



**AudioCodes SBC**  
**in**  
**Microsoft Teams Environment**  
**Essentials & Configuration**

Geoffrey Ruff | Americas Training Manager

**AudioCodes Academy**

<https://www.audiocodes.com/services-support/audiocodes-academy>

- After completing this course, you will be able to:
  - Configure AudioCodes equipment using various management tools
  - Understand the operating, maintenance and monitoring tools of AudioCodes equipment
  - Troubleshoot and debug AudioCodes equipment
  - Integrate the Mediant E-SBC in the Microsoft Teams environment that require integrated voice components
  - Become familiar with Teams for Business related voice configuration aspects
  - Become familiar with SBC application functionalities
  - Understand the Survivability concept

# Lessons & Course Time Table



## Day 1

[AudioCodes Introduction](#)

[AudioCodes Management Interface Introduction](#)

[AudioCodes Documentation](#)

*Hands-on Lab 1 – Management Interface Usage*

[GWs & SBC Product Line](#)

[SBC Application Description](#)

## Day 2

[SBC Basic Terminology](#)

[SBC Configuration](#)

[SBC Wizard](#)

[Debugging Tools](#)

*Hands-on Lab 2 – SBC Routing*

## Day 3

[Teams System Overview](#)

[SBC Configuration for Teams](#)

*Hands-on Lab 3 – Teams to SIP Trunk Connection*

[SBC Number & Message Manipulation Introduction](#)

*Hands-on Lab 4 – SBC Message Manipulation*

## Day 4

[Digital GWs Basic Configuration](#)

[SBC Survivability](#)

*Hands-on Lab 5 – SBC Survivability*

[SBC High Availability](#)

**Certification Exam**



## Lesson 1

# AudioCodes Introduction



# AudioCodes in a glance



- Market leader in VoIP networking products
- Deployed in over than 100 countries in service provider and enterprise networks
- Recognized brand for quality & performance
- Global partnerships with leading telecom players
- Large Fortune 100 install base
- Over 600 employees, ~40% R&D
- More than 25 years of VoIP expertise
- Public since 1999 (NASDAQ:AUDC)



# Global Presence and Support

- Worldwide presence:
  - Headquarters: Israel
  - North America: USA and Canada
  - APAC: Japan, Singapore, Korea, China, India, Australia, Hong Kong
  - EMEA: UK, France, Netherland, Germany, Russia, Italy, South Africa, Poland, Sweden
  - CALA: Miami, Brazil, Mexico, Argentina, Colombia
- Global Distribution Network covering more than 100 countries
- Support Centers covering all time zones
- 3 Logistics Centers in North America, EMEA and APAC

- 49 of Fortune 100 enterprises are using AudioCodes technology
- Hundreds of multinational enterprises
- Energy, Finance and Insurance, Industrial engineering, Food, Commerce, Government and Defense, Pharmaceuticals, High Tech, Automotive
- Thousands of mid-market customers via Service Providers and resellers



# Broadest Portfolio of Products



## Management/Apps



Routing Manager



OVOC



Apps

## IP Phones



405



420



430



440



445



450



UC-HRS Speakers

## Pure SBC



Mediant 2600



Mediant 4000/B



Mediant 90xx



Mediant SE Software Edition

## Virtual & Cloud SBC

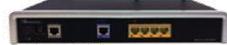


Mediant VE (Virtual Edition)



Mediant CE (Cloud Edition)

## Hybrid SBC/Gateway



Mediant 500/L



Mediant 800/B/C



Mediant 1000B



Mediant 3000\*

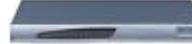
## Gateways/Adaptors



MP-2xx



MP-1xx



MP-124



MP1288

## Covering all aspects of VoIP solutions

Coexistence,  
Migration &  
SIP Trunking



Security  
& Fraud  
Prevention



Devices &  
Productivity



Compliance &  
Recording



Resiliency &  
Recovery



All-in-One  
Voice  
Solution

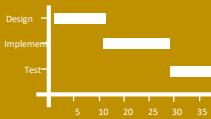


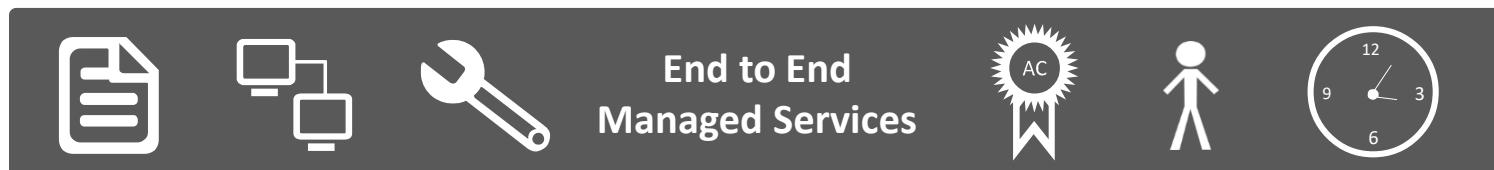
Professional Services & Support



# The Voice Experts @ Your Service



Project Management 	Planning & Design 	Site Survey, Installation & Implementation 	Network Voice Readiness Assessments 	AudioCodes Academy 
24x7 Technical Support 	Hardware Replacement 	Local Technician Dispatch 	Software Upgrades 	Remote Monitoring 



- Full product life cycle
- Plan
  - Determine the right solution and best practices for any project's needs
- Implement
  - Achieve smooth voice implementations with global physical installation and configuration
- Operate
  - Prompt technical support, efficient hardware replacement and ongoing software and hardware upgrades





## Expert

We know our products best - Faster service, better and faster solutions with leading team of specialists



## Complementary

A broad portfolio of services designed to complement partners' own offerings, facilitating a complete solution to the customer



## Global

AudioCodes and AudioCodes-branded service partners are present in over 190 countries, allowing partners to go to market worldwide

- **ACTS:** Direct Support – Tier 2 – 4 (9 x 5 or 24 x 7)
- **CHAMPS:** Back-to-Back Support – Tier 3 – 4 (9 x 5 or 24 x 7)
  - Not including installation, configuration, and provisioning (which can be purchased separately)
  - Support available after AudioCodes products are implemented and in service
  - Support is provided based on serial number entitlement check Extended Hardware Warranty (RMA) included
  - Software Maintenance and all S/W upgrades, patches, maintenance releases and major version releases
  - Certificate of Eligibility issued with each purchase

- AudioCodes Academy offers a comprehensive set of technical training courses for AudioCodes' partners and customers
  - Designed to enable Partners and Customers to successfully install, integrate, configure, and support AudioCodes solutions
  - Instructor-Led
  - Combination of lecture and deep hands-on training with AudioCodes equipment
  - Certification testing at conclusion of each course
  - Certifications are valid for two years



Empowering your networking experts

Learn from the experts

Comprehensive set of technical  
training courses

Flexible course delivery

- Two types of Certification Levels:

- ACA – AudioCodes Certified Associate
  - Basic level certification
  - Required for the installation and maintenance of AudioCodes devices



- ACP – AudioCodes Certified Professional
  - Advanced level certification
  - Required for the installation, maintenance and advanced troubleshooting of all AudioCodes networking products in advanced customer scenarios
  - Prerequisite: ACA certification and 6 months of field experience as ACA



\* Certificates are valid for two years

# Technical Training – Career Certifications

- **Record of Participation courses:**

- AudioCodes SBC: Fundamentals
- AudioCodes CCE: Installation & Configuration
- AudioCodes Routing Manager (ARM)
- AudioCodes OVOC
- VoIP and SIP Fundamentals



- **ACA courses:**

- AudioCodes SBC: Essentials & Configuration
- AudioCodes SBC in Cloud Environments: Essentials & Configuration
- AudioCodes SBC in Microsoft Skype for Business Environment: Essentials & Configuration
- AudioCodes SBC in Microsoft Teams Environment: Essentials & Configuration
- AudioCodes SBC in Microsoft O365 Environment: Essentials & Configuration
- AudioCodes Enterprise GW: Essentials & Configuration
- AudioCodes MSBR: Essentials & Configuration
- AudioCodes Mediant 3000

- **ACP courses:**

- AudioCodes SBC: Advanced Interworking & Security
- AudioCodes SBC: Advanced Routing & Multitenancy

[SOLUTIONS & PRODUCTS](#)[SERVICES & SUPPORT](#)[PARTNERS](#)[Library](#)[Contact us](#)[Partner login](#)

# Skype for Business & Microsoft Teams

Solutions for cloud, hybrid and on-premises deployment

[EXPLORE MORE](#)[Skype for Business & Microsoft Teams](#)[Service Providers](#)[Contact Centers](#)[Get in touch](#)



## Lesson 2

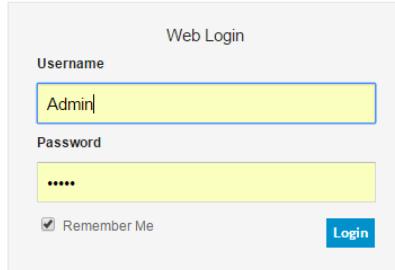
# AudioCodes Devices Management Interface Introduction



- After completing this lesson you will:
  - Be familiar with the AudioCodes GUI
  - Know how to assign IP Networking parameters
  - Be acquainted with the Maintenance Interface
  - Understand ini file structure
  - Know how to upgrade/downgrade firmware
  - Know how to update the License Key

# Management and Maintenance Options

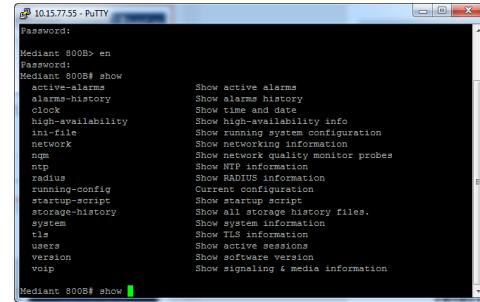
## Embedded Web Server



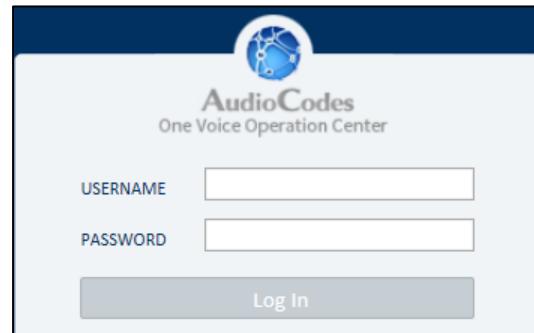
## Configuration file referred to as the *ini* file

```
;*****
;** Ini File **
;*****  
  
;Board: M800B
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 5299378
;Slot Number: 1
;Software Version: 7.20A.154.052
;DSP Software Version: 5014AE3_R => 721.09
;Board IP Address: 10.15.77.55
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 10.15.0.1
;Ram size: 512M  Flash size: 64M  Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 30
;Num of physical LAN ports: 4
;Profile: NONE
;Key features:
;  Board Type: M800B
```

## Command Line Interface (CLI)



## REST-based programs (such as AudioCodes' OVOC)



# Assigning Networking Parameters



- HTTP using Web browser
- BootP
- DHCP
- Console/CLI

# Default Factory IP Address

Product	Default
MP-11x	FXS and FXS/FXO devices – 10.1.10.10
MP-124	FXO devices – 10.1.10.11
MP-1288 Mediant 500 E-SBC Mediant 800 E-SBC Mediant 1000 E-SBC Mediant 2600/4000 SBC Mediant 9000 SBC Software SBC (Mediant SE/VE)	192.168.0.2/24
Mediant 500L MSBR Mediant 500 MSBR Mediant 800 MSBR	LAN Data – 192.168.0.1/24 ( <u>DHCP Server enable</u> ) LAN Voice – 192.168.0.2/24 WAN Data – DHCP Client

- Disconnect the SBC from the network and connect it to a PC
- Change the PC's IP address and subnet mask to correspond with the SBC's factory default networking parameters
- Open a Web browser and access the Web interface
- Change the networking parameters via 'IP Interfaces'
- Reconnect the SBC and your PC to the network
- Restore your PC's IP address and subnet mask to their original settings

# Assigning IP Address – HTTP

audiocodes

SETUP MONITOR TROUBLESHOOT

M500 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions ▾ Entity, parameter, value

