup. Perform a backup first in case an error occurs during the upgrade and the configuration must be restored from backup.

Prerequisites

- System Administrator (*sysadm*) login access to the Command Line Interface (CLI)
- The new ISO image file supplied by Ribbon or available in Ribbon Global Service Center (GSC)

Workflow

Step	Action
1	Back up the System Configuration Settings
2	Copy the New ISO Image File to the Device
3	Upgrade the Edge 8000
4	Perform Post-Upgrade Activities

Back up the System Configuration Settings

Use this procedure to save the configuration settings of your Edge 8000 device to a backup file.

1. Log in to the Edge 8000 CLI as System Administrator (*sysadm*) and enter the password.
2. Change permission to root user by entering the command `sudo -i.` Then enter the *sysadm* user password.
3. Run the system tools (`sys-tools`) command to back up the device's configuration settings.

   ```
   sys-tools config backup <backup_file_name>
   ```

   The following example gives the name "backup_before_alma8to9_upgrade" as the prefix of the backup filename.

   ```
   sys-tools config backup backup_before_alma8to9_upgrade
   ```

4. Store the backup file at an off-site location.

   Note

   Ribbon highly recommends storing the backup at an off-site location to ensure its recovery in the event of an on-site disaster.

Copy the New ISO Image File to the Device

Use this procedure to copy the new ISO image file to the Edge 8000 device.

Note

Before copying the image file to the device, verify its integrity and ensure that there is adequate space for it.

Start

1. Log in to the Edge 8000 CLI as System Administrator (*sysadm*) and enter the password.
2. Change permission to root user by entering the command `sudo -i.` Then enter the *sysadm* user password.
3. Verify the integrity of the image file. Confirm that the file size on the Ribbon download server is the same size as on the management computer.
4. Verify there is sufficient space to copy the new image file to the device.
   a. Check the available space. Compare it to the size of the new image file.

      Example

      ```
      # df -lah /e8k-data/
      Filesystem      Size  Used Avail Use% Mounted on
      /dev/sda1       8.6G  3.3G  4.9G  41% /e8k-data
      ```

   b. List the existing image files.

Example

```
# sys-tools image ls
CommonOs-alma.host-8.6-v1.0.0b17219-x86_64.iso
CommonOs-alma.host-8.6-v23.6.0b18010-x86_64.iso (active)
```

c. If there are two image files, remove the image that is not active to make room for the new image file. Ribbon recommends deleting the non-active image to allow the active image to be available should a downgrade be necessary.

Example

```
# sys-tools image delete CommonOs-alma.host-8.6-v1.0.0b17219-x86_64.iso

# sys-tools image ls
CommonOs-alma.host-8.6-v23.6.0b18010-x86_64.iso (active)
```

5. Transfer the new ISO image file and the associated md5sum file to the persistent partition, directory /e8k-data, using the CLI `scp` command.
   The sys-tools image installation tool verifies that the md5sum of the ISO file matches the value in the md5sum file before starting the installation to avoid any issues with a corrupted ISO file. If there is an error, then the installation will not proceed.

Upgrade the Edge 8000

Use this procedure to make the copied image file the active file, uninstall the existing rpm sys-tools package and install a new sys-tools package, and install the new ISO image file.

Start

1. Log in to the Edge 8000 CLI as System Administrator (*sysadm*) and enter the password.
2. Change permission to root user by entering the command `sudo -i.` Then enter the *sysadm* user password.
3. Make the copied image file the active file.
   Syntax
   `sys-tools image active <ISO_image_file_name>`
4. Uninstall the rpm sys-tools package currently installed in the system.

```
rpm -e $(rpm -qa | grep sys-tools)
```

5. Install the new rpm sys-tools package from the mounted ISO.

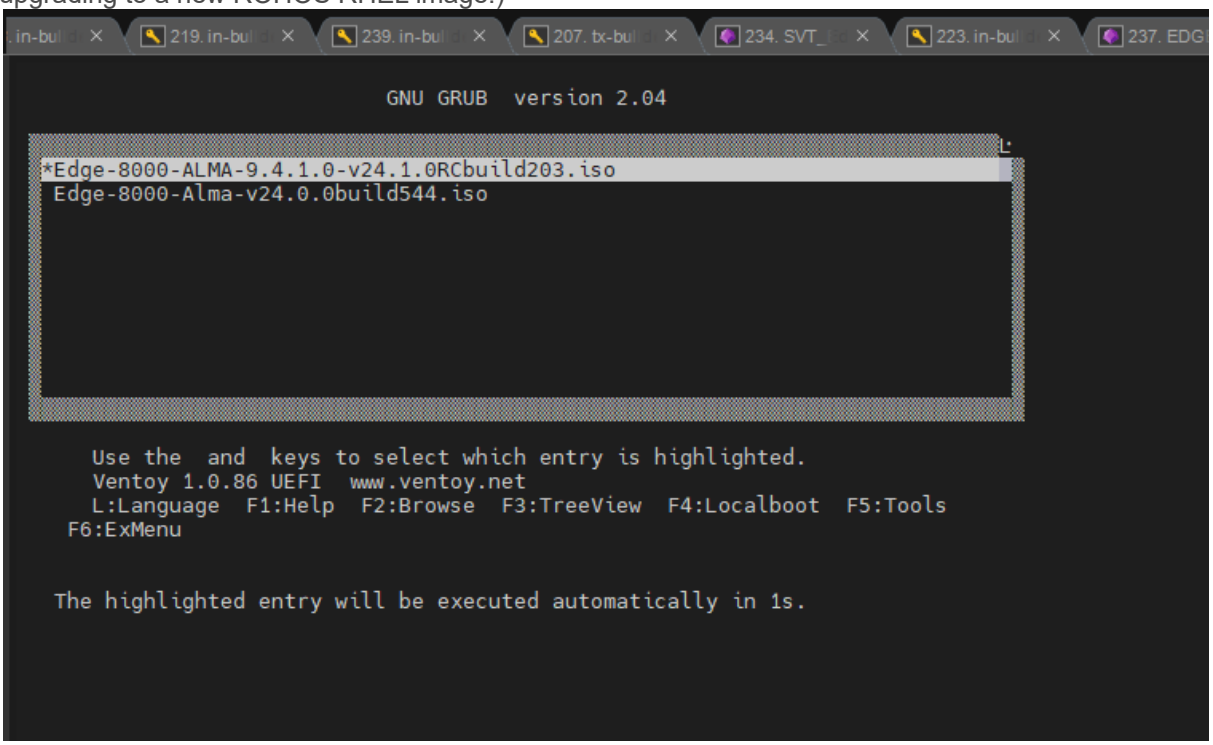
```
rpm -ivh /LocalRepos/E8000/rpm/sys-tools*.rpm
```

6. Run the command to install the active ISO image file (the one you just copied and made active).
   The `sys-tools image install` command backs up the system configuration, reboots from the active ISO image, and restores the system configuration. The entire process takes about 40 minutes.

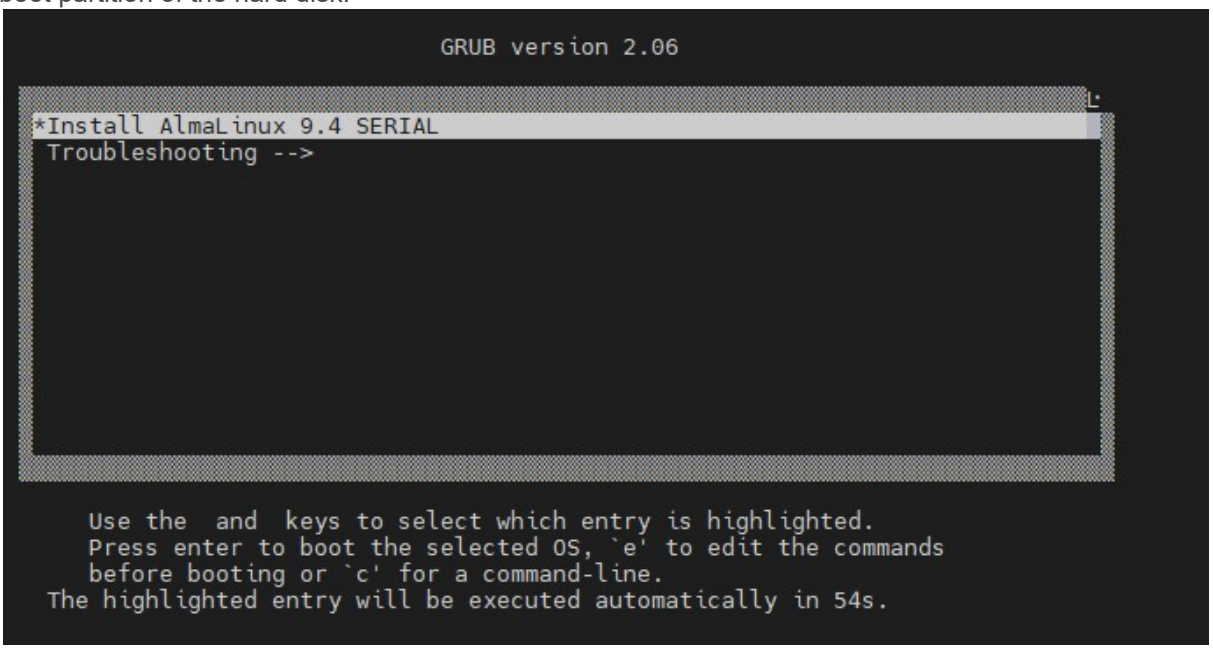
```
sys-tools image install <ISO_image_file_name>
```

The following figures show the sequence of prompts and displays that appear during the installation.

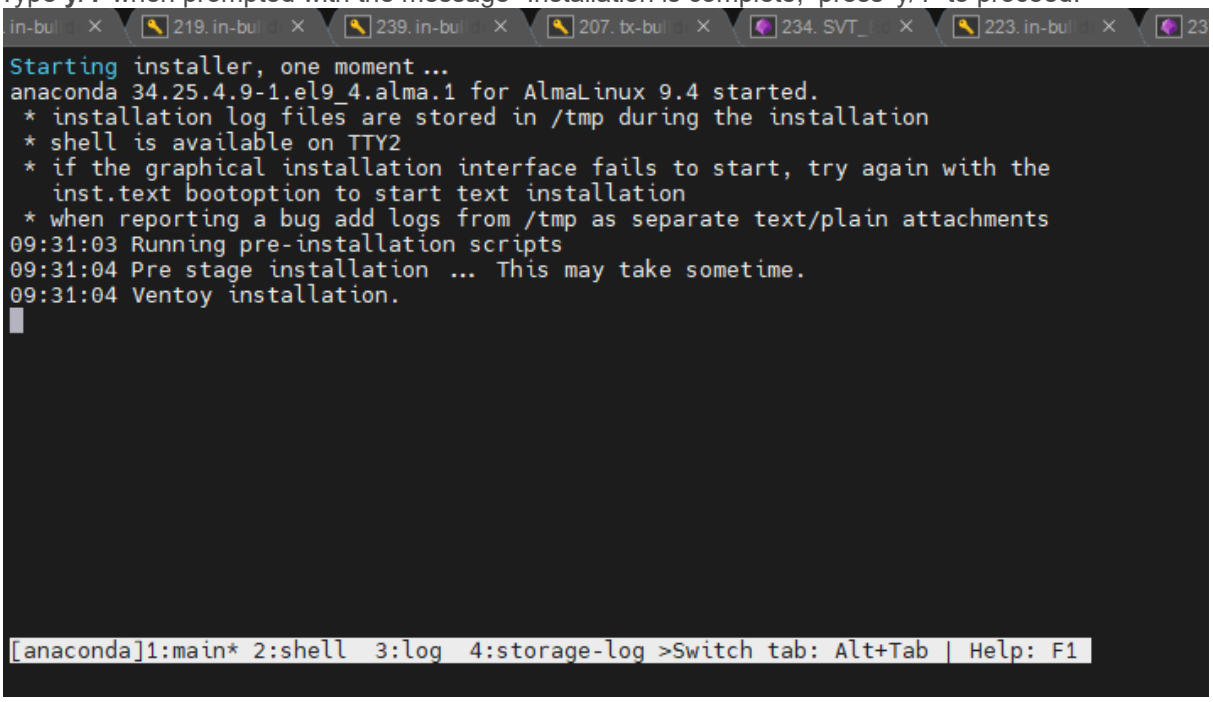
a. Type **yes** when prompted with the message "Continue (yes.no)?" Then press **Enter**.
   The system reboots. The new ISO image is highlighted in the Grub menu and the installation automatically begins within 10 seconds.
   (The following figures illustrate an upgrade from Alma8 to Alma9. A similar sequence appears when upgrading to a new ROHOS RHEL image.)

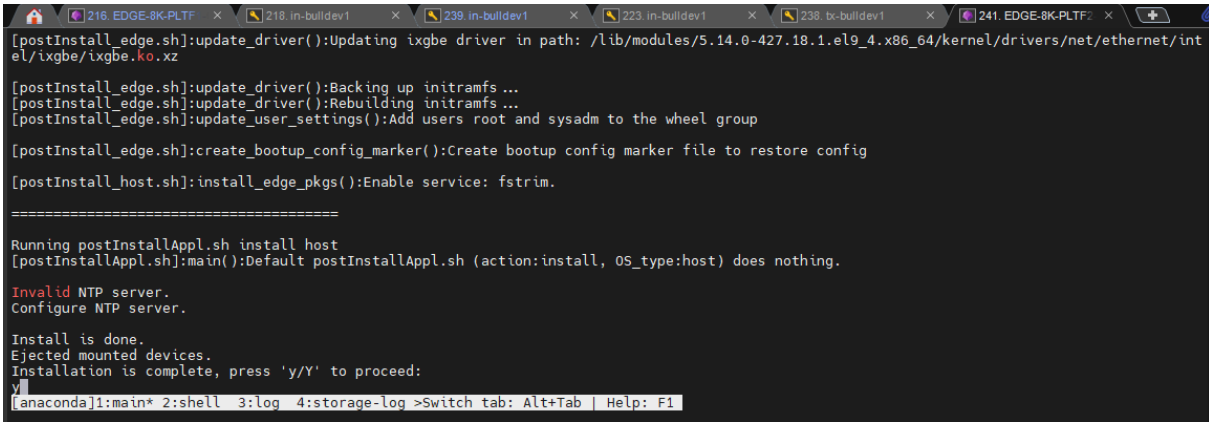


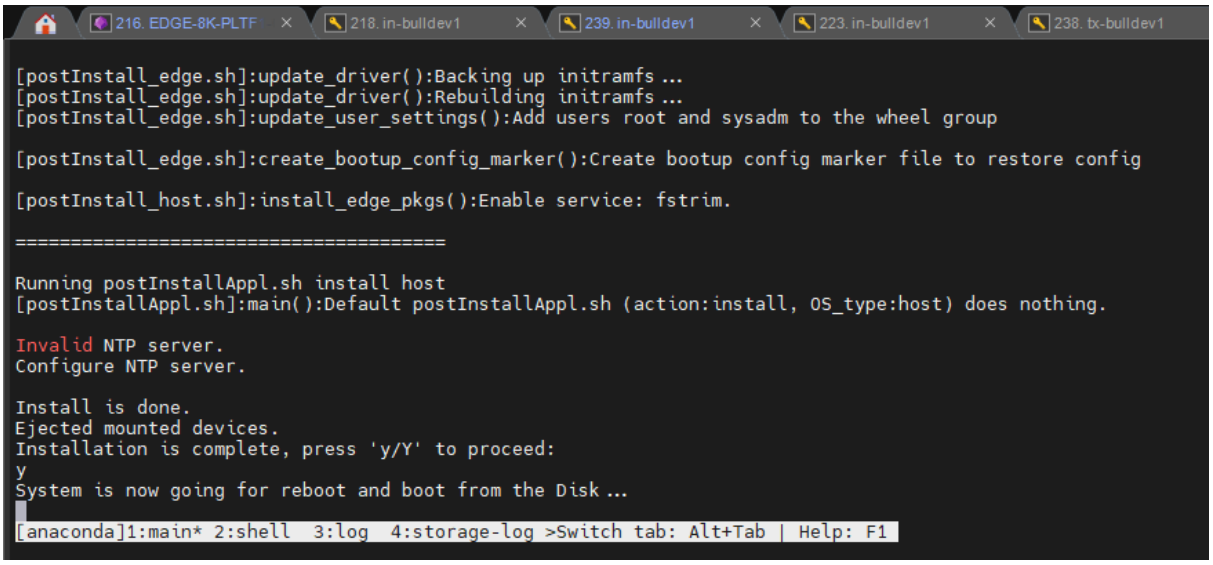
b. Select ***Install AlmaLinux 9.4 SERIAL** and press **Enter** to begin installing the new software on the boot partition of the hard disk.



c. Type **y/Y** when prompted with the message "Installation is complete, press 'y/Y' to proceed:"







7. This completes the software upgrade with the system configuration restored.

Perform Post-Upgrade Activities

Start

1. Configure the RAMP IP address if the upgrade is from 24.0 to 24.1.

   > **Note**
   >
   > This is only required once following an upgrade from 24.0 to 24.1. Thereafter the system maintains the RAMP IP address in the **System** > **Node-Level Settings** of the Edge 8000 webUI.

   a. In the Edge 8000 webUI, click the **Settings** tab.
   b. Navigate to **System** > **Node-Level Settings**.
   c. Select **Yes** from the pull-down menu for field **Connect to RAMP**.
   d. Enter the **Management Address**.
2. Configure a default route for the SWe Edge function in case anyone wants to ping the IPs from endpoints that are not in the same subnet as the interface IPs (BR1, BR4).

Updating the BIOS

Use this workflow to update the BIOS of an Edge 8000 device using a USB flash drive.

This workflow applies to all Edge 8000 Series devices.

> **Caution**
>
> This operation causes a service disruption. Perform this procedure only during a maintenance window.

Prerequisites

- System Administrator (*sysadm*) login access to the Edge 8000 CLI. This is required for checking the current BIOS version of the device.
- The updated BIOS files supplied by Ribbon or available in Ribbon Global Service Center (GSC).
- A USB flash drive of at least 1GB data storage capacity.
- A serial connection to the Console port of the front panel, either directly or via a Telnet connection through a terminal server. This is required for interacting with the device during the system restart.

Workflow

Step	Action
1	View the current BIOS version of the device. See View the Current BIOS Version.
2	Prepare a USB Flash Drive With the Updated BIOS
3	Install the Updated BIOS From the USB Flash Drive
4	Confirm the new BIOS version. See View the Current BIOS Version.

View the Current BIOS Version

1. Log in to the Edge 8000 CLI as user *sysadm*.
2. Switch to user *root*.

Example: Switching User to Root

```
$ sudo -i
[sudo] password for sysadm:
#
```

3. Execute the dmidecode command to view the current BIOS version

Example: Dmidecode Response

```
# dmidecode -s bios-version
```

```
1.1.4
```

Prepare a USB Flash Drive With the Updated BIOS

Use this procedure to format a USB flash drive to the FAT32 file system and to copy the BIOS files onto the flash drive.

1. Insert the USB flash drive into your Windows-based PC or laptop.
2. In Windows File Explorer, right-click on the USB flash drive.
3. Click **Format**. Complete the options.
   a. Make sure you select **FAT32** in the **File system** field.
   b. Provide a meaningful name in the **Volume label** field. Example: E8K_BIOS_1.1.4.
   c. Accept the remaining defaults.
4. Click **Start**.
   A warning will appear stating that the formatting will erase all data on the drive.
5. Click **OK** to begin formatting.
6. Wait for the "Format Complete" message to appear, then click **OK**.
7. Copy the updated BIOS files to the newly formatted flash drive.
   You can simply drag the files into the USB in File Explorer. No additional settings are required.
   Example file names:
   AfuEfix64.efi, EM8300_1.1.4.bin

Install the Updated BIOS From the USB Flash Drive

> **Caution**
>
> This operation causes a service disruption. Perform this procedure only during a maintenance window.

1. Verify that no other USB flash drives are connected to the Edge 8000 device.
2. Insert the USB flash drive into the USB 3.0 port.
   The port is the blue USB port on the front panel next to the Config reset button.
   Refer to Front and Back Panels. (Example: Edge 8100 Front Panel, #USB Ports.)
3. Connect to the front panel's console port, either directly from your laptop or through a terminal server.
   Refer to Front and Back Panels. (Example: Edge 8100 Front Panel, Serial Console Port.)
4. Restart the system and enter the Boot Menu.
   a. Press quickly the Reset button on the front panel to restart the system.
      Refer to Front and Back Panels. (Example: Edge 8100 Front Panel, Reset Button.)
   b. Press **b** or **F7** as the system restarts to enter the boot menu.

   Example: System Restart Sequence

   ```
   Version 2.19.1266. Copyright (C) 2022 American Megatrends, Inc.
   BIOS Date: 03/03/2022 14:02:06 Ver: 1.1.1
   Press <DEL> or <ESC> to enter setup.
   Press <b> or <F7> to enter boot menu.
   Entering Boot Menu...
   ```

5. Select **UEFI: Built-in EFI Shell** from the boot device options and press **ESC** within 4 seconds.
   Pressing **ESC** or any other key within 4 seconds after selecting the EFI shell allows you to skip the startup.nsh shell, which is not needed for this procedure.
   a. Select the **UEFI: Built-in EFI Shell** and press **ENTER**.

Example: Boot Device Menu

```
    Please select boot device:
ubuntu (P4: 64GB SATA Flash Drive)
UEFI: Built-in EFI Shell
ubuntu
ubuntu
Enter Setup
    ENTER to select boot device
    ESC to boot using defaults
```

The system displays the UEFI interactive shell startup.

Example: UEFI Interactive Shell Startup

```
UEFI Interactive Shell v2.1
EDK II
UEFI v2.60 (American Megatrends, 0x0005000D)
Mapping table
      FS1: Alias(s):HD1h0b:;BLK5:
          PciRoot(0x0)/Pci(0x15,0x0)/USB(0x7,0x0)/HD(1,MBR,0x865B99C6,0x800,0xE
537000)
      FS0: Alias(s):HD0e65535a1:;BLK1:
          PciRoot(0x0)/Pci(0x14,0x0)/Sata(0x4,0xFFFF,0x0)/HD(1,GPT,17397099-735
8-497E-A9D5-1760DCFE1229,0x800,0x200000)
     BLK4: Alias(s):
          PciRoot(0x0)/Pci(0x15,0x0)/USB(0x7,0x0)
     BLK0: Alias(s):
          PciRoot(0x0)/Pci(0x14,0x0)/Sata(0x4,0xFFFF,0x0)
     BLK2: Alias(s):
          PciRoot(0x0)/Pci(0x14,0x0)/Sata(0x4,0xFFFF,0x0)/HD(2,GPT,B3C30EB8-00F
8-49A6-A92D-19E83B49D119,0x200800,0x200000)
     BLK3: Alias(s):
          PciRoot(0x0)/Pci(0x14,0x0)/Sata(0x4,0xFFFF,0x0)/HD(3,GPT,3E454928-608
A-408C-AAFB-E135ACFB43FD,0x400800,0x7340000)
```

b. Within 4 seconds, press **ESC** or any other key to skip the startup.nsh shell.
   The startup.nsh: shell is a utility for specifying optional commands and scripts for the UEFI interactive shell to execute. It is not needed for this BIOS update procedure.
   (To get out of startup.nsh, enter **exit** at the prompt.)

6. Change to the FS1 directory and verify the BIOS files are present.

Example: Switching Directories and Verifying the BIOS Files

```
Shell> fs1:
FS1:\> ls
Directory of: FS1:\
12/28/2023  10:55          16,777,216  EM8300_1.1.4.bin
```

```
08/26/2022  02:53             600,912  AfuEfix64.efi
               2 File(s)  17,378,128 bytes
               0 Dir(s)
```

7. Execute the BIOS update command.

Example: Executing the BIOS Update Files

```
FS1:\> afuefix64.efi EM8300_1.1.4.bin /B /P /N
+-------------------------------------------------------------------------------+
|                  AMI Firmware Update Utility v5.15.00.0064                    |
|      Copyright (c) 1985-2021, American Megatrends International LLC.         |
|         All rights reserved. Subject to AMI licensing agreement.              |
+-------------------------------------------------------------------------------+
 Reading flash ..................... Done
 - ME Data Size Checking ........... Pass
 - FFS Checksums ................... Pass
 - Check RomLayout ................. Pass
 Erasing Boot Block ................ Done
 Updating Boot Block ............... Done
 Verifying Boot Block .............. Done
 Erasing Main Block ................ Done
 Updating Main Block ............... Done
 Verifying Main Block .............. Done
 Erasing NVRAM Block ............... Done
 Updating NVRAM Block .............. Done
 Verifying NVRAM Block ............. Done

 Process completed.
```

8. Reset the system from the FS1 shell prompt.

Example: Reseting From the Shell Prompt

```
FS1:\> reset
```

View Current Software Versions

Use this procedure to view the current software versions and build numbers of your Edge 8000 device.

Prerequisites

- Administrator (*admin*) login access to the web-based Edge 8000 user interface

Start

1. Log in to the Edge 8000 web-based user interface as user administrator (*admin*).
2. Click the **Settings** tab.
3. In the navigation pane, select **Home**.
   This displays summary information about the Edge 8000 device, including the software version and build numbers of the Edge 8000 device and the SBC SWe Edge component.

System Security and Administration

Contents

Audit Logging

Contents

About Audit Logging

Audit logging allows you to view user activity for any creation, update, or deletion performed for any element of the Edge 8000 device, including changes to the System, Analog, Routing, or SBC Swe Edge configuration via the webUI. The audit information includes:

- the name of the user who performed the action
- the action performed
- which element the action was performed on
- the IP address from which the request came

The device audit is always on, and the information goes into the standard webui.log file with the category AUDIT. Refer to Working with Logging for general logging information. Refer to Managing Local Logs for specific information about viewing the webui.log file.

View Audit Logs

Use the following procedure to view the audit logs of an Edge 8000 device.

Prerequisites

- Login access to the Edge 8000 webUI as user *admin*.

Start

1. Log in to the Edge 8000 webU as user *admin*.
2. Click the **Diagnostics** tab.
3. Navigate to **Logs** > **Local System Logs**.
4. Expand **webui.log** to see the log entries.

Blocking Unwanted Traffic

Contents

About Blocking Unwanted Traffic

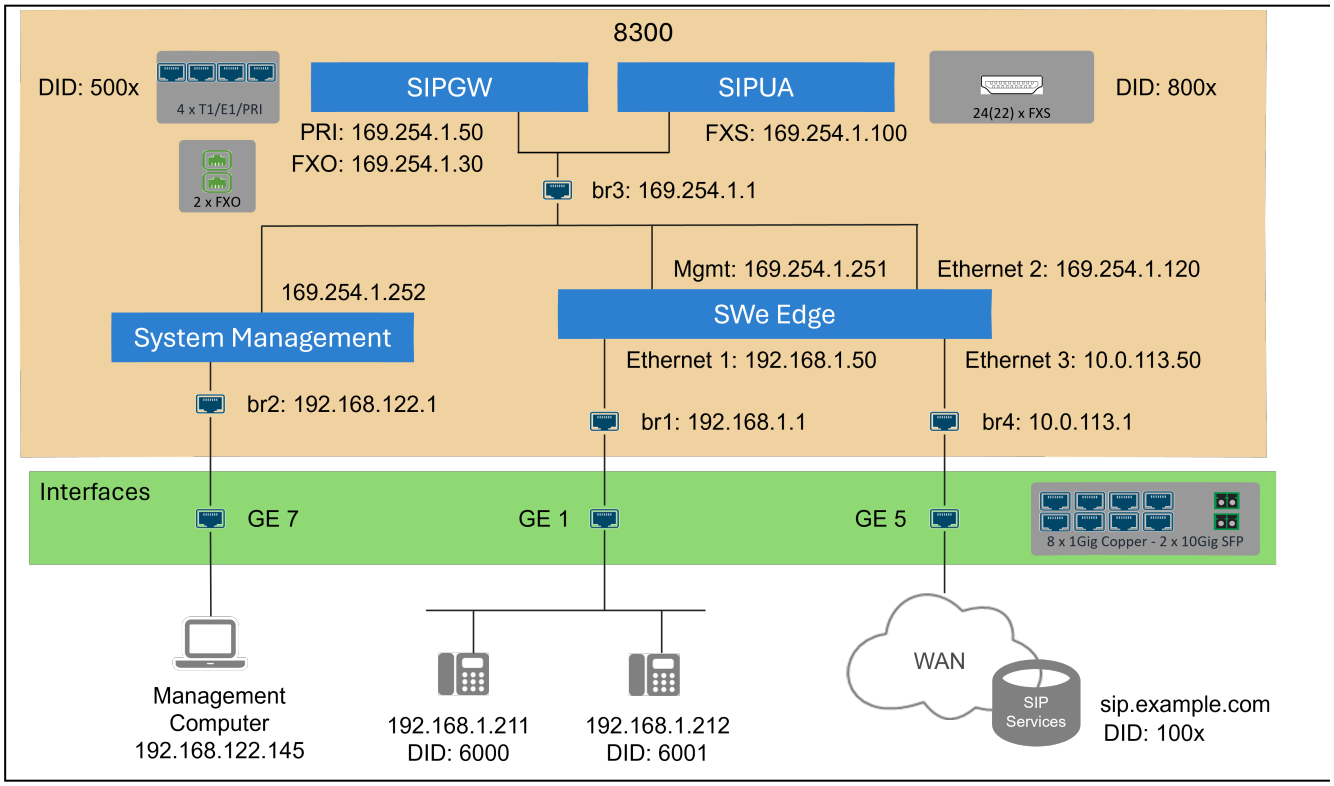
The Ribbon Edge 8000 Series device includes ways to block unwanted traffic at the network interface level. This can be accomplished using 6Wind nc-cli commands or the Edge 8000 webUI.

As an aid to understanding the Edge 8000 interfaces, see the following diagram illustrating the interface assignments for a typical Edge 8300 deployment. The Bridge 4 (br4) interface is the public or WAN interface of the device.

Attention

The IP addresses shown in the examples may conflict with an existing or planned production network. Consult with your network administrator for the specific IP addresses required for your deployment.

Example of Network Interface Assignments for an Edge 8300



Example of Blocking Common Service Ports on BR4 Interface

The following example illustrates the blocking of a set of services on the BR4 interface using 6Wind configuration commands and the Edge 8000 webUI. The services blocked are:

- port 111 (portmapper)
- port 22 (ssh)
- port 443 (https)
- port 161 (snmp)
- port 830 (netconf-ssh)
- port 80 (http)

Block Service Ports Using 6Wind Configuration Commands

Prerequisites

- Login access as user *sysadm* to the Edge 8000 CLI.

Start

1. Log in to the Edge 8000 CLI as user *sysadm*.
2. Switch to user *root*.
   # sudo -i
3. Enter the 6WIND cli environment.
   # nc-cli
4. Run the following commands.

Example: Direct-Access Blocking

```
nc-cli
vrf main firewall ipv4 filter input
rule 50 action drop description Dport22DROP destination port 22 inbound-interface
 br4 protocol tcp
rule 51 action drop description Dport443DROP destination port 443 inbound-interfac
e br4 protocol tcp
rule 52 action drop description Dport161DROP destination port 161 inbound-interfac
e br4 protocol udp
rule 53 action drop description Dport111DROP destination port 111 inbound-interfac
e br4 protocol tcp
rule 54 action drop description Dport830DROP destination port 830 inbound-interfac
e br4 protocol tcp
rule 55 action drop description Dport80DROP destination port 80 inbound-interface
 br4 protocol tcp
commit
exit
copy running startup
exit

# iptables -nvL
Chain INPUT (policy ACCEPT 88 packets, 6751 bytes)
 pkts bytes target     prot opt in     out     source               destination
   10   600 DROP       tcp  --  br4    *       0.0.0.0/0            0.0.0.0/0
tcp dpt:22 /* yams-rule-id 50 */ /* Dport22DROP */
```

```
    0     0 DROP       tcp  --  br4    *       0.0.0.0/0            0.0.0.0/0
tcp dpt:443 /* yams-rule-id 51 */ /* Dport443DROP */
    0     0 DROP       udp  --  br4    *       0.0.0.0/0            0.0.0.0/0
udp dpt:161 /* yams-rule-id 52 */ /* Dport161DROP */
    0     0 DROP       tcp  --  br4    *       0.0.0.0/0            0.0.0.0/0
tcp dpt:111 /* yams-rule-id 53 */ /* Dport111DROP */
    0     0 DROP       tcp  --  br4    *       0.0.0.0/0            0.0.0.0/0
tcp dpt:830 /* yams-rule-id 54 */ /* Dport830DROP */
    0     0 DROP       tcp  --  br4    *       0.0.0.0/0            0.0.0.0/0
tcp dpt:80 /* yams-rule-id 55 */ /* Dport80DROP */
```

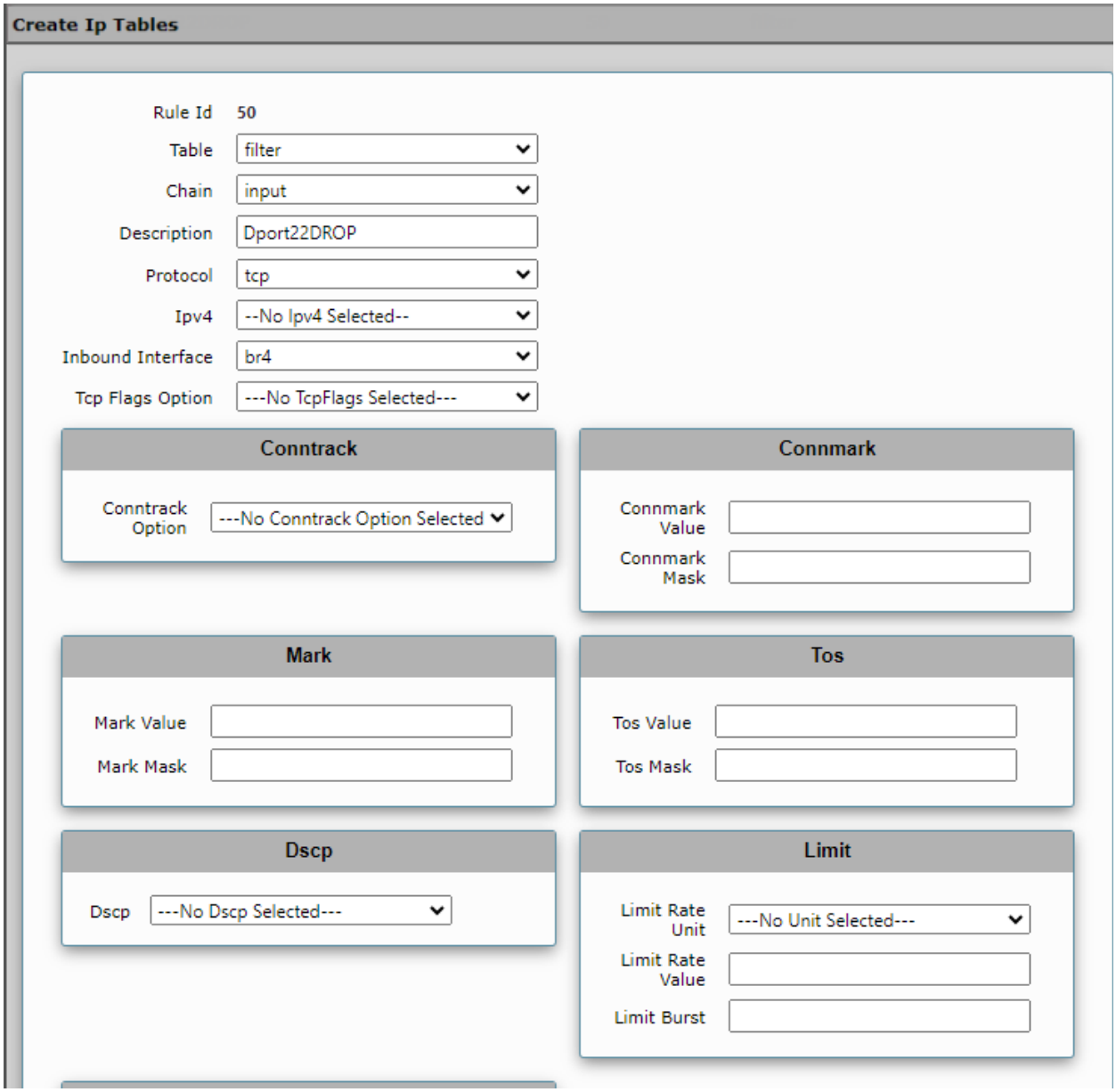
Block Service Ports Using the Edge 8000 webUI

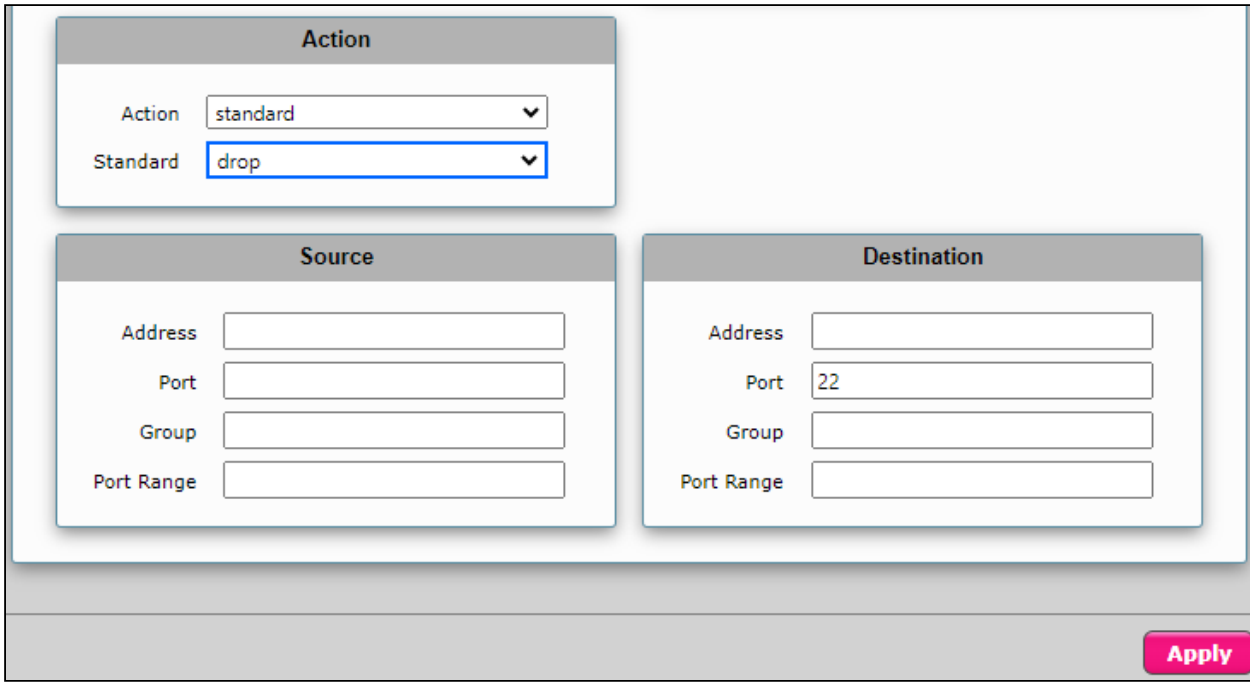
Prerequisites

- Login access as user *admin* to the Edge 8000 webUI.