SRD All

**NETWORK VIEW**

**CORE ENTITIES**

**IP Interfaces (1)**

- Ethernet Devices (1)
- Ethernet Groups (12)
- Physical Ports (12)
- Static Routes (0)
- HA Settings**
- HA Network Monitor (0)
- NAT Translation (0)

**SECURITY**

TLS Contexts (1)

Firewall (0)

Security Settings

QUALITY

DNS

WEB SERVICES

HTTP PROXY

RADIUS & LDAP

ADVANCED

**IP Interfaces (1)**

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	O+M+C	OAMP + Media + Control	IPv4 Manual	192.168.0.2	24	0.0.0.0	0.0.0.0	0.0.0.0	vlan 1

#0[O+M+C]

Edit

**GENERAL**

Name: O+M+C

Application Type: OAMP + Media + Control

Ethernet Device: # [vlan 1] [View](#)

**IP ADDRESS**

Interface Mode: IPv4 Manual

IP Address: 192.168.0.2

Prefix Length: 24

Default Gateway: 0.0.0.0

**DNS**

Primary DNS: 0.0.0.0

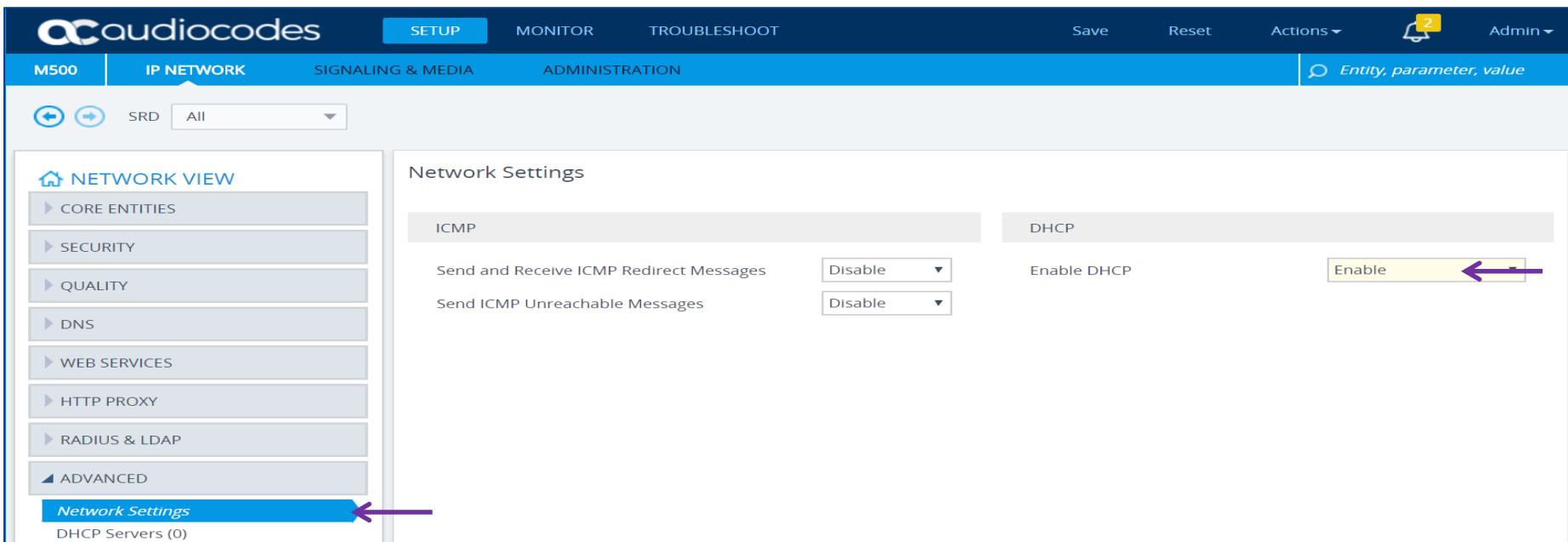
Secondary DNS: 0.0.0.0

[IP Interface Status Table >>](#)

- Bootstrap Protocol allows a host to configure itself dynamically
- Provides two main services:
  - Assigns IP address and networking parameters
  - Provides the name of the software (cmp) file and configuration (ini) file to be loaded by the device (via TFTP)
    - Provides the IP address of the TFTP server
- MediaPack
  - Hardware reset triggers a BootP request
- Mediant
  - BootP request on startup is not supported on Mediant SBCs
  - To force a BootP request, press the Reset button for 30 seconds (Rescue Mode)

# Assigning IP Address – DHCP

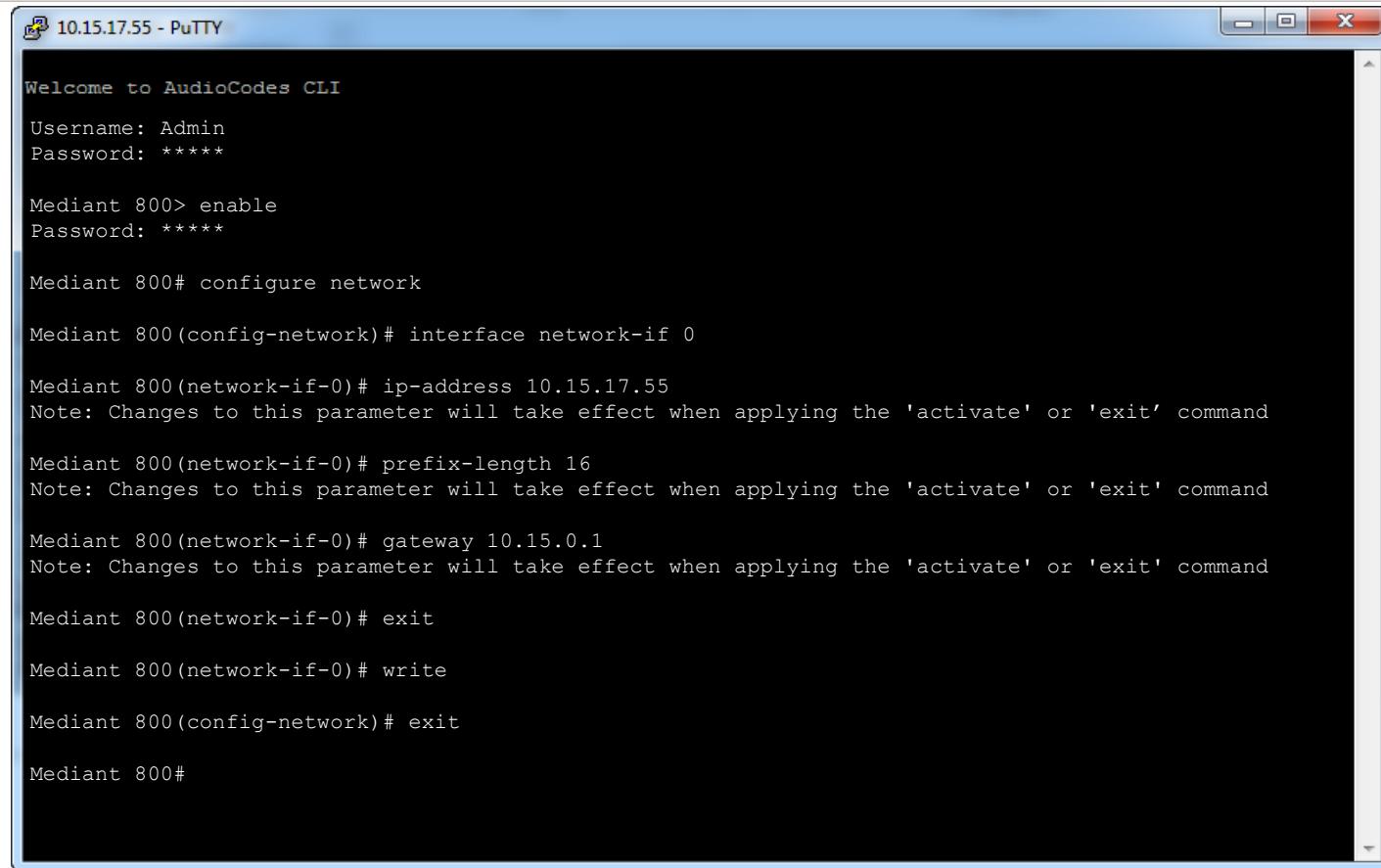
- Dynamic Host Control Protocol – provides a mechanism for allocating IP addresses dynamically so that addresses can be reused
- After the Device is powered up if DHCP is enabled (`DHCPEnable = 1`), the Device attempts to obtain its IP address and other network parameters from the DHCP server



The screenshot shows the audiocodes M500 web interface. The top navigation bar includes the audiocodes logo, a search bar, and tabs for SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, and Admin. The main menu on the left lists categories like CORE ENTITIES, SECURITY, QUALITY, DNS, WEB SERVICES, HTTP PROXY, RADIUS & LDAP, and ADVANCED. The ADVANCED section is expanded, showing **Network Settings** and **DHCP Servers (0)**. A blue arrow points to the **Network Settings** link. In the center, the **Network Settings** page displays the **Network Settings** section. It has two tabs: ICMP and DHCP. Under the ICMP tab, there are dropdown menus for "Send and Receive ICMP Redirect Messages" (set to Disable) and "Send ICMP Unreachable Messages" (set to Disable). Under the DHCP tab, there is a dropdown menu for "Enable DHCP" which is set to **Enable**, with a purple arrow pointing to it.

- Establish a Console (VGA or COM) or CLI (Telnet/SSH) session with the device
- Use these communications port settings:
  - Baud Rate: 115,200 bps
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
- At the CLI prompt, type the following (case sensitive):
  - Default Username: Admin
  - Default Password: Admin

# Assigning IP Address – RS-232



10.15.17.55 - PuTTY

```
Welcome to AudioCodes CLI

Username: Admin
Password: *****

Mediant 800> enable
Password: *****

Mediant 800# configure network

Mediant 800(config-network)# interface network-if 0

Mediant 800(network-if-0)# ip-address 10.15.17.55
Note: Changes to this parameter will take effect when applying the 'activate' or 'exit' command

Mediant 800(network-if-0)# prefix-length 16
Note: Changes to this parameter will take effect when applying the 'activate' or 'exit' command

Mediant 800(network-if-0)# gateway 10.15.0.1
Note: Changes to this parameter will take effect when applying the 'activate' or 'exit' command

Mediant 800(network-if-0)# exit

Mediant 800(network-if-0)# write

Mediant 800(config-network)# exit

Mediant 800#
```

After '**exit**' the address changed. Logon again using the [new IP address](#)

# Configuration File (ini file)

```
;*****
;** Ini File **
;*****  
  
;Board: Mediant 1000  
;HW Board Type: 47 FK Board Type: 71  
;Serial Number: 3929294 ←  
;Slot Number: 1  
;Software Version: 7.20A.200.016 ←  
;DSP Software Version: 624AE3=> 660.15  
;Board IP Address: 10.15.10.5  
;Board Subnet Mask: 255.255.0.0  
;Board Default Gateway: 10.15.0.1  
;Ram size: 512M Flash size: 64M  
;Num of DSP Cores: 20 Num DSP Channels: 120  
;Num of physical LAN ports: 7  
;Profile: NONE  
;SBC Sessions Capability:  
; Local License: 200 SBC Sessions (up to 200 if all legacy telephony inter.  
; Pool License: 0 SBC Sessions (from License Pool Manager)  
; Total (Actual): 0 SBC Sessions (up to 200 if all legacy telephony inter.  
; TDM Sessions Used for SBC Sessions: 50  
; Key features:  
; Board Type: Mediant 1000  
; DSP Voice features: RTCP-XR AMRPolicyManagement  
; Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol  
; Channel Type: DspCh=150 IPMediaDspCh=150  
; HA  
; DATA features:  
; IP Media: Conf VoicePromptAnnounc(H248.9)  
; PSTN Protocols: CAS  
; Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC  
; QOE features: VoiceQualityMonitoring MediaEnhancement  
; PSTN FALLBACK Supported  
; E1Trunks=6  
; FXSPorts=24  
; FXOPorts=24  
; E&M Ports=18  
; BRITrunks=18  
; Control Protocols: MSFT TRANSCODING=200 FEU=200 TestCall=100 SIPRec=100  
; Default features:  
; Coders: G711 G726
```

Serial Number = Decimal representation of the last 6 digits of the MAC address (i.e., 00:90:8F:**3B:F4:CE**)

**7.20** – Major software version

**A** – Indicates that this is a SIP version (e.g., not Megaco)

**200.016** – Minor software version

# Configuration File (ini file)

```
[WEB Params]

UseRProductName = 'AudioCodes'
LogoWidth = '145'
WebLogoText = 'M1KB Group 1'
HTTPSCipherString = 'RC4:EXP'
;HTTPSPkeyFileName is hidden but has non-default value
;HTTPSCertFileName is hidden but has non-default value

[SIP Params]

LOCALSIPPORT = 5040
MEDIACHANNELS = 120
SIPDESTINATIONPORT = 5080
GWDEBUGLEVEL = 5
TCPLOCALSIPPORT = 5040
TLSLOCALSIPPORT = 5041
RETRYAFTERTIME = 300
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10485760
HTTPProxyApplication = 1
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port, PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_0_1", 1, 4, "User Port #0", "GROUP_1", "Active";
PhysicalPortsTable 1 = "GE_0_2", 1, 4, "User Port #1", "GROUP_1", "Redundant";
PhysicalPortsTable 2 = "GE_4_3", 0, 4, "User Port #2", "None", " ";
PhysicalPortsTable 3 = "GE_4_4", 0, 4, "User Port #3", "None", " ";
PhysicalPortsTable 4 = "FE_5_1", 1, 4, "User Port #4", "GROUP_3", "Active";
PhysicalPortsTable 5 = "FE_5_2", 1, 4, "User Port #5", "GROUP_3", "Redundant";
PhysicalPortsTable 6 = "FE_5_3", 1, 4, "User Port #6", "GROUP_4", "Active";
PhysicalPortsTable 7 = "FE_5_4", 1, 4, "User Port #7", "GROUP_4", "Redundant";
PhysicalPortsTable 8 = "FE_5_5", 1, 4, "User Port #8", "GROUP_5", "Active";
PhysicalPortsTable 9 = "FE_5_6", 1, 4, "User Port #9", "GROUP_5", "Redundant";
PhysicalPortsTable 10 = "FE_5_7", 1, 4, "User Port #10", "GROUP_6", "Active";
PhysicalPortsTable 11 = "FE_5_8", 1, 4, "User Port #11", "GROUP_6", "Redundant";
```

- The ini file can be loaded via BootP/TFTP, Web interface, or using the automatic update mechanism
- Case insensitive
- Lines beginning with semi-colon (;) as first character are ignored
- Carriage Return must be each line's final character
- Number of spaces before and after equal ( = ) is irrelevant
- Values of string parameters must be placed between two single quotes ( ' ' )
- Syntax errors in value can cause unexpected errors (may be set to wrong values)
- Syntax error in the parameter name is ignored (error message is generated)
- When a parameter is missing from the ini file, its default is assigned
- Subsection names are optional

```
[Sub Section Name]
Parameter_Name = Parameter_Value
Parameter_Name = Parameter_Value
; REMARK
```

- Tables are used in ini files to represent parameters that have several instances (e.g., Coders, Proxy servers, Routing tables, etc.)
- Examples:

```
[ Authentication ]
FORMAT Authentication_Index = Authentication_UserId, Authentication_UserPassword;
Authentication 0 = "port 1", "pass 1";
Authentication 1 = "port 2", "pass 2";
Authentication 2 = "port 3", "pass 3";
[ \Authentication ]

[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode,
InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 6, 10, 10.15.7.70, 16, 10.15.0.1, 1, VOICE, 0.0.0.0, 0.0.0.0, ;
InterfaceTable 15 = 11, 10, 10.15.7.130, 16, 0.0.0.0, 1, DATA, 0.0.0.0, 0.0.0.0, ;
[ \InterfaceTable ]
```

# AudioCodes INI Viewer & Editor



- A simple viewer and editor for configuration (INI) files used by AudioCodes Media Gateway and Session Border Controller (SBC) products

- Two Modes:

- View Mode:

- Standalone and Table parameters can be viewed in a very friendly way

- Edit Mode:

- Standalone and Table parameters can be edited (modified, added, removed, etc.) for a very easy way of changing their contents

- Once this is done, the new INI file can be saved and uploaded to the device in order to apply the new configuration

```
BOARD_SN5685437 (5).ini - INI Viewer & Editor
File Edit Help
View Edit
[SYSTEM Params]
SyslogServerIP = 10.15.183.183
EnableSyslog = 1 (Enable)
NTPServerUTCOffset = 3600

;VpFileLastUpdateTime is hidden but has non-default value
DialPlanFileName = 'dialplan_lab1v2.dat'
DayLightSavingTimeStart = '01:SUN/01:00:00'
DayLightSavingTimeEnd = '01:SUN/01:00:00'
NTPServerIP = '0.0.0.0'

;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]
PCMLawSelect = 1 (ALaw)
TDMBusClockSource = 4 (network)
ExtBootPReqEnable = 1
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[ControlProtocols Params]
AdminStateLockControl = 0

[MEGACO Params]
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]
ProtocolType = 1 (acPROTOCOL_TYPE_E1_EURO_ISDN)
FramingMethod = c (e1-framing-miff-crc4-ext)
```

```
BOARD_SN5685437 (5).ini - INI Viewer & Editor
File Edit Help
View Edit
[SYSTEM Params]
SyslogServerIP = 10.15.183.183
EnableSyslog = 1 (Enable)
NTPServerUTCOffset = 3600

;VpFileLastUpdateTime is hidden but has non-default value
DialPlanFileName = 'dialplan_lab1v2.dat'
DayLightSavingTimeStart = '01:SUN/01:00:00'
DayLightSavingTimeEnd = '01:SUN/01:00:00'
NTPServerIP = '0.0.0.0'

;LastConfigChangeTime is hidden but has non-default value
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]
PCMLawSelect = 1
TDMBusClockSource = 4
ExtBootPReqEnable = 1
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

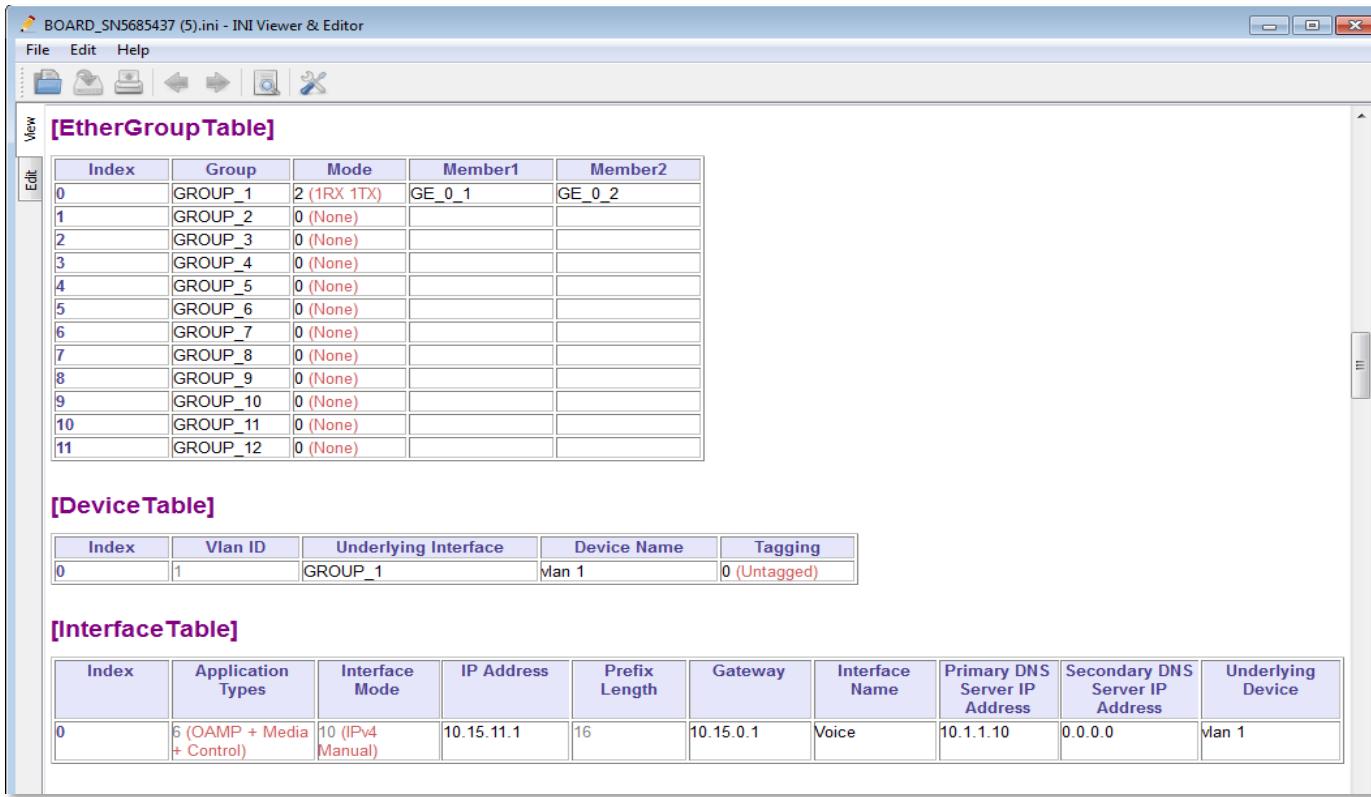
[Analog Params]

[ControlProtocols Params]
AdminStateLockControl = 0

[MGCP Params]

[MEGACO Params]
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0
```

- Table Parameters in View Mode



The screenshot shows the INI Viewer & Editor application interface with three tables displayed:

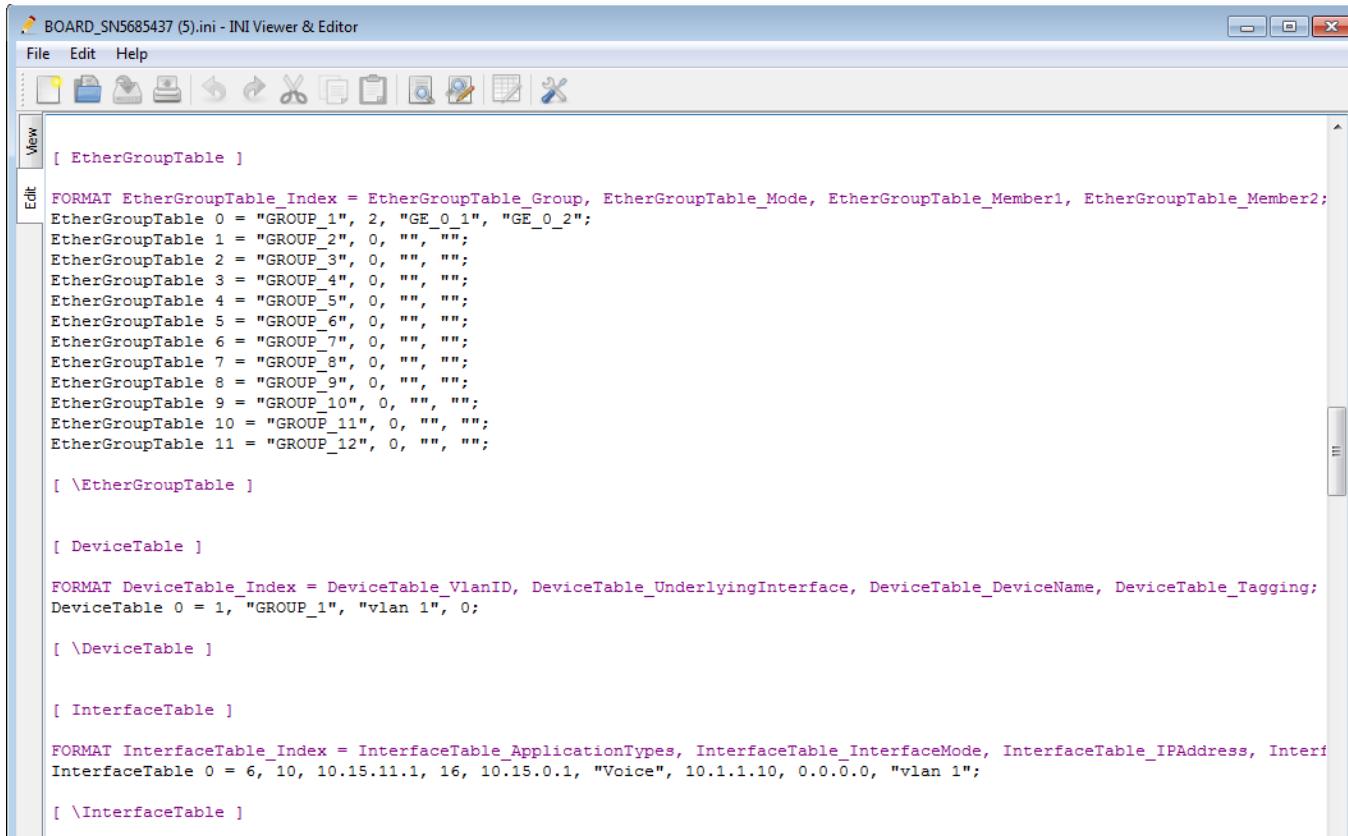
- [EtherGroupTable]**

Index	Group	Mode	Member1	Member2
0	GROUP_1	2 (1RX 1TX)	GE_0_1	GE_0_2
1	GROUP_2	0 (None)		
2	GROUP_3	0 (None)		
3	GROUP_4	0 (None)		
4	GROUP_5	0 (None)		
5	GROUP_6	0 (None)		
6	GROUP_7	0 (None)		
7	GROUP_8	0 (None)		
8	GROUP_9	0 (None)		
9	GROUP_10	0 (None)		
10	GROUP_11	0 (None)		
11	GROUP_12	0 (None)		
- [DeviceTable]**