Start

1. Log in to the Edge 8000 webUI, and click the **Settings** tab.
2. Navigate to **Routing** > **Vrf Firewall**.
3. Click the "+" in the banner to create a new rule.
4. Complete the fields in the **Create Ip Tables** window.
   Example for creating a rule to drop any port 22 tcp messages coming inbound to interface Bridge 4 (br4):





5. Click **Apply**.
6. Repeat for each rule.

Password Management

Contents

Password Defaults

Upon initial login, the system instructs you to change the password. The following passwords are the default passwords for the *sysadm* and *admin* user accounts:

Edge 8000 Default Passwords

System	Login	Default Password
Edge 8000 CLI	sysadm	Ribbon%@@%5225
Edge 8000 webUI	admin	admin

Managing Passwords

Restore the CLI Password to Its Factory Default

Use the following procedure to restore the CLI password to its factory (first-time login) default.

Prerequisites

- Physical access to the front panel of the device

Start

1. Press the Config button (not the Reset button) on the front panel for 3 to 5 seconds.

   > **Attention**
   >
   > Do not press the Config button for more than 5 seconds. At 10 seconds, the system resets the entire router configuration, resulting in a service outage. Refer to Front and Back Panels for a complete description of the Config button on the Edge 8000 Series front panel.

2. Log back into the CLI user interface using the default, first-time login password. (Refer to First-Time Login Passwords.)
   The system immediately instructs you to change the password.

Change the Password of an Edge 8000 CLI Account

Prerequisites

- Login access to the Edge 8000 command line interface (CLI).

Start

1. Log in to the Edge 8000 CLI through an SSH connection.
2. Enter the `passwd` command and follow the prompts to change the password.

   Example

   ```
   # passwd
   Changing password for user sysadm
   Current password:
   New password:
   Retype new password:
   passwd: all authentication tokens updated successfully.
   ```

The new password must meet the following criteria:

- at least 12 characters
- at least one non-alphanumeric character
- at least one digit
- at least one lowercase letter

Change the Password of an Edge 8000 webUI Account

Prerequisites

- Login access to the Edge 8000 web-based user interface (webUI) as user administrator (*admin).*

Start

1. Log in to the Edge 8000 webUI.
2. Select the **Settings** tab.
3. Navigate to **System** > **Security** > **Users** > **Local User Management**.
4. Select the account you wish to change.
5. Click **Reset Password**.
6. Change the password.
7. Click **Ok**.

The new password must meet the following criteria:

- at least 8 characters
- at least one non-alphanumeric character
- at least one digit
- at least one lowercase letter
- at least one uppercase letter

Refer to Managing Local Users and Managing Global Security Options for additional information about setting and managing password requirements.

Troubleshooting, Repairs, and System Status

Contents

Debugging

Use the following Workflow as an aid to debugging an Edge 8000 Series device. The procedures explain how to collect information about the Edge 8000 device.

Prerequisites

- Login access to the Edge 8000 Command Line Interface (CLI), as user *sysadm* and then as user *root,* using an SSH client such as Putty. (Some actions require you to capture the CLI output using the Putty collection function.)
- Login access to the Edge 8000 webUI as user *admin*.

Workflow

Step	Action
1	Log in to the Edge 8000 CLI
2	Collect Logs from the SIPUA
3	Collect PCAPS from the SIPGW or SIPUA
4	Configure Analog (FXS/FXO) and PRI Logs

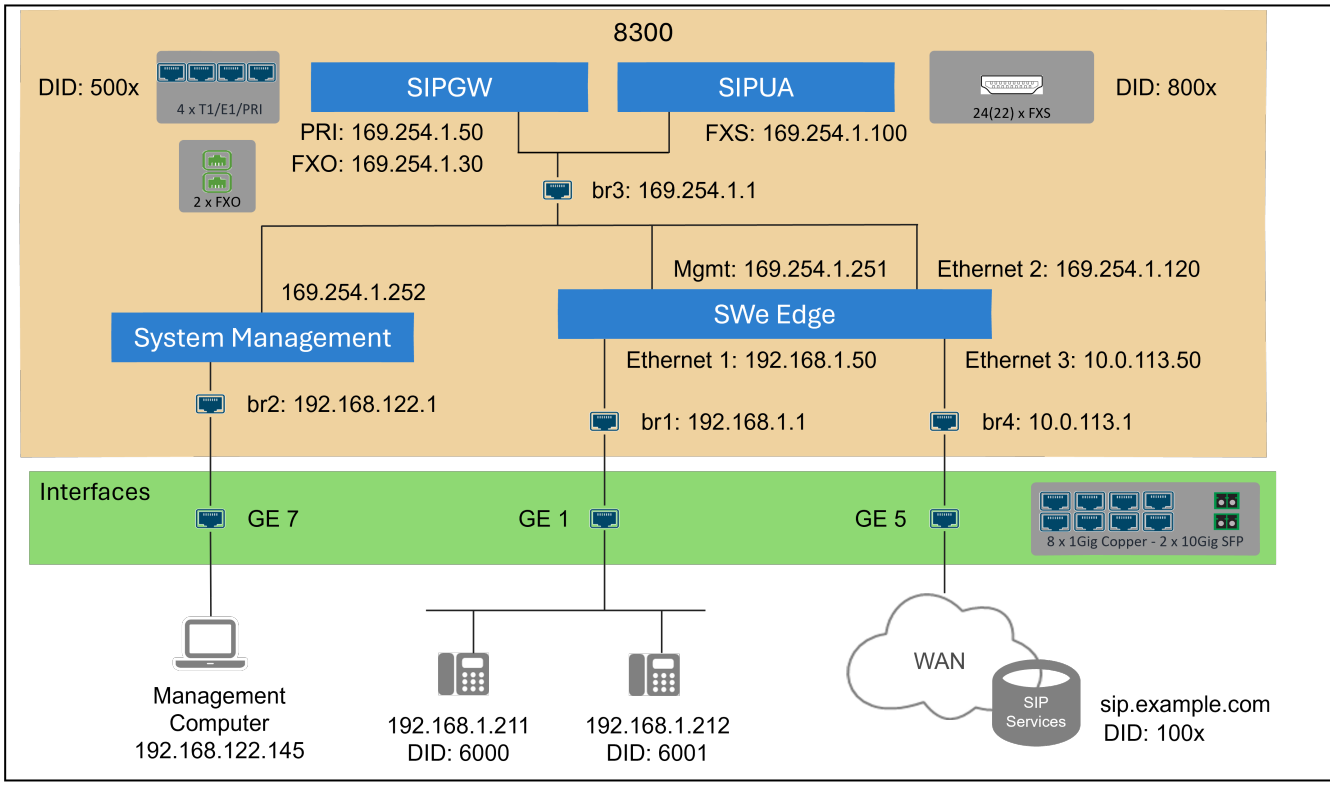
Step	Action
5	Collect Logs and PCAPS from the SWE Edge
6	Generate a System Report
7	Generate a System Debug Report
8	View 6WIND Router Logs

Job Aid: Network Diagram

Use the following diagram as an aid to understanding the various interfaces typical of an Edge 8300 device. (Note that an Edge 8100 model is the same except without the FXO, PRI, and FXS interfaces.)

> **Attention**
>
> The IP addresses shown in the examples may conflict with an existing or planned production network. Consult with your network administrator for the specific IP addresses required for your deployment.

Example Network Diagram: Edge 8300 Model



Log in to the Edge 8000 CLI

1. From the Edge 8000 CLI, log in as user system administrator (*sysadm*).
2. Change to user *root*.

```
$ sudo -i
```

Collect Logs from the SIPUA

1. As user *root* in the CLI, access the SIP User Agent (SIPUA) module.

   ```
   db-manager-ctl cli
   ```

2. Enter number `4` to access the SIPUA.
3. Run the following command to enable log collection.
   Make sure that the Putty session is set to capture the output.

   ```
   debugsipgw 7 <enable debug>
   ```

4. After completing your test calls, run the following command to disable log collection.

   ```
   debugsipgw 0 <disable debug>
   ```

Collect PCAPS from the SIPGW or SIPUA

Prerequisites

- Login access to the Edge 8000 CLI as user *sysadm*.

Start

1. As user *root* in the CLI, access the SIP Gateway (SIPGW) or SIPUA module.

   ```
   db-manager-ctl cli
   ```

   a. Enter number `9` to access the SIPGW.

   b. Enter number `4` to access the SIPUA.

2. Mount the filesystem to provide a memory disk area for writing pcaps.
   Note that the /etc/images directory already exists on the host. When setting the size, do not exceed 10 Mb (10m).

   ```
   mount -t tmpfs tmpfs /etc/images -o size=4m
   tcpdump -s 0 -ni eth0 port 5060 -w /etc/images/sip1.pcap
   ```

3. After completing your test calls, open a new session to transfer the captured file to the host. Note the different internal IP addresses for SIPGW and SIPUA:
   IP address for SIPGW: 192.168.188.250
   IP address for SIPUA: 192.168.188.100

   ```
   cd /E8000/backup_config
   scp root@<IP>:/etc/images/sip1.pcap
   ```

```
Password - <shift key plus 234567890>
```

4. Change permissions on the pcap file so you can delete it.

```
chmod 770 sip1.pcap
```

5. Delete the pcap file and unmount the filesystem from the session where pcaps data was captured.

```
rm /etc/images/sip1.pcap
umount /etc/images
```

Collect Logs and PCAPS from the SWE Edge

For collecting logs and packet captures (PCAPS) from the SWE Edge, refer to Working with Logging in the SBC Edge Portfolio Documentation.

> **Note**
>
> The Edge 8000 Series product reuses Ribbon SBC SWe Edge and 6WIND software. Therefore, at times you will be directed to the customer documentation of the other product where a complete documentation suite describes all the features and functions of that software.
>
> Refer to Related Documents for links to the documentation suites applicable to the Edge 8000 Series product.

Configure Analog (FXS/FXO) and PRI Logs

The Edge 8000 device enables debug message collection from its internal SIP User Agent (sipua) and SIP Gateway (sipgw) functions into the SWe Edge log collection screen so that the functions all write their logs to /var/log/messages. You then can use the syslog configuration screen to populate the host syslog settings so that the logs from the SWe Edge and Analog Manager functions can all be written out to an external syslog server.

To configure log collection for Analog Manager and SIPGW functions, use the following procedure.

Prerequisites

- Login access to the Edge 8000 webUI as user *admin*.

Start

1. As user admin in the Edge 8000 webUI, select the **Settings** tab.
2. Navigate to **System** > **Logging Configuration** > **Diagnostic Logging > By Subsystem**.
3. Click the "**+**" symbol to add a Subsystem Configuration.
4. Complete the fields in the Subsystem Configuration window.

Field	Description
Subsystem Name	From the dropdown list, choose one of the available Edge 8000 subsytems, such as Analog (FXS/FXO) or PRI.

Field	Description
Log Level	From the dropdown list, choose a log level from Default to Fatal. Refer to Supported Logging Levels for logging level definitions.
Log Destination	From the dropdown list, choose either Local Logs or one of the Remote Logs already defined.

5. Click **OK**.

Generate a System Report

As user *root* in the CLI, generate a system report using the following command:

```
sys-tools report <reportName>
```

The report format is <reportName>_<year>-<month>-<day>-<time>.tgz

For example, SBC_NODE_1_2024-08-31-00.12.14.tgz

The system report file is saved in the /e8k-data/reports directory. The file contains information about the Setup Wizard configuration, software versions, ifconfig, iptables, route, bridge, arp, dmesg, systemctl, memory information, and NTP information, plus a config backup and various other Linux level files, for example,/var/log/messages.

> **Note**
>
> You can generate the system report at any time since it does not disrupt service on the SWE Edge system.

Generate a System Debug Report

As user *root* in the CLI, generate a system debug report using the following command:

```
sys-tools debug
```

The system debug report file is displayed in the terminal window. The file contains information about the Setup Wizard configuration, software versions, ifconfig, iptables, route, bridge, arp, dmesg, systemctl, memory information, NTP information, and other data useful to the support engineer.

Make sure that the Putty session is set to capture the output.

> **Note**
>
> You can generate the system debug report at any time since it does not disrupt service on the SWE Edge system.

View 6WIND Router Logs

View logs specific to the 6WIND data router function of the Edge 8000 device. Refer to 6WIND Router Documentation. Once in the documents, search the User Guide for System Logging to learn about logging services, local logging configuration, remote syslog configuration, and transport layer security for syslog messages.

Returning a Defective Unit (RMA Process)

Ribbon offers a product defect return policy, known as Return of Material (RMA), as part of the Edge 8000 Series product support.

Use the following workflow to obtain, install, and configure a replacement unit for an Edge 8000 device per Ribbon's RMA policy.

Prerequisites

- You have contacted Ribbon Technical Support for assistance, and Ribbon has advised you to request an RMA replacement unit.
- You have on hand:
  - A recent backup of the Edge 8000 unit
  - System Administrator (*sysadm*) login access to the Edge 8000 CLI
  - Administrator (*admin*) login access to the Edge 8000 WebUI

Workflow

Step	Action
1	Open a Ribbon Salesforce ticket to request a replacement unit.
2	Receive the replacement unit.
3	Mount and cable the replacement unit. Power it on. Refer to Installing Edge 8000 Hardware.
4	Download from Salesforce the software image file of the Edge 8000 software you require.
5	Install an Edge 8000 Software Image File.
6	Restore the previous site-specific settings from your Ribbon backup. Refer to Restore the Configuration Settings from Backup.
7	Obtain and install the Router and SBC SWe Edge licenses. Refer to License Management.

System Status

Contents

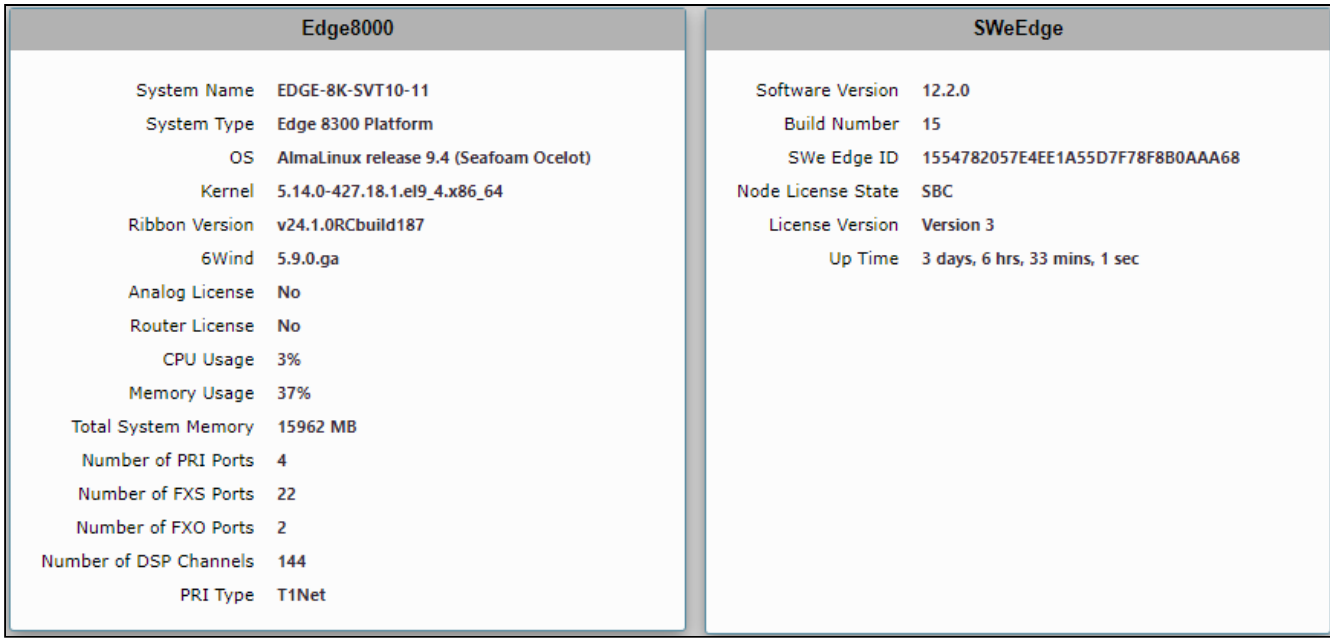
The Edge 8000 webUI offers a system status view of the Edge 8000 device and all its call channels:

- To view the system status, click the **Home** folder of the **Settings** tab. There you will find the device status and the call channels status.
- To refresh the status information, refresh the browser page.

Device Status

The device status summarizes the Edge 8000 hardware and software and the onboard SWe Edge VNF.

Example of the Device Status



Edge8000	
System Name	EDGE-8K-SVT10-11
System Type	Edge 8300 Platform
OS	AlmaLinux release 9.4 (Seafoam Ocelot)
Kernel	5.14.0-427.18.1.el9_4.x86_64
Ribbon Version	v24.1.0RCbuild187
6Wind	5.9.0.ga
Analog License	No
Router License	No
CPU Usage	3%
Memory Usage	37%
Total System Memory	15962 MB
Number of PRI Ports	4
Number of FXS Ports	22
Number of FXO Ports	2
Number of DSP Channels	144
PRI Type	T1Net

SWeEdge	
Software Version	12.2.0
Build Number	15
SWe Edge ID	1554782057E4EE1A55D7F78F8B0AAA68
Node License State	SBC
License Version	Version 3
Up Time	3 days, 6 hrs, 33 mins, 1 sec

Call Channels Status

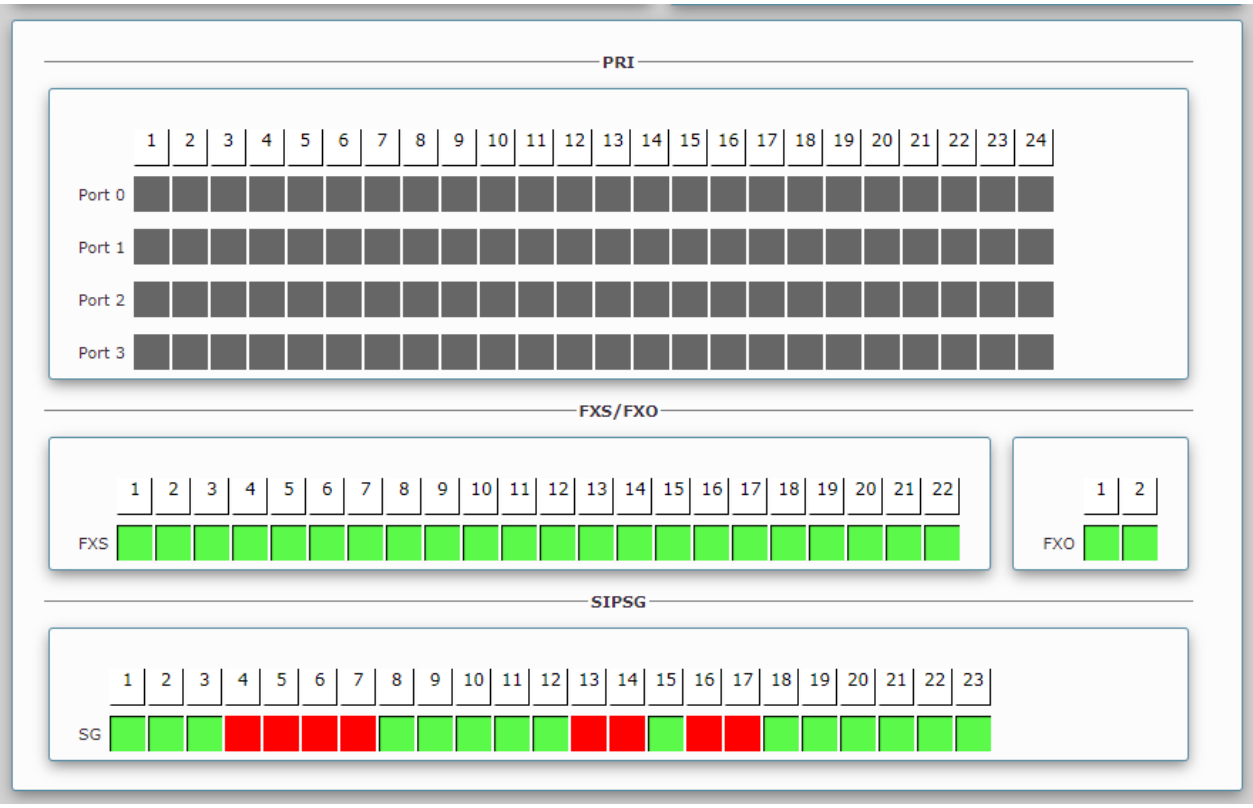
The call channels status indicates the state of SIP Signaling Groups and, for the Edge 8300 model, the PRI and FXS/FXO ports.

Characteristics of the call channels display include:

- The report is a snapshot of the channels' status. To update the report, manually refresh the web browser page. (The report does not refresh automatically.)
- The SG row represents all the Signaling Groups configured for the device.
  In the example below, 23 Signaling Groups have been created for the device.
- Color-coded cells indicate different channel states:
  - grey = not available or not provisioned
  - red = offhook (FXS/FXO) or down (SIPSG)
  - green = onhook (FXS/FXO) or up (SIPSG)
- Hovering over a cell invokes a pop-up message indicating the state of a particular channel:
  - For PRI the possible values are Idle, Busy, NotConnected, AdminDisabled, DChanDisabled, Unknown, Up, Initializing, or Disabled.

- For FXS/FXO the possible values are ONHOOK, OFFHOOK, Incall, Busy, Unknown.
- For SIPSG the possible values are UP/DOWN.

Example of the Call Channels Status



Configuration Examples

Contents

FXS Configuration for IP PBX Deployment

The following example demonstrates a complete FXS to IP PBX deployment using an Edge 8300 model and the Edge 8000 Series 24.1 software release. The example includes screenshots and specific values for all the major configuration areas of the deployment:

- Setup Wizard
- Licensing
- SWe Edge provisioning
- SIP User Agent provisioning for FXS ports

For the entire provisioning process, including physically Installing Edge 8000 Hardware, refer to Workflow for Initial Setup.

While the goal of this example is not to provide a detailed configuration that meets the needs of every scenario, it does provide a starting point for building your own customized configuration for an FXS to IP PBX deployment.

Attention

The IP addresses shown in the examples may conflict with an existing or planned production network. Consult with your network administrator for the specific IP addresses required for your deployment.

Contents

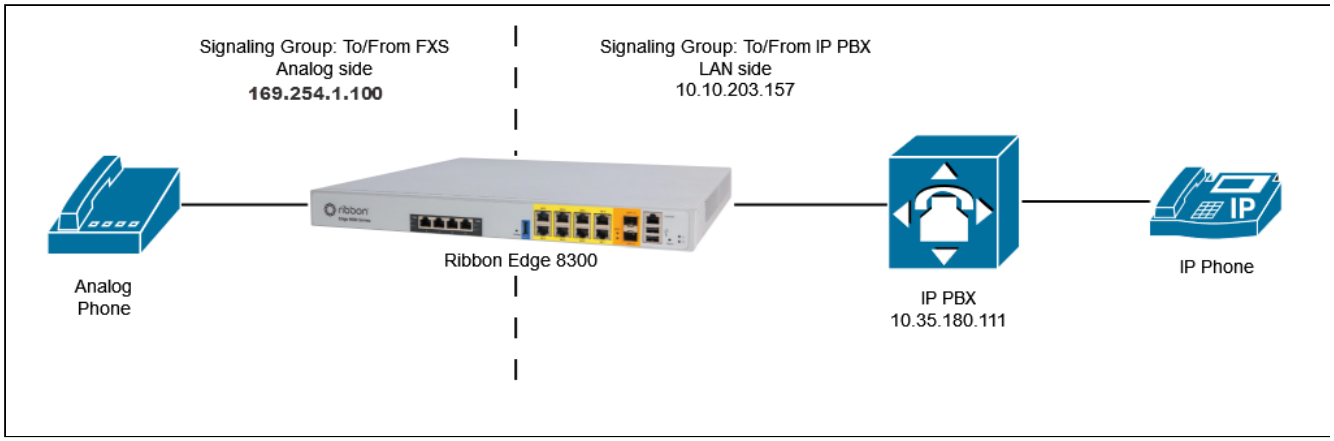
Network and Call Flow Diagrams

In this demonstration, an Edge 8300 is configured to support two signaling groups:

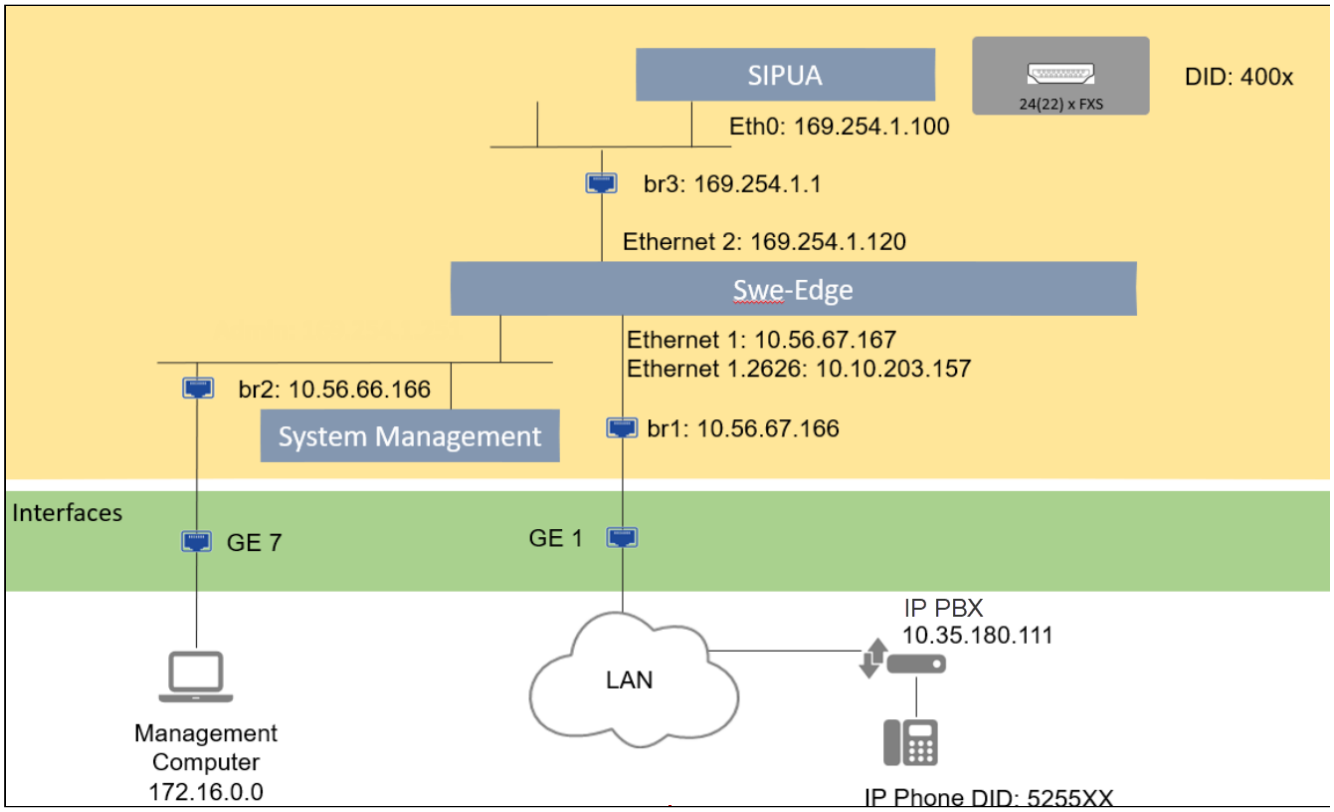
- On the analog side, an FXS port connected to an analog phone
- On the private or LAN side, an IP PBX with VLAN logical sub-interfaces connected to an IP phone

The following diagrams depict the deployment topology, network interfaces, and call flows for this demonstration.

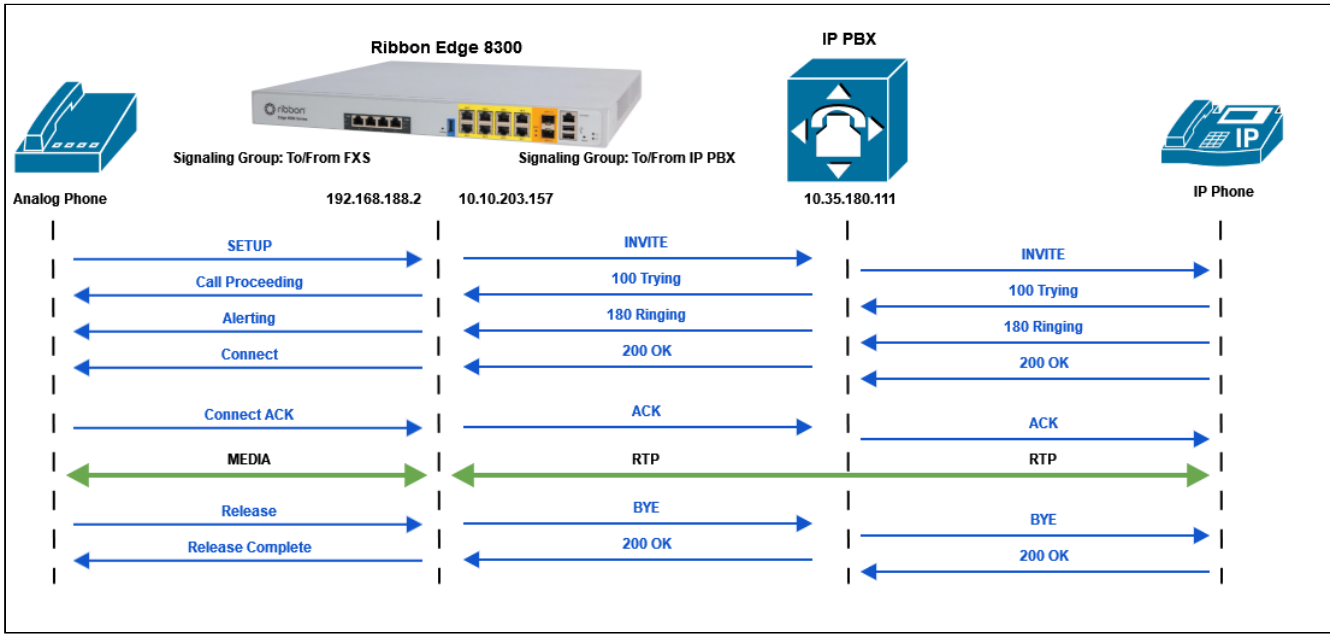
Deployment Topology



Network Interfaces



Signaling and Media Call Flows



Setup Wizard Values

After physically installing the device, the deployment team uses the Edge 8000 Setup Wizard to establish basic platform settings.

The following tables show the values entered in Setup Wizard for this FXS to SIP IP PBX demonstration. Consult your network design and deployment teams for the specific values appropriate for your network.

System Configuration

Hostname	Time Zone	6WIND fastpath cores
e8000	America/Mexico_City	4 (default)

Bridge Settings (BR1-4)

Interface	Interface Name	IPv4 Address	Netmask	Members	DHCP server (default = enabled)	Enable DHCP client (default = enabled)	Setup Wizard Note
BR1 VNF Private	br1	10.56.67.166	24	ge1	[ ] disabled (press the space bar to toggle)	n/a	
BR2 VNF Management	br2	10.56.66.166	26	ge7 (default)	[ ] disabled (press the space bar to toggle)	n/a	
BR3 VNF Internal	br3	169.254.1.1 (default)	24 (default)	n/a	n/a	n/a	
BR4 VNF Public	br4	0.0.0.0	24 (default)	_____ (default)	n/a	[*] enabled (default)	DHCP Client requires manual configuration of the gateway and DNS settings.

Gigabit Ethernet Settings (GE1-8)

Interface	Interface Name	IPv4 Address	Netmask Length		Setup Wizard Note
GE1	ge1	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE2	ge2	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE3	ge3	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE4	ge4	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE5	ge5	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE6	ge6	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE7	ge7	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE8	ge8	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.

Small Form-factor Pluggable (SFP9-10)

Interface	Interface Name	IPv4 Address	Netmask Length	Enable DHCP Client (default = disabled)		Setup Wizard Notes
SFP9	sfp9	0.0.0.0 (default)	0 (default)	[ ] disabled		If the interface is a member of a bridge interface, do not set these values. DHCP Client requires manual configuration of the gateway and DNS settings.
SFP10	sfp10	0.0.0.0 (default)	0 (default)	[ ] disabled		If the interface is a member of a bridge interface, do not set these values. DHCP Client requires manual configuration of the gateway and DNS settings.

Default Gateway

IPv4 Address	Setup Wizard Note
10.10.216.1	MUST be an IPv4 address within a subnet on an interface. Note: This is the external gateway that the Edge 8000 device routes to in order to reach outside of itself, beyond its own subnet. It's how the gateway can respond when you ping it. Without this, the Edge 8000 device doesn't know where to send its responses.

SWe Edge Settings

CPUs (1 2 4)	Memory (MBs)	Extra Interface 1	Extra Interface 2	Setup Wizard Note
2 (default)	2048 (default)	br4	_____	The Extra Interface values are any of the physical port names, for example, ge1, sfp9 or the VNF Public bridge interface name, br4.

SWe Edge and Analog Licenses

In this demonstration, the Edge 8300 device requires SWe Edge and Analog licenses.

To view the license features, open a browser and enter the SBC SWe Edge webUI IP address. Log in as user *admin.*

> **Note**
>
> In this demonstration, the SBC SWe Edge webUI IP address is 10.56.66.166. This is the address assigned as the BR2 VNF Management IP in Setup Wizard.

Click the **Settings** tab and navigate to **System** > **Licensing > Current Licenses**.

The following screenshots illustrate the Analog and SWe Edge licenses employed for this demonstration.

Analog License Features

Total **9 AnalogLicense** Rows

Feature	Licensed	Total Licenses
LICENSE_CALLS	✓	144
LICENSE_SIP	✓	on
LICENSE_T1	✓	on
LICENSE_NUM_T1_PORTS	✓	4
LICENSE_FXO_ENABLED	✓	on
LICENSE_FXO_NUM_PORTS	✓	unlimited
LICENSE_FXS_ENABLED	✓	on
LICENSE_FXS_NUM_PORTS	✓	unlimited
LICENSE_PRI_NUM_PORTS	✓	4

SWe Edge License Features

Total **10 Feature License** Rows

Feature	Licensed	Total Licenses	Available Licenses	Feature Expiration
SIP Signaling Sessions	✓	1000	1000	January 06, 2025 23:59:59
Enhanced Media Sessions with Transcoding	✓	1000	1000	January 06, 2025 23:59:59
Enhanced Media Sessions without Transcoding	✓	1000	1000	January 06, 2025 23:59:59
SIP Registrations	✓	1000	1000	January 06, 2025 23:59:59
AMR-WB	✓	Unlimited	Unlimited	January 06, 2025 23:59:59
SIP Recording	✓	1000	1000	January 06, 2025 23:59:59
Virtual Direct Routing SBA	✓	Unlimited	Unlimited	January 06, 2025 23:59:59
AMR-NB	✓	Unlimited	Unlimited	January 06, 2025 23:59:59
V150	⊘	Not Licensed	Not Licensed	Not Applicable
RHEL	✓	Unlimited	Unlimited	January 06, 2025 23:59:59

SWe Edge Configuration

Network Interface Values

Network Interfaces define the way the Edge 8000 device communicates with the external network.

The Edge 8000 supports system-created logical interfaces known as **Admin IP**, **Ethernet 1 IP**, **Ethernet 2 IP**, and **Ethernet 3 IP** for the SWe Edge function. In addition to the system-created logical interfaces, the Edge 8000 supports user-created VLAN logical sub-interfaces.

In this demonstration:

- The Admin IP is an internal logical SWe Edge IP address that is not reachable from an external network. Its value is pre-set at the factory.
- The Ethernet 2 IP is an internal logical SWe Edge interface supporting a connection to the analog ports. Its value is pre-set at the factory.