Index	Vlan ID	Underlying Interface	Device Name	Tagging
0	1	GROUP_1	Vlan 1	0 (Untagged)
- [InterfaceTable]**

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Device
0	6 (OAMP + Media + Control)	10 (IPv4 Manual)	10.15.11.1	16	10.15.0.1	Voice	10.1.1.10	0.0.0.0	Vlan 1

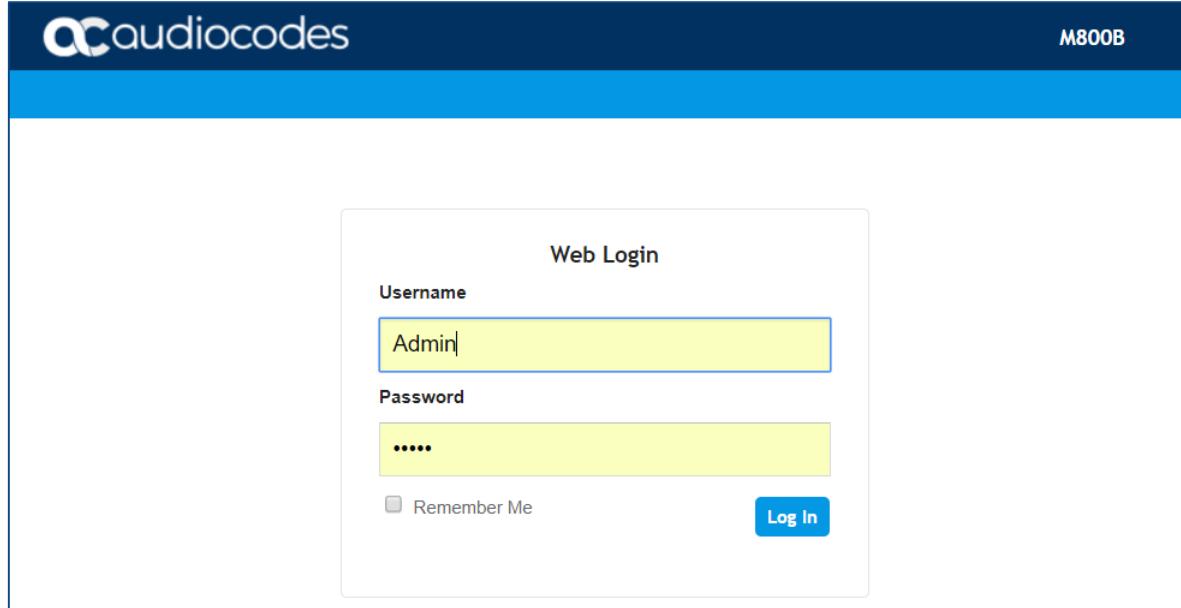
- Table Parameters in Edit Mode



The screenshot shows the INI Viewer & Editor application window with the file `BOARD_SN5685437 (5).ini` open. The interface includes a menu bar (File, Edit, Help) and a toolbar with various icons. The main area displays the INI configuration code:

```
[ EtherGroupTable ]  
  
FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;  
EtherGroupTable 0 = "GROUP_1", 2, "GE_0_1", "GE_0_2";  
EtherGroupTable 1 = "GROUP_2", 0, "", "";  
EtherGroupTable 2 = "GROUP_3", 0, "", "";  
EtherGroupTable 3 = "GROUP_4", 0, "", "";  
EtherGroupTable 4 = "GROUP_5", 0, "", "";  
EtherGroupTable 5 = "GROUP_6", 0, "", "";  
EtherGroupTable 6 = "GROUP_7", 0, "", "";  
EtherGroupTable 7 = "GROUP_8", 0, "", "";  
EtherGroupTable 8 = "GROUP_9", 0, "", "";  
EtherGroupTable 9 = "GROUP_10", 0, "", "";  
EtherGroupTable 10 = "GROUP_11", 0, "", "";  
EtherGroupTable 11 = "GROUP_12", 0, "", "";  
  
[ \EtherGroupTable ]  
  
[ DeviceTable ]  
  
FORMAT DeviceTable_Index = DeviceTable_VlanID, DeviceTable_UnderlyingInterface, DeviceTable_DeviceName, DeviceTable_Tagging;  
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0;  
  
[ \DeviceTable ]  
  
[ InterfaceTable ]  
  
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_MACAddress;  
InterfaceTable 0 = 6, 10, 10.15.11.1, 16, 10.15.0.1, "Voice", 10.1.1.10, 0.0.0.0, "vlan 1";  
  
[ \InterfaceTable ]
```

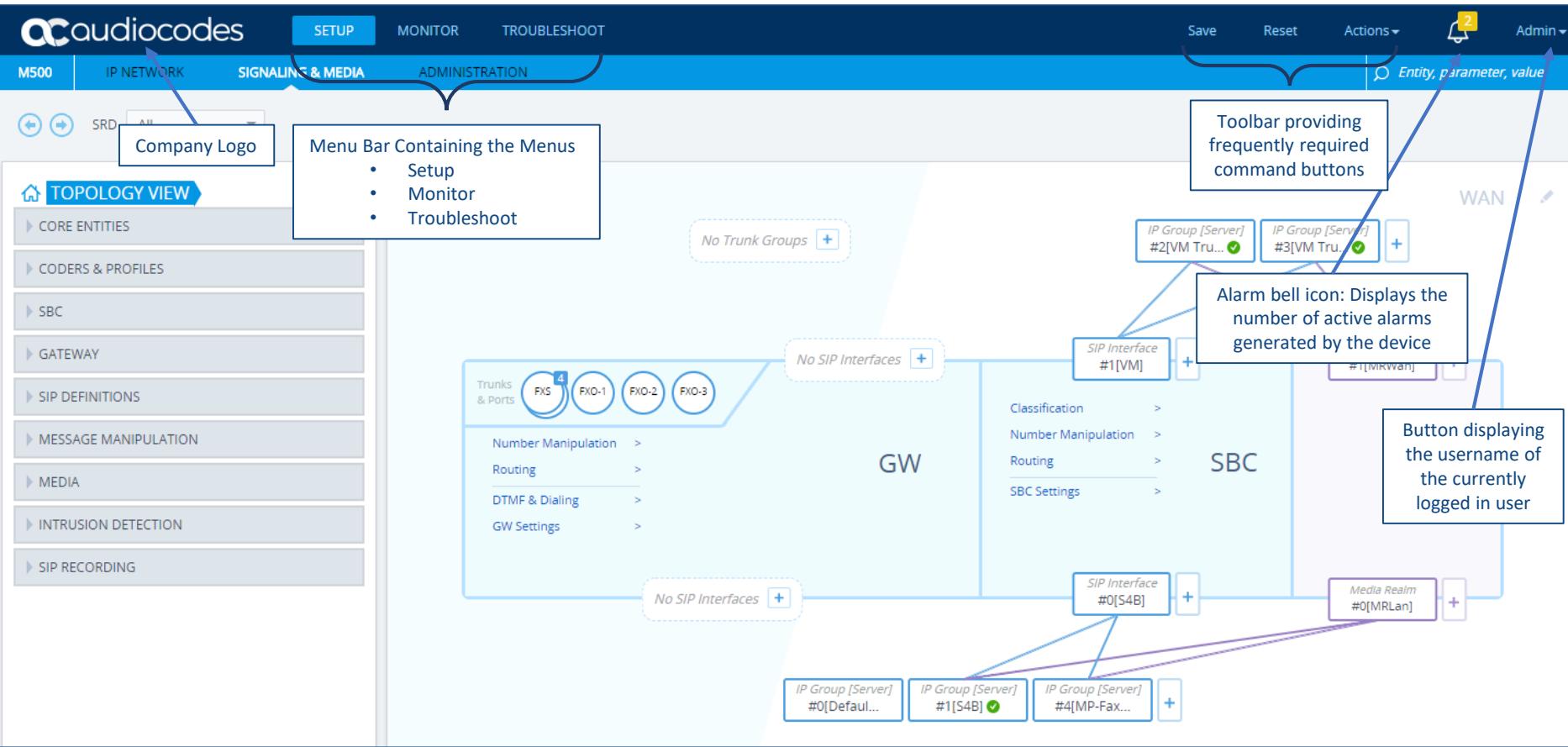
# Accessing the Web Interface



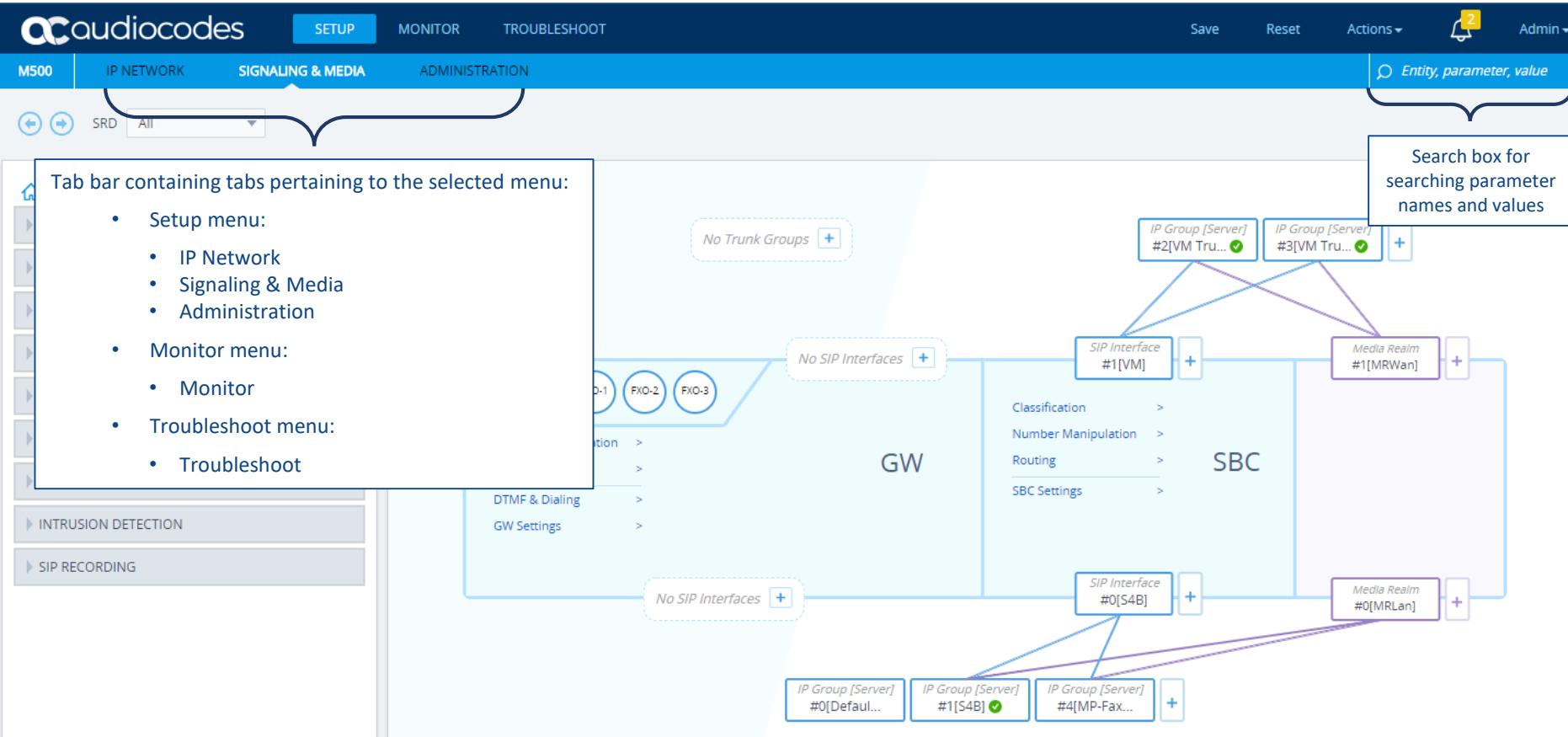
**Default Username:** Admin

**Default Password:** Admin

# GUI Areas



# GUI Areas



The screenshot illustrates the audiocodes M500 GUI interface, specifically the **SIGNALING & MEDIA** tab. The main area shows a hierarchical configuration tree for a **GW** and **SBC**. The tree structure includes:

- GW:** Contains sections for **No Trunk Groups**, **No SIP Interfaces** (with three FXO ports listed), and **Classification**, **Number Manipulation**, **Routing**, **SBC Settings**.
- SBC:** Contains sections for **SIP Interface #1[VM]** and **Media Realm #1[MRWan]**.
- Bottom Level:** Contains **SIP Interface #0[S4B]** and **Media Realm #0[MRLan]**.

A search bar at the top right is highlighted with a callout, labeled "Search box for searching parameter names and values". Another callout highlights the **Tab bar containing tabs pertaining to the selected menu:**

- Setup menu:
  - IP Network
  - Signaling & Media
  - Administration
- Monitor menu:
  - Monitor
- Troubleshoot menu:
  - Troubleshoot

Other visible tabs include **IP NETWORK**, **ADMINISTRATION**, and **DTMF & Dialing**, **GW Settings** under the **GW** section.

# GUI Areas



Back and Forward buttons that enable quick-and-easy navigation through previously opened pages

SRD All

TOPOLOGY VIEW

- CORE ENTITIES
- CODERS & PROFILES
- SBC
- GATEWAY
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- MEDIA
- INTRUSION DETECTION
- SIP RECORDING

OOT

Save Reset Actions ▾ Entity, parameter, value

Admin ▾

SRD filter  
When your configuration includes multiple SRDs, you can filter tables in the Web interface by a specific SRD

WAN

GW

SBC

Classification >  
Number Manipulation >  
Routing >  
SBC Settings >

No SIP Interfaces +

Trunks & Ports

- 4 FXS
- FXO-1
- FXO-2
- FXO-3

Number Manipulation >  
Routing >  
DTMF & Dialing >  
GW Settings >

No SIP Interfaces +

SIP Interface #1[VM] +

Media Realm #1[MRWan] +

IP Group [Server] #2[VM Tru... ✓]

IP Group [Server] #3[VM Tru... ✓]

Media Realm #0[MRLan] +

SIP Interface #0[S4B] +

IP Group [Server] #0[Default...]

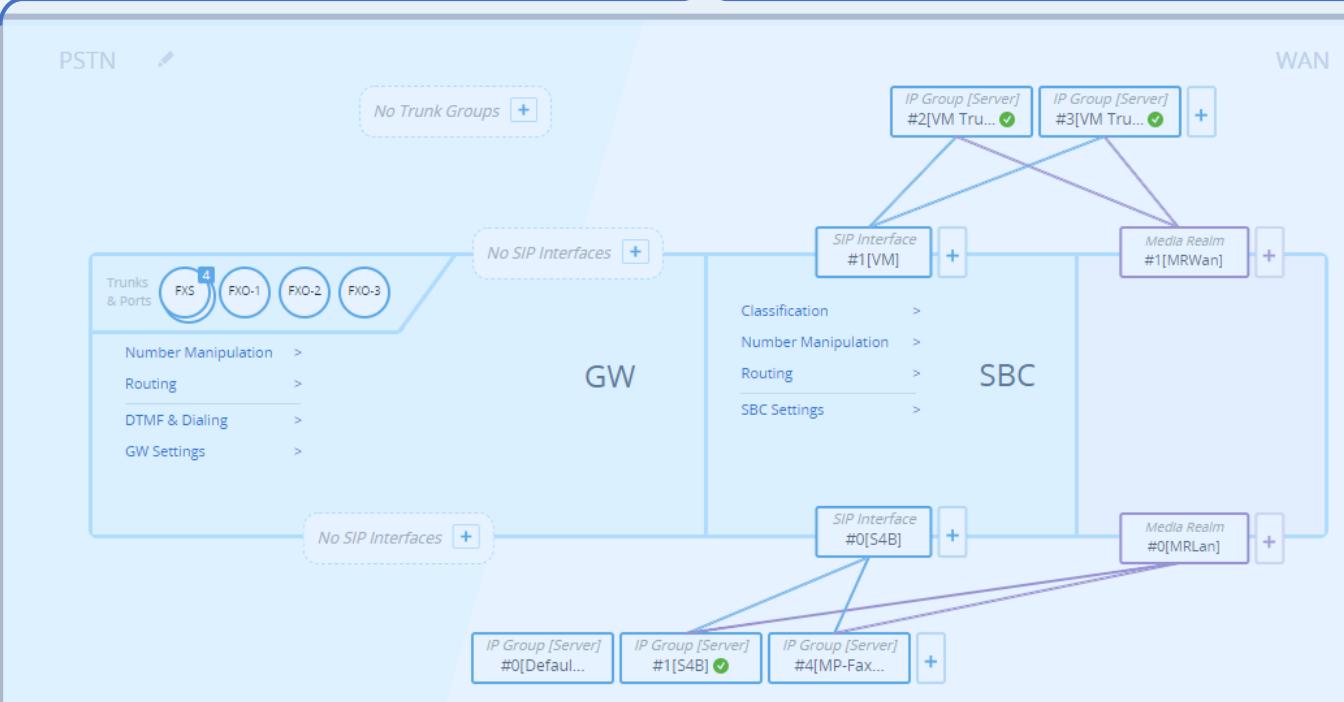
IP Group [Server] #1[S4B] ✓

IP Group [Server] #4[MP-Fax...]

+

# GUI Areas

Work pane:  
Where configuration pages are displayed



TOPOLOGY VIEW

- CORE ENTITIES
- CODERS & PROFILES
- SBC
- GATEWAY
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- MEDIA
- INTRUSION DETECTION
- SIP RECORDING

SETUP MONITOR TROUBLESHOOT

Save Reset Actions ▾ Admin ▾

IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

PSTN WAN

GW

SBC

No Trunk Groups +

No SIP Interfaces +

Trunks & Ports

- 4 FXS
- FXO-1
- FXO-2
- FXO-3

Number Manipulation >

Routing >

DTMF & Dialing >

GW Settings >

No SIP Interfaces +

SIP Interface #1[VM] +

Classification

Number Manipulation

Routing

SBC Settings

Media Realm #1[MRWan] +

No SIP Interfaces +

SIP Interface #0[S4B] +

Media Realm #0[MRLan] +

IP Group [Server] #2[VM Tru...]

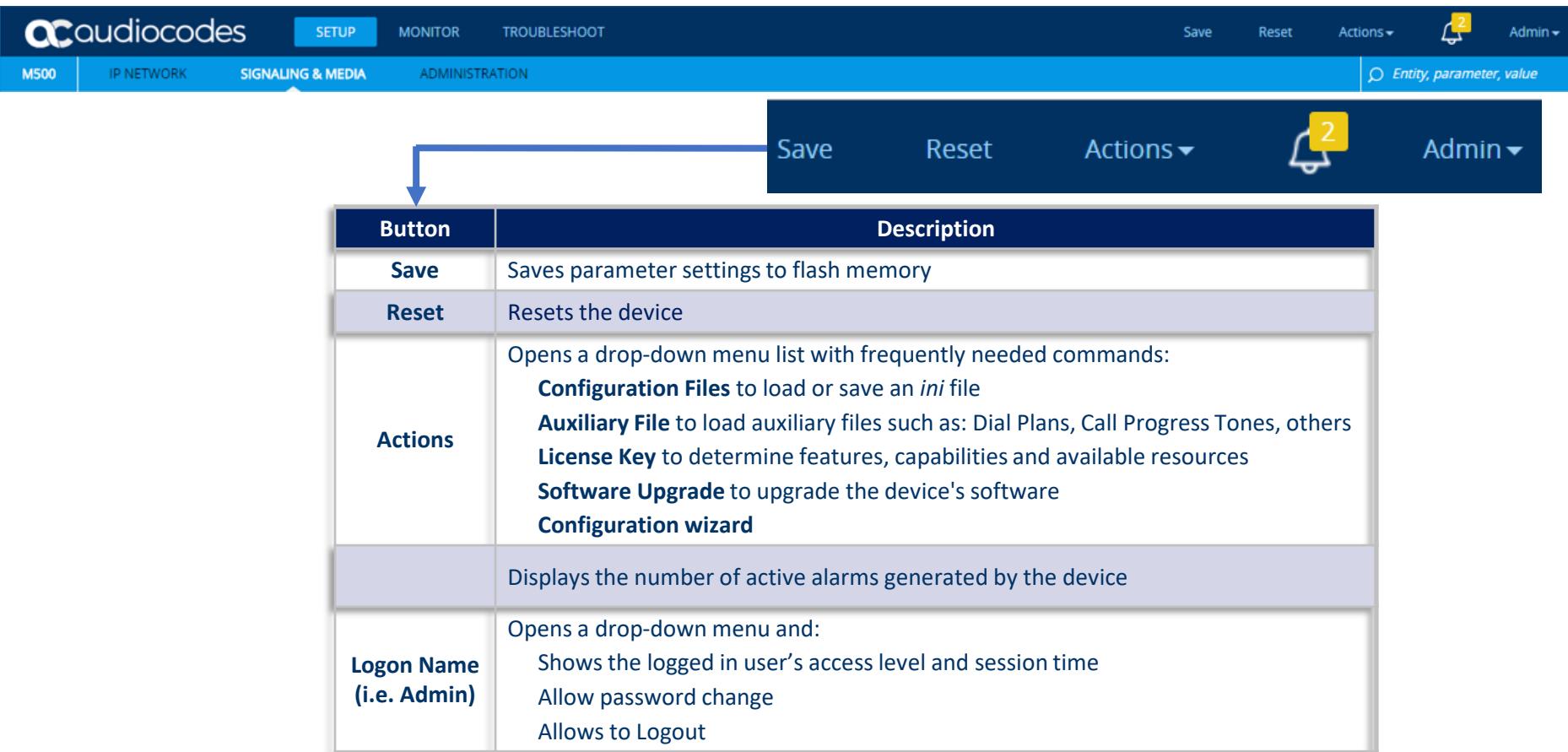
IP Group [Server] #3[VM Tru...]

IP Group [Server] #0[Default...]

IP Group [Server] #1[S4B]

IP Group [Server] #4[MP-Fax...]

# Tool Bar

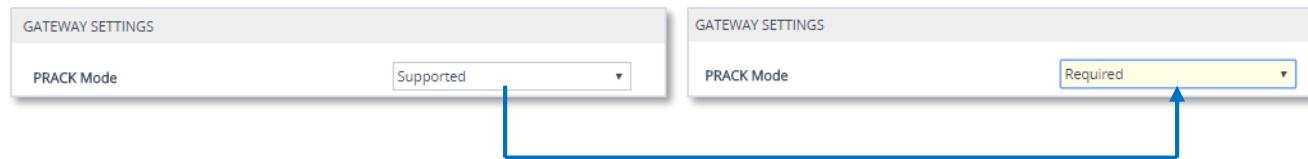


The screenshot shows the audiocodes M500 web interface. At the top, there's a navigation bar with tabs: SETUP (highlighted in blue), MONITOR, TROUBLESHOOT, and ADMINISTRATION. Below the tabs, there are buttons for Save, Reset, Actions (with a dropdown arrow), and Admin (with a dropdown arrow). A bell icon with a '2' notification count is also present. The main content area has a table describing the functions of these buttons.