The following IP addresses must be entered manually using the Edge 8000 webUI:

- the Ethernet 1 IP address, which is a SWe Edge logical interface supporting a connection to the LAN IP PBX
- the Ethernet 1.2626 IP address, which is a SWe Edge logical interface supporting a connection to a VLAN logical sub-interface to the LAN IP PBX

For this demonstration, the following Network Interface values have been set:

Network Interface Assignments

Interface Name	IP Assign Method	Primary Address	Primary Netmask	Media Next Hop IP
Admin IP	Static	169.254.1.251	255.255.255.240	
Ethernet 1 IP	Static	10.56.67.167	255.255.255.0	10.56.67.1
Ethernet 1.2626 IP	Static	10.10.203.157	255.255.255.128	10.10.203.129
Ethernet 2 IP	Static	169.254.1.120	255.255.255.128	

Note

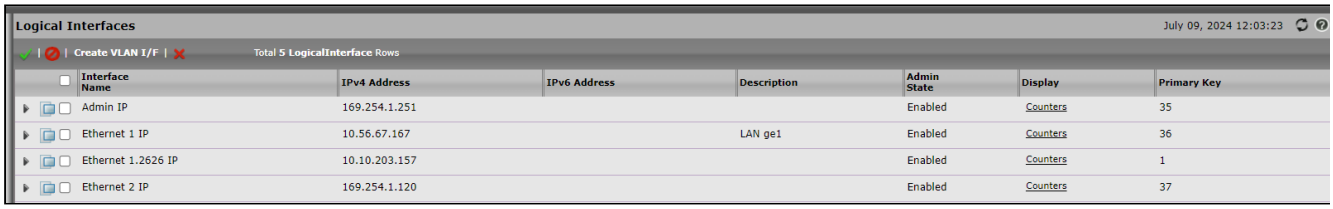
To create a VLAN I/F for a Logical Interface, navigate to **SBC > Networking Interfaces > Logical Interfaces > Create VLAN I/F**.

To display Network Interfaces in the SWe Edge WebUI:

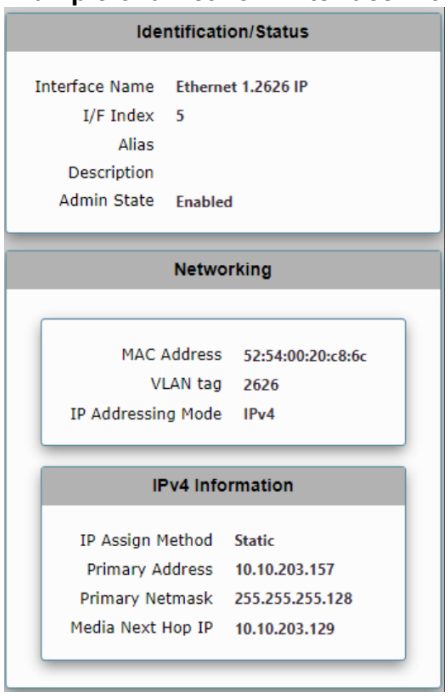
- click the **Settings** tab
- navigate to **SBC > Networking Interfaces > Logical Interfaces**

The following screenshots illustrate the Network Interfaces defined for this demonstration.

Network Interfaces



Example of a Network Interface: Ethernet 1.2626 IP



Static Route Values

Static routes enable communication with remote networks. In a production environment, static routes are mainly configured for routing from a specific network to another network that can only be accessed through one point or one interface (single path access or default route). Points to consider include:

- For smaller networks with just one or two routes, configuring static routing is preferable. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- For networks that have a LAN-side gateway on Voice VLAN or Multi-Switch Edge Devices (MSEs) with voice VLAN towards the SBC Edge, static routing configurations are not required.

> **Note**
>
> This demonstration does not have a LAN-side gateway, nor does it have MSEs.

For this demonstration, a Static Route is defined to give access to the IP PBX.

Static Route fields include:

- **Destination IP** – Specifies the destination IP address.
- **Mask** – Specifies the network mask of the destination host or subnet. (If the 'Destination IP Address' field and 'Mask' field are both 0.0.0.0, the static route is called the 'default static route'.)
- **Gateway** – Specifies the IP address of the next-hop router to use for this static route.

To display Static Routes in the SWe Edge WebUI:

- click the **Settings** tab
- navigate to **SBC > Protocols** > **IP** > **Static Routes**

The following screenshot illustrates the Static Routes defined for this demonstration.

Static Routes

Static IP Route Table — July 10, 2024 15:09:57

Total 1 IP Route Row

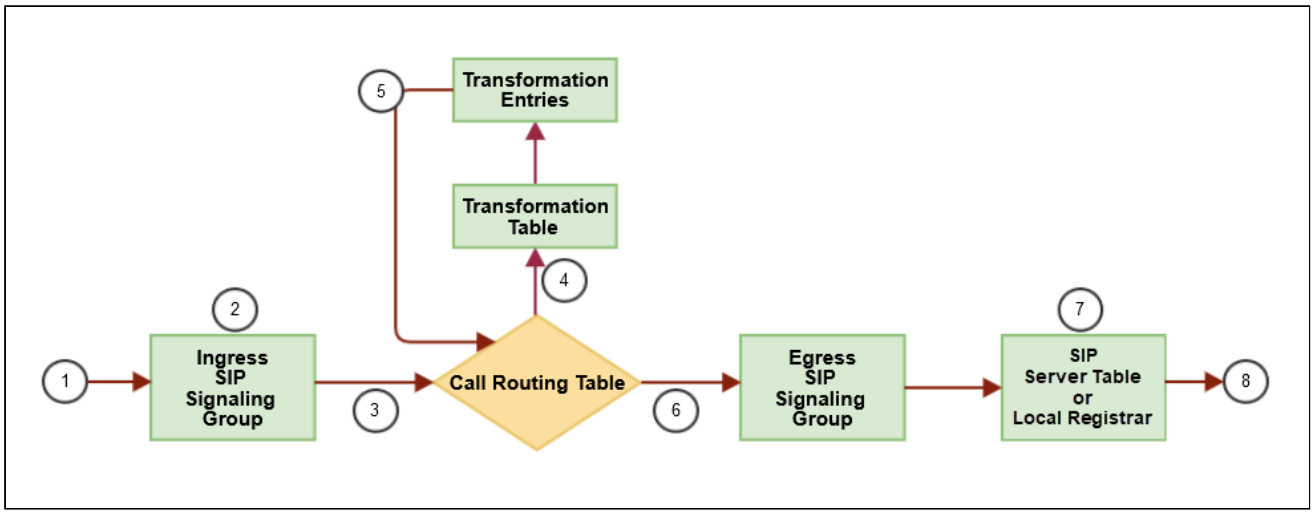
Row ID	Destination IP	Mask	Gateway	Metric	Primary Key
2	10.35.180.111	255.255.255.255	10.10.203.129	1	2

Signaling Groups

Signaling groups allow telephony channels to be grouped together for routing and shared configuration purposes. They are the locations from which ingress calls enter and to which egress calls route out. They are also the location from which Tone Tables are selected. In the case of SIP, they specify protocol settings and are linked to server, media, and mapping tables.

The following diagram depicts the role of Signaling Groups in a typical call flow sequence. Every call enters through an ingress Signaling Group, traverses through a Call Routing Table and its associated Transformation Table or Tables, and exits through an egress Signaling Group. For each Signaling Group, a SIP Server Table or Local Registrar defines where the call should go on egress.

SIP to SIP Call Flow Sequence



For this demonstration, two Signaling Groups are defined :

- To/From IP PBX Signaling Group – serves the LAN-side IP PBX and associated IP phones
- To/From FXS Signaling Group – serves the analog-side FXS ports and associated analog phones

The following fields must be modified, as a minimum, for each Signaling Group:

- **SIP Profile**
- **Tone Table**
- **Call Routing Table**
- **SIP Mode**
- **SIP server table / Local Registrar**
- **Media List ID**
- **Signaling/Media Source IP**
- **Listen Ports**
- **Federated IP/FQDN**

Additional fields may be modified per end-user requirements.

Note

Be sure to set the following parameters correctly per your network plan:

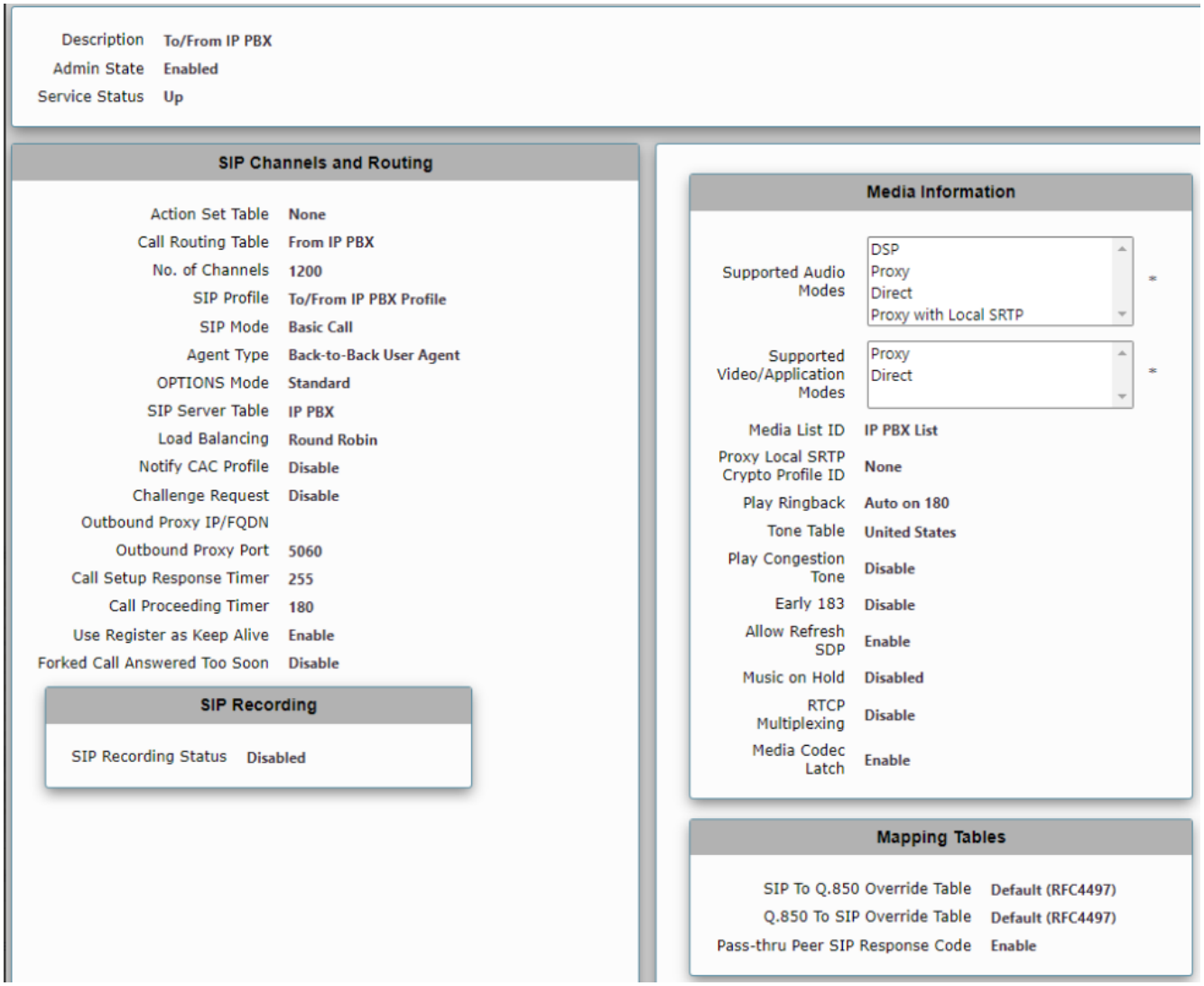
- **Signaling/Media Source IP** – this value is specific to the associated Signaling Group
- **Federated IP/FQDN** – this value is specific to the associated Signaling Group
  - as the IP address of the IP PBX (10.35.180.111 in this example) for the IP PBX Signaling Group, or
  - as the IP address of the internal SIP User Agent (169.254.1.100 in this example) for the FXS Signaling Group

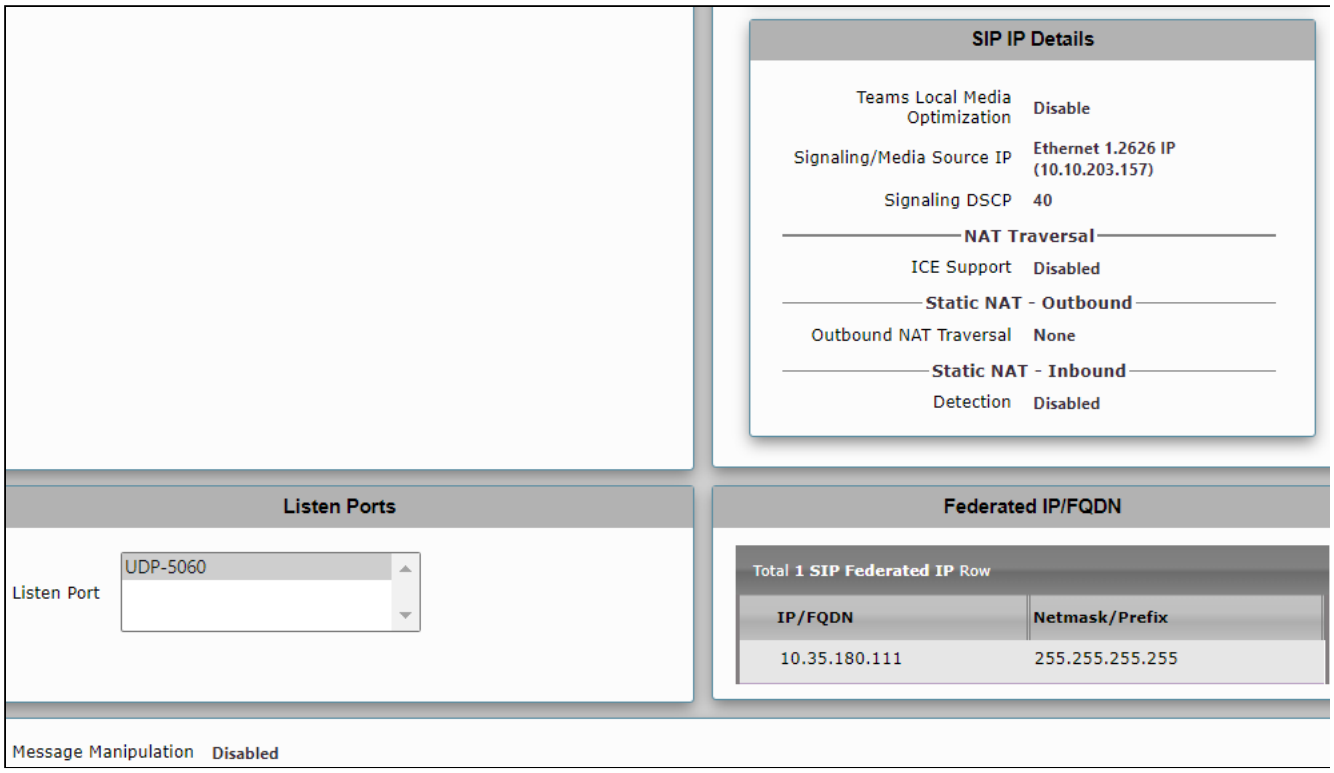
To display Signaling Groups in the Edge 8000 webUI:

- click the **Settings** tab
- navigate to **SBC > Signaling Groups**

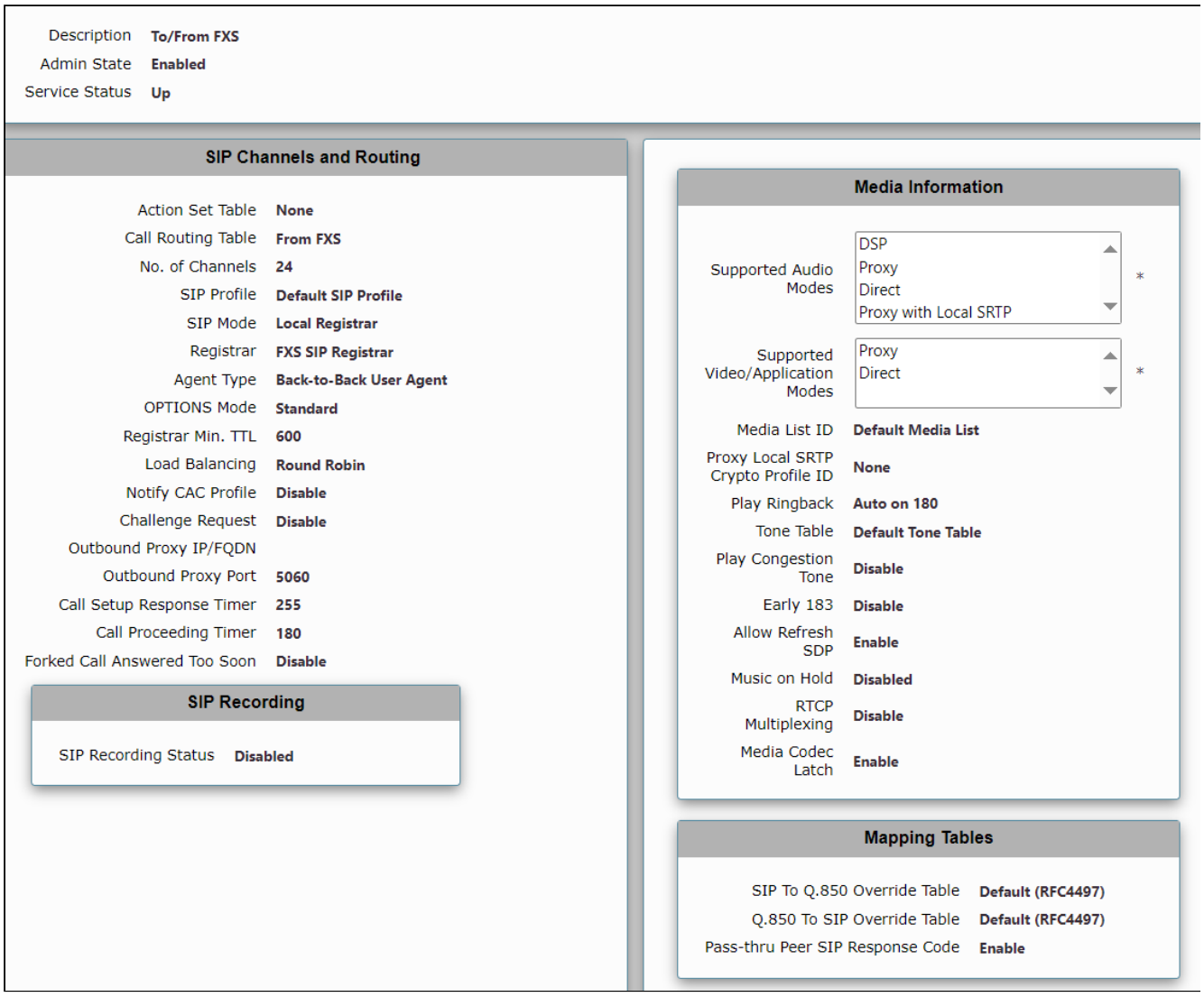
The following screenshots illustrate the Signaling Groups defined for this demonstration.

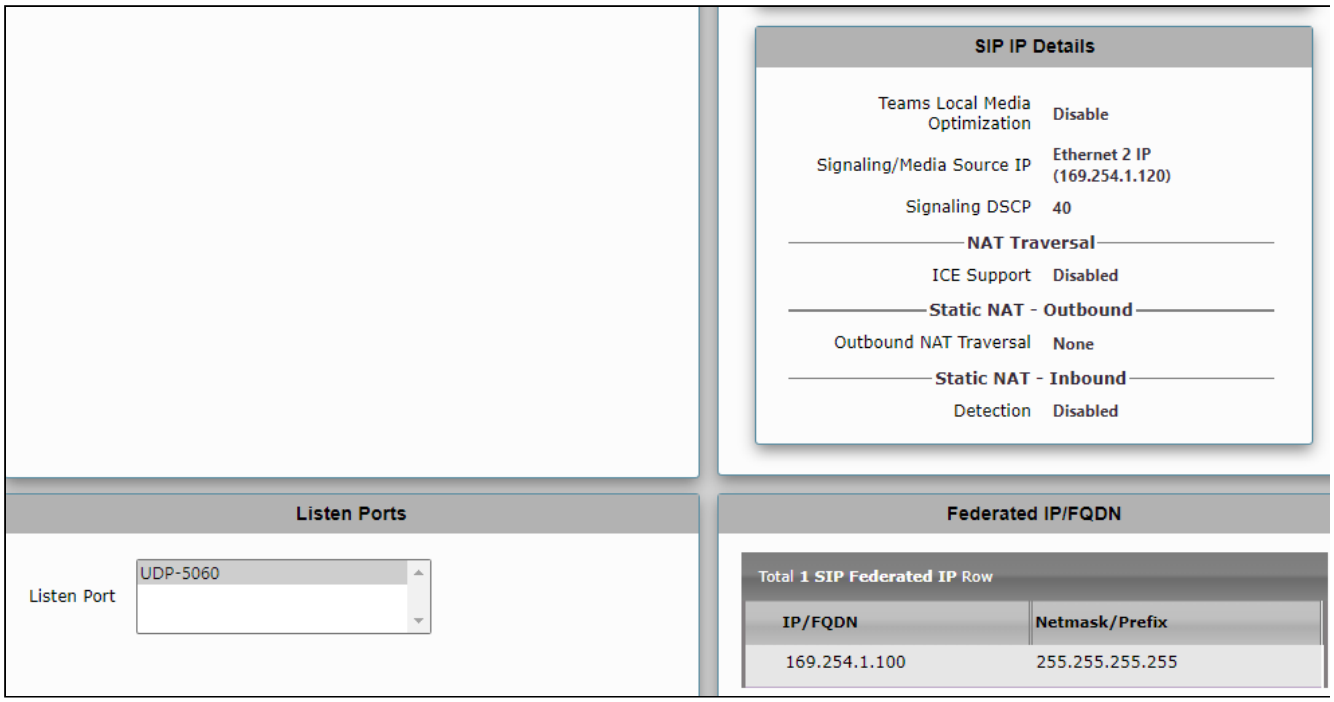
To/From IP PBX Signaling Group





To/From FXS Signaling Group





SIP Profiles

SIP Profiles control how the Edge 8000 device communicates with other SIP devices. SIP Profiles control important characteristics such as session timers, SIP header customization, SIP timers, MIME payloads, and option tags.

In this demonstration, two SIP Profiles are defined, one for each Signaling Group:

- To/From IP PBX Profile – serves the To/From IP PBX Signaling Group
- Default SIP Profile – serves the To/From FXS Signaling Group

To display SIP Profiles in the Edge 8000 webUI:

- click the **Settings** tab
- navigate to **SBC > SIP** > **SIP Profiles**

The following screenshots illustrate the SIP Profiles defined for this demonstration.

To/From IP PBX Profile

Description To/From IP PBX Profile

Session Timer

Session Timer	Enable
Minimum Acceptable Timer	600
Offered Session Timer	600
Session Timer Offset	5
Terminate On Refresh Failure	False

MIME Payloads

ELIN Identifier	LOC
PIDF-LO Passthrough	Enable
Unknown Subtype Passthrough	Disable

Header Customization

FQDN in From Header	Disable
Options Passthrugh	Access UA
FQDN in Contact Header	Disable
Send Assert Header	Trusted Only
SBC Edge Diagnostics Header	Enable
Trusted Interface	Enable
UA Header	Ribbon
Calling Info Source	RFC Standard
Diversion Header Selection	Last
Record Route Header	RFC 3261 Standard

Options Tags

100rel	Supported
Path	Not Present
Timer	Supported
Update	Supported

Timers

Transport Timeout Timer	5000
Maximum Retransmissions	RFC Standard
Redundancy Retry Timer	180000

RFC Timers

Timer T1	500
Timer T2	4000
Timer T4	5000
Timer D	32000
Timer B	32000 *ms*
Timer F	32000 *ms*
Timer H	32000 *ms (64*TimerT1)*
Timer J	4000

SDP Customization

Send Number of Audio Channels	True
Connection Info in Media Section	True
Origin Field Username	SBC
Session Name	VoipCall
Digit Transmission Preference	RFC 2833/Voice
SDP Handling Preference	Legacy Audio/Fax

Default SIP Profile

Description **Default SIP Profile**

Session Timer

Session Timer	**Disable**

MIME Payloads

ELIN Identifier	**LOC**
PIDF-LO Passthrough	**Enable**
Unknown Subtype Passthrough	**Disable**

Header Customization

FQDN in From Header	**Disable**
Options Passthrugh	**Access UA**
FQDN in Contact Header	**Disable**
Send Assert Header	**Trusted Only**
SBC Edge Diagnostics Header	**Enable**
Trusted Interface	**Enable**
UA Header	**Ribbon**
Calling Info Source	**RFC Standard**
Diversion Header Selection	**Last**
Record Route Header	**RFC 3261 Standard**

Options Tags

100rel	**Supported**
Path	**Not Present**
Update	**Supported**

Timers

Transport Timeout Timer	**5000**
Maximum Retransmissions	**RFC Standard**
Redundancy Retry Timer	**180000**

RFC Timers

Timer T1	**500**
Timer T2	**4000**
Timer T4	**5000**
Timer D	**32000**
Timer B	**32000** *ms*
Timer F	**32000** *ms*
Timer H	**32000** *ms (64*TimerT1)*
Timer J	**4000**

SDP Customization

Send Number of Audio Channels	**True**
Connection Info in Media Section	**True**
Origin Field Username	**SBC**
Session Name	**VoipCall**
Digit Transmission Preference	**RFC 2833/Voice**
SDP Handling Preference	**Legacy Audio/Fax**

Tone Tables

Tone Tables allow the Edge 8000 administrator to customize the tones a user hears when placing a call. You can modify the tone to match your local PSTN or PBX. The default Tone Table is configured for the values used in the United States for the following categories: Ringback, Dial, Busy, Congestion, Call Waiting, Disconnect, and Confirmation.

In this demonstration, each Signaling Group uses a unique Tone Table:

- United States Tone Table – serves the To/From IP PBX Signaling Group
- Default Tone Table – serves the To/From FXS Signaling Group

To display Tone Tables and associated profiles in the Edge 8000 webUI:

- click the **Settings** tab
- navigate to **SBC > Tone Tables**

The following screenshots illustrate the Tone Table and associated Tone Profiles defined for this demonstration.

United States Tone Table

United States

Total **2 Tone Profile** Rows

Tone Type	Frequency 1 (Hz)	Amplitude 1 (dBm)	Frequency 2 (Hz)	Amplitude 2 (dBm)
Ringback	440	-19	480	-19
Congestion	480	-24	620	-24

Default Tone Table

Default Tone Table

Total **2 Tone Profile** Rows

Tone Type	Frequency 1 (Hz)	Amplitude 1 (dBm)	Frequency 2 (Hz)	Amplitude 2 (dBm)
Ringback	440	-19	480	-19
Congestion	480	-24	620	-24

Ringback Tone Profile

Frequency

Tone Type	Ringback	
Frequency 1	440	* [100..3400] Hz
Amplitude 1	-19	* [-40..0] dBm
Configure Frequency 2	Yes	
Frequency 2	480	[10..3400] Hz
Amplitude 2	-19	[-40..0] dBm

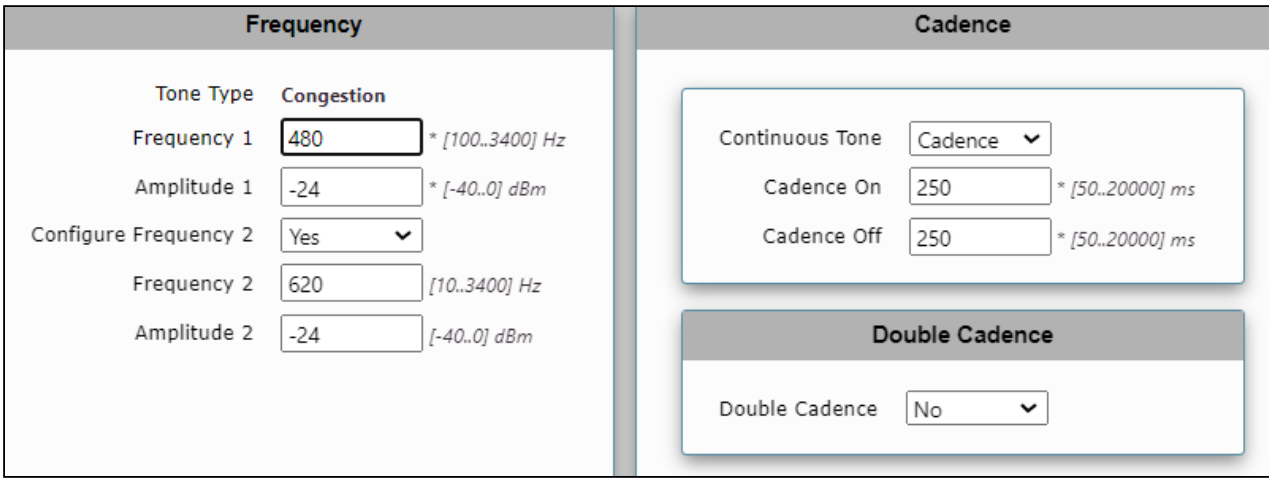
Cadence

Continuous Tone	Cadence	
Cadence On	2000	* [50..20000] ms
Cadence Off	4000	* [50..20000] ms

Double Cadence

Double Cadence	No

Congestion Tone Profile



Transformation Tables

Transformation Tables facilitate the conversion of names, numbers, and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number or into a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table.

In this demonstration, two Transformation Tables are defined:

- Transformation Table, IP PBX Numbers
  - supports the Call Routing Table, From IP PBX
  - matches the telephone number ranges of the IP phones
- Transformation Table, FXS Numbers
  - supports the Call Routing Table, From FXS
  - matches the telephone number ranges of the analog phones

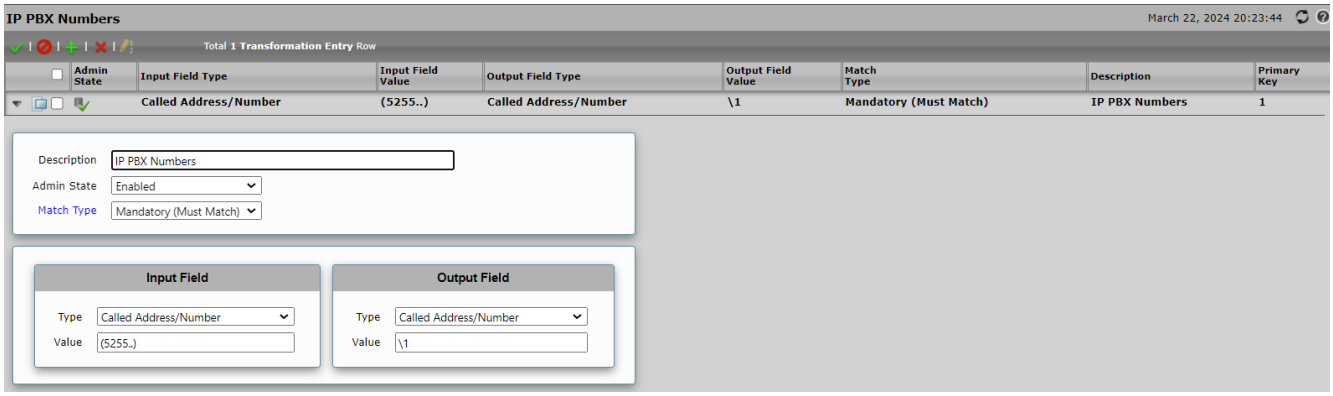
To display Transformation Tables in the Edge 8000 webUI:

- click the **Settings** tab
- navigate to **SBC > Call Routing** > **Transformation**

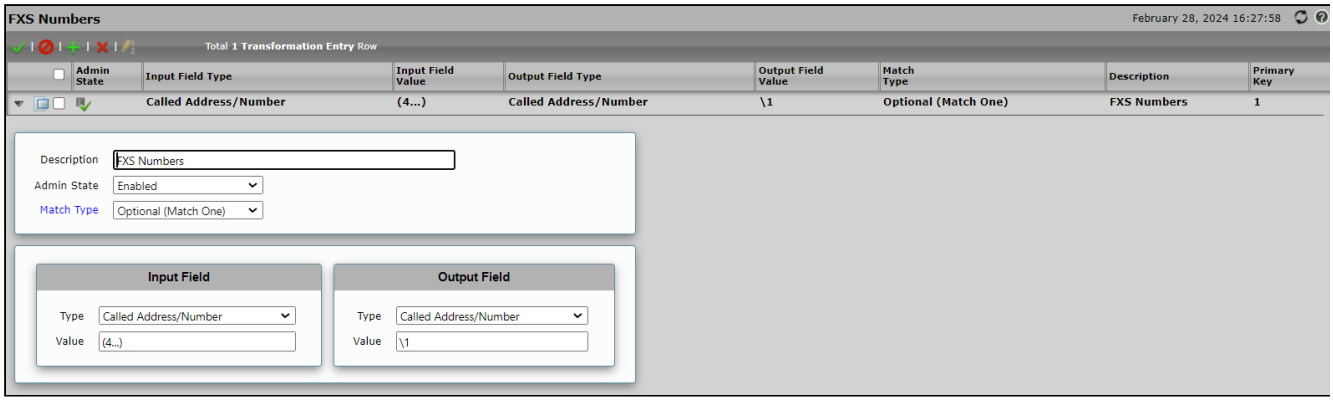
The following screenshots illustrate the Transformation Tables defined for this demonstration.

> **Note**
>
> To understand Input Field and Output Field values, refer to SBC Edge Regular Expressions for Number Matching and Transformation.

Transformation Table – IP PBX Numbers



Transformation Table – FXS Numbers



Call Routing Tables

Call Routing Tables allow calls to be carried between signaling groups, thus allowing calls to be carried between ports and between protocols. Call Routing Tables define routes, which allow for flexible configuration of which calls are carried and how they are translated. These tables are one of the central connection points of the system, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists, and the Signaling Groups.

Each Signaling Group has one Call Routing Table. In this demonstration, two Signaling Groups, each with its own Call Routing Table, are defined:

Signaling Group and Matching Call Routing Table

Signaling Group	Call Routing Table
To/From IP PBX	From IP PBX
To/From FSX	From FXS

The following fields of the Call Routing Table must be modified as a minimum:

- **Number/Name Transformation Table**
- **Destination Signaling Groups**

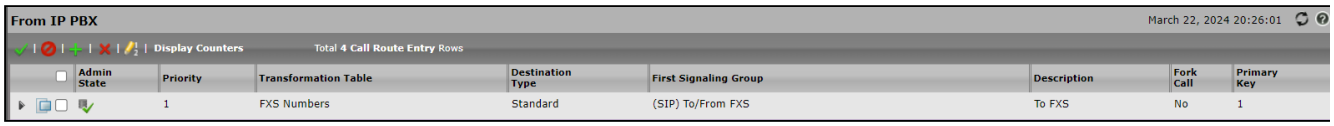
Additional fields may be modified per end-user requirements.

To display Call Routing Tables in the Edge 8000 webUI:

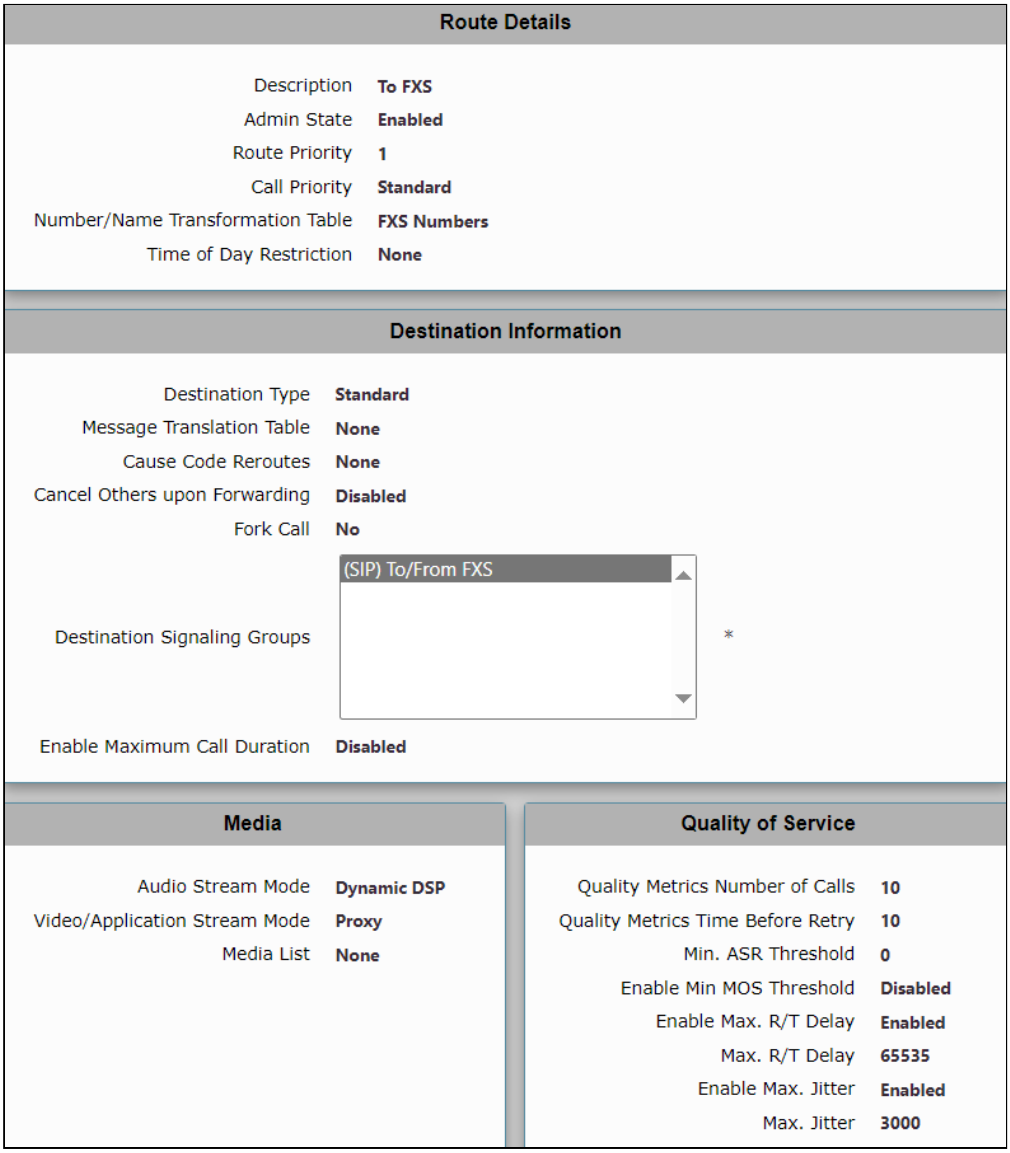
- click the **Settings** tab
- navigate to **SBC > Call Routing > Call Routing Table**

The following screenshots show the two Call Routing Tables and the entry in each table. Each entry specifies a different Transformation Table.

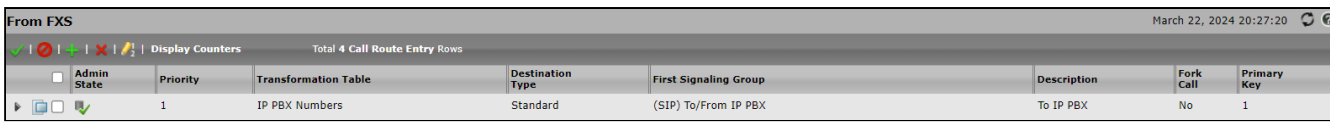
Call Routing Table – From IP PBX



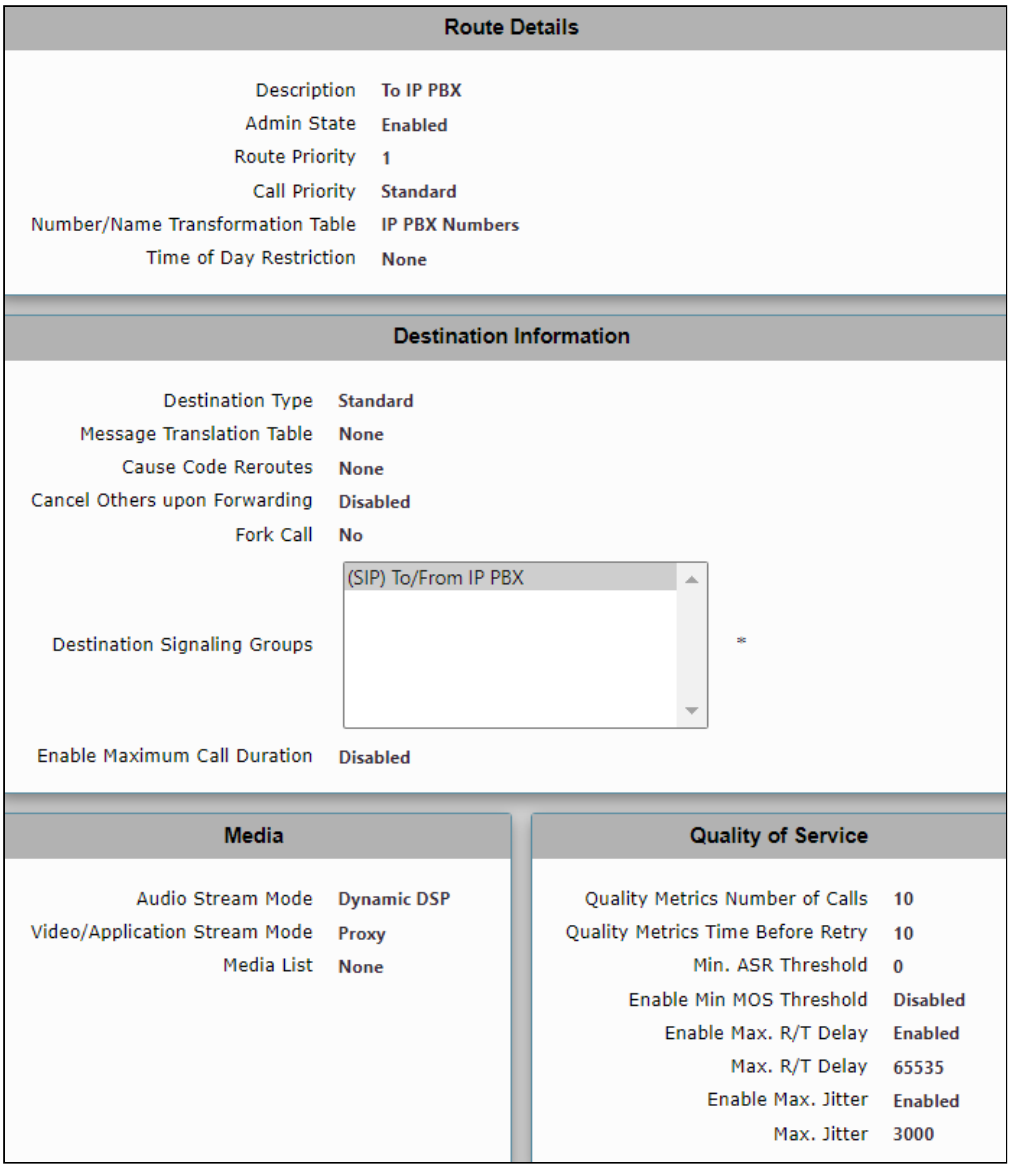
Entry – To FXS



Call Routing Table – From FXS



Entry – To IP PBX



SIP Server Tables

SIP Server tables contain the IP address or FQDN of one or more SIP servers where INVITE messages can be sent to egress calls on a Signaling Group. The entries in the tables provide information about the IP Addresses, ports, and protocols used to communicate with the servers. The entries also contain links to counters that are useful for troubleshooting.

In this demonstration, one SIP Server Table, IP PBX, serves the To/From IP PBX Signaling Group.

The following fields of the SIP Server Table must be modified as a minimum:

- **Host FQDN/IP**
- **Port**
- **Protocol**

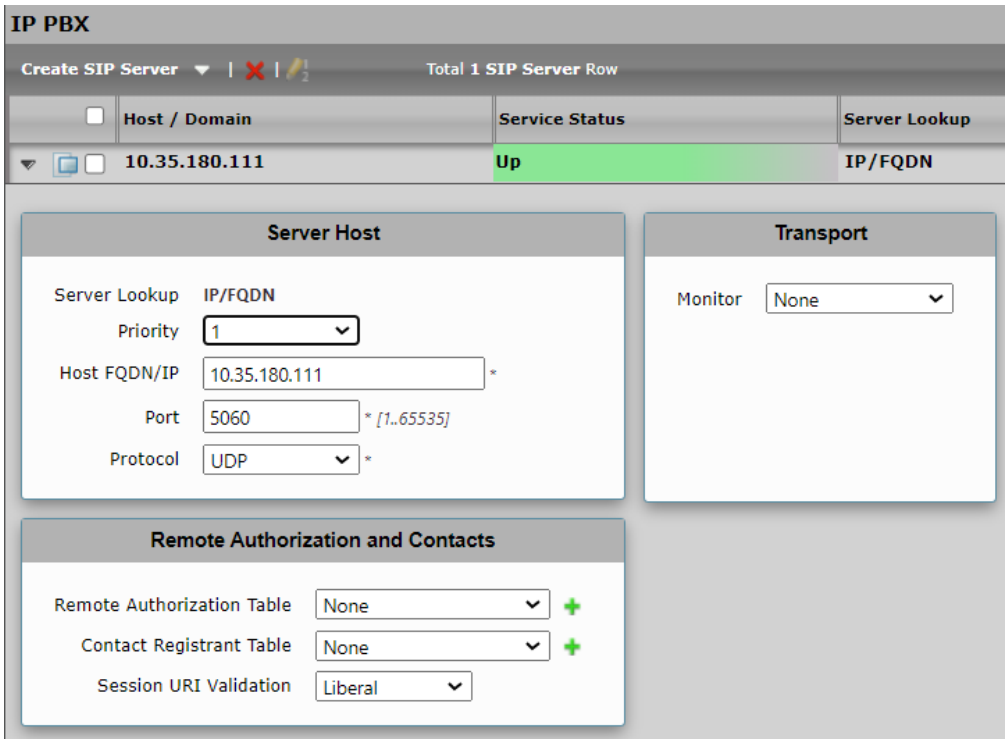
Additional fields may be modified per end-user requirements.

To display SIP Server Tables in the Edge 8000 webUI:

- click the **Settings** tab
- navigate to **SBC > SIP > SIP Server Tables**

The following screenshot shows the SIP Server Table, IP PBX, created for this demonstration.

SIP Server Table – IP PBX



Local Registrar

SIP provides a registration function that allows IP phone users to upload their current location for use by proxy servers. Registration creates a binding in a location service for a particular domain that associate an address-of-record URI with one or more contact addresses.

Registration entails sending a REGISTER request to a special type of UAS (User-Agent Server) known as a registrar. A registrar acts as the front end to the location service for a domain, reading and writing mappings based on the contents of REGISTER requests. This location service is then typically consulted by a proxy server that is responsible for routing requests for that domain.

In this demonstration, one SIP Local Registrar Table is defined.

The following field of a Local Registrar Table must be defined as a minimum:

- **Maximum Number of Users**

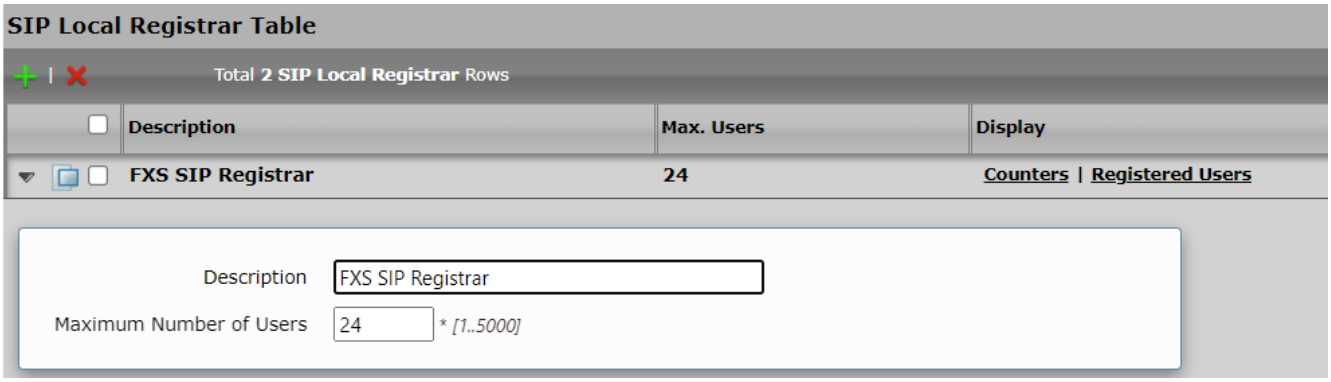
Additional fields may be modified per end-user requirements.

To display Local Registrars in the Edge 8000 webUI:

- click the **Settings** tab
- navigate to **SBC > SIP > Local Registrars**

The following screenshot shows the FXS SIP Registrar local registrar associated with the To/From FXS Signaling Group in this demonstration.

FXS SIP Registrar



Media Profiles

Media Profiles allow you to specify individual voice and fax compression codecs and their associated settings for inclusion in a Media List. Different codecs provide varying levels of compression, allowing a tradeoff between reducing bandwidth at the expense of reducing voice quality.

The following field of a Media Profile must be modified as a minimum:

- **Codec**

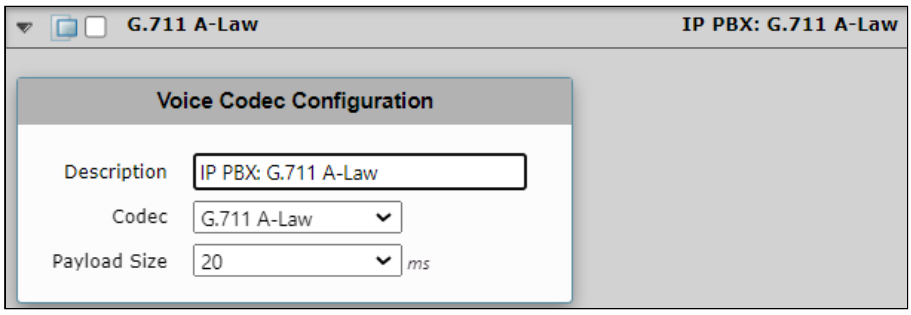
Additional fields may be modified per end-user requirements.

To display Media Profiles in the Edge 8000 webUI:

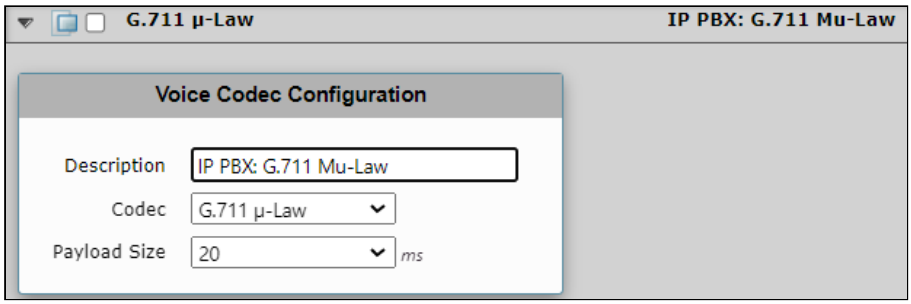
- click the **Settings** tab
- navigate to **SBC > Media > Media Profiles**

The following screenshots show the Media Profiles created for this demonstration.

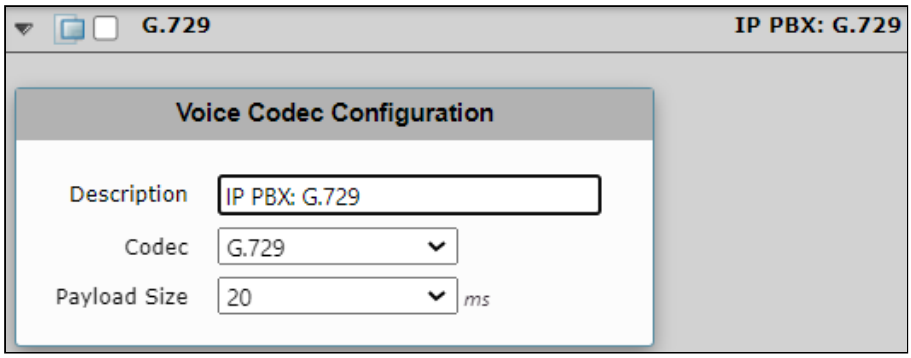
IP PBX: G.711 A-Law



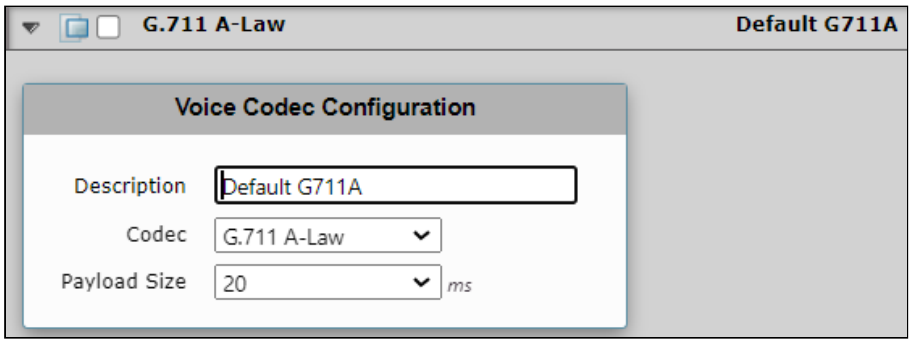
IP PBX: G.711 Mu-Law



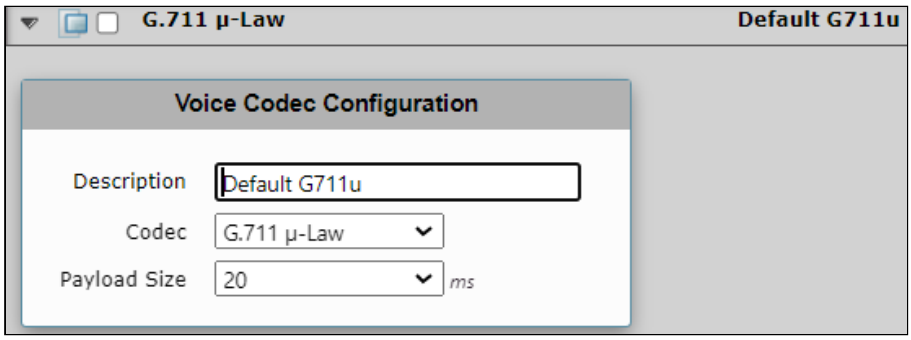
IP PBX: G.729



Default G.711 A-Law



Default G.711 Mu-Law



Media Lists

A Media List contains a list of media profiles you order to give preference to more desirable codecs above less desirable ones. Profile order determines the order in which codecs are specified in SIP message(s) sent to a peer.

The following field of a Media List must be modified as a minimum:

- **Media Profiles List**

Additional fields may be modified per end-user requirements.

To display Media Lists in the Edge 8000 webUI:

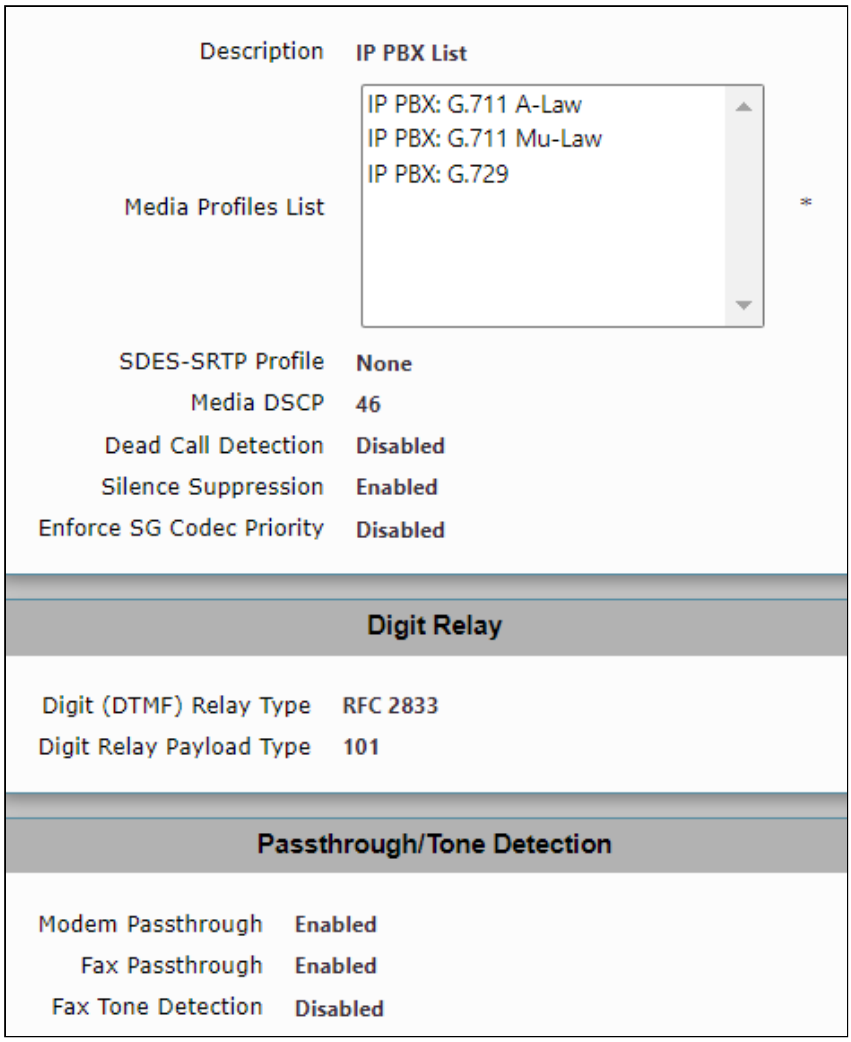
- click the **Settings** tab
- navigate to **SBC > Media > Media List**

The following screenshots show the two Media Lists created for this demonstration:

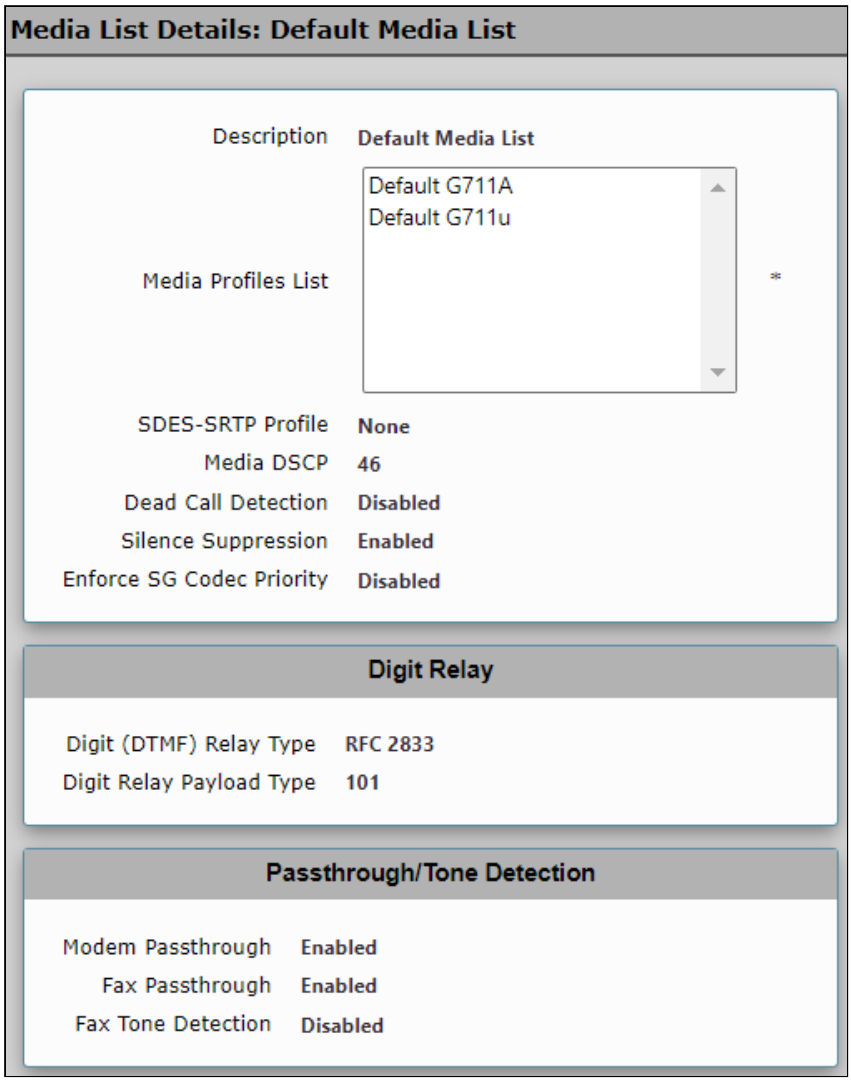
- IP PBX List associated with the To/From IP PBX Signaling Group

- Default Media List associated with the To/From FXS Signaling Group

IP PBX List



Default Media List



FXS Port Configuration

Before an FXS port can be used for calls, it must be enabled and configured through the Ribbon Edge 8000 webUI. To configure FXS ports, you must configure global and port-level SIP User Agent (SIP UA) settings.

Global SIP UA Settings

The following parameters must be modified as a minimum for the SIP UA Global Configuration:

Minimum Global Configuration Settings for the SIP User Agent

Parameter	Setting
Enable-SIPUA	This flag activates the FXS ports. This value is set to True for this demonstration.

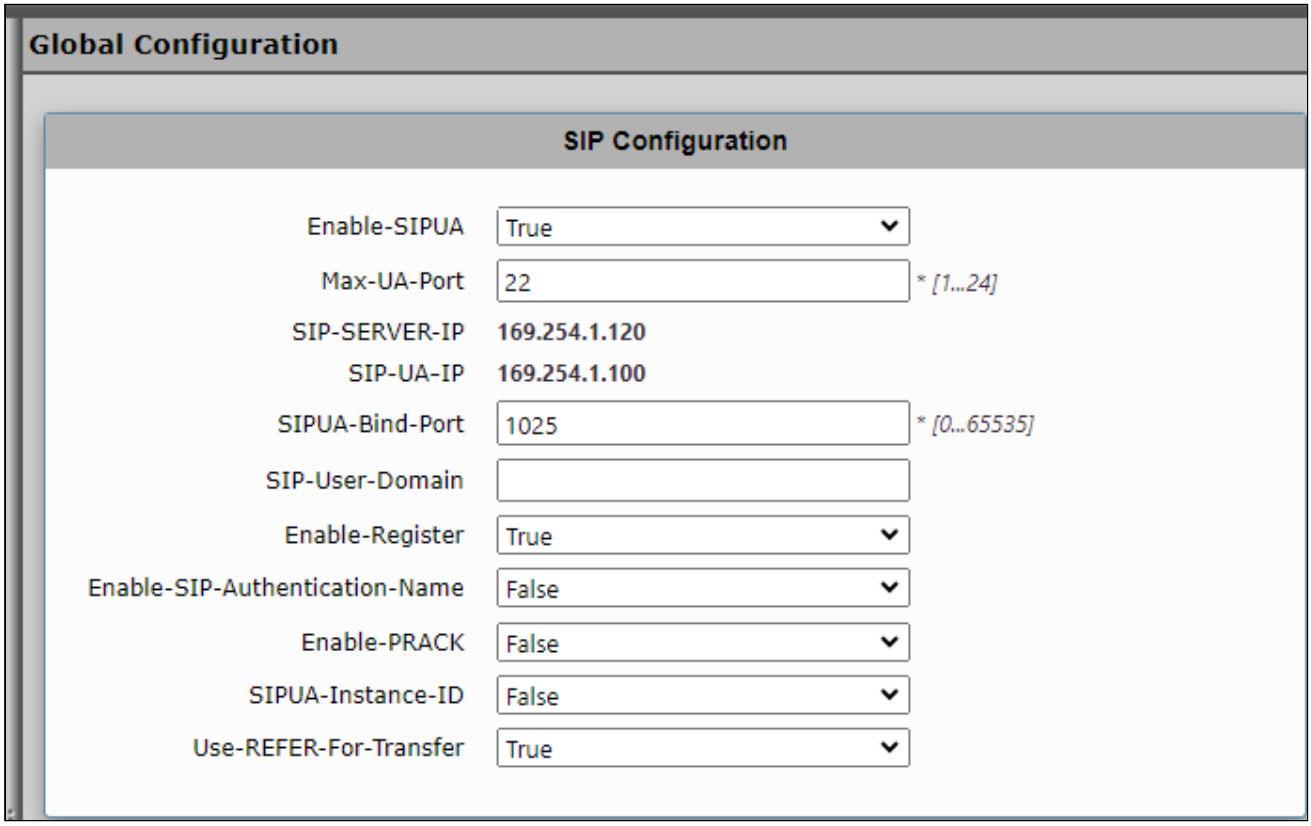
Parameter	Setting
SIP-SERVER-IP	This address is allocated to the internal packet port on the SWe Edge for internal SIP communication with PRI/FXS/FXO. It is set to the IP address of the SBC SWe Edge's Ethernet 2 interface. This IP address is factory set to 169.254.1.120 and is not configurable.
SIP-UA-IP	This is the IP address allocated to FXS ports for SIP signaling to the SWe Edge. This IP address is factory set to 169.254.1.100 and is not configurable.
SIPUA-Bind-Port	This is set to 1025 for this demonstration.
Enable-Register	This is set to True for this demonstration, to allow the FXS ports to register to the SIP Server IP.

To configure the SIP UA global settings in the Edge 8000 WebUI:

- click the **Settings** tab
- navigate to **Gateway > SIP-User-Agent** > **UA-Setting** > **Global-Configuration**

The following screenshots show the settings used for this demonstration.

SIP User Agent – Global Configuration

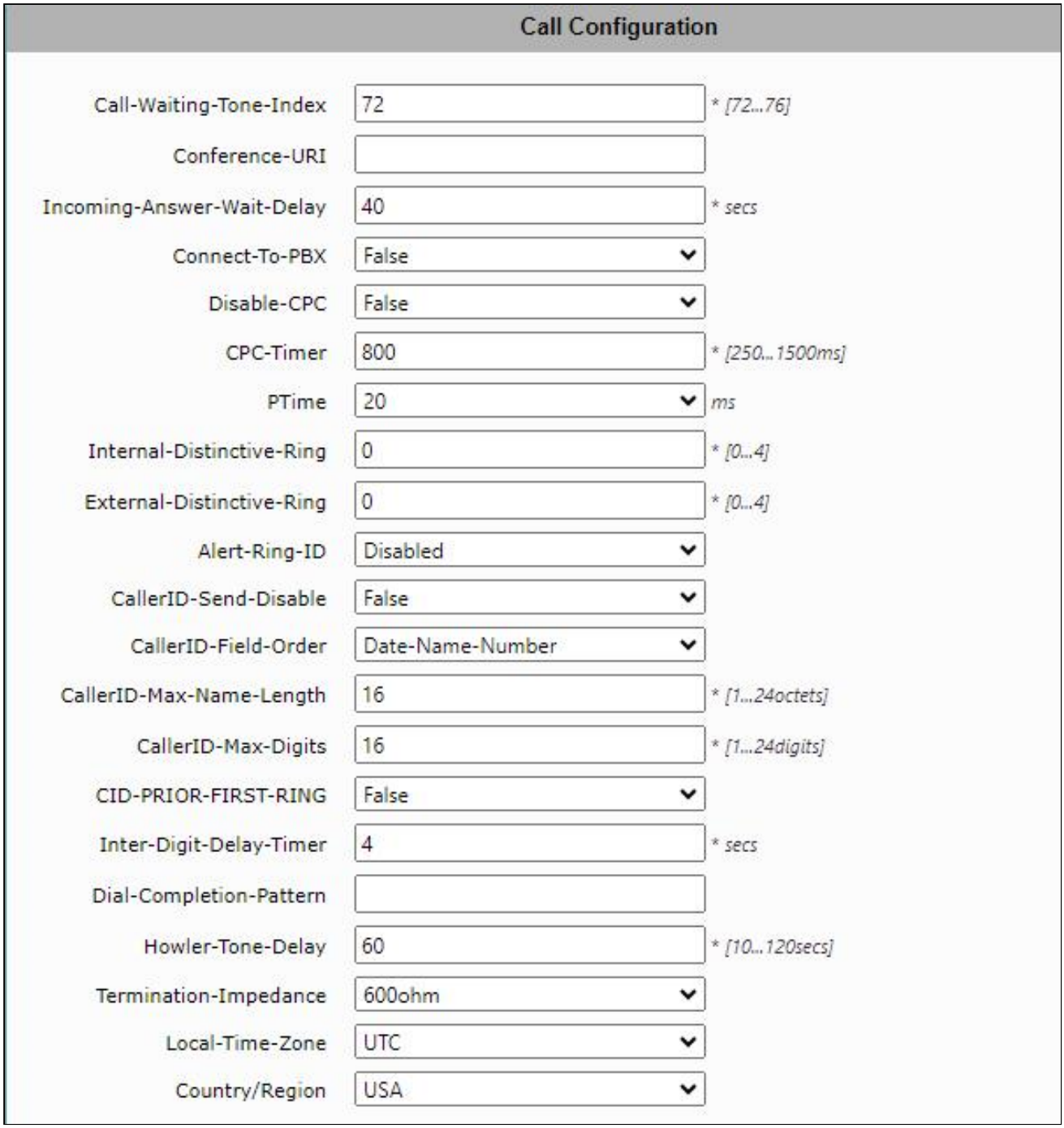


Media

RTP-Min-Port	22000	* [20000...65535]
RTP-Max-Port	41600	* [RTP-Min-Port+1...65535]
Codec-Preference	G711-uLaw	
Use-Preferred-Codec-Only	True	
Enable-Access-Code	False	
VAD-Enabled	Enabled	
Jitter-Buffer-Value	60	* [10..90ms]

Tone Configuration

Ignore-FAX-Over-Audio	False	
Disable-T38-Reject	False	
Enable-ADTRAN-T38-INTEROP	True	
Enable-T38-Offer-Outbound	False	
Disable-RFC2833	False	
Enable-RFC2833-IB	False	
RFC2833-Event-Payload	101	* [100...101]



Port-Level SIP UA Settings

The following parameters must be modified as a minimum for the SIP UA Port-Level Configuration:

Minimum Port-Level Configuration Settings for the SIP User Agent

Parameter	Setting
SIP Display Name	This is a string containing a name for the identified user.
SIP User Name	This is usually the phone number or extension.

To configure the SIP UA port-level settings in the Edge 8000 WebUI:

- click the **Settings** tab
- navigate to **Gateway > SIP-User-Agent** > **UA-Setting** > **Port-Level-Configuration**

> **Note**
>
> In this demonstration, an analog phone is connected to the first FXS port, which is port [0].

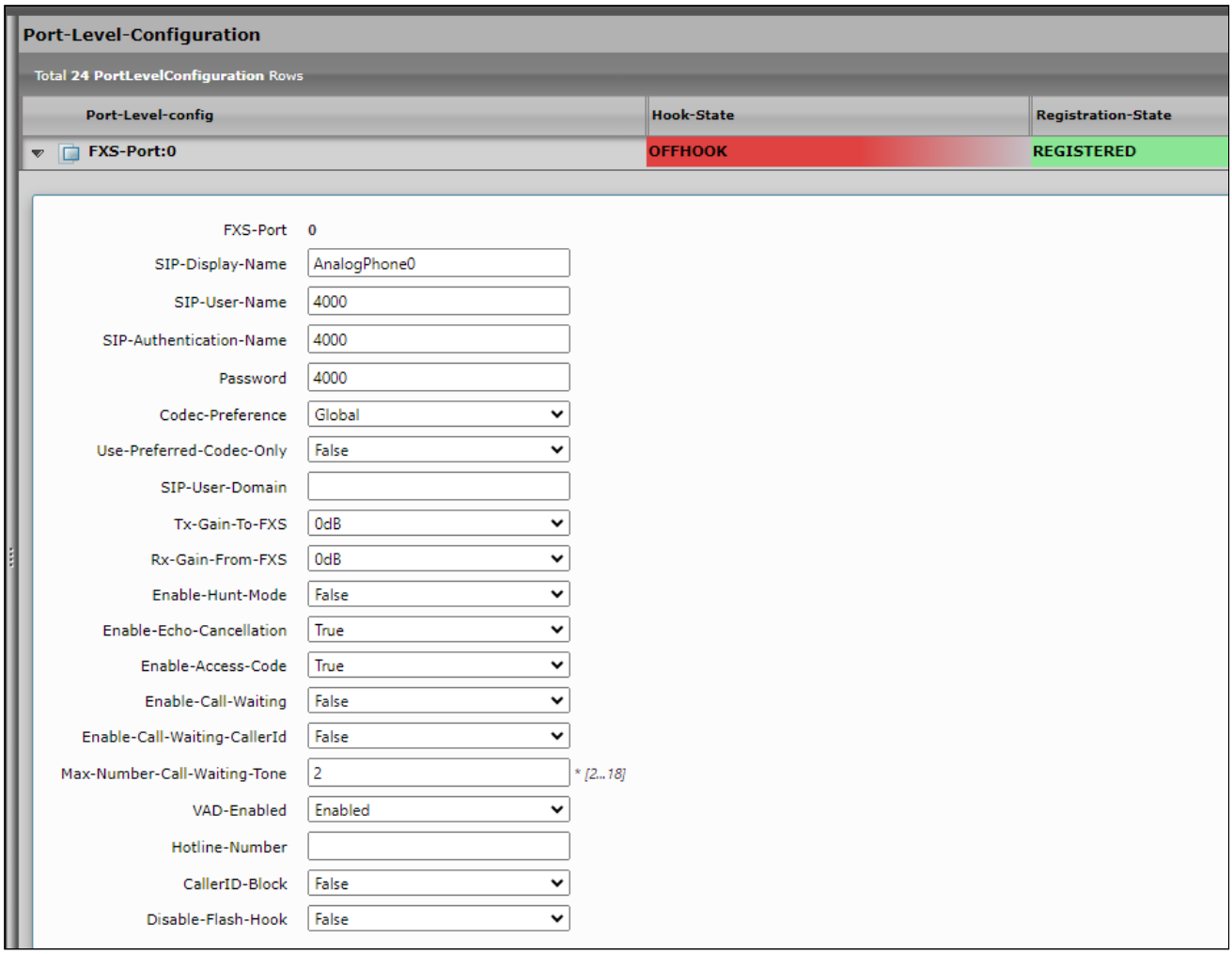
The following screenshots show the settings used for this demonstration.

SIP User Agent – Port-Level Configuration

Port-Level-Configuration

Total **24 PortLevelConfiguration** Rows

Port-Level-config	Hook-State
FXS-Port:0	OFFHOOK
FXS-Port:1	OFFHOOK
FXS-Port:2	OFFHOOK
FXS-Port:3	OFFHOOK
FXS-Port:4	OFFHOOK
FXS-Port:5	OFFHOOK
FXS-Port:6	OFFHOOK
FXS-Port:7	OFFHOOK
FXS-Port:8	OFFHOOK
FXS-Port:9	OFFHOOK
FXS-Port:10	OFFHOOK
FXS-Port:11	OFFHOOK
FXS-Port:12	OFFHOOK
FXS-Port:13	OFFHOOK
FXS-Port:14	OFFHOOK
FXS-Port:15	OFFHOOK
FXS-Port:16	OFFHOOK
FXS-Port:17	OFFHOOK
FXS-Port:18	OFFHOOK
FXS-Port:19	OFFHOOK
FXS-Port:20	OFFHOOK
FXS-Port:21	OFFHOOK
FXS-Port:22	OFFHOOK
FXS-Port:23	OFFHOOK



SIP Trunk Configuration for IP PBX Deployment

The following example demonstrates a complete SIP Trunk to IP PBX deployment using an Edge 8300 model and the Edge 8000 Series 24.0 software release. Screenshots and specific values are included for all the major configuration areas of the deployment:

- Setup Wizard
- Licensing
- Network Interface provisioning
- Static Route provisioning
- Easy Configuration Wizard

For the entire provisioning process, including physically Installing the Edge 8000 Hardware, refer to Workflow for Initial Setup and Configuring SIP Trunk to SIP IP PBX.