Button	Description
Save	Saves parameter settings to flash memory
Reset	Resets the device
Actions	<p>Opens a drop-down menu list with frequently needed commands:</p> <ul style="list-style-type: none"><li><b>Configuration Files</b> to load or save an <i>ini</i> file</li><li><b>Auxiliary File</b> to load auxiliary files such as: Dial Plans, Call Progress Tones, others</li><li><b>License Key</b> to determine features, capabilities and available resources</li><li><b>Software Upgrade</b> to upgrade the device's software</li><li><b>Configuration wizard</b></li></ul>
	Displays the number of active alarms generated by the device
Logon Name (i.e. Admin)	Opens a drop-down menu and: <ul style="list-style-type: none"><li>Shows the logged in user's access level and session time</li><li>Allow password change</li><li>Allows to Logout</li></ul>

# Modifying/Saving Parameters

- When changing parameter values, the changed parameter has a yellow background
- To save configuration changes to volatile memory (RAM), click the **Apply** button



- Modifications to parameters with on-the-fly capabilities are immediately applied to the device and immediately take effect
- Parameters displayed with a lightning  symbol are not changeable on-the-fly and require a device reset



# Modifying/Saving Parameters

- If you click the Apply button after modifying parameters a red rectangle appears surrounding the Save button
- This is a reminder to save your settings to flash memory



- If you click the Apply button after modifying parameters that take effect only after a device reset, a red rectangle appears surrounding the both, the Save and Reset buttons
- This is a reminder to later save your settings to flash memory and reset the device



# Stand-alone Parameters

- Parameters that are not contained in a table are referred to as stand-alone parameters

Transport Settings

GENERAL

SIP NAT Detection	Enable
SIPS	Disable
SIP Transport Type	UDP
ENUM Resolution	e164.arpa
SIP 408 Response upon non-INVITE	Enable
DNS Query Type	A-Record

TCP CONNECTION

TCP/TLS Connection Reuse	Enable
TCP Timeout	0
Reliable Connection Persistent Mode	Disable

RETRANSMISSION

SIP T1 Retransmission Timer [msec]	500
SIP T2 Retransmission Timer [msec]	4000
SIP Maximum RTX	3

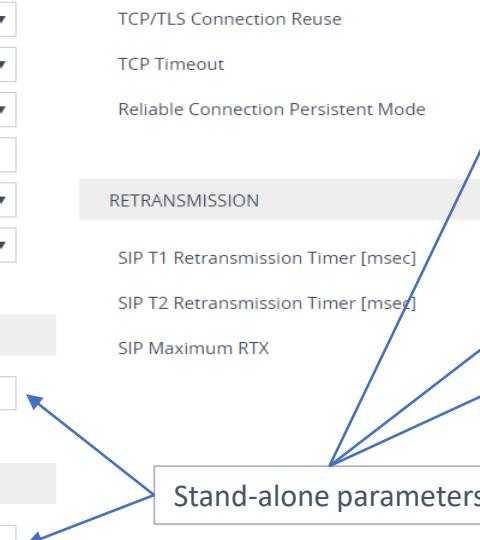
SBC SETTINGS

WebSocket Keep-Alive Period [sec]	0
-----------------------------------	---

GATEWAY SETTINGS

SIP Destination Port	5060
----------------------	------

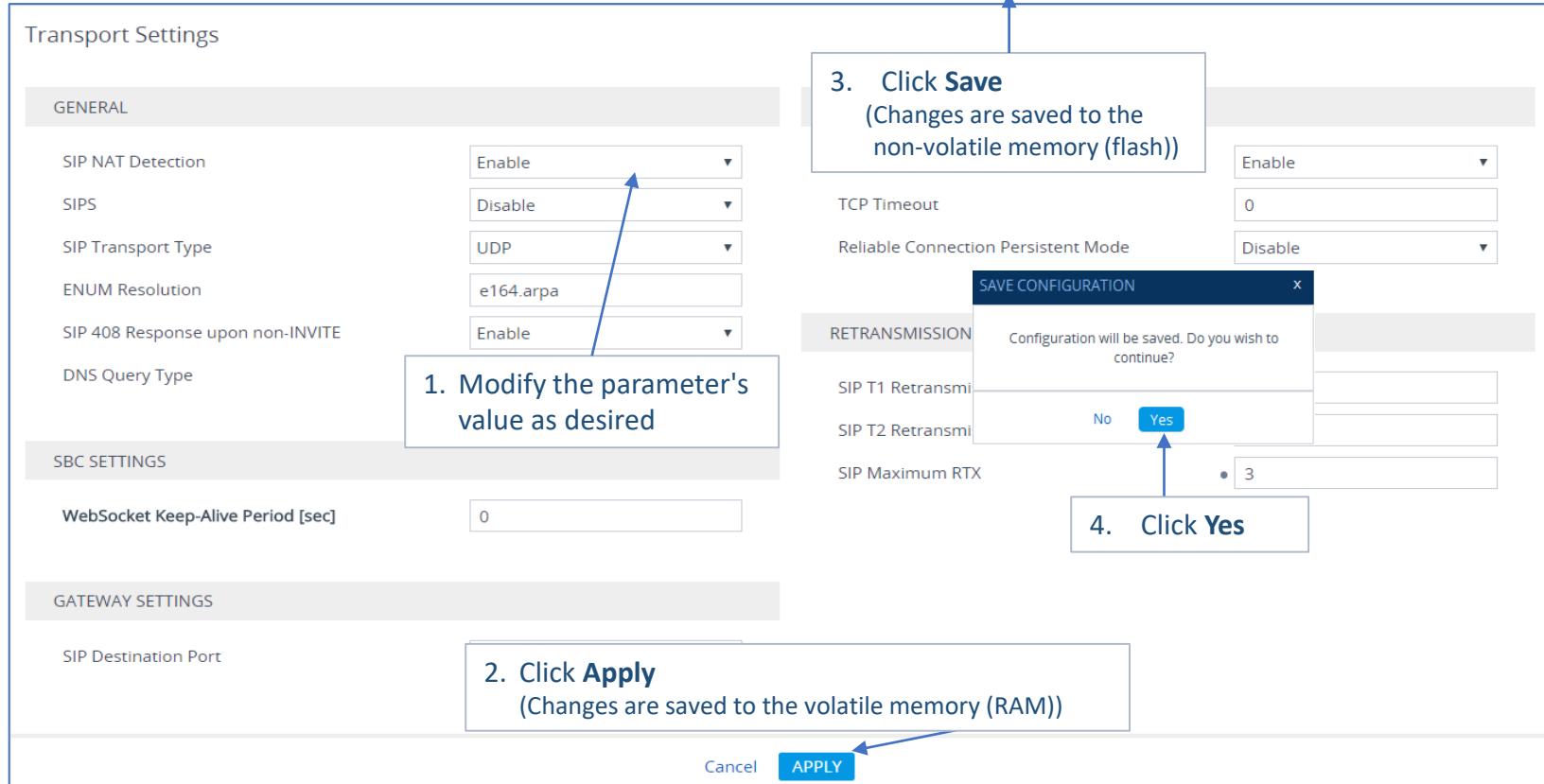
Stand-alone parameters



Cancel APPLY

# Stand-alone Parameters Configuration

- Parameters not requiring a device reset



Transport Settings

GENERAL

- SIP NAT Detection: Enable
- SIPS: Disable
- SIP Transport Type: UDP
- ENUM Resolution: e164.arpa
- SIP 408 Response upon non-INVITE: Enable

SBC SETTINGS

- WebSocket Keep-Alive Period [sec]: 0

GATEWAY SETTINGS

- SIP Destination Port

3. Click **Save**  
(Changes are saved to the non-volatile memory (flash))

4. Click **Yes**

1. Modify the parameter's value as desired

2. Click **Apply**  
(Changes are saved to the volatile memory (RAM))

Cancel **APPLY**

Save Reset Actions ▾ Admin ▾

RETRANSMISSION

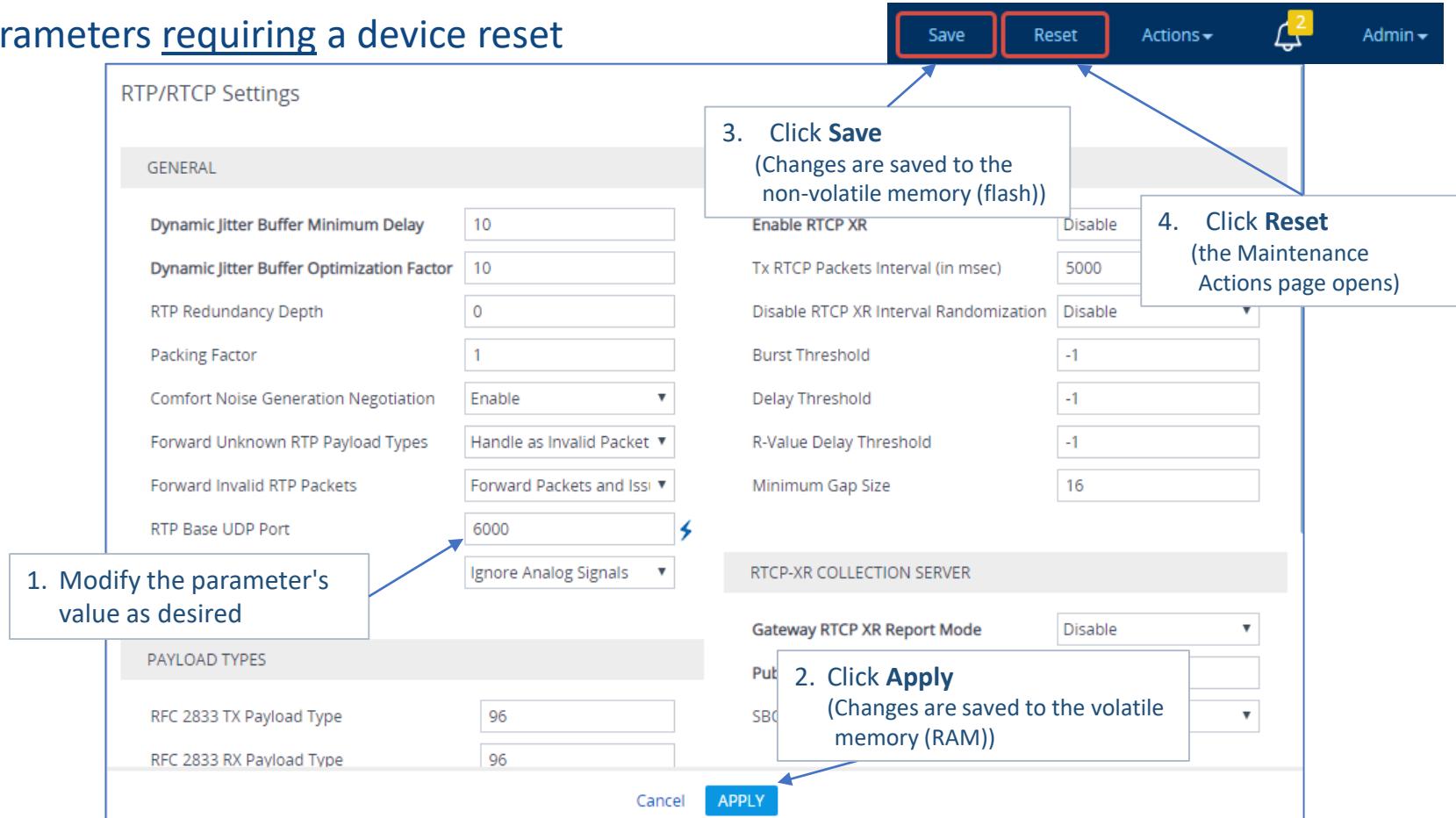
SAVE CONFIGURATION

Configuration will be saved. Do you wish to continue?