While the goal of this example is not to provide a detailed configuration that meets the needs of every deployment scenario, it does provide a starting point for building your own customized configuration for a SIP Trunk to IP PBX deployment.

Attention

The IP addresses shown in the examples may conflict with an existing or planned production network. Consult with your network administrator for the specific IP addresses required for your deployment.

Contents

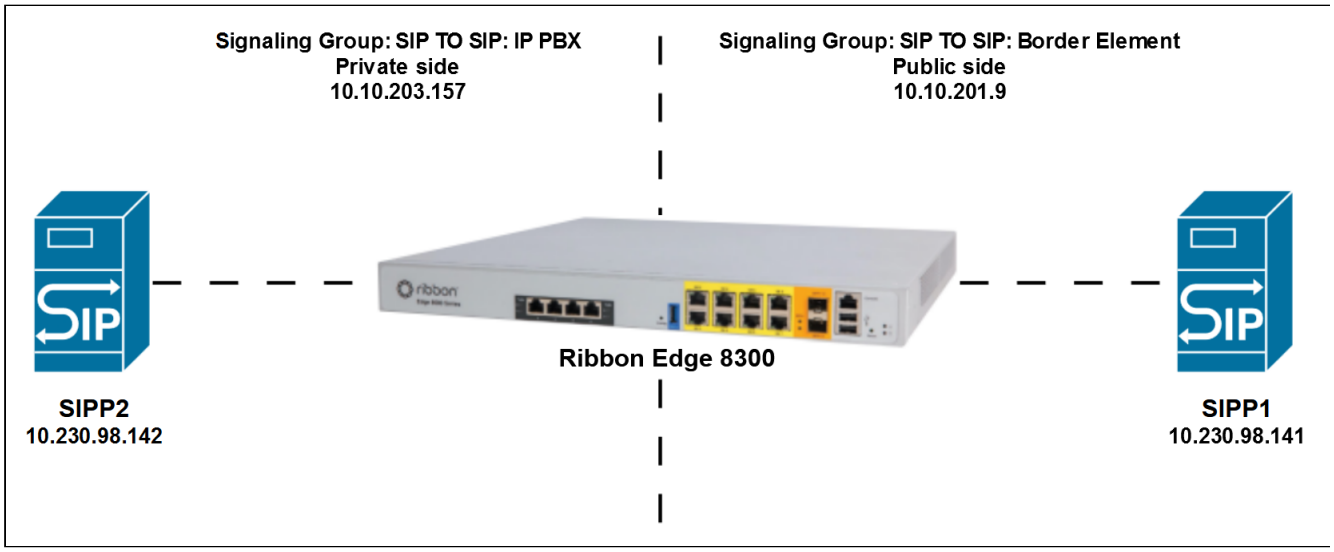
Network and Call Flow Diagrams

In this demonstration, an Edge 8300 is configured to support two signaling groups:

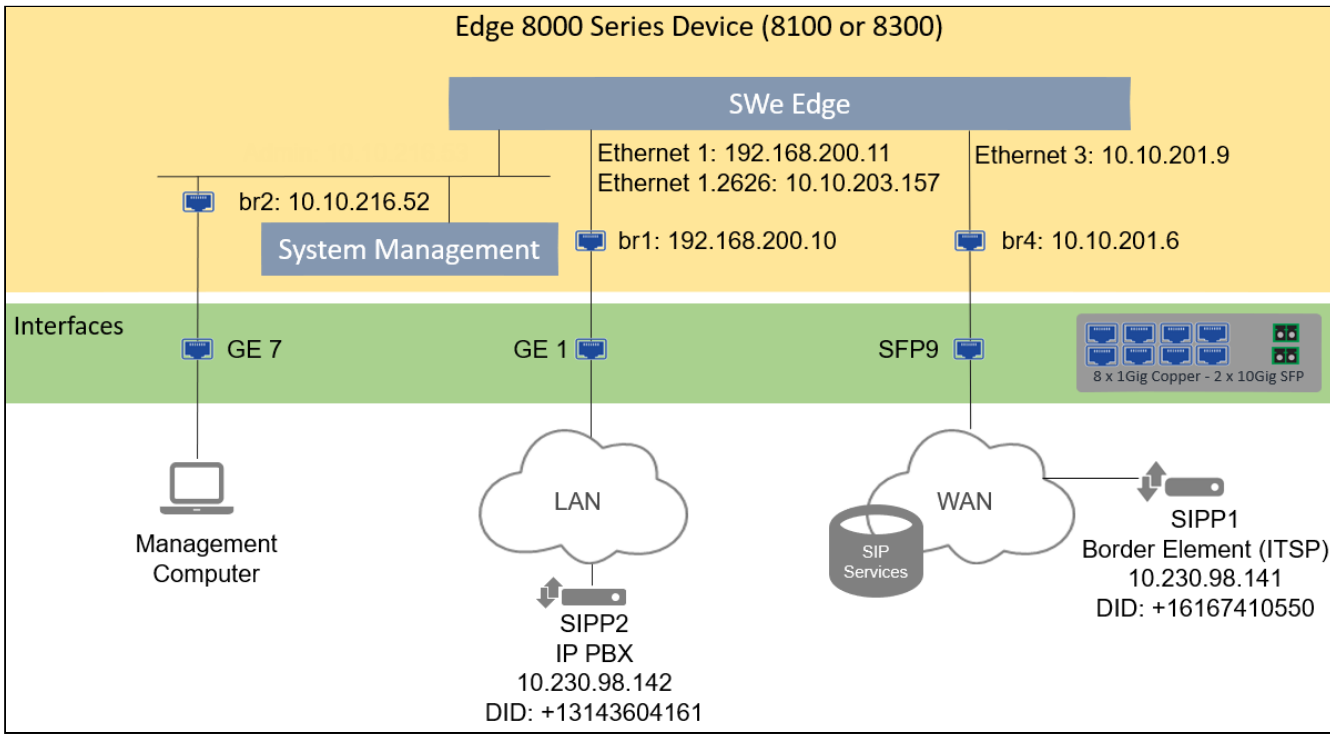
- On the private or LAN side, an IP PBX with VLAN logical sub-interfaces
- On the public or WAN side, a SIP trunk to an Internet Telephony Service Provider (ITSP) Border Element

The following diagrams depict the deployment topology, network interfaces, and call flows for this deployment demonstration.

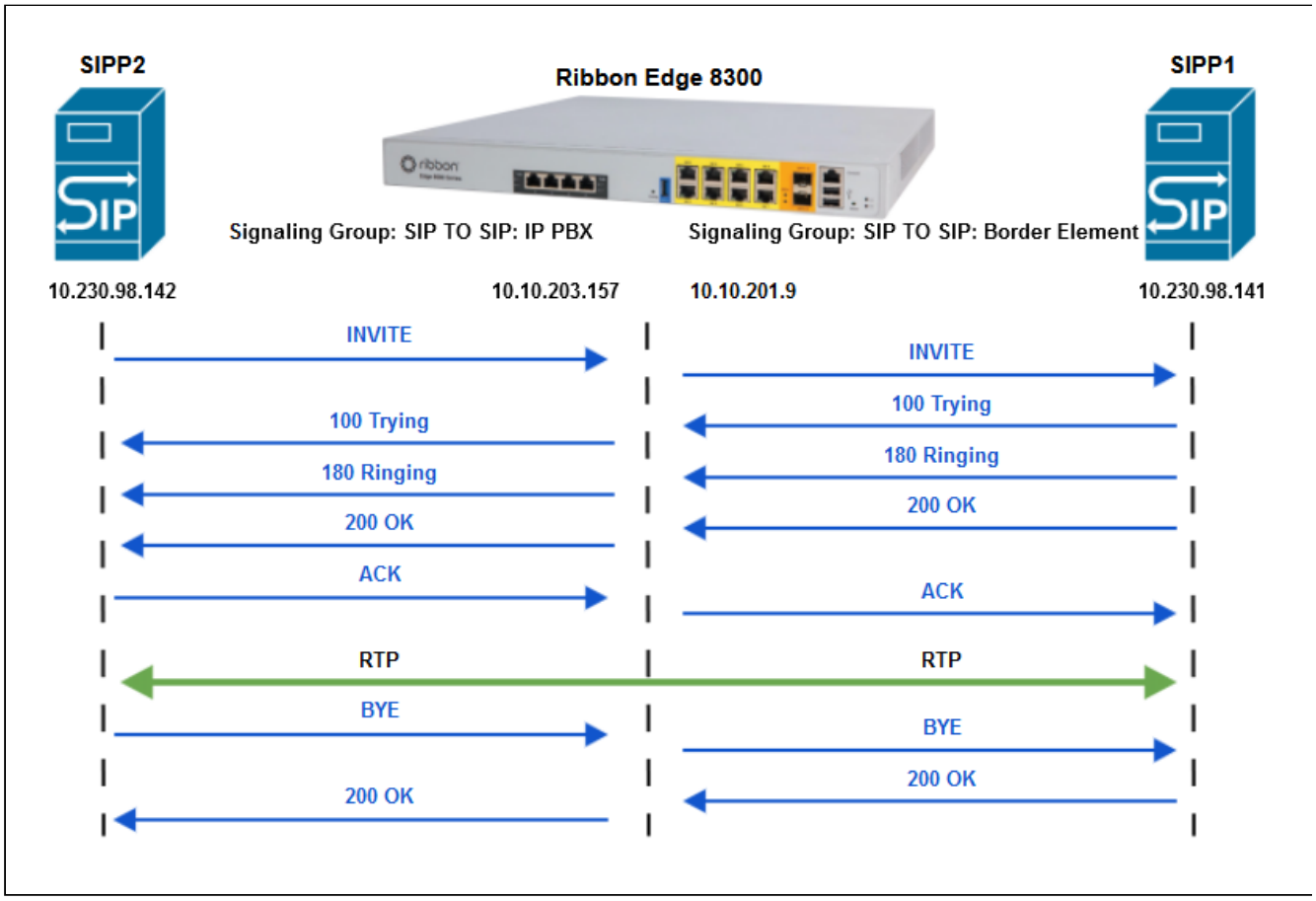
Deployment Topology



Network Interfaces



Signaling and Media Call Flows



Setup Wizard Values

After physically installing the device, the deployment team uses the Edge 8000 Setup Wizard to establish basic platform settings.

The following tables show the values entered in Setup Wizard for this SIP Trunk to SIP IP PBX demonstration. Consult your network design and deployment teams for the specific values appropriate for your network.

System Configuration

Hostname	Time Zone	Time Server	Ramp Server	PRI Type	6WIND fastpath cores
e8000	America/Mexico_City	10.10.199.228 Note: The Time Server allows the device to stay in sync with other devices in the network. This is helpful for troubleshooting logs, examining CDRs, etc.	10.10.216.62	T1Net (default)	4 (default)

Bridge Settings (BR1, 2, 4)

Interface	Interface Name	IPv4 Address	Netmask	Members	DHCP server (default = enabled)	Enable DHCP client (default = enabled)	Setup Wizard Note
BR1 VNF Private	br1	192.168.200.10	24 (default)	ge1	[ ] disabled (press the space bar to toggle)	n/a	
BR2 VNF Management	br2	10.10.216.52	26	ge7 (default)	[ ] disabled (press the space bar to toggle)	n/a	
BR4 VNF Public	br4	10.10.201.6	26	sfp9	n/a	[ ] disabled (press the space bar to toggle)	DHCP Client requires manual configuration of the gateway and DNS settings.

Gigabit Ethernet Settings (GE1-8)

Interface	Interface Name	IPv4 Address	Netmask Length		Setup Wizard Note
GE1	ge1	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE2	ge2	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE3	ge3	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE4	ge4	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.

Interface	Interface Name	IPv4 Address	Netmask Length		Setup Wizard Note
GE5	ge5	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE6	ge6	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE7	ge7	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.
GE8	ge8	0.0.0.0 (default)	0 (default)		If the interface is a member of a bridge interface, do not set these values.

Small Form-factor Pluggable (SFP9-10)

Interface	Interface Name	IPv4 Address	Netmask Length	Enable DHCP Client (default = disabled)		Setup Wizard Notes
SFP9	sfp9	0.0.0.0 (default)	0 (default)	[ ] disabled		If the interface is a member of a bridge interface, do not set these values. DHCP Client requires manual configuration of the gateway and DNS settings.
SFP10	sfp10	0.0.0.0 (default)	0 (default)	[ ] disabled		If the interface is a member of a bridge interface, do not set these values. DHCP Client requires manual configuration of the gateway and DNS settings.

Default Gateway

IPv4 Address	Setup Wizard Note
10.10.216.1	MUST be an IPv4 address within a subnet on an interface. Note: This is the external gateway that the Edge 8000 device routes to in order to reach outside of itself, beyond its own subnet. It's how the gateway can respond when you ping it. Without this, the Edge 8000 device doesn't know where to send its responses.

SWe Edge Settings

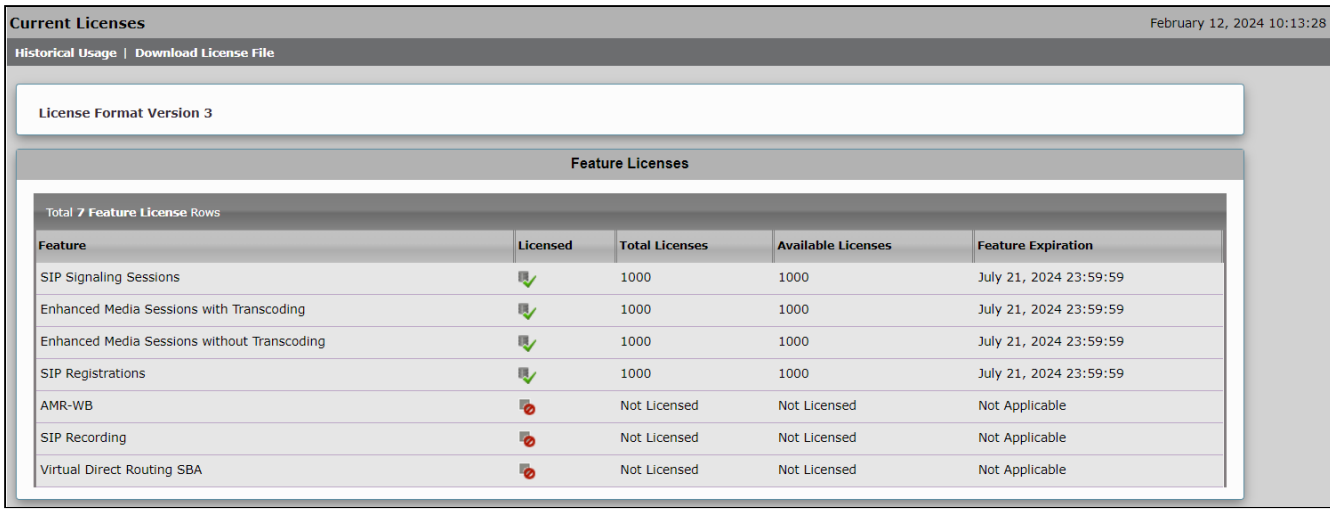
CPUs (1 2 4)	Memory (MBs)	Extra Interface 1	Extra Interface 2	Setup Wizard Note
2 (default)	2048 (default)	br4	_____ _____	The Extra Interface values are any of the physical port names, for example, ge1, sfp9 or the VNF Public bridge interface name, br4.

SWe Edge License Features

To view the SWe Edge license features, log in to the SBC SWe Edge WebUI as user *admin*, click the **Settings** tab, and navigate to **Licensing > Current Licenses**.

The following screenshot illustrates the SWe Edge license features used in this demonstration.

SWe Edge License Features



Network Interface Values

Network Interfaces define the way the SBC SWe Edge operates within the Edge 8000 to communicate with the external network.

The Edge 8000 supports system-created logical interfaces known as **Administrative IP**, **Ethernet 1 IP**, **Ethernet 2 IP**, and **Ethernet 3 IP** for the SWe Edge function. In addition, the Edge 8000 supports user-created VLAN logical sub-interfaces.

In this demonstration,

- The Admin IP is set as the Mgmt Host IP in the Swe-Edge Settings of the Setup Wizard
- The following IP addresses are not set during the Setup Wizard and must be entered manually:
  - the Ethernet 1 IP address, which provides a connection to the LAN IP PBX
  - the Ethernet 1.2626 IP address, which supports a connection to a VLAN logical sub-interface to the LAN IP PBX
  - the Ethernet 3 IP address, which provides a connection to the WAN Border Element (ITSP)
- The Ethernet 2 IP interface is not used

For this demonstration, the following Network Interface values have been assigned:

Network Interface Assignments

Interface Name	IP Assign Method	Primary Address	Primary Netmask	Media Next Hop IP
Admin IP	Static	10.10.216.53	255.255.255.192	
Ethernet 1 IP	Static	192.168.200.11	255.255.255.0	192.168.200.1
Ethernet 1.2626 IP	Static	10.10.203.157	255.255.255.128	10.10.203.129
Ethernet 3 IP	Static	10.10.201.9	255.255.255.192	10.10.201.1

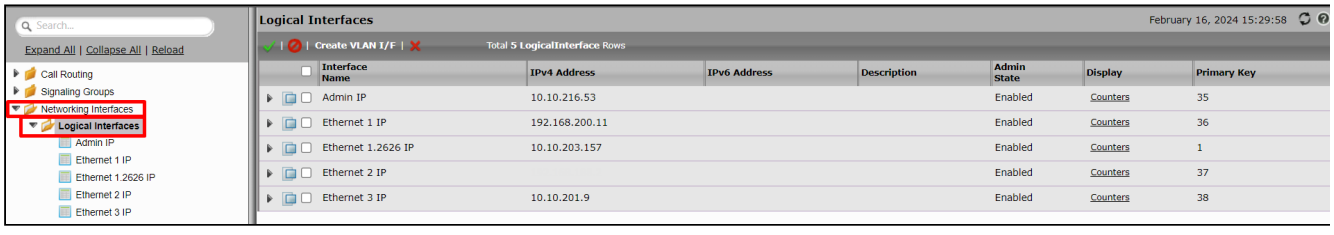
> **Note**
>
> To create a VLAN I/F for a Logical Interface, navigate to **Networking Interfaces > Logical Interfaces > Create VLAN I/F**.

To display Network Interfaces in the SWe Edge WebUI:

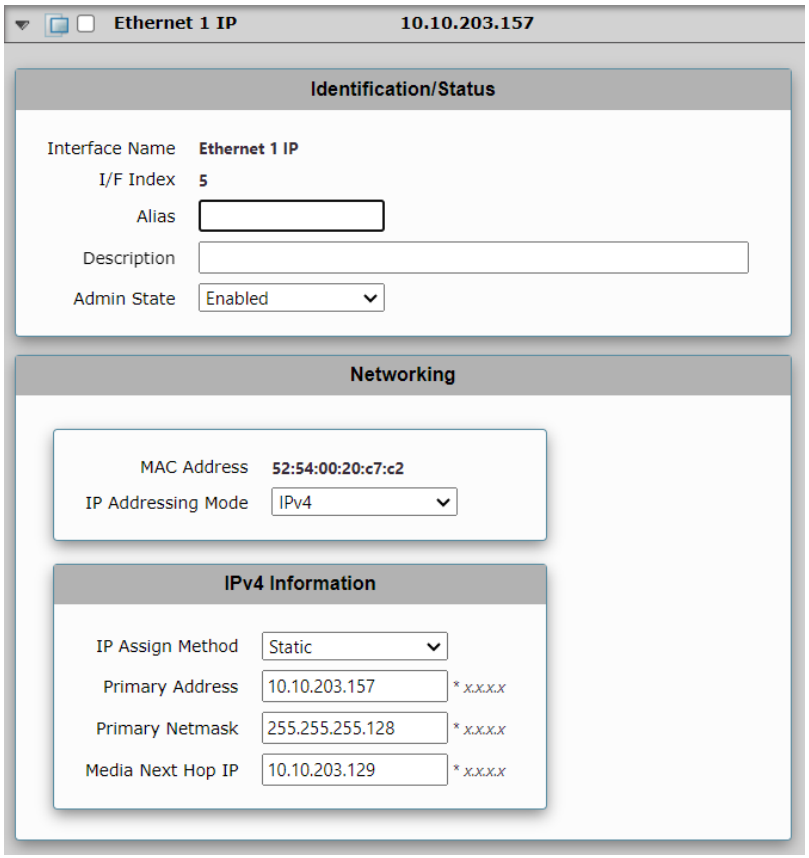
- click the **Settings** tab
- navigate to **Networking Interfaces > Logical Interfaces**

The following screenshots illustrate the Network Interfaces defined for this demonstration.

Network Interfaces



Example of a Network Interface: Ethernet 1 IP



Static Route Values

Static routes enable communication with remote networks. In a production environment, static routes are mainly configured to route traffic from one network to another network that can only be accessed through one point or one interface (single path access or default route).

- For smaller networks with just one or two routes, configuring static routing is preferable. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- For networks that have a LAN-side gateway on Voice VLAN or Multi-Switch Edge Devices (MSEs) with voice VLAN towards the SBC Edge, static routing configurations are not required.

> **Note**
>
> This demonstration does not have a LAN-side gateway, nor does it have MSEs.

Two Static Routes are defined for this demonstration:

- The first Static Route gives access to the SWe Edge WebUI on a management computer through a VPN subnet.
- The second Static Route gives access to SIPP servers on the WAN side of the Edge 8000 device.

Static Route fields include:

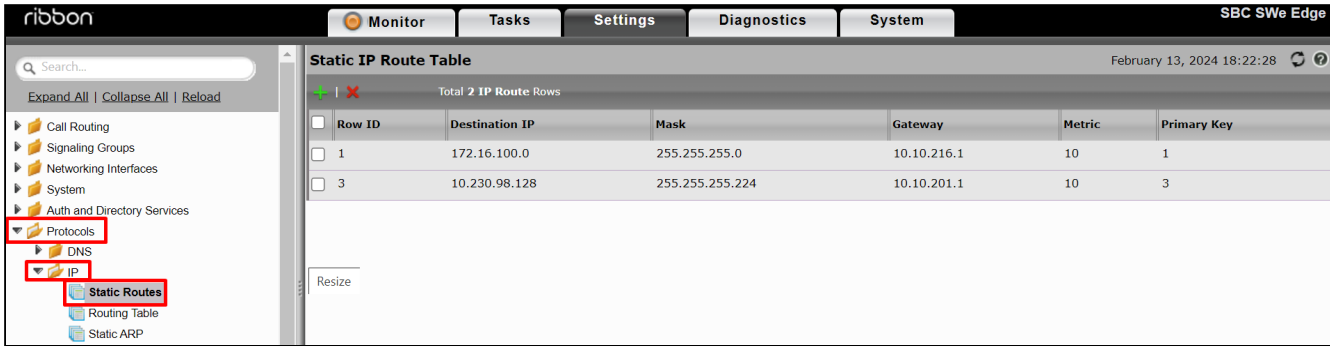
- **Destination IP** – Specifies the destination IP address.
- **Mask** – Specifies the network mask of the destination host or subnet. (If the 'Destination IP Address' field and 'Mask' field are both 0.0.0.0, the static route is called the 'default static route'.)
- **Gateway** – Specifies the IP address of the next-hop router to use for this static route.

To display Static Routes in the SWe Edge WebUI:

- click the **Settings** tab
- navigate to **Protocols** > **IP** > **Static Routes**

The following screenshot illustrates the Static Routes defined for this demonstration.

Static Routes



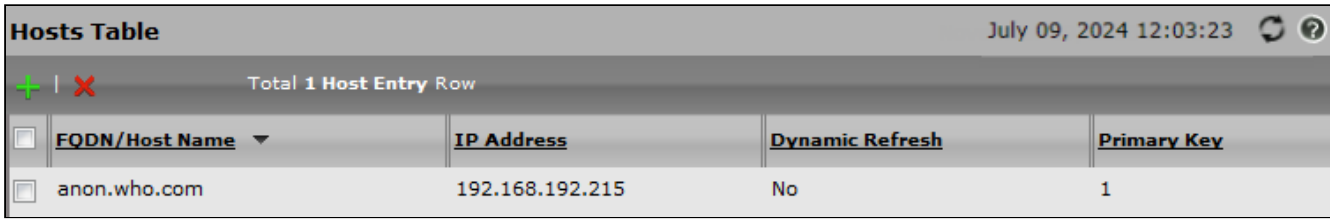
DNS Settings

DNS settings allow the Edge 8000 device to get an actual IP address when it needs to resolve a domain name. Ask your network system administrator for the IP address to use.

To display DNS settings in the Edge 8000 webUI:

- click the **Settings** tab
- navigate to **Protocols** > **DNS**> **Hosts**

DNS Settings

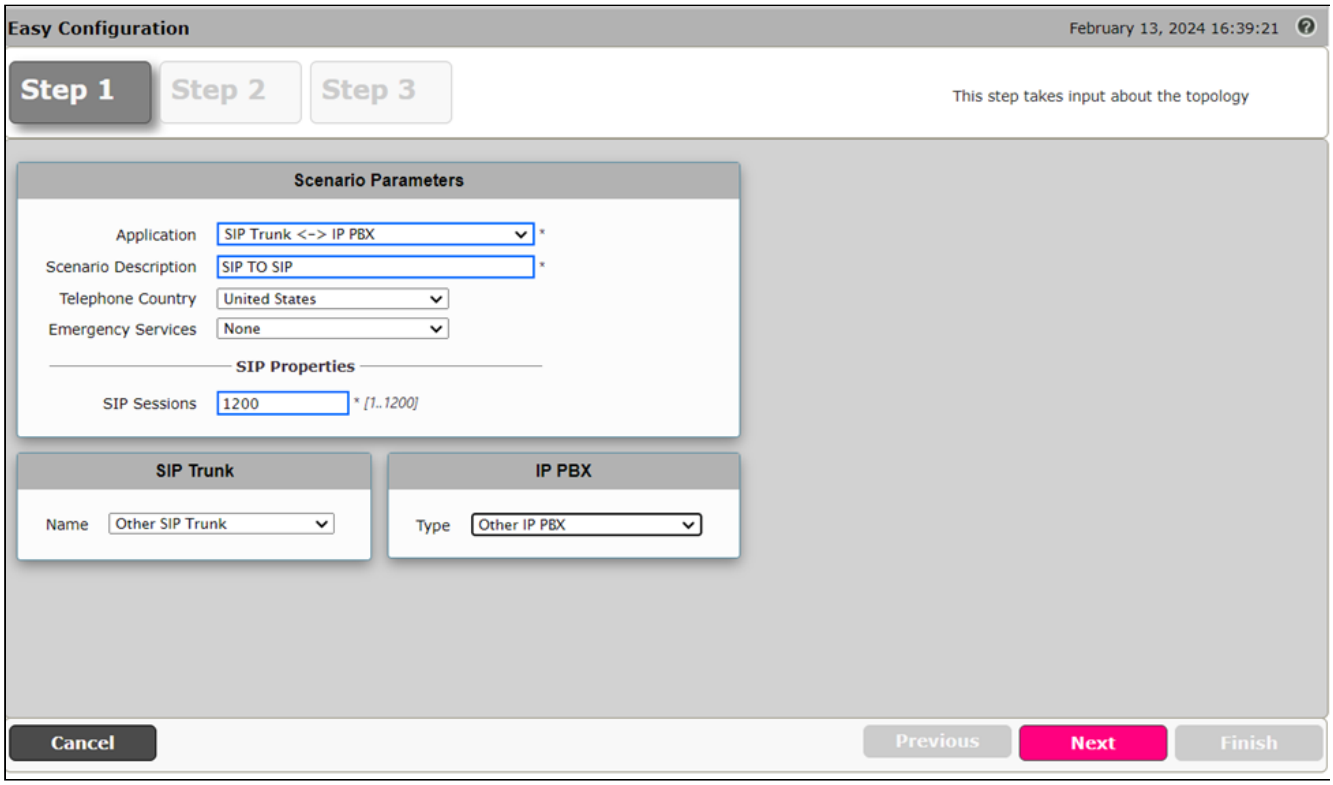


Easy Config Values

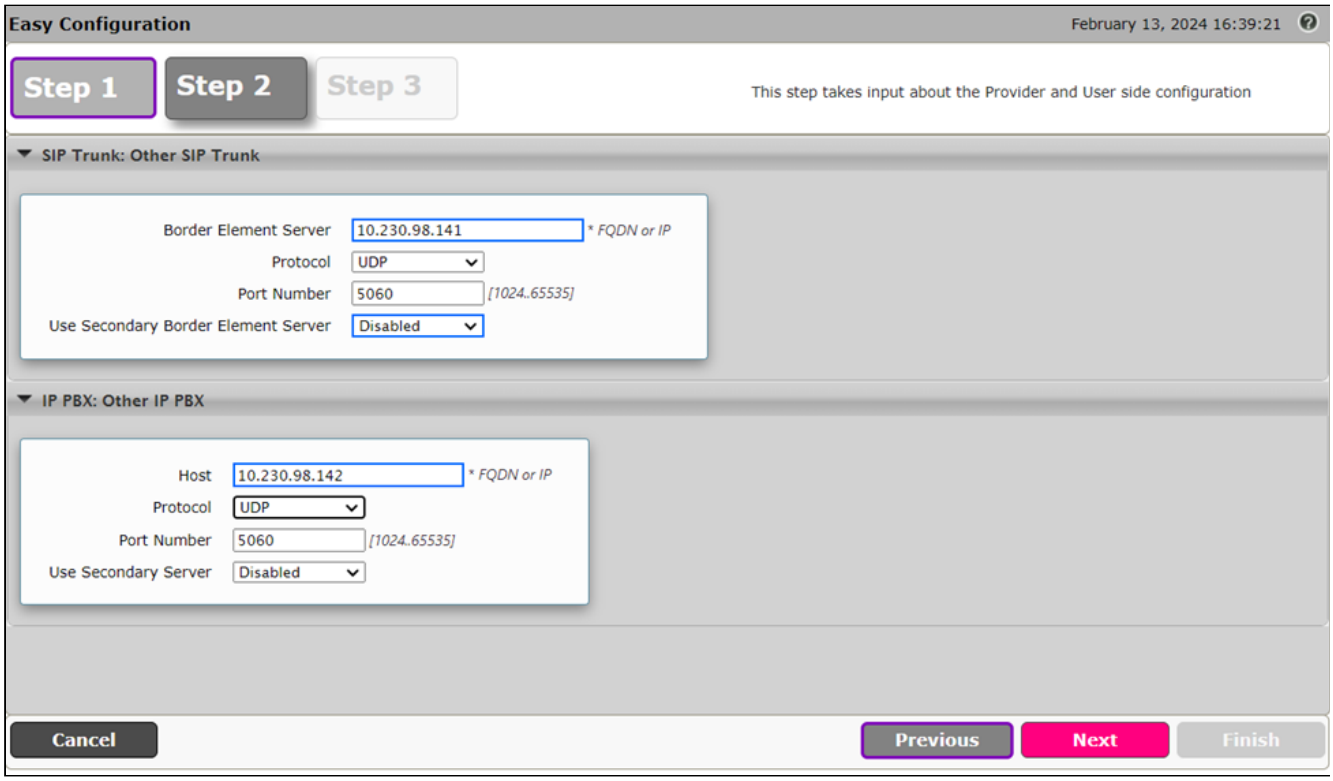
Running the SBC Edge Easy Configuration establishes the basic call routing framework for a particular scenario. In this demonstration, the SIP Trunk ↔ IP PBX application is chosen as the scenario.

The following screenshots show the values entered in the three steps of Easy Config. (To access Easy Config, click the **Tasks** tab in the SBC Edge WebUI, then navigate to **SBC Easy Setup** > **Easy Config Wizard**.)

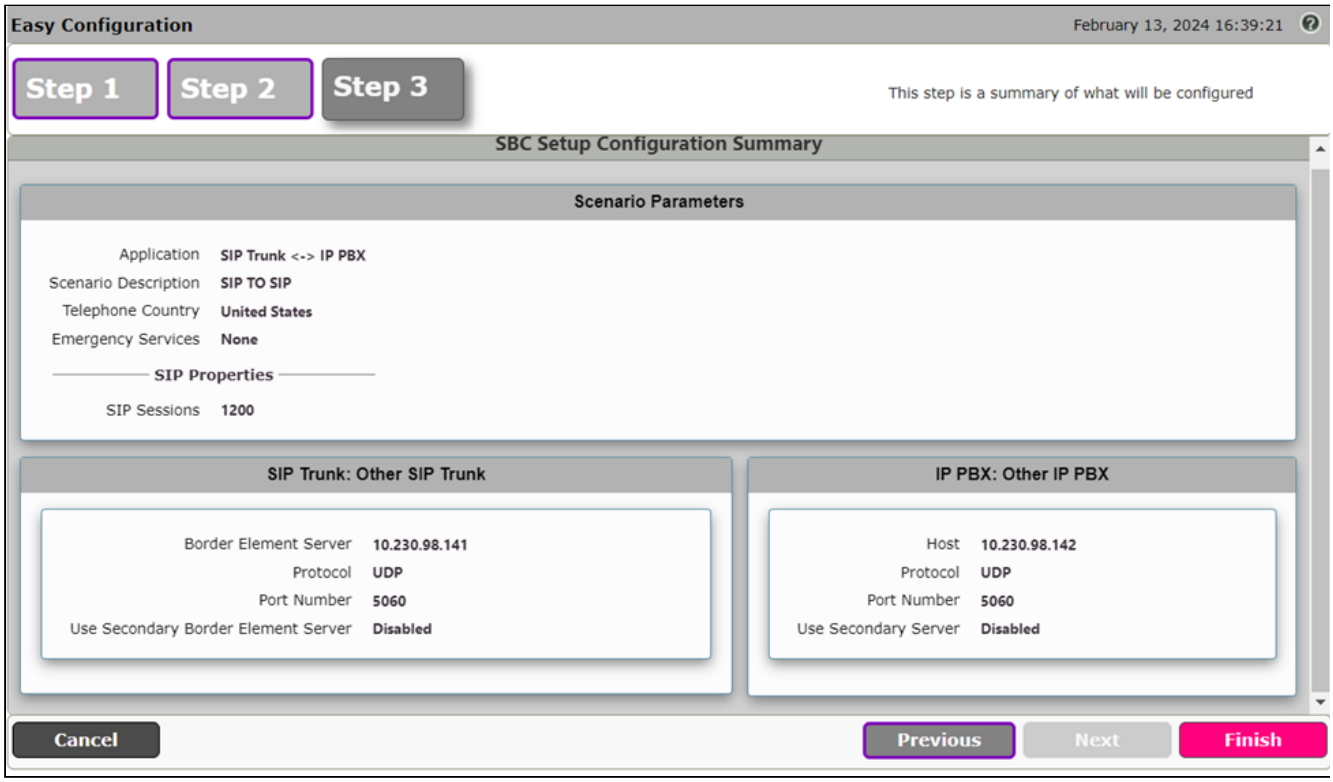
Step 1: Scenario Selection

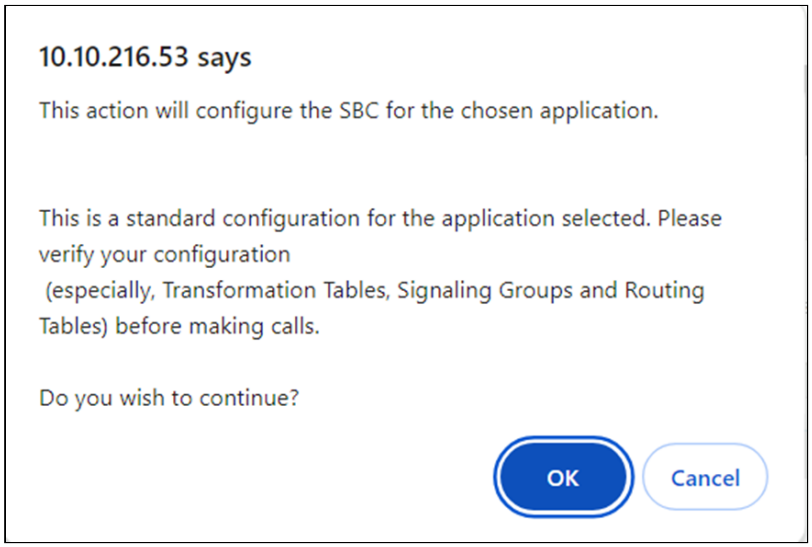


Step 2: End Point Configuration



Step 3: Summary and Confirmation



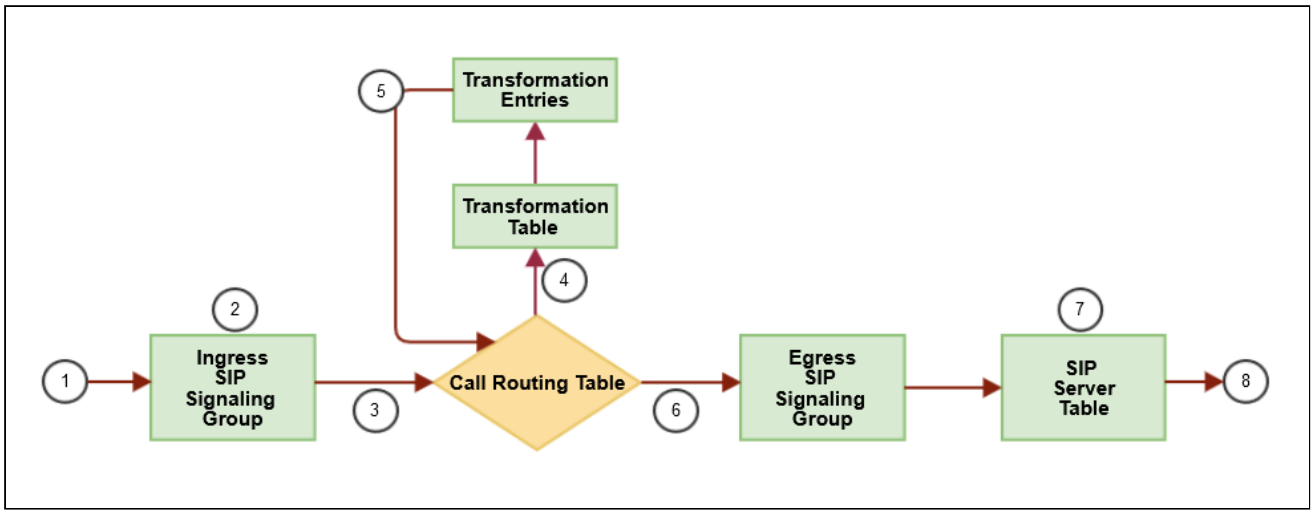


Easy Config Output

The following screenshots capture the resulting output of the Easy Configuration Wizard. Remember, the values shown are for illustration only. Do not use these values to define the configuration of your network.