No Yes

# Stand-alone Parameters Configuration

- Parameters requiring a device reset



1. Modify the parameter's value as desired

3. Click Save  
(Changes are saved to the non-volatile memory (flash))

4. Click Reset  
(the Maintenance Actions page opens)

2. Click Apply  
(Changes are saved to the volatile memory (RAM))

RTP/RTCP Settings

GENERAL

Dynamic Jitter Buffer Minimum Delay: 10

Dynamic Jitter Buffer Optimization Factor: 10

RTP Redundancy Depth: 0

Packing Factor: 1

Comfort Noise Generation Negotiation: Enable

Forward Unknown RTP Payload Types: Handle as Invalid Packet

Forward Invalid RTP Packets: Forward Packets and Discard

RTP Base UDP Port: 6000

Ignore Analog Signals: ▾

PAYOUT TYPES

RFC 2833 TX Payload Type: 96

RFC 2833 RX Payload Type: 96

Cancel

APPLY

Save

Reset

Actions ▾

Admin ▾

Enable RTCP XR: Disable

Tx RTCP Packets Interval (in msec): 5000

Disable RTCP XR Interval Randomization: Disable

Burst Threshold: -1

Delay Threshold: -1

R-Value Delay Threshold: -1

Minimum Gap Size: 16

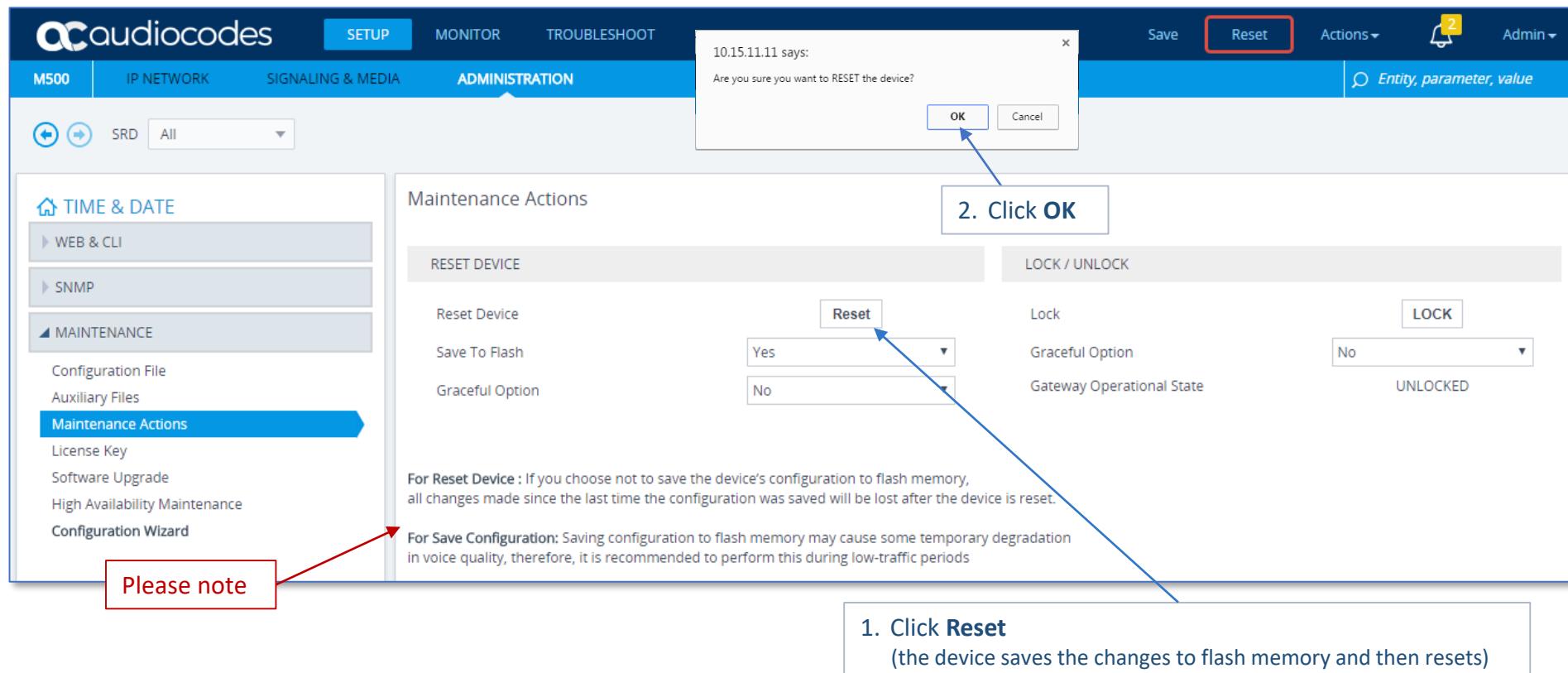
RTCP-XR COLLECTION SERVER

Gateway RTCP XR Report Mode: Disable

Put SBC: ▾

# Stand-alone Parameters Configuration

- Resetting the device



The screenshot shows the audiocodes M500 web interface. The navigation bar includes SETUP, MONITOR, TROUBLESHOOT, ADMINISTRATION (selected), and other tabs like IP NETWORK and SIGNALING & MEDIA. The left sidebar has sections for TIME & DATE, WEB & CLI, SNMP, MAINTENANCE (selected), Configuration File, Auxiliary Files, Maintenance Actions (highlighted in blue), License Key, Software Upgrade, High Availability Maintenance, and Configuration Wizard.

In the main content area, under ADMINISTRATION, the Maintenance Actions section is selected. It contains two tabs: RESET DEVICE and LOCK / UNLOCK. Under RESET DEVICE, there are three options: Reset Device, Save To Flash (with dropdown choices Yes or No), and Graceful Option. A note below states: "For Reset Device : If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset." Under LOCK / UNLOCK, there are two options: Lock (with dropdown choice LOCK) and Graceful Option (with dropdown choice No). A note below states: "For Save Configuration: Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods".

A modal dialog box is displayed in the top right corner, asking "Are you sure you want to RESET the device?". It has OK and Cancel buttons. A blue arrow points from the text "1. Click Reset" to the "Reset" button in the Maintenance Actions section. Another blue arrow points from the text "2. Click OK" to the "OK" button in the modal dialog.

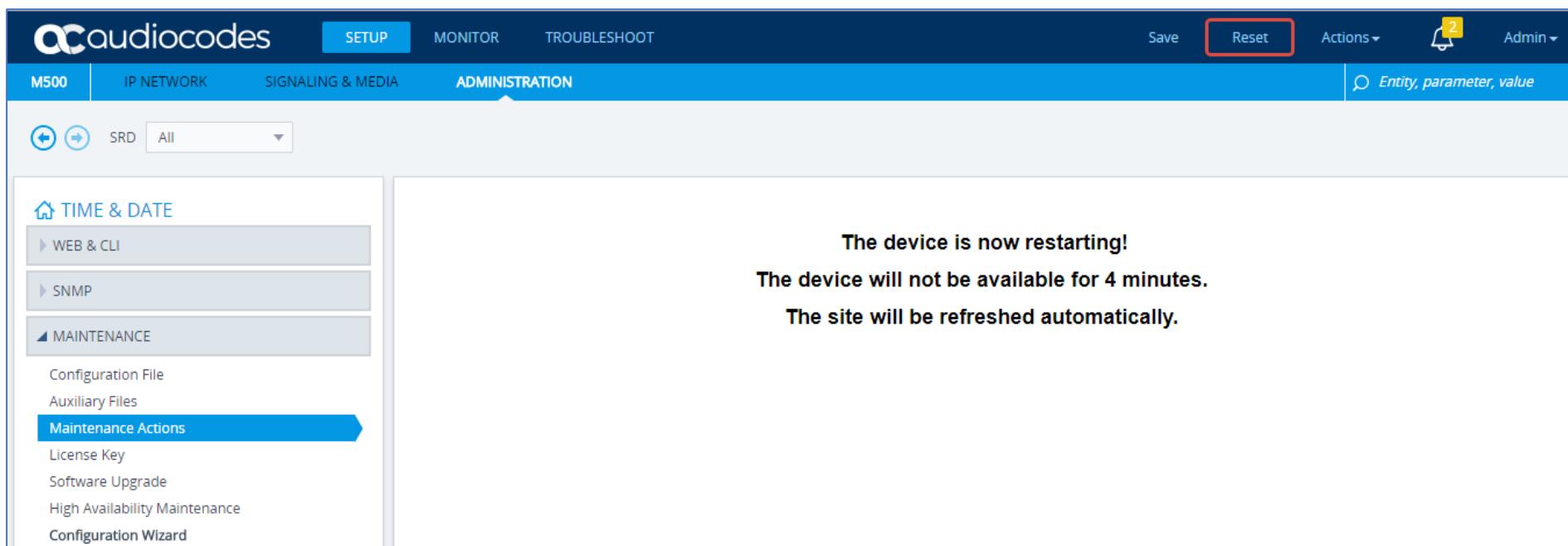
**Please note** (highlighted in red)

**1. Click Reset**  
(the device saves the changes to flash memory and then resets)

**2. Click OK**

# Stand-alone Parameters Configuration

- Restarting the devices

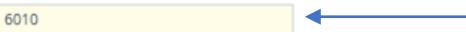


The screenshot shows the audiocodes M500 web interface. The top navigation bar includes the audiocodes logo, a search bar, and tabs for SETUP, MONITOR, TROUBLESHOOT, Save, Reset (which is highlighted with a red border), Actions, and Admin. Below the navigation is a secondary menu with tabs for M500, IP NETWORK, SIGNALING & MEDIA, and ADMINISTRATION (which is also highlighted with a red border). A search bar on the right contains the placeholder "Entity, parameter, value".

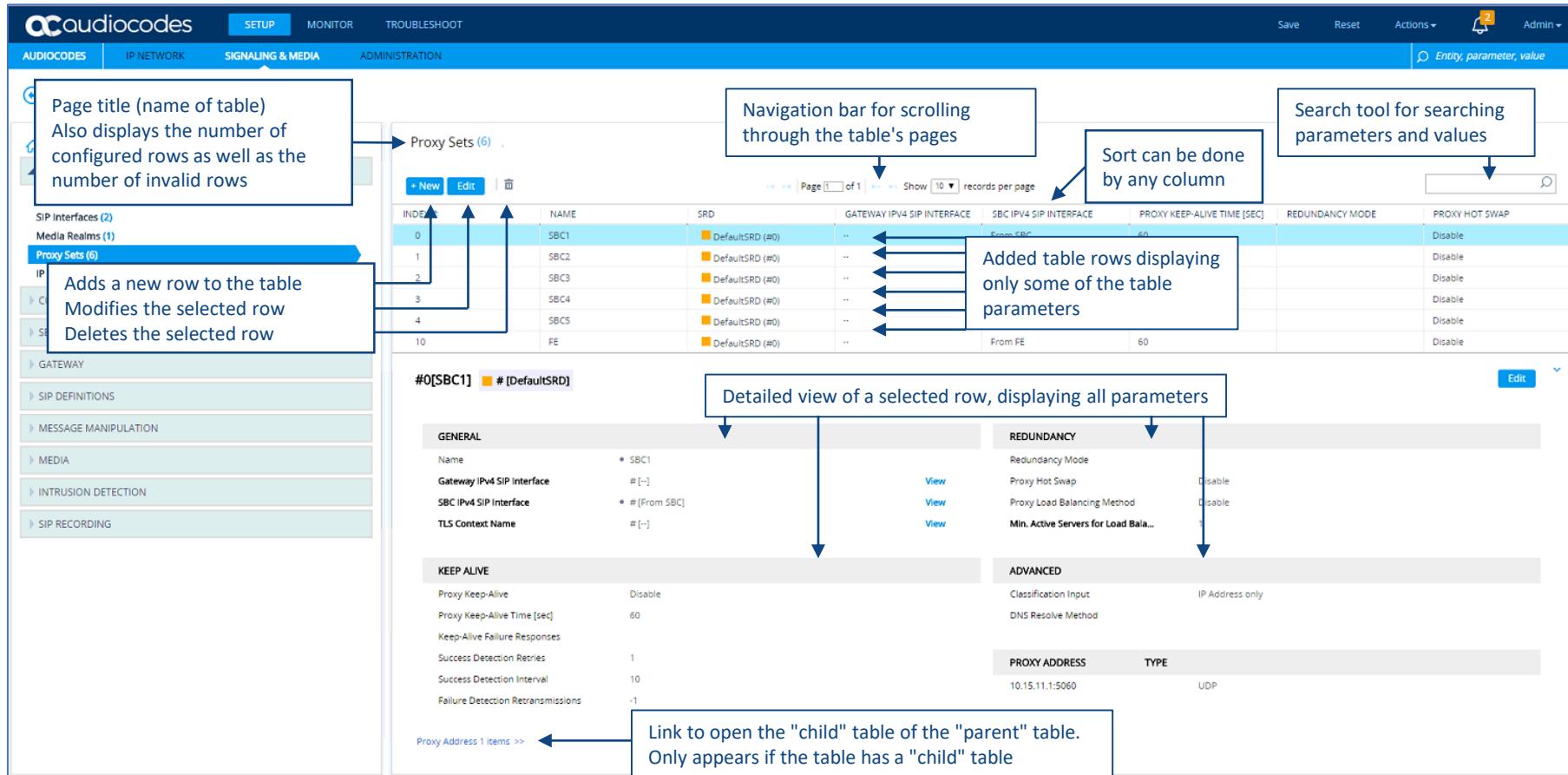
In the main content area, there are navigation icons for back, forward, and SRD, followed by a dropdown menu set to "All". On the left, a sidebar under "TIME & DATE" lists "WEB & CLI", "SNMP", and "MAINTENANCE". The "MAINTENANCE" section contains links for "Configuration File", "Auxiliary Files", "Maintenance Actions" (which is highlighted with a blue arrow), "License Key", "Software Upgrade", "High Availability Maintenance", and "Configuration Wizard".