As an aid to understanding, the following diagram depicts a typical call flow sequence. Every call enters through an ingress Signaling Group, traverses through a Call Routing Table and its associated Transformation Table or Tables, and exits through an egress Signaling Group. A SIP Server Table for each Signaling Group defines where the call should go on egress.

SIP to SIP Call Flow Sequence



Signaling Groups

Signaling groups allow telephony channels to be grouped together for routing and shared configuration purposes. They are the locations from which ingress calls enter and to which egress calls are routed out. They are also the location from which Tone Tables are selected. In the case of SIP, they specify protocol settings and are linked to server, media, and mapping tables.

Two Signaling Groups are defined for this demonstration:

- SIP TO SIP: IP PBX Signaling Group – serves the LAN-side IP PBX
- SIP TO SIP: Border Element Signaling Group – serves the WAN-side SIP Trunk

The following fields of each Signaling Group must be modified as a minimum per your deployment plan:

- **SIP Profile**
- **Tone Table**
- **Call Routing Table**
- **SIP Mode**
- **SIP server table / Local Registrar**
- **Media List ID**
- **Signaling/Media Source IP**
- **Listen Ports**
- **Federated IP/FQDN**

Additional fields may be modified per end-user requirements.

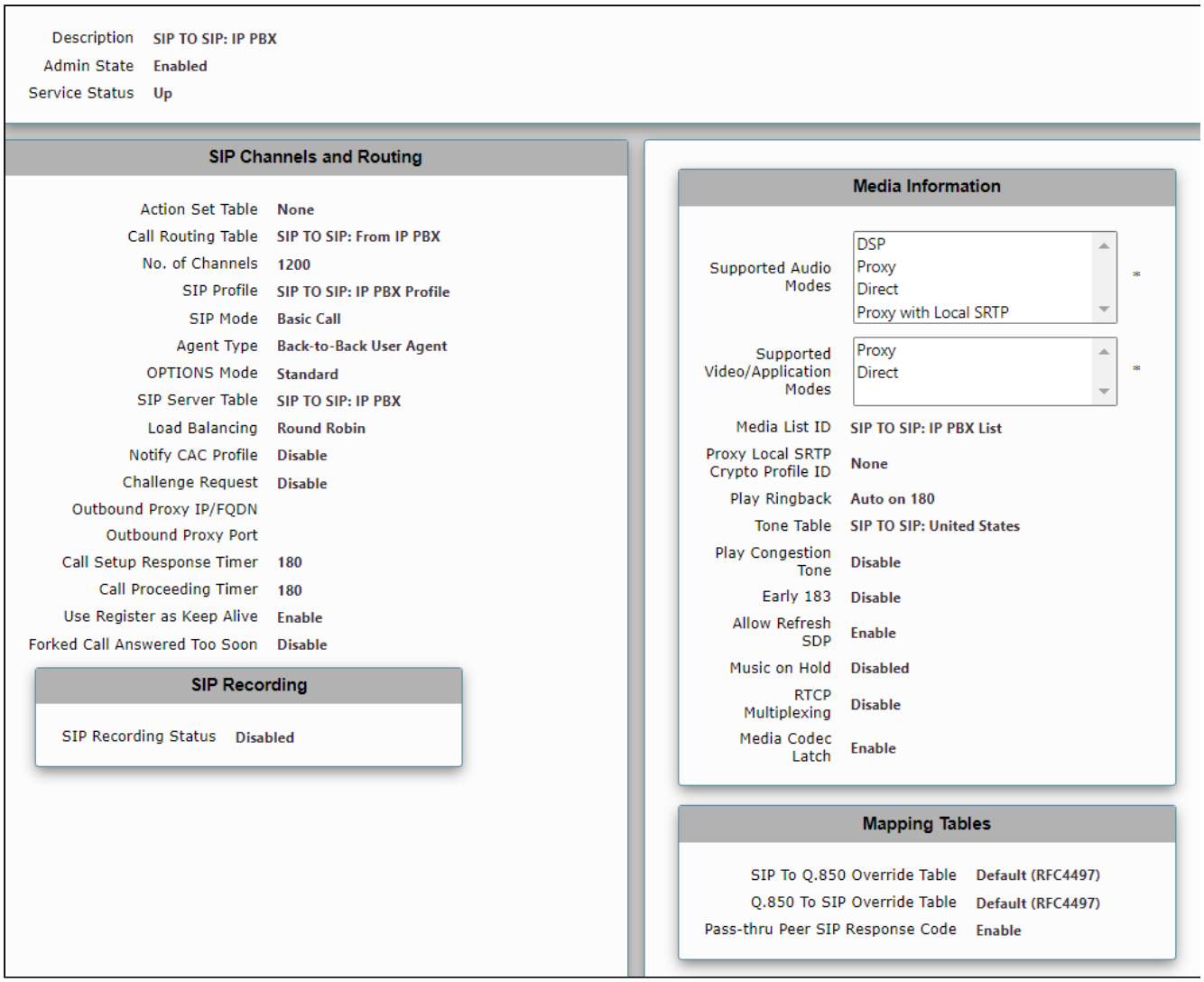
> **Note**
> Be sure to set the **Signaling/Media Source IP** value correctly for each Signaling Group per your network topology plan.

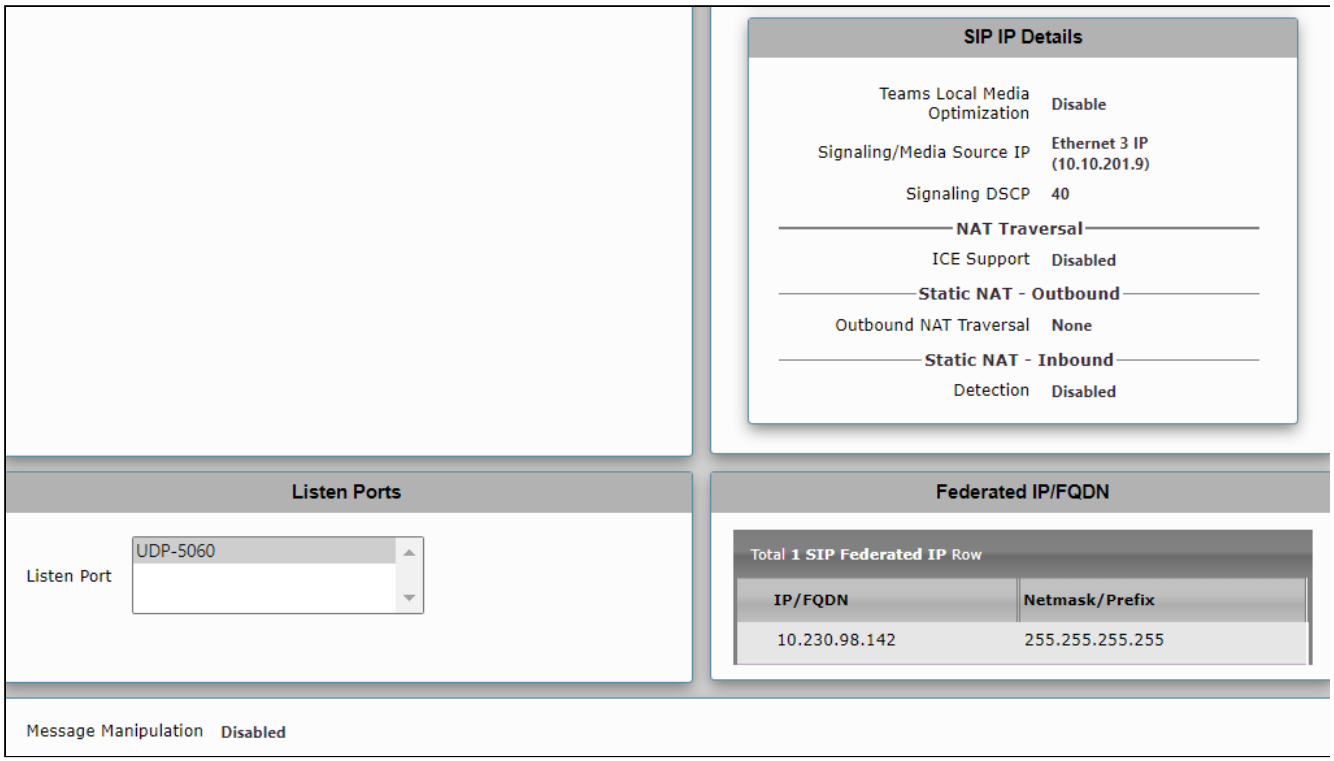
To display Signaling Groups in the SWe Edge WebUI:

- click the **Settings** tab
- navigate to **Signaling Groups**

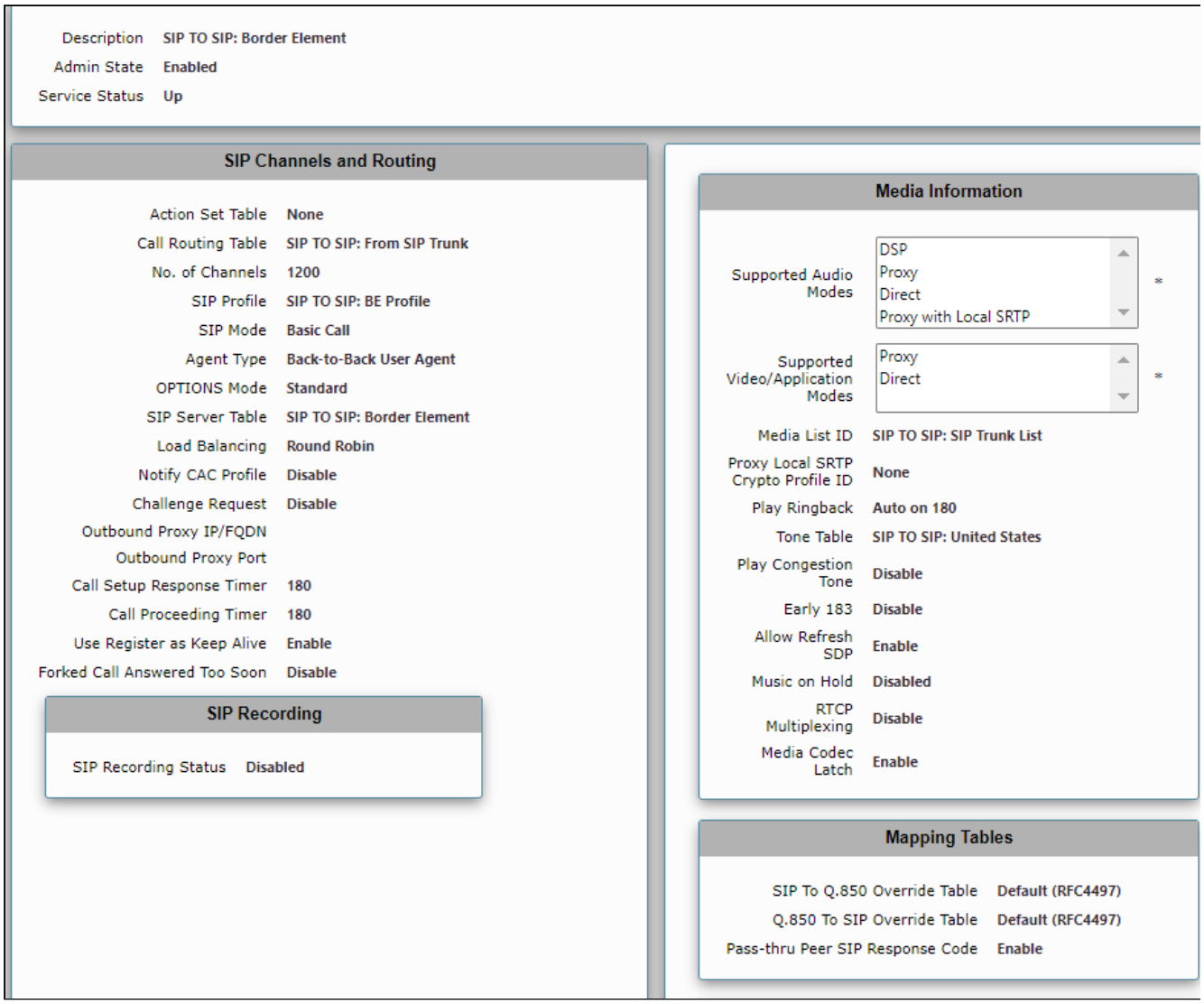
The following screenshots illustrate the Signaling Groups created by the Easy Configuration Wizard.

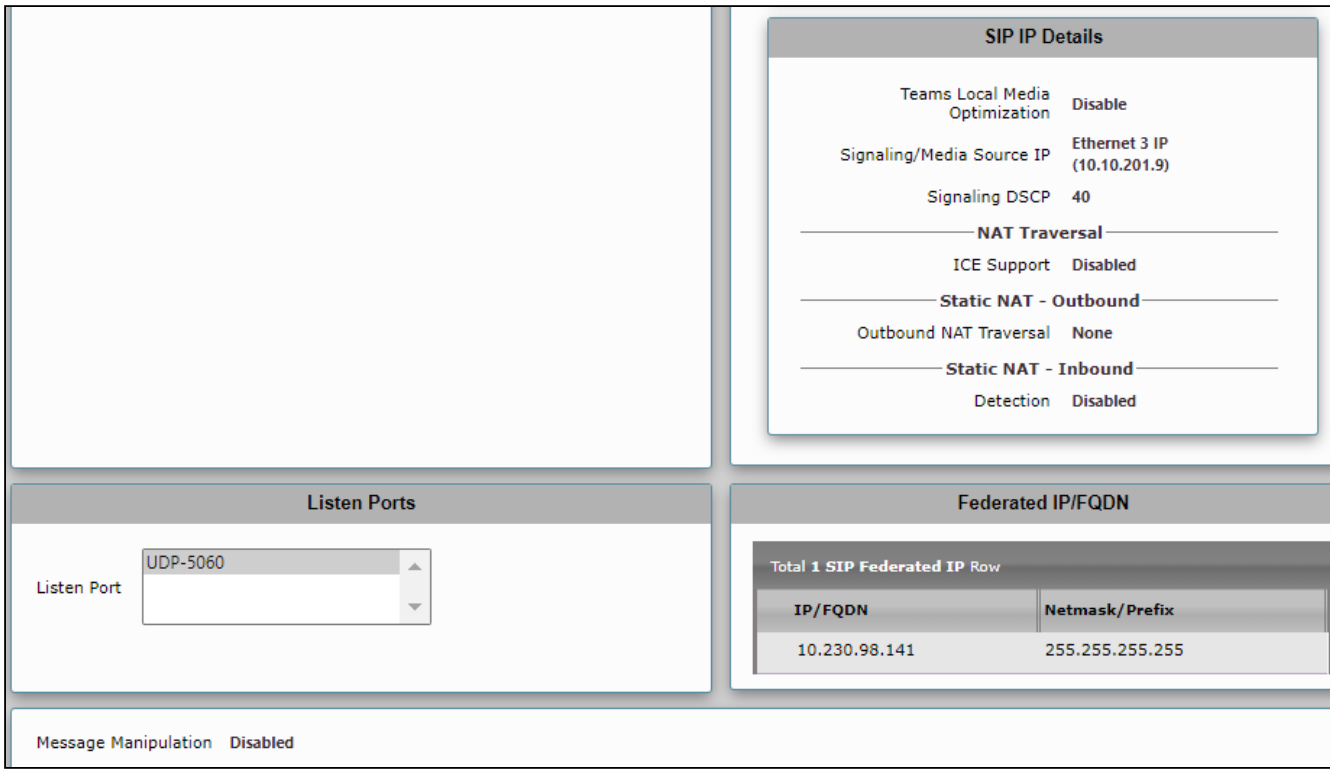
SIP TO SIP: IP PBX Signaling Group





SIP TO SIP: Border Element Signaling Group





SIP Profiles

SIP Profiles control how the Edge 8000 device communicates with other SIP devices. SIP Profiles control important characteristics such as session timers, SIP header customization, SIP timers, MIME payloads, and option tags.

In this demonstration, two SIP Profiles are defined, one for each Signaling Group:

- SIP TO SIP: IP PBX Profile – serves the SIP TO SIP: IP PBX Signaling Group
- SIP TO SIP: BE Profile – serves the SIP TO SIP: Border Element Signaling Group

To display SIP Profiles in the SWe Edge WebUI:

- click the **Settings** tab
- navigate to **SIP** > **SIP Profiles**

The following screenshots illustrate the SIP Profiles created by the Easy Configuration Wizard.

SIP TO SIP: IP PBX Profile

Description SIP TO SIP: IP PBX Profile

Session Timer

Session Timer	Enable
Minimum Acceptable Timer	600
Offered Session Timer	600
Session Timer Offset	5
Terminate On Refresh Failure	False

MIME Payloads

ELIN Identifier	LOC
PIDF-LO Passthrough	Enable
Unknown Subtype Passthrough	Disable

Header Customization

FQDN in From Header	Disable
Options Passthrugh	Access UA
FQDN in Contact Header	Disable
Send Assert Header	Trusted Only
SBC Edge Diagnostics Header	Enable
Trusted Interface	Enable
UA Header	Ribbon
Calling Info Source	RFC Standard
Diversion Header Selection	Last
Record Route Header	RFC 3261 Standard

Options Tags

100rel	Supported
Path	Not Present
Timer	Supported
Update	Supported

Timers

Transport Timeout Timer	5000
Maximum Retransmissions	RFC Standard
Redundancy Retry Timer	180000

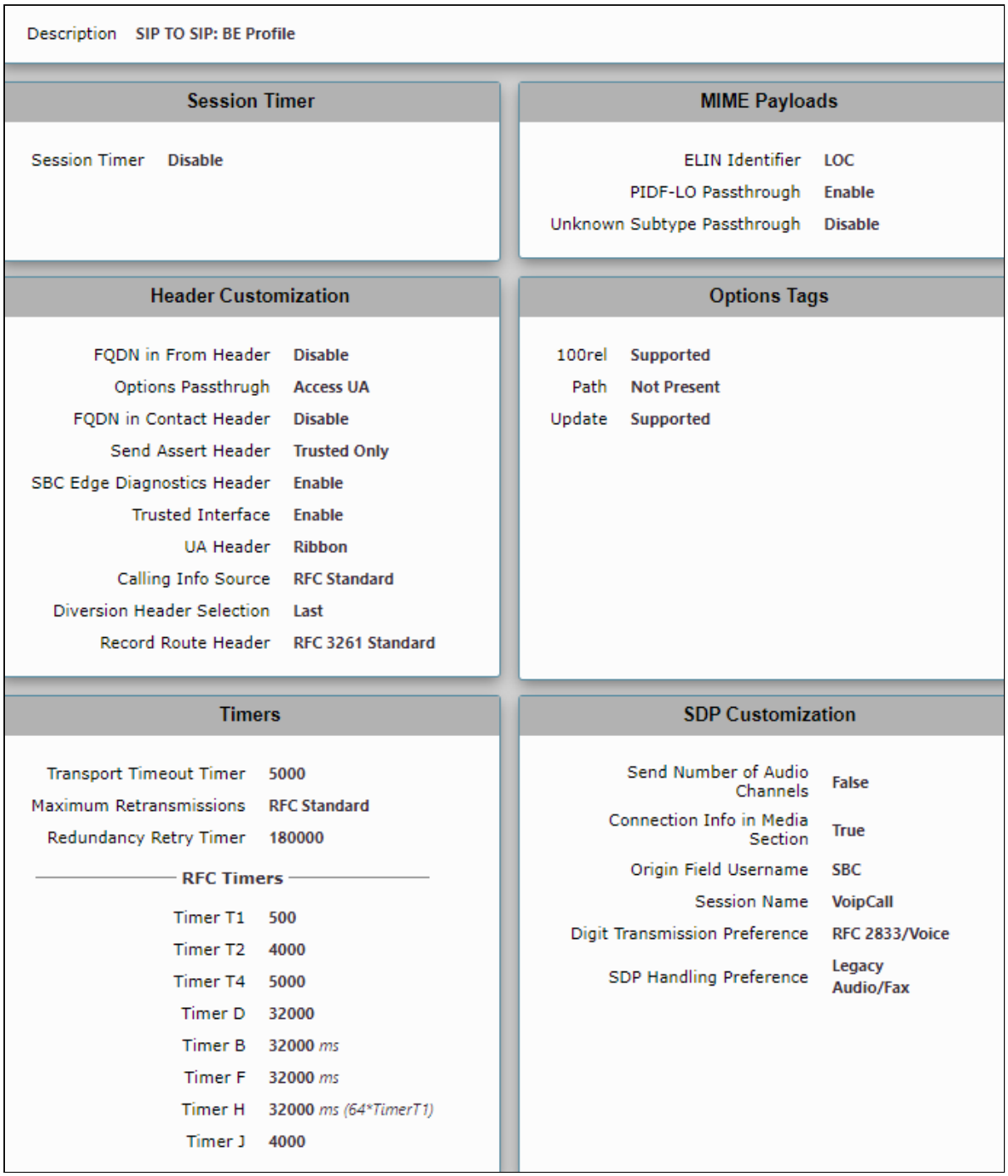
RFC Timers

Timer T1	500
Timer T2	4000
Timer T4	5000
Timer D	32000
Timer B	32000 *ms*
Timer F	32000 *ms*
Timer H	32000 *ms (64*TimerT1)*
Timer J	4000

SDP Customization

Send Number of Audio Channels	True
Connection Info in Media Section	True
Origin Field Username	SBC
Session Name	VoipCall
Digit Transmission Preference	RFC 2833/Voice
SDP Handling Preference	Legacy Audio/Fax

SIP TO SIP: BE Profile



Description SIP TO SIP: BE Profile

Session Timer

Session Timer	Disable

MIME Payloads

ELIN Identifier	LOC
PIDF-LO Passthrough	Enable
Unknown Subtype Passthrough	Disable

Header Customization

FQDN in From Header	Disable
Options Passthrugh	Access UA
FQDN in Contact Header	Disable
Send Assert Header	Trusted Only
SBC Edge Diagnostics Header	Enable
Trusted Interface	Enable
UA Header	Ribbon
Calling Info Source	RFC Standard
Diversion Header Selection	Last
Record Route Header	RFC 3261 Standard

Options Tags

100rel	Supported
Path	Not Present
Update	Supported

Timers

Transport Timeout Timer	5000
Maximum Retransmissions	RFC Standard
Redundancy Retry Timer	180000

RFC Timers

Timer T1	500
Timer T2	4000
Timer T4	5000
Timer D	32000
Timer B	32000 *ms*
Timer F	32000 *ms*
Timer H	32000 *ms (64*TimerT1)*
Timer J	4000

SDP Customization

Send Number of Audio Channels	False
Connection Info in Media Section	True
Origin Field Username	SBC
Session Name	VoipCall
Digit Transmission Preference	RFC 2833/Voice
SDP Handling Preference	Legacy Audio/Fax

Tone Tables

Tone Tables allow the Edge 8000 administrator to customize the tones a user hears when placing a call. You can modify the tone to match your local PSTN or PBX. The default Tone Table is configured for the values used in the United States for the following categories: Ringback, Dial, Busy, Congestion, Call Waiting, Disconnect, and Confirmation.

In this demonstration, both Signaling Groups – the IP PBX Signaling Group and the Border Element (SIP Trunk) Signaling Group – use the same Tone Table:

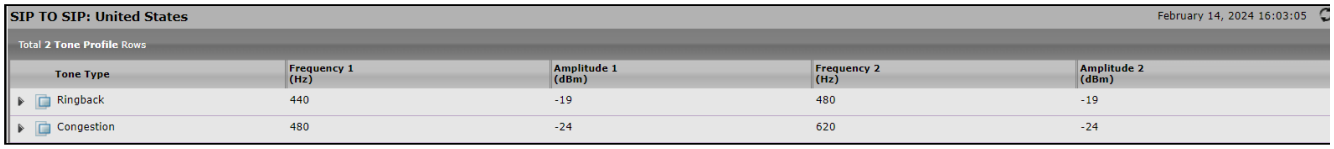
- SIP TO SIP: United States.

To display Tone Tables and associated profiles in the SWe Edge WebUI:

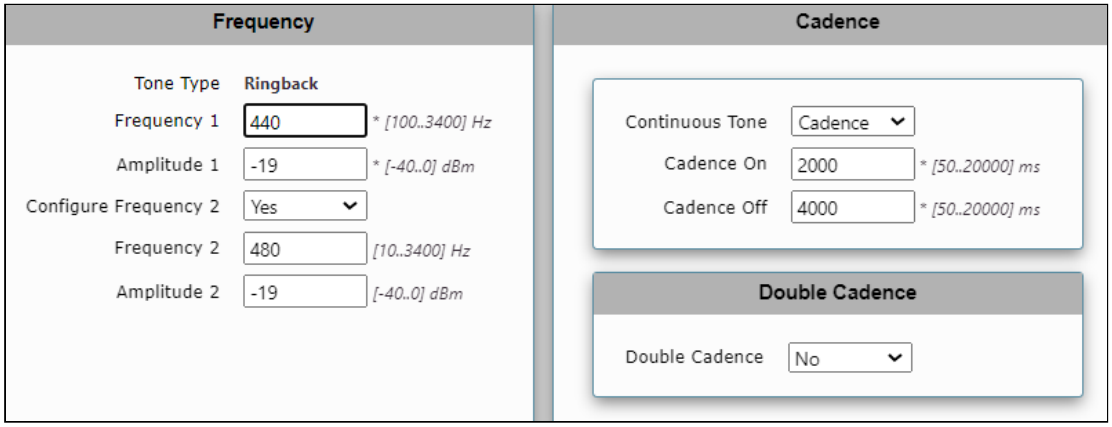
- click the **Settings** tab
- navigate to **Tone Tables**

The following screenshots illustrate the Tone Table and associated Tone Profiles created by the Easy Configuration Wizard.

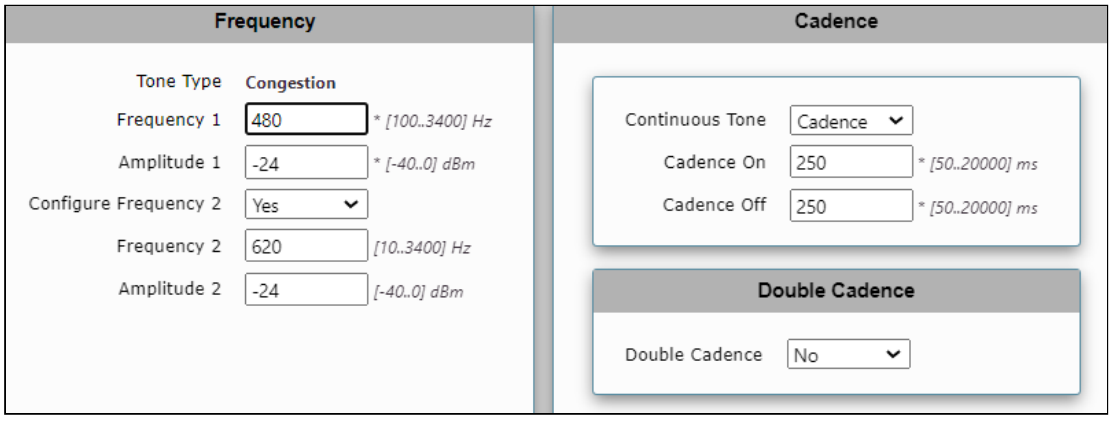
SIP TO SIP: United States Tone Table



Ringback Tone Profile



Congestion Tone Profile



Transformation Tables

Transformation Tables facilitate the conversion of names, numbers, and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number or into a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table.

In this demonstration, six Transformation Tables are defined:

- three supporting the Call Routing Table, SIP TO SIP: From IP PBX
- three supporting the Call Routing Table, SIP TO SIP: From SIP Trunk

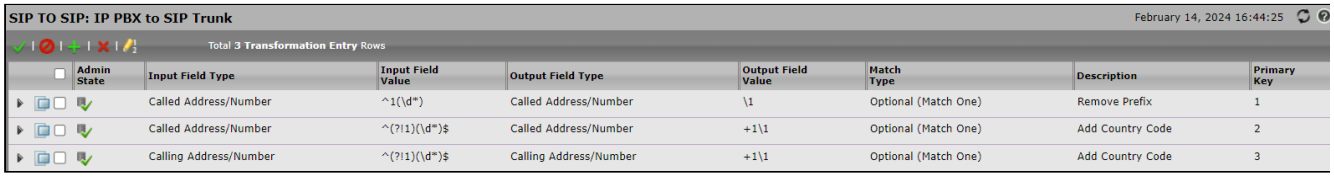
To display Transformation Tables in the SWe Edge WebUI:

- click the **Settings** tab
- navigate to **Call Routing** > **Transformation**

The following screenshots illustrate one of the six Transformation Tables, SIP TO SIP: IP PBX to SIP Trunk, and its three associated entries, as created by the Easy Configuration Wizard.

> **Note**
>
> To understand Input Field and Output Field values, refer to Regular Expressions for Number Matching and Transformation.

Transformation Table – SIP TO SIP: IP PBX to SIP Trunk

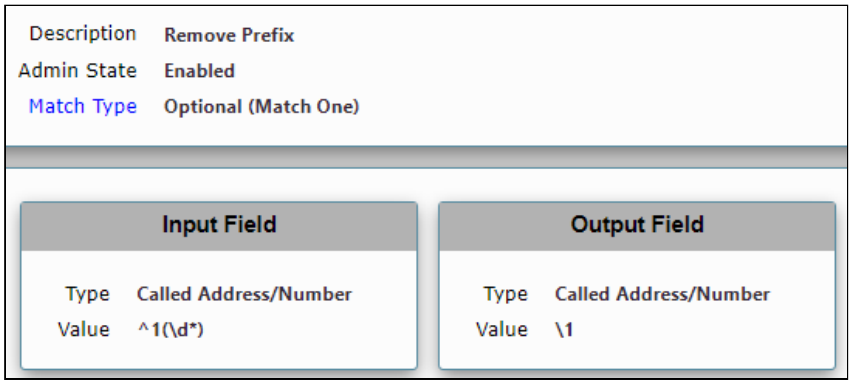


SIP TO SIP: IP PBX to SIP Trunk — February 14, 2024 16:44:25

Total 3 Transformation Entry Rows

Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description	Primary Key
	Called Address/Number	^1(\d*)	Called Address/Number	\1	Optional (Match One)	Remove Prefix	1
	Called Address/Number	^(?!1)(\d*)$	Called Address/Number	+1\1	Optional (Match One)	Add Country Code	2
	Calling Address/Number	^(?!1)(\d*)$	Calling Address/Number	+1\1	Optional (Match One)	Add Country Code	3

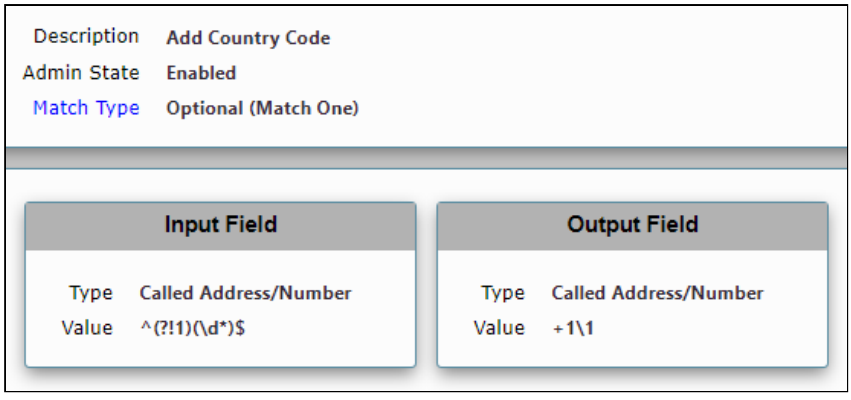
Transformation Table Entry – Remove Prefix



Description: Remove Prefix
Admin State: Enabled
Match Type: Optional (Match One)

Input Field		Output Field	
Type	Called Address/Number	Type	Called Address/Number
Value	^1(\d*)	Value	\1

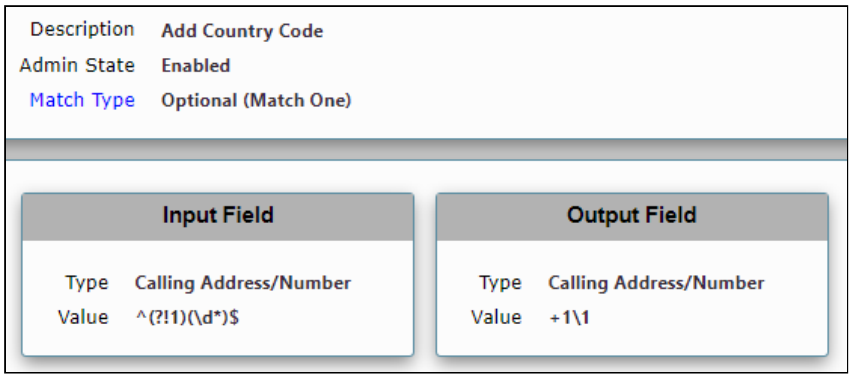
Transformation Table Entry – Add Country Code (Output Field Type: Called Address/Number)



Description: Add Country Code
Admin State: Enabled
Match Type: Optional (Match One)

Input Field		Output Field	
Type	Called Address/Number	Type	Called Address/Number
Value	^(?!1)(\d*)$	Value	+1\1

Transformation Table Entry – Add Country Code (Output Field Type: Calling Address/Number)



Call Routing Tables

Call Routing Tables allow calls to be carried between signaling groups, thus allowing calls to be carried between ports and between protocols (like ISDN to SIP). Call Routing Tables define routes, which allow for flexible configuration of which calls are carried and how they are translated. These tables are one of the central connection points of the system, linking Transformation Tables, Message Translations, Cause Code Reroute Tables, Media Lists, and Signaling Groups.

Each Signaling Group has one Call Routing Table. In this demonstration, the Easy Configuration Wizard has created the following two Signaling Groups and their corresponding Call Routing Table:

Signaling Group and Matching Call Routing Table

Signaling Group	Call Routing Table
SIP To SIP: IP PBX	SIP to SIP: From IP PBX
SIP to SIP: Border Element	SIP to SIP: From SIP Trunk

The following fields of the Call Routing Table must be modified as a minimum:

- **Number/Name Transformation Table**
- **Destination Signaling Groups**

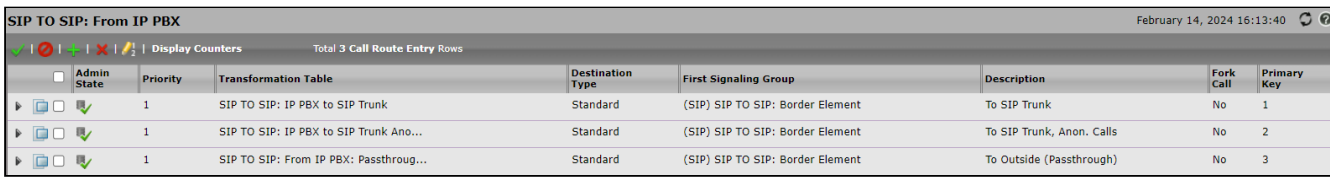
Additional fields may be modified per end-user requirements.

To display Call Routing Tables in the SWe Edge WebUI:

- click the **Settings** tab
- navigate to **Call Routing** > **Call Routing Table**

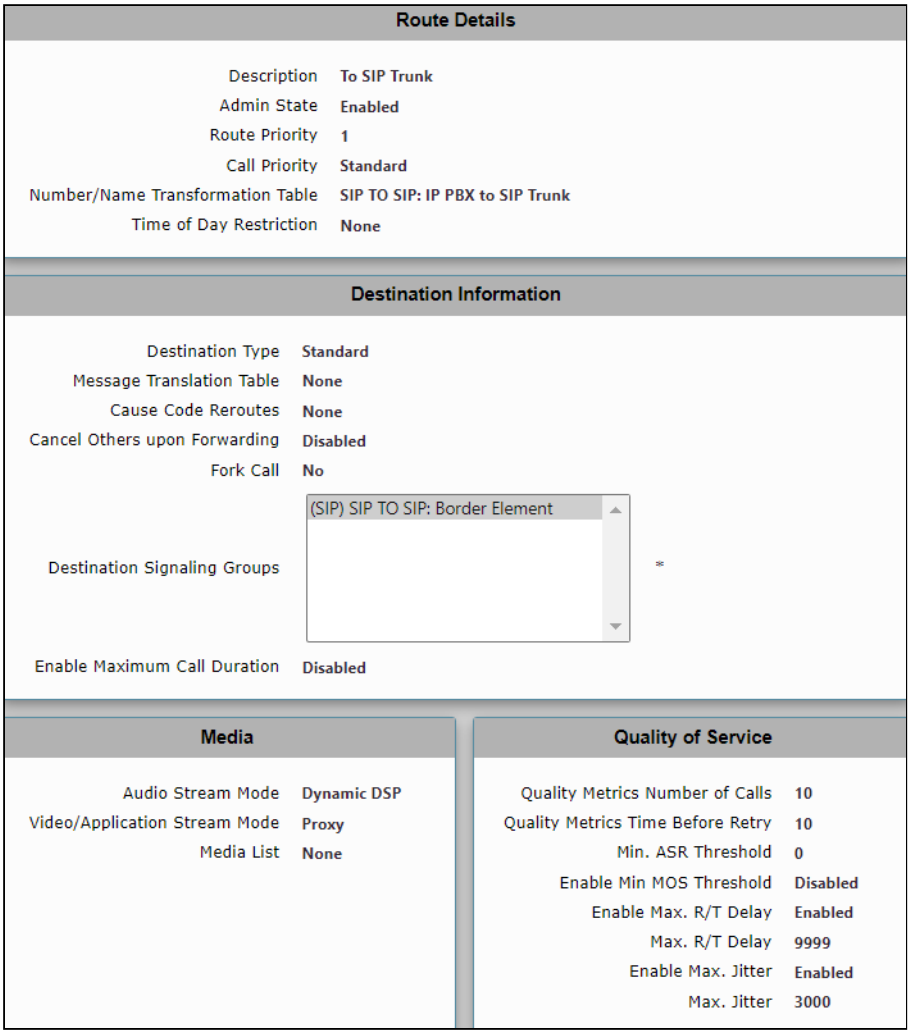
The following screenshots show the two Call Routing Tables and the three entries in each table, as created by the Easy Configuration Wizard. Each entry specifies a different Transformation Table. Note that in this demonstration, the second entry of each table allows for the routing of an anonymous ("anon") call where the calling number is not disclosed.

Call Routing Table – SIP TO SIP: From IP PBX



Admin State	Priority	Transformation Table	Destination Type	First Signaling Group	Description	Fork Call	Primary Key
	1	SIP TO SIP: IP PBX to SIP Trunk	Standard	(SIP) SIP TO SIP: Border Element	To SIP Trunk	No	1
	1	SIP TO SIP: IP PBX to SIP Trunk Ano...	Standard	(SIP) SIP TO SIP: Border Element	To SIP Trunk, Anon. Calls	No	2
	1	SIP TO SIP: From IP PBX: Passthroug...	Standard	(SIP) SIP TO SIP: Border Element	To Outside (Passthrough)	No	3

Entry – To SIP Trunk



Route Details

Description	To SIP Trunk
Admin State	Enabled
Route Priority	1
Call Priority	Standard
Number/Name Transformation Table	SIP TO SIP: IP PBX to SIP Trunk
Time of Day Restriction	None

Destination Information

Destination Type	Standard
Message Translation Table	None
Cause Code Reroutes	None
Cancel Others upon Forwarding	Disabled
Fork Call	No
Destination Signaling Groups	(SIP) SIP TO SIP: Border Element *
Enable Maximum Call Duration	Disabled

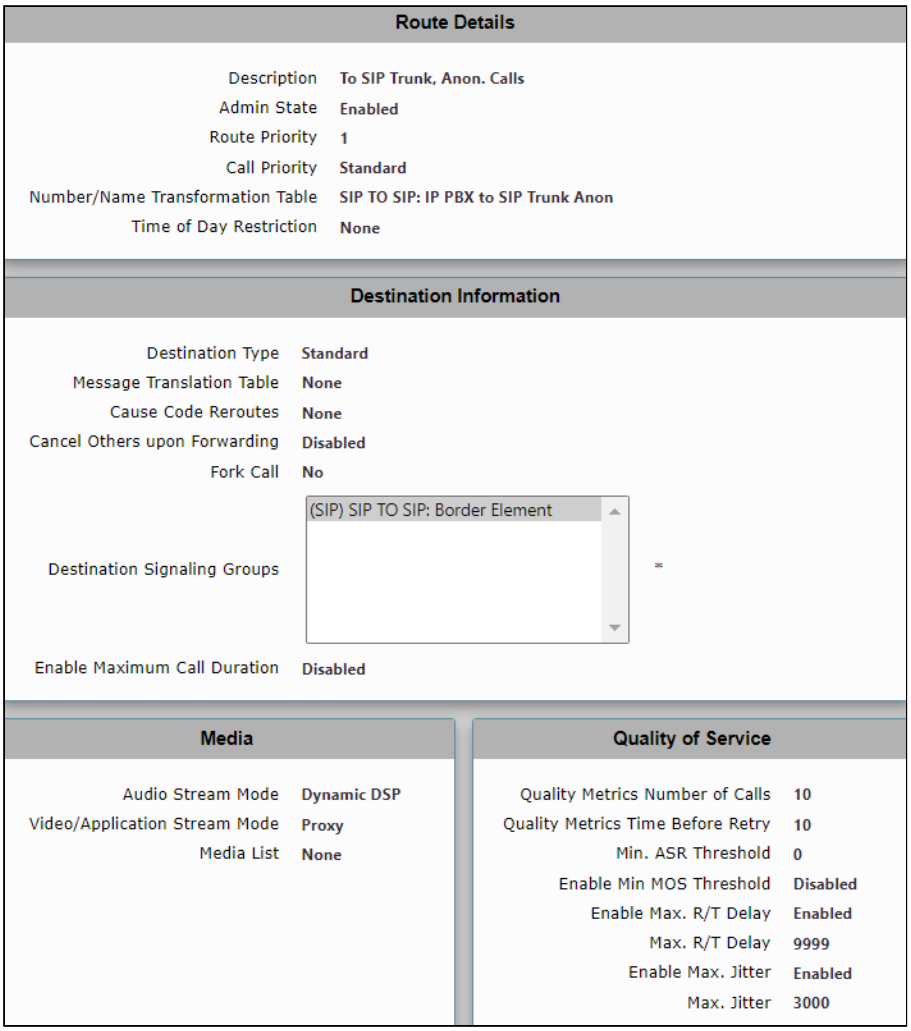
Media

Audio Stream Mode	Dynamic DSP
Video/Application Stream Mode	Proxy
Media List	None

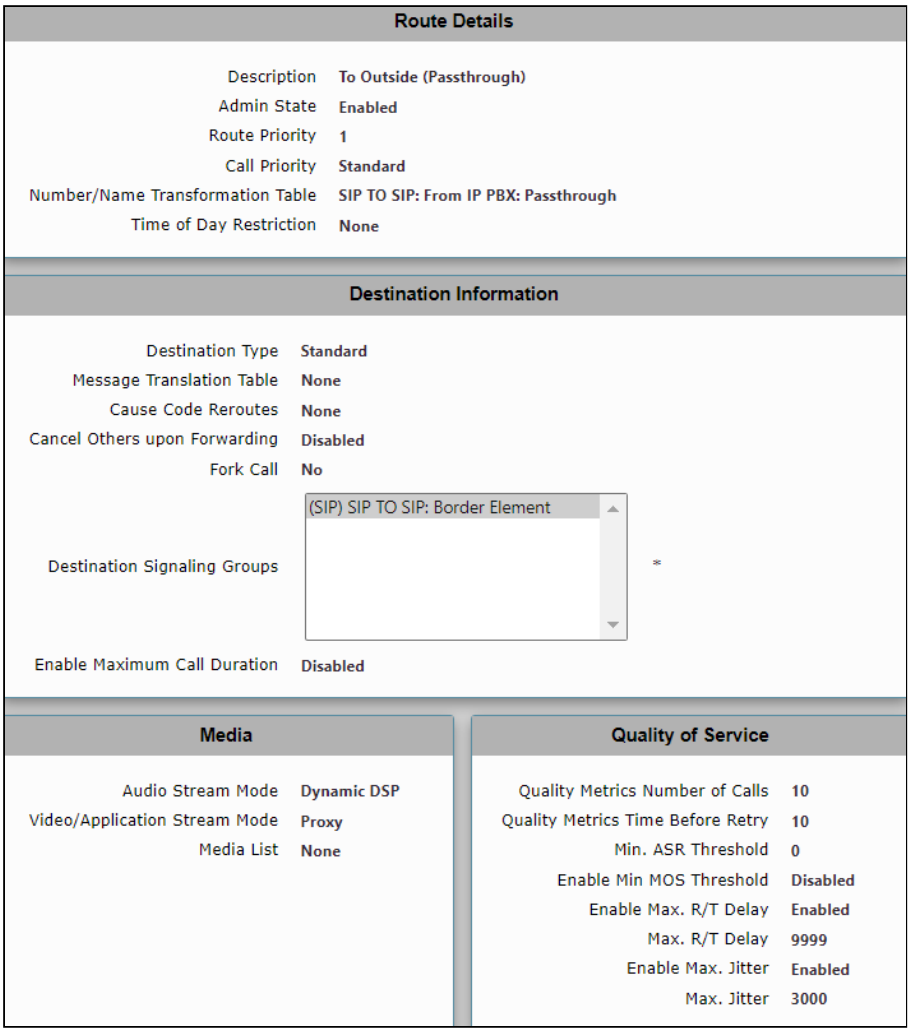
Quality of Service

Quality Metrics Number of Calls	10
Quality Metrics Time Before Retry	10
Min. ASR Threshold	0
Enable Min MOS Threshold	Disabled
Enable Max. R/T Delay	Enabled
Max. R/T Delay	9999
Enable Max. Jitter	Enabled
Max. Jitter	3000

Entry – To SIP Trunk (Anonymous Calls)



Entry – To SIP Trunk (Passthrough)



Route Details

Description	To Outside (Passthrough)
Admin State	Enabled
Route Priority	1
Call Priority	Standard
Number/Name Transformation Table	SIP TO SIP: From IP PBX: Passthrough
Time of Day Restriction	None

Destination Information

Destination Type	Standard
Message Translation Table	None
Cause Code Reroutes	None
Cancel Others upon Forwarding	Disabled
Fork Call	No
Destination Signaling Groups	(SIP) SIP TO SIP: Border Element *
Enable Maximum Call Duration	Disabled

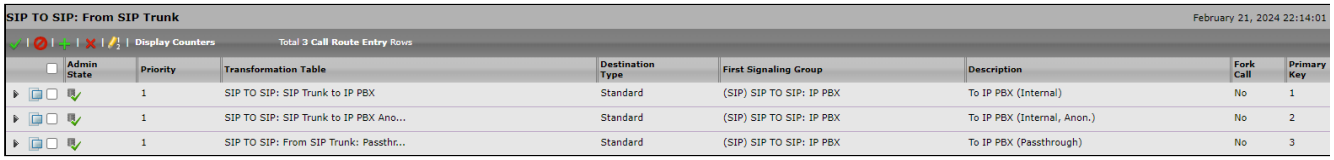
Media

Audio Stream Mode	Dynamic DSP
Video/Application Stream Mode	Proxy
Media List	None

Quality of Service

Quality Metrics Number of Calls	10
Quality Metrics Time Before Retry	10
Min. ASR Threshold	0
Enable Min MOS Threshold	Disabled
Enable Max. R/T Delay	Enabled
Max. R/T Delay	9999
Enable Max. Jitter	Enabled
Max. Jitter	3000

Call Routing Table – SIP TO SIP: From SIP Trunk

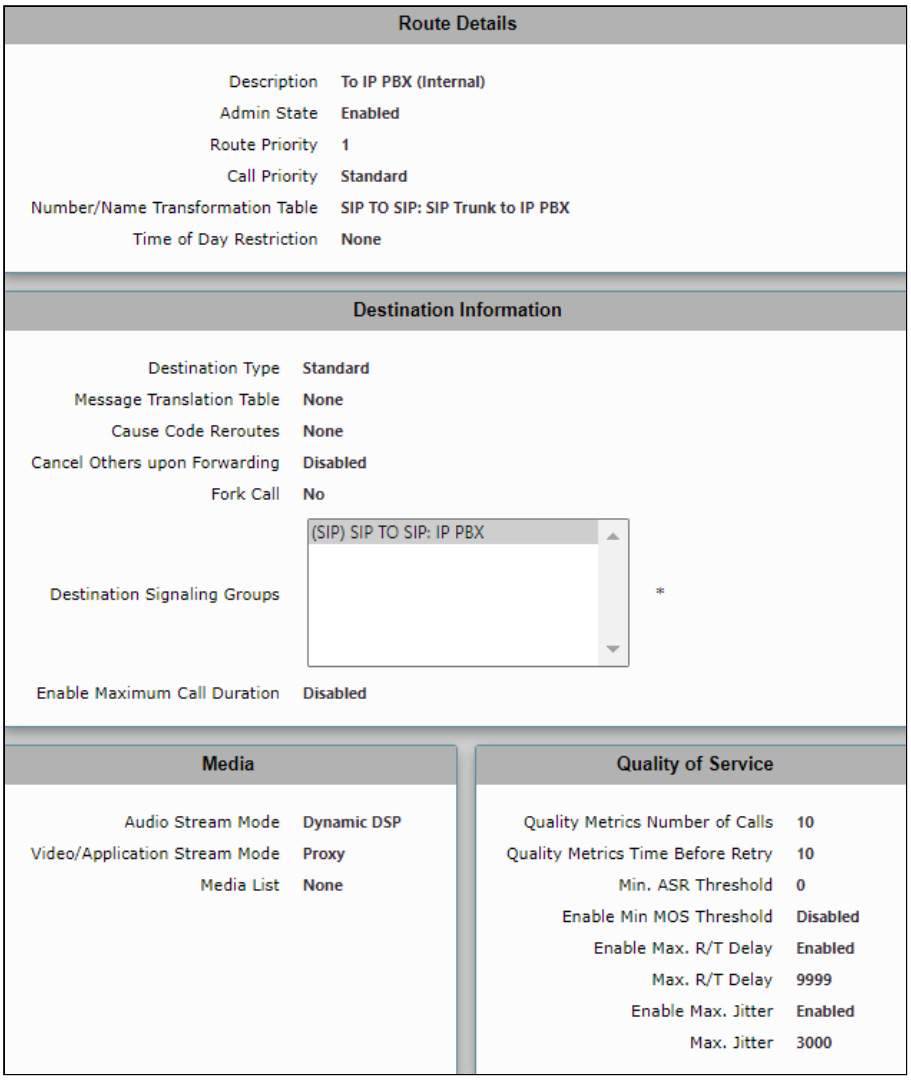


SIP TO SIP: From SIP Trunk February 21, 2024 22:14:01

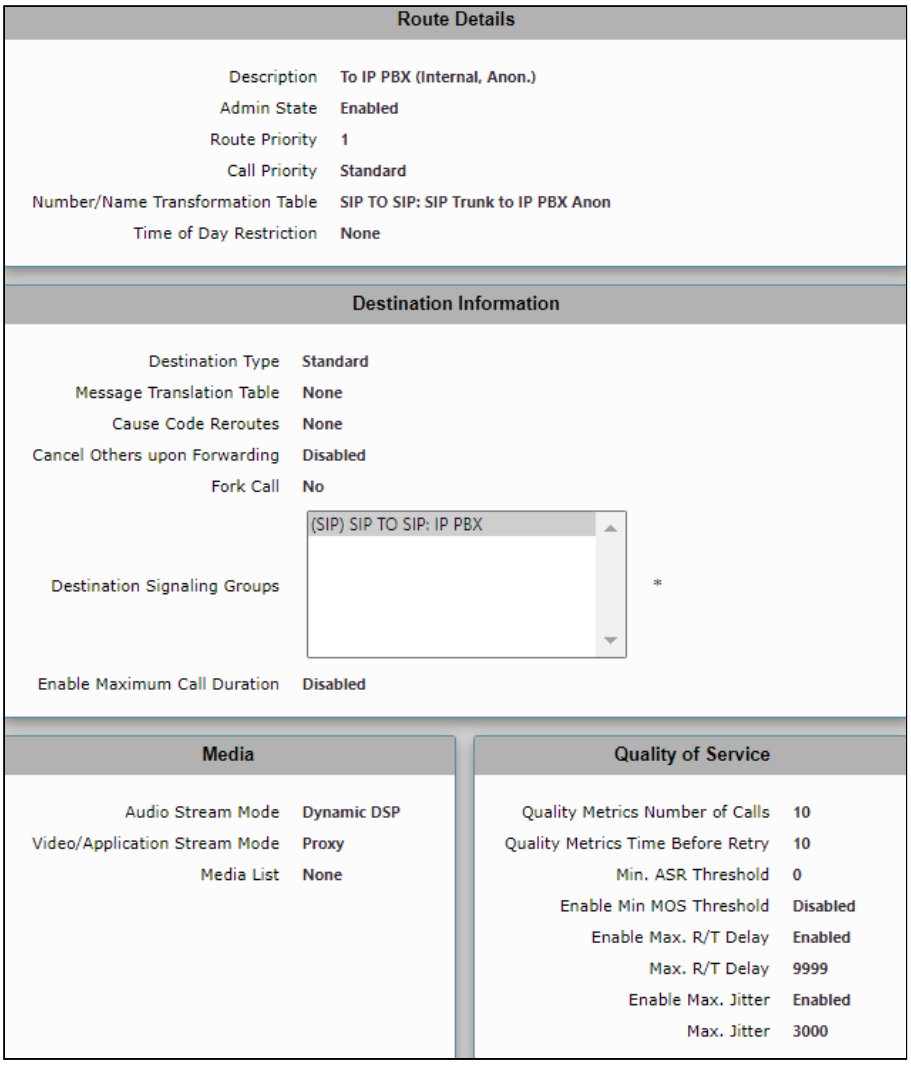
Display Counters Total 3 Call Route Entry Rows

Admin State	Priority	Transformation Table	Destination Type	First Signaling Group	Description	Fork Call	Primary Key
	1	SIP TO SIP: SIP Trunk to IP PBX	Standard	(SIP) SIP TO SIP: IP PBX	To IP PBX (Internal)	No	1
	1	SIP TO SIP: SIP Trunk to IP PBX Ano...	Standard	(SIP) SIP TO SIP: IP PBX	To IP PBX (Internal, Anon.)	No	2
	1	SIP TO SIP: From SIP Trunk: Passthr...	Standard	(SIP) SIP TO SIP: IP PBX	To IP PBX (Passthrough)	No	3

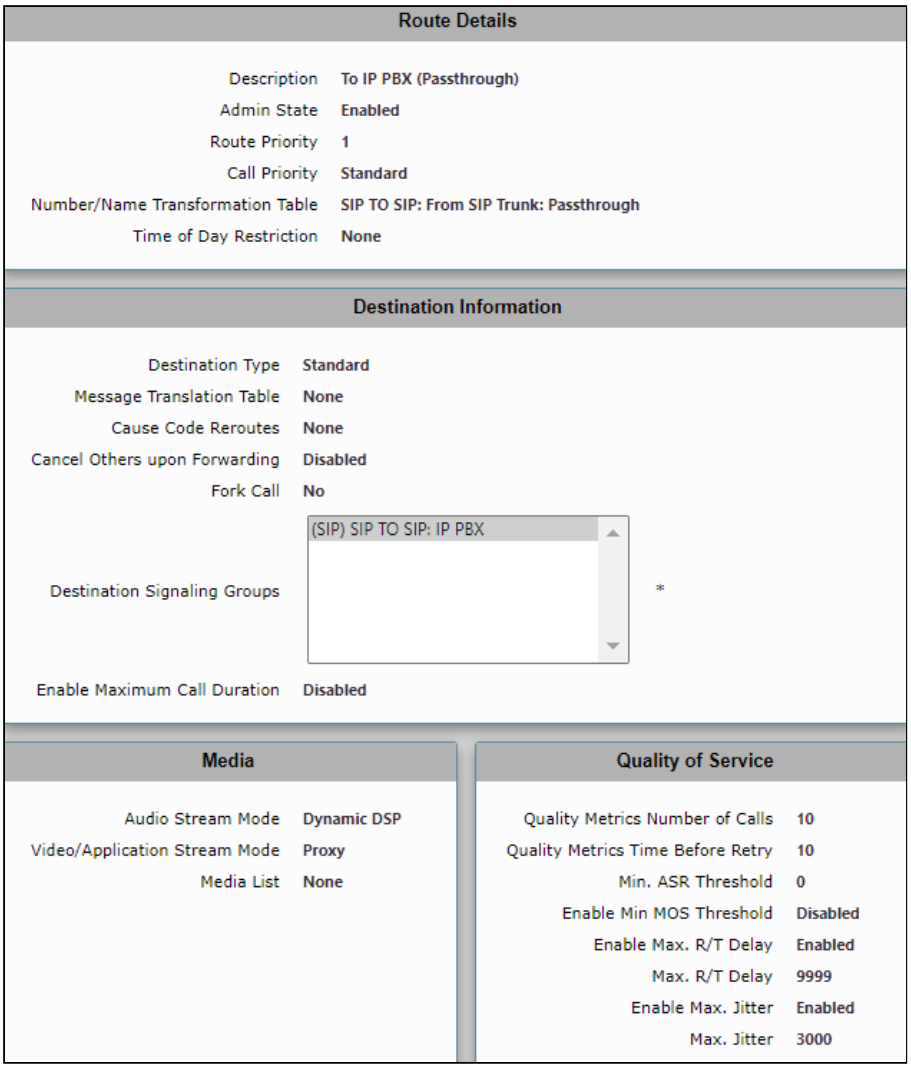
Entry – To IP PBX



Entry – To IP PBX (Anonymous Calls)



Entry – To IP PBX (Passthrough)



SIP Server Tables

SIP Server tables contain the IP address or FQDN of one or more SIP servers where INVITE messages can be sent to egress calls on a Signaling Group. The entries in the tables provide information about the IP Addresses, ports, and protocols used to communicate with the servers.

In this demonstration, two SIP Server Tables, one for each Signaling Group, are defined:

Signaling Group and Matching SIP Server Table

Signaling Group	SIP Server Table
SIP To SIP: IP PBX	SIP TO SIP: IP PBX
SIP to SIP: Border Element	SIP TO SIP: Border Element

The following fields of the SIP Server Table must be modified as a minimum:

- **Host FQDN/IP**
- **Port**

- **Protocol**

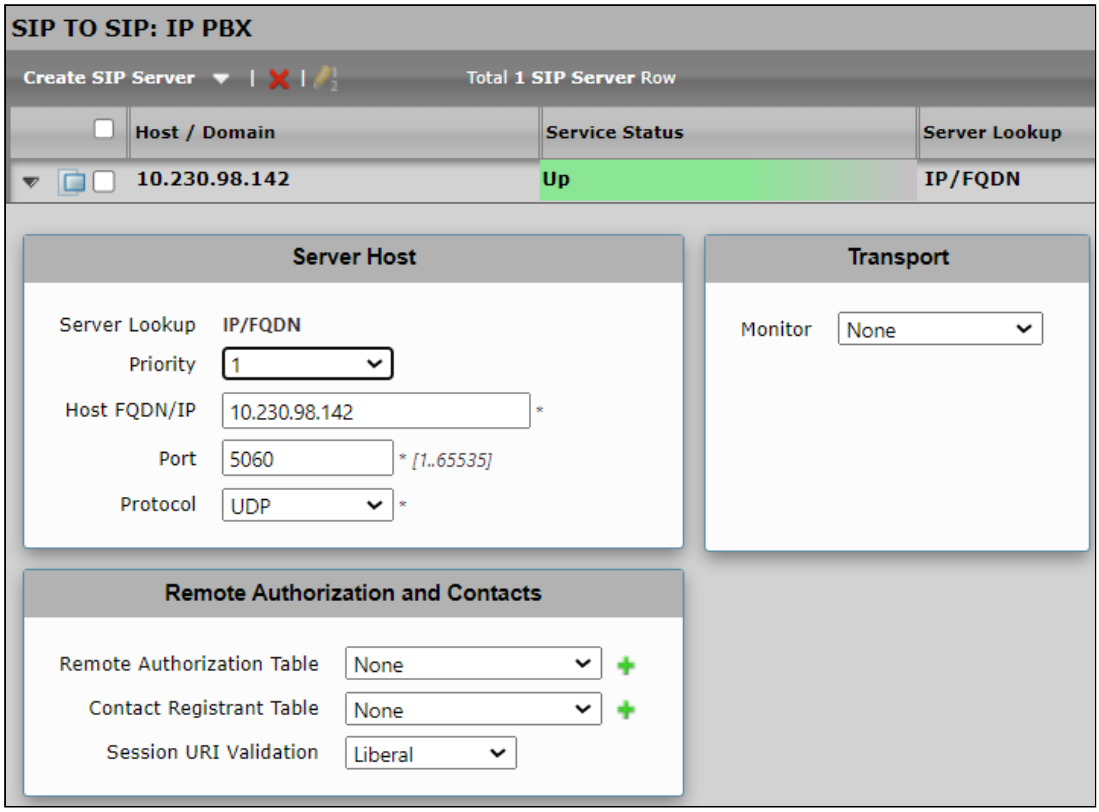
Additional fields may be modified per end-user requirements.

To display SIP Server Tables in the SWe Edge WebUI:

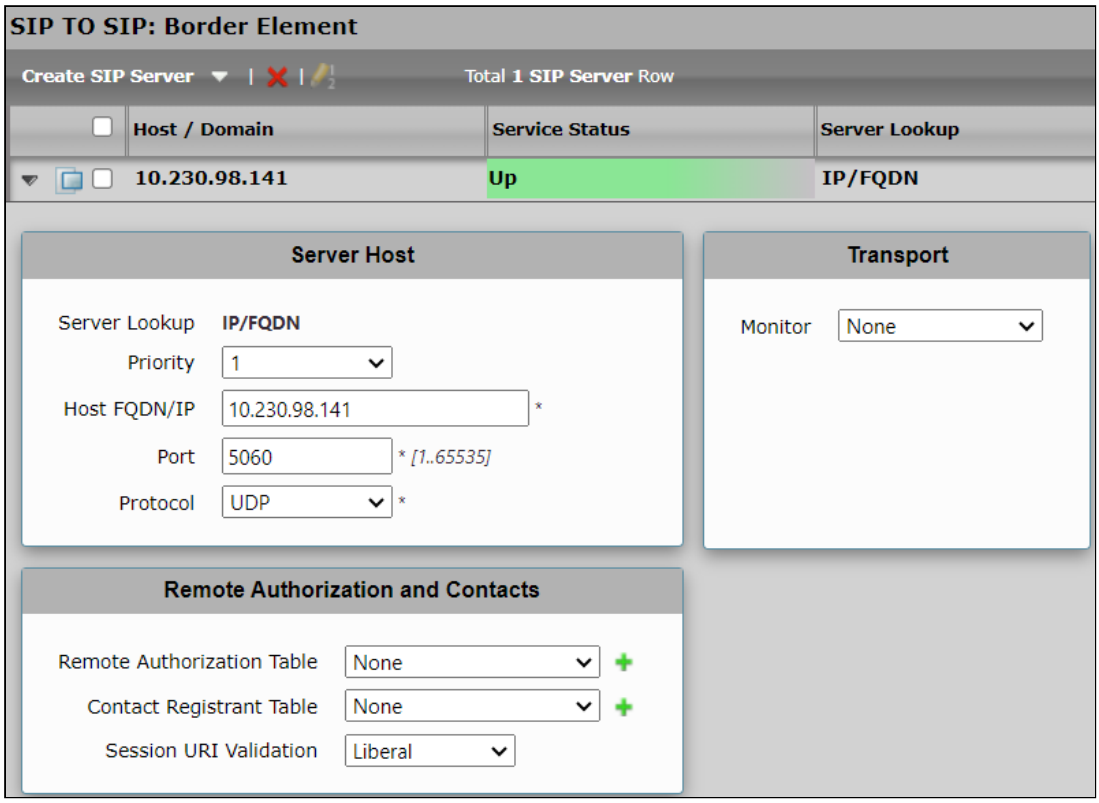
- click the **Settings** tab
- navigate to **SIP** > **SIP Server Tables**

The following screenshots show the two SIP Server Tables created by the Easy Configuration Wizard.

SIP Server Table – SIP TO SIP: IP PBX



SIP Server Table – SIP TO SIP: Border Element



Media Profiles

Media Profiles allow you to specify individual voice and fax compression codecs and their associated settings for inclusion in a Media List. Different codecs provide varying levels of compression, allowing a tradeoff between reducing bandwidth at the expense of reducing voice quality.

The following field of a Media Profile must be modified as a minimum:

- Codec

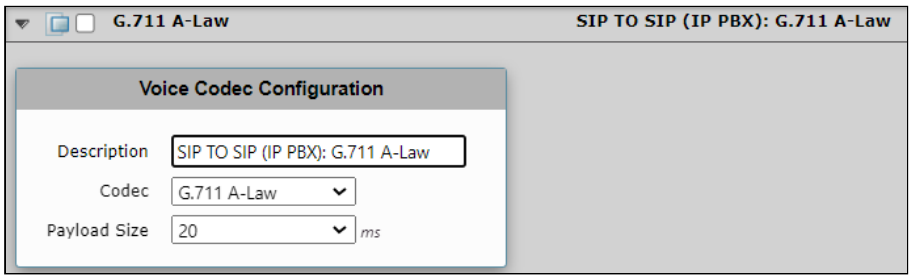
Additional fields may be modified per end-user requirements.

To display Media Profiles in the SWe Edge WebUI:

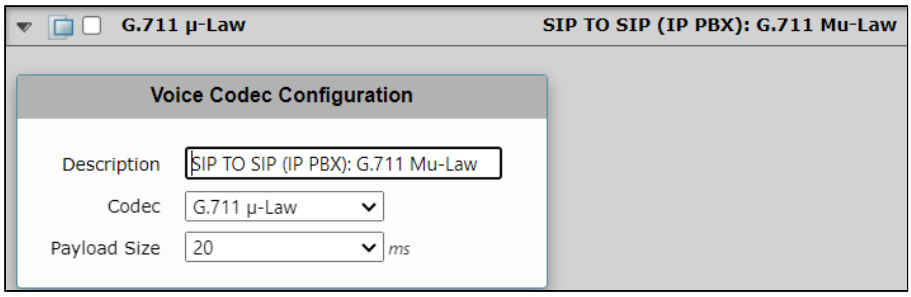
- click the **Settings** tab
- navigate to **Media** > **Media Profiles**

The following screenshots show several different Media Profiles created by the Easy Configuration Wizard for this demonstration.

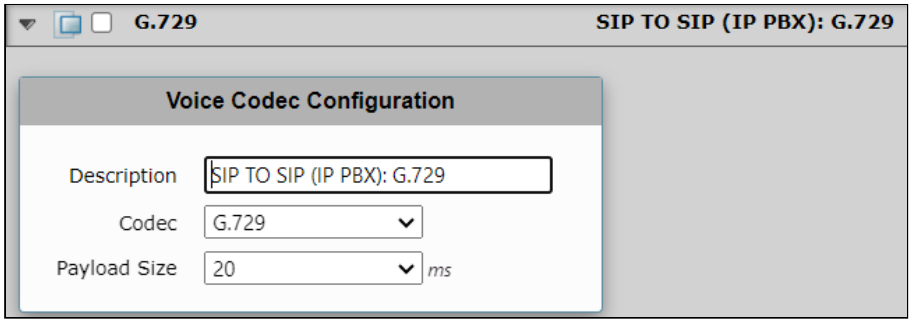
SIP TO SIP (IP PBX): G.711 A-Law



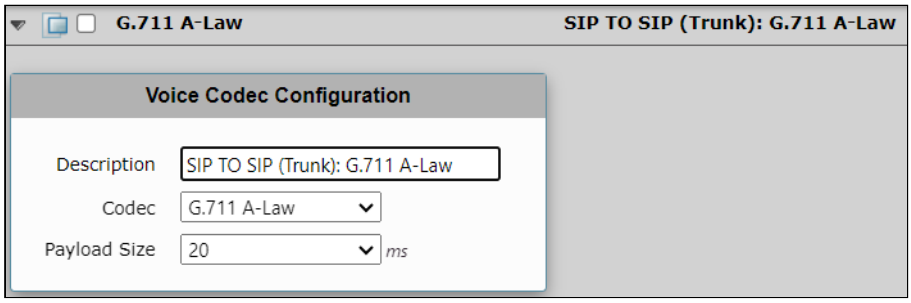
SIP TO SIP (IP PBX): G.711 Mu-Law



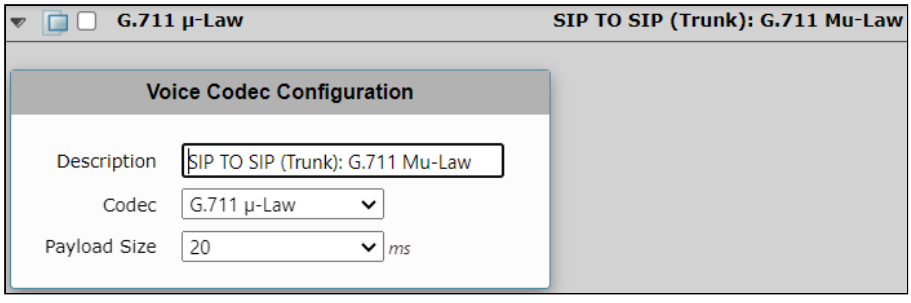
SIP TO SIP (IP PBX): G.729



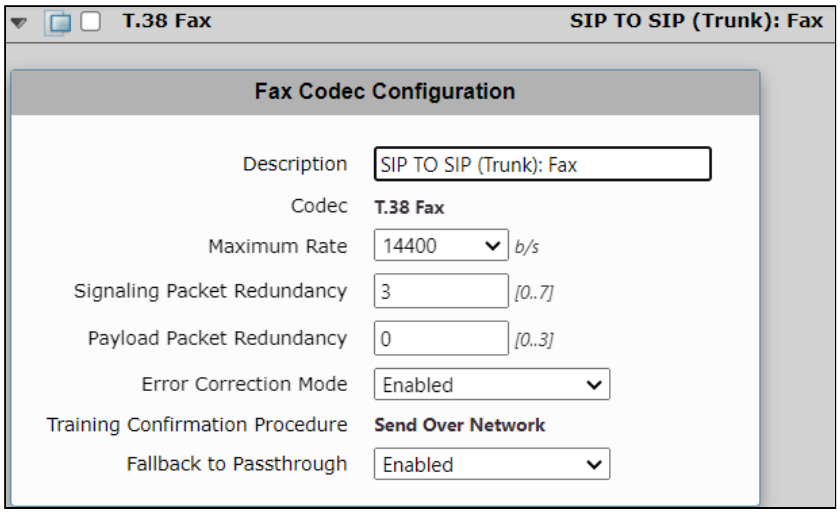
SIP TO SIP (Trunk): G.711 A-Law



SIP TO SIP (Trunk): G.711 Mu-Law



SIP TO SIP (Trunk): Fax



Media Lists

A Media List contains a list of media profiles you order to give preference to more desirable codecs above less desirable ones. Profile order determines the order in which codecs are specified in SIP message(s) sent to a peer.

The following field of a Media List must be modified as a minimum:

- Media Profiles List

Additional fields may be modified per end-user requirements.

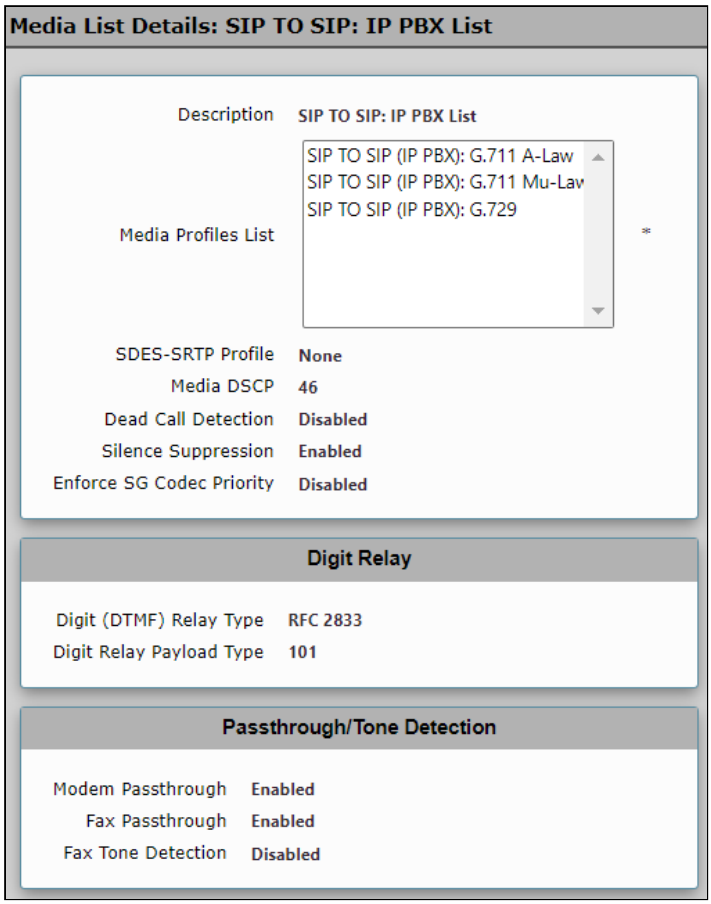
To display Media Lists in the SWe Edge WebUI:

- click the **Settings** tab
- navigate to **Media** > **Media List**

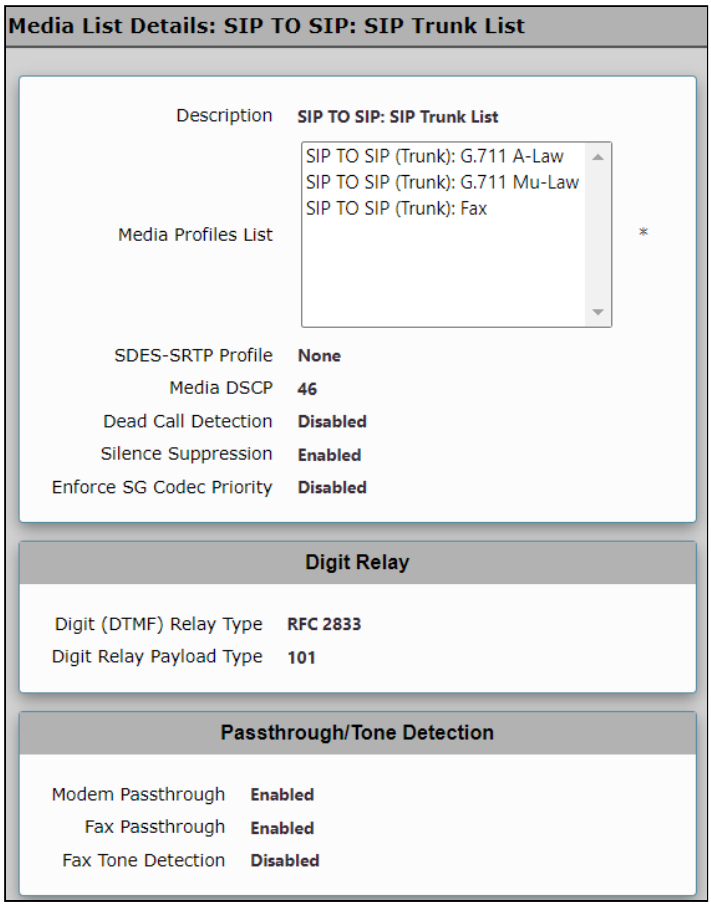
The following screenshots show the two Media Lists created by the Easy Configuration Wizard for this demonstration:

- SIP TO SIP: IP PBX List
- SIP TO SIP: SIP Trunk List

SIP TO SIP: IP PBX List



SIP TO SIP: SIP Trunk List



Ribbon Product Interoperability Testing

One of the primary objectives at Ribbon is to ensure interoperability between Ribbon products and the existing network equipment of Ribbon customers. Refer to Edge 8K - Wiki Articles to view sample scenarios of specific service equipment inter-working with the Ribbon Edge 8000 Series product.

Gateway Reference

Edge 8000 GUI Gateway parameters and descriptions.

> **Attention**
>
> Any configuration changes through the Gateway folder are service impacting. After making a change, wait for approximately 30 seconds, then verify the associated ports are available.

Contents

SIP-User-Agent

Contents

UA-Setting

Contents

Edge 8000 GUI's UA-Setting hierarchy

- UA Global-Configuration
- UA Port-Level-Configuration

UA Global-Configuration

Introduction

Use the following parameters to configure the gateway with global configurations.

SIP Configuration

Parameter	Description
Enable-SIPUA	Default is False. This field enables or disables the gateway feature.
Max-UA-Port	This field defines the maximum number for the FXS port that your deployment supports. This field has a value of 22 when an FXS/FXO card is present. This field has a value of 24 when an FXS card is present. The value should not be changed.
SIP-SERVER-IP	This field is read-only. The value represents the SWe Edge IP address used for SIP signaling communication (169.254.1.120).
SIP-UA-IP	This field is read-only. The value is 169.254.1.100. This field represents the SIP-UA SIP signaling IP address used for communication with SWe Edge.
SIPUA-Bind-Port	Default is the internal port 1025 (including when the field is left empty). The range is 0 to 65535. Enter a port number to which SIP UA binds and listens for SIP messages. **Note**: You can use port 5060 in IAD mode or bind-to-WAN. In all other cases, port 5060 cannot be used here.
SIP-User-Domain	Default is blank. The default indicates that all FXS ports use the system's ALG LAN IP address as the domain unless the value is overwritten at the port level. Each FXS port will be provisioned in the Softswitch domain, and the SIP-User domain is also the authentication domain for each FXS port.

Parameter	Description
Enable-Register	Default is True. Select the checkbox to instruct each configured FXS port to send a REGISTER request to the configured domain through a configured outbound proxy. If this checkbox is not checked, FXS ports will not register. **Note**: Some VoIP deployments use static registration for the FXS ports and do not require port registration.
Enable-SIP-Authentication-Name	Default is False. When selected, the value configured for the port's username is used for the port's registration request.
Enable-PRACK	Default is False. When enabled, PRACK and UPDATE are advertised in the SIP Supported header, and support for the SIP option Tags “100rel” and “timer” is enabled.
SIPUA-Instance-ID	Default is True. If set to true, the SIP Instance parameter is added to SIP Contact header.
Use-REFER-For-Transfer	Default is True. Select True if your VoIP switch supports REFER requests as outlined in RFC3515 to perform call transfer. Note: For release 24.1, this value should always be set to True.

Tone Configuration

Parameter	Description
Ignore-FAX-Over-Audio	Default is False. Select the checkbox to specify that an initial FAX request be ignored and to establish an audio call instead. On calls terminating onto a FXS port, in rare cases a FAX request can arrive in the initial INVITE message. Unless this option is specifically needed, this field should be left as False.
Disable-T38-Reject	Default is False. By default, a SIP 488 reject response is sent when T38 offer comes and T38 FAX support is disabled, followed by a G711 response. When set to True, a 488 response will not be sent, only a G711 response.
Enable-ADTRAN-T38-INTEROP	Default is True. When True, Redundance Recovery mode is forced for better interop.
Enable-T38-Offer-Outbound	Default is False. If FAX is detected, the recommendation is to have the Receiving T38 gateway always offer T38. Note that some implementations of the software might break if T38 is not offered. When enabled, the sending gateway will offer T38.

Parameter	Description
Disable-RFC2833	Default is False. If True, the FXS port do not advertise the telephone-event in SDP offer.
Enable-RFC2833-IB	Default is False. If RFC2833 is disabled by **Disable-RFC2833**, you can enable this attribute to still answer with RFC-2833.
RFC2833-Event-Payload	Default is 101. The range is 100 to 101. This field allows you to define a telephone-event payload with any value.

Media

Parameter	Description
RTP-Min-Port	Default is 22000. The range is 20000 to 65535. Enter the minimum number of RTP ports that SIP UA uses for media.
RTP-Max-Port	Default is 41600. The range is from 1 to 65535. Enter the maximum number of RTP ports that SIP UA uses for media.
Codec-Preference	Default is G7110-uLaw. Choose a codec type from the Codec Preference drop-down list. Edgemarc chooses this codec when offered by the far end regardless of the order of appearance in the SIP SDP. This selects the codec that is used by all FXS ports for encoding analog data. The codec must be part of the negotiated codec list: G.711 ulawG.711 alawG.729G.728G.726,16 Kbps G.726, 24 Kbps G.726, 32 Kbps G.726, 40 Kbps.
Use-Preferred-Codec-Preference	Default is False. Select the checkbox for this field to specify that only the preferred codec is used when the FXS places a call. If an incoming call does not have the preferred codec, the call is rejected.
Enable-Access-Code	Default is False. By default '#' is used to auto-terminate dialing on FXS port. If '#' is required as part of dial-pattern for access-codes, this field should be set to true.
VAD-Enabled	Default is Enabled. Choose whether to enable voice activity detection globally.
Jitter-Buffer-Value	Default is 60 msec. The range is 10 to 90 msec. This field defines the Jitter Buffer value in unit of msecs.

Call Configuration

Parameter	Description
Call-Waiting-Tone-Index	Default is 72. The range is 72 to 76. Each value in the range represents a variant of the call-waiting tones. The default tone is sufficient in most deployments.
Conference-URI	Default is empty. Enter the Conference URI if your softswitch supports creating a conference using ad hoc SIP methods as outlined in RFC 4579, section 5.4. Format in the same manner as a SIP endpoint (user@host).
Incoming-Answer-Wait-Delay	Default is 40 seconds. This field limits the time (in seconds) that a FXS port should keep ringing on an incoming call without an answer. Note that 40 seconds is equivalent to about 10 rings in the United States.
Connect-To-PBX	Default is False. When enabled, certain mid-call features that the FXS port completes will be disabled, as they are handled by the PBX.
Disable-CPC	Default if False. This field is relevant when an FXS port is connected to a PBX or Key system. When enabled, the FXS port will generate a Calling Party Control signal on the PBX or Key system port to release lines internally, when the call is ended by the IP side.
CPC-Timer	Default is 800 ms. CPC (Calling Party Control) timer (in milliseconds). Enter the CPC timer value in milliseconds. The range is 250 to 1500ms. CPC is a signal sent from electronic COs to indicate that the Calling Party has hung up. When programming telephone equipment, CPC is also referred to as Open Loop Disconnect. CPC is normally sent as an open (0 volts DC) signal, ranging from 250 to 500 milliseconds. When FXS is on call and the remote party hangs up, FXS sends the CPC disconnect signal to the PBX/key system connected to FXS.
PTime	Default is 20 ms. Packetization Time controls the length of audio (in milliseconds) contained in each RTP packet. This parameter is advertised in the SIP SDP as Ptime.

Parameter	Description
Internal-Distinctive-Ring	Default is 0. Choose the ring index to use for ringing the called phone. Range is Ring-0 to Ring-4. If the Alert-Internal header is missing, a ringing pattern is used based on the distinct ring rules configured on the FXS/Phone Port Distinctive Ring configuration page. The header must look like this: Alert-Info:info=alert-internal
External-Distinctive-Ring	Default is 0. Choose the ring index to use for ringing the called phone. Range is Ring-0 to Ring-4. If the Alert-External header is missing, a ringing pattern is used based on the distinct ring rules configured on the FXS/Phone Port Distinctive Ring configuration page. The header must look like this: Alert-Info:info=alert-external
Alert-Ring-ID	Default is Disabled. This field allows the selection of ring cadence. In most deployments, the country specific default ringing (the default) is chosen.
CallerID-Send-Disable	Default is False. This field controls if Caller-ID data will be sent as part of the ringing process. When True, no Caller-ID data will be sent as part of ringing the device connected to the FXS port.
CallerID-Field-Order	Default is Date-Name-Number. Call-ID data usually consists of date, name and number. This field allows you to choose the order of each element, in the case that end-points that require a specific order.
CallerID-Max-Name-Length	Default is 16. The range is 1 to 24 octets. This field limits the length of the Name element of Caller-ID.
CallerID-Max-Digits	Default is 16. The range is 1 to 24 octets. This field limits the length of the Digit element of Caller-ID.
CID-PRIOR-FIRST-RING	Default is False. CID is sent after the first ring. However, for some country types, this should be enabled to send CID data before the first ring.
Inter-Digit-Delay-Timer	Default is 4 seconds. Enter the maximum delay between two dialed digits in seconds. If a key is not pressed within the defined delay, dialing is auto-completed, and the collected digits are dialed out.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Dial-Completion-Pattern</td><td>Default is empty. Enter the dial-completion pattern that is used to auto-complete the dialed string on the FXS port. Each pattern can be defined in a list separated by the pipe character (“ | ”).
Dial completion pattern formatting:
<table>
<tr><th>Symbol</th><th>Description</th></tr>
<tr><td>.</td><td>Matches one or more digits.</td></tr>
<tr><td>[x-y]</td><td>Matches any single digit between x and y. For example, [1-3] matches 1, 2, or 3.</td></tr>
<tr><td>X</td><td>Matches any digit between 0 and 9, equivalent to [0-9].</td></tr>
<tr><td>Z</td><td>Matches any digit between 1 and 9, equivalent to [1-9].</td></tr>
<tr><td>N</td><td>Matches any digit between 2 and 9, equivalent to [2-9].</td></tr>
<tr><td colspan="2">Dial Completion Pattern Example
911|XXXX|XXXXXXX
If the dialed pattern matched 911 or any 4 or 7 digit number, dial operation is complete and the call is placed.</td></tr>
</table></td></tr>
<tr><td>Howler-Tone-Delay</td><td>Default is 60 seconds. The range is 10 to 120 seconds. When a call ends, but a user forgets to put phone on-hook, this tone is a reminder and play when phone stays off-hook for the set time in this field.</td></tr>
<tr><td>Termination-Impedance</td><td>Default is 600 ohm (for connections less than 5,000 meters in length). Choose the impedance on the outboard port based on the connected analog devices and the length of cable hooking up the device.</td></tr>
<tr><td>Local-Time-Zone</td><td>Default is UTC. Choose the local time zone for FXS ports. The local time zone is used when sending date/time information in CallerID to an analog device connected to the FXS port. For US time zones, daylight savings observation is taken into account.</td></tr>
<tr><td>Country</td><td>Default is USA. Choose the country where the Edge 8000 is located.</td></tr>
</table>

UA Port-Level-Configuration

Introduction

Use the following parameters to configure the analog with port-level configurations.

FXS-Port

Parameter	Description
SIP-Display-Name	Specifies the display name for outbound calling party name purposes.
SIP-User-Name	Identifies the analog phone connected to the FXS port. This value can be either a name or a number that callers use to reach the analog phone. This username is added to the Edge 8300's client list for call routing.
SIP-Authentication-Name	Specifies the name the FXS port uses to authenticate itself if the USE SIP Username for the SIP authentication box is not checked in Global Settings.
Password	Specifies the passwords to authenticate the SIP UA against the softswitch or outbound proxy.
Codec-Preference	Choose a codec type from the Codec Preference drop-down list. Edgemarc chooses this codec when offered by the far end regardless of the order of appearance in the SIP SDP. This selects the codec that is used by all FXS ports for encoding analog data. The codec must be part of the negotiated codec list: G.711 uLaw, G.711 aLaw, G.729, G.728, G.726-16, G.726-24. G.726-32, G.726-40, G723-63, G723-53, G729E, and Global.
Use-Preferred-Codec-Only	Select the **Use preferred codec only** checkbox to specify that only the preferred codec is used when the FXS places a call. The call is rejected if an incoming call does not have the preferred codec.
SIP-User-Domain	Enter a domain in this field to use a value other than the domain configured on the main SIP configuration page.
FXS-Port-Number	This is the port of the FXS channel.

Parameter	Description
Tx-Gain-To-FXS	Choose the analog transmit gain for the FXS port. The default setting of 0dB is appropriate for most installations; however, you can adjust the setting to interoperate with user endpoints such as phones, fax, or key systems. Range is -16dB to 16dB, default is 0dB. **Note** If dealing with echo on line, ensure a delta of at least 6DB between Tx and Rx gain settings.
Rx-Gain-From-FXS	Choose the analog to receive gain for the FXS port. The default setting of 0dB is appropriate for most installations; however, you can adjust the setting to interoperate with user endpoints such as phones, fax, or key systems. Range is -16dB to 16dB, default is 0dB. **Note** If dealing with echo on line, ensure a delta of at least 6DB between Tx and Rx gain settings.
Enable-Echo-Cancellation	Choose the setting for the echo cancellation. The default setting is True. Range of options are: True and False.
Enable-Call-Waiting	Select the Enable Call Waiting checkbox to enable call waiting at the port level.
Enable-Call-Waiting-CallerId	Select the Enable Call Waiting CallerID checkbox to enable call-waiting caller-ID feature at port level.
Max-Number-Call-Waiting-Tone	Specifies the amount of Call Waiting Tones to play. The default value is 2. Range is 2 to 18.
VAD-Enabled	Choose voice activity detection for the FXS port: • Enabled • Disabled • Global Setting—Allows global VAD settings to be applied at the port level.
Hotline-Number	Enter the number that a port calls automatically when it goes off-hook. If the field is empty, the feature is disabled.

Parameter	Description
CallerID-Block	Select the **Restrict CallerID** checkbox to enable endpoint call privacy - user provisioned on the port - in a trusted SIP network (RFC 3325). Caller Identity in From SIP header is restricted and is instead carried in P-Preferred-Identity SIP header. If the endpoint does not trust the proxy that it sends request to, leave the box un-checked.
Disable-Flash-Hook	Select the Disable Flash Hook checkbox and click Submit to disable Flash Hook on SIPUA FXS Ports.

Fax-Settings

Introduction

Use the following parameters to configure the gateway with Fax settings.

FAX Settings

Parameter	Description
Use-T38-For-FAX	Default is True. If disabled, G711ulaw is used to send and receive faxes.
Fax-Bit-Rate	Default is 14400 bps. Choose a rate from the Fax Bit rate (bps) drop-down list. This field specifies the data rate that the fax machine support. **Note**: Super G3/G4 Fax is not supported.
Fax-TCF	Default is Local. Choose the data rate management method for the Training Check Function (TCF) signal. Data rate management is carried out by the emitting gateway, which takes the T30 data and encodes it into T38 packets, port 1 or 2, based on training results from local and remote FAX terminals. This method is used for TCP connections and is optional for UDP. • Local—Requires that the TCF training signal is generated locally by the receiving gateway, which receives the T38 data and translates it into T30 data, port 1 or 2. • Transferred—Requires that the TCF signal is transferred from the emitting gateway to the receiving gateway. In this case, the speed selection is carried out by the G3FEs in the same way as a PSTN connection. This method is mandatory for UDP.

Parameter	Description
Fax-Options	Default is none. Choose special settings for the fax machine: None- No special settings selected. • BitRemoval—Fill bits can be inserted or removed in the Message Transmission Phase C, non-ECM data to reduce bandwidth in the packet network. • TransMMR—Conversion between Modified Modified READ (MMR) T.6 and the line format to increase data compression and reduce bandwidth in the packet network. • JBIGTranscoding—Joint Bi-level Image Experts Group (JBIG) T.30 provides the ability to convert to/from JBIG to reduce bandwidth.
UDP-Max-Buffer	Default is 1024. The range is 200 to 4096 octets. Enter the maximum number of octets that can be stored on the remote device before an overflow condition occurs.
UDP-Max-Datagram-Size	Default is 256. The range is 200 to 512 bytes. Enter the maximum size of a UDP Transport Layer (UDPTL) packet or the maximum size of the payload within an RTP packet that can be accepted by the remote side.
Fax-Error-Correction	Default is Redundancy. Choose the error correction method used by the fax machine.

Distinctive-Ring

Introduction

Use the following parameters to configure a distinctive ring for analog calls.

Distinctive-Ring

Parameter	Description
ID	(READ ONLY)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Caller-Pattern-Match</td><td>Uses the ring pattern if the caller’s phone number matches the pattern.
Caller-Pattern-Match formatting:<table><tr><th>Symbol</th><th>Description</th></tr><tr><td>.</td><td>Matches one or more digits.</td></tr><tr><td>[x-y]</td><td>Matches any single digit between x and y. For example, [1-3] matches 1, 2, or 3.</td></tr><tr><td>X</td><td>Matches any digit between 0 and 9, equivalent to [0-9].</td></tr><tr><td>Z</td><td>Matches any digit between 1 and 9, equivalent to [1-9].</td></tr><tr><td>N</td><td>Matches any digit between 2 and 9, equivalent to [2-9].</td></tr></table></td></tr>
<tr><td>Called-Pattern-Match</td><td>Uses the ring pattern if the called phone number matches the pattern.
Called-Pattern-Match formatting:<table><tr><th>Symbol</th><th>Description</th></tr><tr><td>.</td><td>Matches one or more digits.</td></tr><tr><td>[x-y]</td><td>Matches any single digit between x and y. For example, [1-3] matches 1, 2, or 3.</td></tr><tr><td>X</td><td>Matches any digit between 0 and 9, equivalent to [0-9].</td></tr><tr><td>Z</td><td>Matches any digit between 1 and 9, equivalent to [1-9].</td></tr><tr><td>N</td><td>Matches any digit between 2 and 9, equivalent to [2-9].</td></tr></table></td></tr>
</table>

Parameter	Description
Ring-Type	Choose a ring type from the Ring Type drop-down list: • Ring-2secOn4secOff (default) • Ring-1secOn4secOff • Ring-0.4secOn0.8secOff • Ring-2secOn0.8secOff • Ring-04.secOn0.4secOff • Ring-2secOn4.8secOff • Ring-4secOn4secOff • Disabled

SIP-Gateway

Contents

Edge 8000 GUI's SIP-Gateway hierarchy

Global-Configuration

Introduction

Use the following parameters to configure the SIP gateway with global configuration settings.

Global Configuration

Parameter	Description
Enable-SIP-Gateway	Default is False. This field enables the FXO gateway feature.
SIP-Virtual-IP	Read-only field. This value is hardcoded to 169.254.1.30. The field represents the IP where SIPGW will listen for all SIP/IP requests.
Max-FXO-Port	This field is read-only, with a value of 2. This field is the maximum number of FXO ports.
Add-Dial-Out-Prefix	The range is from 0 to 9. The value to prepend to the Caller-ID received from PSTN to create the FROM field when trunking a call from the PSTN to the IP network.
Register-With-SIP-Server	Register the FXO/GW with the SIP server using Override SIP FROM as SIP username.

Parameter	Description
SIP-SERVER-IP	This field is read-only, with a value of 169.254.1.120. This is the IP address for the SWE Edge SIP communication.
Override-FROM-User-Name	Enter a message to override the system default SIP message FROM field. The FXO/GW registers with this name. **Note**: When the Override FROM field is specified with the SIP username, it replaces Dial Out Prefix and CallerID.
SIP-Authentication-Name	Enter a name and password in the SIP Authentication Name and Password fields only if the SIP FXO/Line port needs to be authenticated.
SIP-Authentication-Password	Enter the password to authenticate the SIP FXO/Line port against the SIP softswitch or outbound proxy. This field is only needed if SIP FXO/Line port must be authenticated.
Override-FROM-Display-Name	Enter a display name to override the default “anonymous” display name. If an override display name is not configured, the system uses information received from the PSTN as part of the CallerID by default. If CallerID feature is not present on the PSTN line, the default is “anonymous.”
CO-Disconnect-Timer	The range is 0 - 60 seconds. Enter the time in seconds for the PSTN CO to terminate the connection. This specifies the time after the SIP caller has hung up for the PSTN CO line to terminate the connection when the call originated from the PSTN through the FXO port. The time is usually 12-13 seconds. During this defined time value, the FXO port is not be available for making any outbound calls to the PSTN.
	Default is False. Select the checkbox to enable priority calling services for FXO ports. When priority call services are enabled, any call placed to a priority calling number from any FXS port or LAN-side SIP phone is routed on priority basis to the FXO port and connected. **Note**: Enabling Priority Calling Services overrides (or hides) the following settings for individual ports: • Enable InBound (from PSTN) two-stage dialing • Forwarded To settings

Parameter	Description
Priority-Call-Number	This is the default callback extension. When priority calling is enabled, all incoming calls are forwarded to this number. When priority calling is not enabled, incoming calls are forwarded to the Forward-To number defined at Port-Level-Configuration.
Priority-Call-Window	Default is 0. Enter the amount of time in seconds during which an inbound call from PSTN is forwarded to the last IP caller that made an outbound priority call through that FXO port. The window starts when an outbound priority call is completed. If the window has lapsed and an inbound call from the PSTN is made, the call is forwarded to the Default Callback Extension instead. This field is only visible when Priority Calling Services are enabled.
PSTN-Track-Window	Default is 0 seconds. The range is 0 - 20 seconds. Enter the amount of time that the gateway senses the port to check if the PSTN line is connected to the FXO port and the line is alive. If there is no analog signal during this sensing period, the call is rejected with a “486” error.
Inter-Digit-Delay	Default is 300 ms. The range is 100 - 2000 ms. Enter the delay in milliseconds between dialed digits to the PSTN.

Port-Level-Configuration

Introduction

Use the following parameters to configure the specific FXO port.

Port-Level-Configuration

Parameter	Description
FXO-Port	READ-ONLY VALUE: 0 or 1
Enable-FXO-Port	Select the **Enable FXO port** dropdown to enable the FXO/Line port for incoming and outgoing calls. When this field is not checked, the FXO/Line port is disabled. The options are True and False.

Parameter	Description
Two-Stage-Dialing-From-IP	Select the Enable InBound (from IP network) two-stage dialing dropdown to allow two-stage dialing for incoming calls from the IP network. The options are True and False. Default is False
Two-Stage-Dialing-From-PSTN	Select **Enable InBound (from PSTN) two-stage dialing** to allow two-stage dialing for incoming calls from the PSTN. Provides dial tone when a call is answered. The caller can then dial an extension to further complete the call or hang up. The options are True and False. Default is False.
Forward-To	If the **Enable InBound (from PSTN) two-stage dialing** is not selected, enter a name or number in the Forward to field to automatically forward incoming calls from the PSTN to this name or number.
PSTN-Incoming-Accept-Method	Provides a connection for a call from PSTN to IP under two conditions: 1. If caller ID is detected, then a call connects. 2. When using a simple ring detect, connect the call to IP. The options are **CallerID Detection** and **Ring Detected Counts**. Default is CallerID Detection.
PSTN-Accept-Ring-Counts	Provide the **PSTN Accept Ring Counts** value to define the number of rings to connect to the IP. This value applies when the ring is selected as an accepted method. The range is 2 to 8.
Tx-Gain	Choose the Analog Transmit gain. Control the gain of media signal coming to FXO from IP side. The options are in the following list (Default is 0db). **Note**: In cases where the default value does not optimize echo cancellation, adjust the gain with -6DB in steps to -10DB until the echo is gone.
Rx-Gain	Choose the Analog Receive gain. Control the gain of media signal coming to FXO from PSTN side. Based on the line conditions, sometimes the level of the DTMF signal needs to be boosted to make DTMF detection more reliable. Default is 0dB.

PRI-Setting

Contents

Edge 8000 GUI's PRI-Setting hierarchy

T1-Common Setting

Introduction

Use the following parameters to configure encoding and framing settings for all T1 ports.

T1-Common Setting

Parameter	Description
SIP-SERVER-IP	(READ ONLY) Indicates the IP of the SIP server (SWE Edge SIP IP - 169.254.1.120) to which all SIP/IP requests will be sent if the PRI feature is enabled on the interface.

Parameter	Description
Framing Mode	Specifies either T1 or E1. Framing Mode Defines the number of frames that are grouped together for T1. • T1—All T1 Framed modes use a 193-bit frame supporting one framing bit and 24 8-bit channels. There are 8000 frames per second with 1544000 bits per second data rate. ◦ ESF—Extended Super Frame groups 24 193-bit frames together, making a 24-bit frame word. Six of the 24 bits are used for the framing pattern, and the other 18 bits are used for other services. ◦ SF—Super Frame groups 12 193-bits frames together, making a 12 bit frame word. All 12 bits for the framing word are used for the framing pattern. • E1—E1 supports three framing modes and an unframed mode. E1 Framed mode has a 2.048Mbit channel divided into 32 basic channels. Channel 0 is always reserved for framing and cannot be used for media. Channel 16 is the signaling channel and is used for different purposes. E1 frames are 256 bits (32 x 8bits). There are 8000 frames per second with 2048000 bits per second data rate. ◦ Double Frame—Basic E1 mode. Two frames are form a 16-bit framing word (2 8bit samples of channel 0). PRI can be used, and channel 16 is typically used for the D-channel. No cyclic redundancy check (CRC) is performed in this mode. ◦ Multi Frame CRC—Groups 16 256-bit frames together, creating a 128-bit framing word. Some of the framing bits are used to add a CRC-4 error check. PRI can be used, and channel 16 is typically used for the D-channel. ◦ Unframed—No framing support and can be used for data. The options are F24-ESF and F12-D3-D4.
Line-Encoding	Defines the bit encoding method used while transmitting data over the line. B8ZS (Bipolar 8 bit zero substitution) and AMI (Alternative Mark Inversion) are currently supported. The options are B8Z2 and AMI.

T1-Configuration

Introduction

Configuration settings applicable to specific T1 ports.

T1-Configuration

Parameter	Description
T1-Line	READ-ONLY Value: 0, 1, 2 or 3
Line-Build-Out	Configures the power and attenuation characteristics of the transmit signal from T1 interfaces. The default value is 0-133ft. Select one of the following values: • -22.5db • -15.0db • -7.5db • -0.0db • 0-133ft • 133-266ft • 399-533ft • 533-655ft
PRI-Enable	Specifies that the T1 port will be used for PRI. The default setting is False.

Net-Side

Introduction

The Network side PRI enables the Edge 8000 to provide a standard ISDN PRI network-side interface to a PBX. This allows the Edge 8000 to be used with most legacy TDM PBXs.

Net-Side

Parameter	Description
PRI-Line	(READ ONLY)
T1-Trunk-Switch-Type	Enter the switch type that client-side ISDN PRI will be simulating. NI2 is selected by default. The switch type must match the Network-side switch type to which this interface is connected.
T1-D-Channel-Number	Choose a number from the D Channel drop-down list to use for Q.931 signaling.
Internal-Clocking	Select the **Internal clocking** checkbox to set the internal clocking mode for PRI. External clocking is used by default.
Device-Name	If caller information is not available in a call coming into the PRI trunk from the remote PRI/T1 link, enter a device name for the SIP FROM user.

Parameter	Description
Enable-SIP-Update	When enabled, the SIP update is shown in the Supported Header.
B-Channel-Order-Descending	Select the **B Channel** checkbox to change the B channel order to descending (24-1). By default, when setting up a call, B channel ordering is ascending (1-24).
International-Prefix	Enter the value to prepend as an international prefix to the dialed number when a call of type international is received from the PRI. No action is taken if the field is empty or a prefix is already part of the called number.
Jitter-Buffer	Enter the jitter buffer value based on the IP network condition. Value is equal to or greater than 40 ms. The default is 100 ms. The range is 40-200ms.
Jitter-Buffer-Type	Choose the Jitter buffer type from the drop-down list: • **Fixed (Default)** • **Adaptive**
Register-With-SIP-Server	Enable **Register with SIP server** if your SIP service provider requires endpoints to be registered. The SIP Authentication name and password is used in the registration request.
Override-From-Enable	Enable override SIP FROM user name. The options are True and False.
Override-FROM-User-Name	Enter a name to override the system default DISPLAY name when sending an SIP request to the IP side. A call coming in Network-side PRI/GW from the PBX is terminated on the IP network. By default, the gateway uses the PRI callerID in the FROM field of the SIP INVITE message when terminating the call on the IP side. If the callerID is absent, the gateway uses the specified internal name.
SIP-Authentication-Name	If the gateway registers with the name defined in the Register FROM Username field, enter the SIP authentication name used to authenticate the PRI/GW.
SIP-Authentication-Password	Define the SIP authentication password used to authenticate the PRI/GW in case GW registers with the name defined in the 'Register FROM Username' field.

Parameter	Description
Override-FROM-Display-Name	When sending SIP requests to the IP side, enter a name to override the DISPLAY name. An Inbound call coming into PRI/GW from the remote PRI/T1 link is terminated on the IP network. By default, the gateway uses this name as part of the DISPLAY name in the SIP FROM header.
Disable-Facility-IE	The Caller's Name is carried in FACILITY IE but sometimes in DISPLAY IE. When true, the caller's name is carried in the DISPLAY IE.
Codec-Preference	Select the preferred codec. When making a call, this codec will be the first one offered. When receiving a call, if this codec is part of the negotiated codec list, it will be used to encode and send voice packets.
Use-Preferred-Codec-Only	Select the **Use Preferred codec only** checkbox to use your selected codec preference as the only codec offered or responded to in the call setup. All other calls are rejected.
Handle-PROGRESS	This is relevant when making inbound calls from PRI to PBX. A PROGRESS message is sent from PBX in response to a PROG indicator in the SETUP message. However, some PBX sends this message regardless. Since SETUP did not ask for PROGRESS, this message is ignored by default. Select the **Handle PROGRESS** config to handle this PBX behavior. This will ensure that PROGRESS is handled and an appropriate SIP message is generated.
Enable-RTCP	Select the **Enable RTCP** checkbox to enable RTCP support for voice media. The Enable-RTCP is True/False and False is default.
RTCP-Interval	Specifies the interval at which the RTCP report is sent. The default is 5, and the range is from 1-30 sec.
Display-IE-Enable	Displays the info in the DISPLAY IE, regardless of facility IE settings.
Enable-VAD	Select the **Enable VAD** checkbox to enable Voice Activity Detection (VAD) support for voice media.
Disable-RFC2833-Outbound	When enabled for any OB call, PRI will not advertise the support for RFC2833 when making a call to IP. The options are True and False. The default is False.

Parameter	Description
Disable-RFC2833	With DSP-based PRI solutions, RFC2833 (out-of-band tone-events) is enabled by default. The options are True and False. The default is False.
RFC2833-Event-Payload	DTMF packets will send with configured payload type when any DTMF key pressed. The values range from 100-101. The default value is 100.
Channel-Release-Time	The value indicates the time in hours after which the PRI client-side channel will be pre-empted for a new call if no other channel is free.Default is disabled if the parameter is absent or the value is 0. The default is 0 hours.
T200-Timer-Value	Value of T200 Timer in Milliseconds for ISDN signaling. Added for interoperability with Ancient Merlin-Magic PBX. A value of 1110 works well with Merin-Magic. Must be used with caution. The range is 1010 to 2000ms.
T200-Retry-Count	Value of T200 timer retries before declaring error.Added for interoperability with Ancient Merlin-Magic PBX. A value of 5 works well for Merlin-Magic. Must be used with caution. The range is from 3 to 10.
Enable-FAX-Modem-Support	PRI will monitor FAX/MODEM tones in a voice call when enabled. If a tone is detected, PRI will automatically change the voice call to FAX/MODEM data call. To enable T.38 FAX, define the T.38 configuration.
PRI-Gateway-Virtual-IP	(READ-ONLY) The IP address is hardcoded to 169.254.1.50. The SIP IP address on the PRI Gateway used for communication with SWE Edge.
Service-Message-Protocol-Rev-1	Displays the ISDN maintenance message with two revs. Select one of the options based on PBX support. The default is false.
DTMF-Max-Time	Default is 0. Range 0 or 50-300.
Enable-Port-Admin	An internal variable is defined if a remote party has asked a specific b-channel to be turned off when sending a service maintenance message. This variable should not be defined by any external config. It is applicable in fractional T1/PRI configurations.The options are True and False. The default is True.
Bring-B-Channel-Down	Define to bring down all active calls if d-channel on PRI goes down. One-off config for a customer to interop. The options are True and False. The default is False.

Parameter	Description
Send-B-Channel-Restarts	Define to force B-channel to restart SERVICE message when D-channel connects. One-off config for customer Interop. The options are True and False. The default is False.
Enable-Early-Media	This is relevant when making outbound calls from PBX to PRI. After sending ALERT with Early Media indication, PRI sends CONNECT to the PBX when enabled. Some PBXs will not cut-through media if CONNECT is not sent after Early Media, and so if a PBX user is trying to access an IVR, DTMF from the PBX user will not be sent to IVR.

B Channel Setting

Parameter	Description
B-Channel	(READ-ONLY)
Enable	Select the **Enable** check-box for each PRI channel you want to enable during the call. The options are True and False. The default is True.
Enable-Port-Admin	Set the value to false to send a maintenance message to disable this channel on the remote side. If the remote decides to disable the channel, this status will reflected as False. The options are True and False. The default is True.

PRI-IE-Setting

Introduction

The page defines the Information element settings sent as part of the ISDN SETUP and DISCONNECT messages. For most of the deployment, no configuration change is needed.

PRI-IE-Setting

Parameter	Description
SETUP-Channel-Slotmap	Enable this setting to send a B Channel number as a number or a bitmap in the setup message.
SETUP-Chan-Prefered-Exclusive	Enable this setting to send a B Channel number in the setup message with an exclusive flag. The default is Preferred.

Parameter	Description
Enable-DISC-Progress-Indicator8-IE	Enable this setting to add Progress Indicator 8 IE in the Disconnect message and play a local busy tone to the caller at the PRI User side. Default is Disabled.

FAX-Setting

Introduction

Use the following parameters to configure the PRI with Fax settings.

FAX-Settings

Parameter	Description
Enable-FAX-T38	Use this setting to enable or disable the FAX T38 feature.
Fax-Bit-Rate	This field determines the bit rate in bps. The maximum rate is 14400 bps. Note: Super G3/G4 Fax is not supported.
Fax-TCF	This field is used to select the method for the Training Check Function signal. Options are Local or Transferred (from the emitting gateway to the receiving gateway).
Fax-Options	Options include Default, BitRemoval, TransMMR, or JBIG Transcoding.
UDP-Max-Buffer	Default is 1024. The range is 200 to 4096 octets. Enter the maximum number of octets that can be stored on the remote device before an overflow condition occurs.
UDP-Max-Datagram-Size	Default is 256. The range is 200 to 512 bytes. Enter the maximum size of a UDP Transport Layer (UDPTL) packet or the maximum size of the payload within an RTP packet that can be accepted by the remote side.
Fax-Error-Correction	Default is Redundancy. Choose the error correction method used by the Fax machine.
MAX-T38-Session	Limits the number of fax sessions allowed. On 4808DB, the max limit is 5. On 4808 the Max limit is set to 9. Since the tone-detection and Fax is done in the software, this is to limit the CPU resources.

Parameter	Description
Ignore-FAX-Over-Audio	If enabled, any invite that comes with mutiple media in SDP, one for voice and one of T.38, T.38 media will be ignored. This is special case for some soft switch.
Offer-T38-Outgoing	The Fax-over-IP recommendation is to have the Receiving T.38 gateway always offer the T.38 if FAX is detected. Some gateway implementations break that and do not offer T.38. When this is true, even the sending gateway will offer the T.38.
Enable-ADTRAN-T38-Interop	Default is False. When True, Redundance Recovery mode is forced for better interop.

Related Documents

Contents

Overview

Edge 8000 Series devices consist of several key components, including 6WIND Router, RAMP, and SBC SWe Edge. This section provides links to available documentation about the components.

6WIND Router Documentation

To access 6Wind router documentation, click 6Wind Router Documentation.

RAMP Documentation

To access Ribbon Application Management Platform (RAMP) documentation, click Ribbon Application Management Platform

SBC Edge Documentation

To access SBC Edge documentation, refer to SBC Edge Portfolio Documentation.

> **Note**
>
> The SBC Edge Portfolio Documentation describes all the SBC Edge products, including the SBC SWe Edge which is the application included with the Edge 8000 Series.