The central panel displays a message: "The device is now restarting! The device will not be available for 4 minutes. The site will be refreshed automatically." This message is displayed in large, bold, black text.

# Stand-alone Parameters Indications Meaning

	Parameters changed and not applied are highlighted
	A dot appears next to parameters changed from their default values and when the Apply button was clicked
	Changes on parameters displaying a lightning-bolt ⚡ icon, require to be saved to flash memory followed by a device reset for your changes to take effect
Media Security Media Security Behavior	Typically required parameters are displayed in bold font
	An invalid value for a parameter reverts to its previous value and is surrounded by a colored border
Media Security Media Security Behavior	To get help on a parameter, hover your mouse over the parameter's field  A pop-up help appears, displaying a brief description of the parameter

# Table Parameters – General Description



The screenshot shows the audiocodes web interface with the 'Proxy Sets' table selected. The interface includes a navigation bar, search tool, and detailed row view.

**Annotations:**

- Page title (name of table)**  
Also displays the number of configured rows as well as the number of invalid rows
- Navigation bar for scrolling through the table's pages**
- Sort can be done by any column**
- Search tool for searching parameters and values**
- Adds a new row to the table**  
Modifies the selected row  
Deletes the selected row
- Detailed view of a selected row, displaying all parameters**
- Link to open the "child" table of the "parent" table.**  
Only appears if the table has a "child" table

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	SBC1	DefaultSRD (#0)	...	From SBC	60	Disable	Disable
1	SBC2	DefaultSRD (#0)	...			Disable	Disable
2	SBC3	DefaultSRD (#0)	...			Disable	Disable
3	SBC4	DefaultSRD (#0)	...			Disable	Disable
4	SBC5	DefaultSRD (#0)	...			Disable	Disable
10	FE	DefaultSRD (#0)	From FE		60		

**#0[SBC1] # [DefaultSRD]**

**GENERAL**

- Name: SBC1
- Gateway IPv4 SIP Interface: # [-]
- SBC IPv4 SIP Interface: # [From SBC]
- TLS Context Name: # [-]

**KEEP ALIVE**

- Proxy Keep-Alive: Disable
- Proxy Keep-Alive Time [sec]: 60
- Keep-Alive Failure Responses: 1
- Success Detection Retries: 10
- Success Detection Interval: -1
- Failure Detection Retransmissions: -1

**REduNDANCY**

- Redundancy Mode: Disable
- Proxy Hot Swap: Disable
- Proxy Load Balancing Method: Disable
- Min. Active Servers for Load Bal...: 1

**ADVANCED**

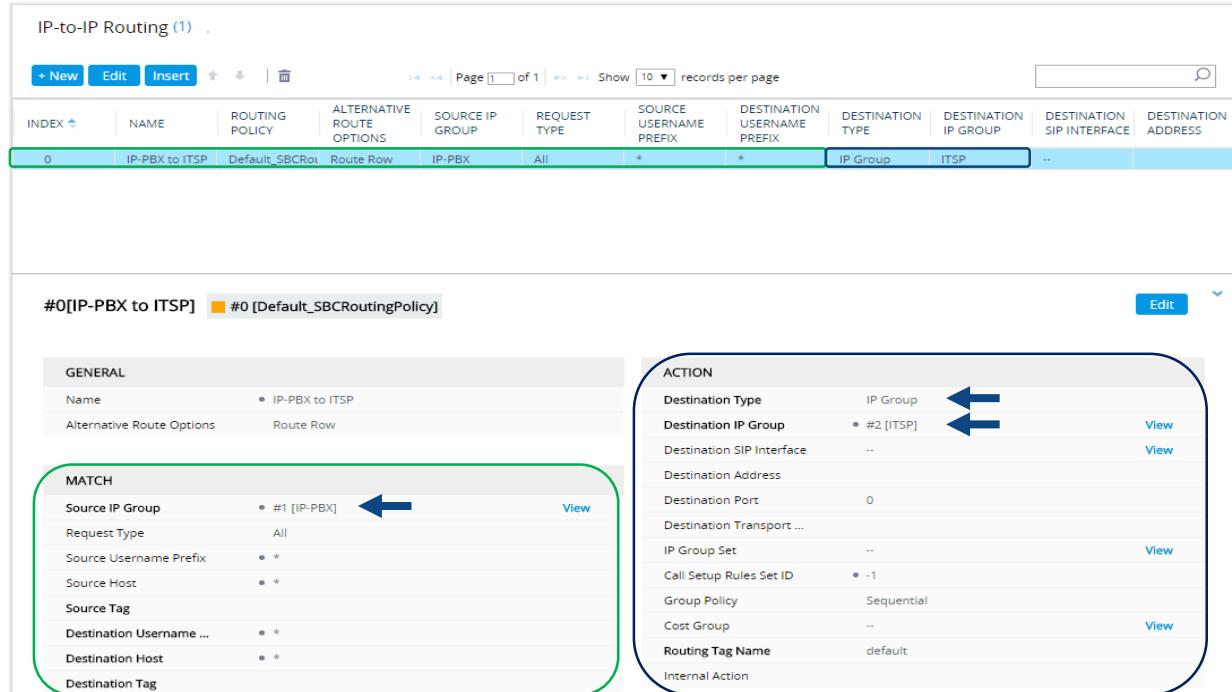
- Classification Input: IP Address only
- DNS Resolve Method:

**PROXY ADDRESS**

TYPE	
10.15.11.1:5060	UDP

# Table Syntax

- The table is divided into two main areas: Matching characteristics and Action to take
- If the incoming call matches the characteristics of a rule, then the call is sent to the destination configured for that rule
- Non-configured parameter fields may appear with different values, for example, “-1”, “0” or empty



The screenshot shows the 'IP-to-IP Routing' configuration page. At the top, there's a table header with columns: INDEX, NAME, ROUTING POLICY, ALTERNATIVE ROUTE OPTIONS, SOURCE IP GROUP, REQUEST TYPE, SOURCE USERNAME PREFIX, DESTINATION USERNAME PREFIX, DESTINATION TYPE, DESTINATION IP GROUP, DESTINATION SIP INTERFACE, and DESTINATION ADDRESS. Below the header, a single row is selected: #0 [IP-PBX to ITSP] under NAME, Default\_SBCRoi under ROUTING POLICY, Route Row under ALTERNATIVE ROUTE OPTIONS, IP-PBX under SOURCE IP GROUP, All under REQUEST TYPE, \* under SOURCE USERNAME PREFIX, \* under DESTINATION USERNAME PREFIX, IP Group under DESTINATION TYPE, ITSP under DESTINATION IP GROUP, and .. under DESTINATION SIP INTERFACE.

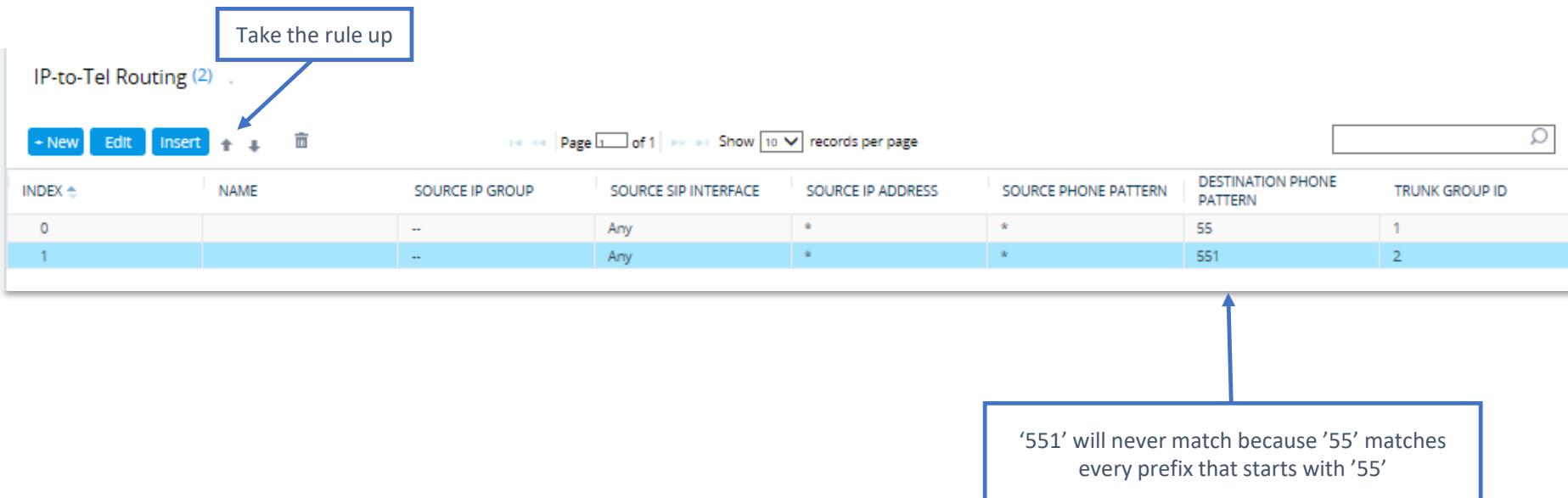
Below the table, two detailed configuration panels are shown:

- GENERAL** panel:
  - Name: IP-PBX to ITSP
  - Alternative Route Options: Route Row
- MATCH** panel:
  - Source IP Group: #1 [IP-PBX]
  - Request Type: All
  - Source Username Prefix: \*
  - Source Host: \*
  - Source Tag
  - Destination Username ...: \*
  - Destination Host: \*
  - Destination Tag
- ACTION** panel:
  - Destination Type: IP Group
  - Destination IP Group: #2 [ITSP]
  - Destination SIP Interface: ..
  - Destination Address
  - Destination Port: 0
  - Destination Transport ...
  - IP Group Set: ..
  - Call Setup Rules Set ID: -1
  - Group Policy: Sequential
  - Cost Group: ..
  - Routing Tag Name: default
  - Internal Action

Blue arrows point from the 'Source IP Group' field in the MATCH panel to the 'Destination IP Group' field in the ACTION panel, and from the 'Source IP Group' field in the ACTION panel back to the 'Source IP Group' field in the MATCH panel, indicating a bidirectional relationship or dependency between these settings.

# Fields to Match

- Device attempts to match patterns at the top of the table first (first match)
- More specific rules should be at the top and more generic ones at the bottom



Take the rule up

IP-to-Tel Routing (2)								
INDEX	NAME	SOURCE IP GROUP	SOURCE SIP INTERFACE	SOURCE IP ADDRESS	SOURCE PHONE PATTERN	DESTINATION PHONE PATTERN	TRUNK GROUP ID	
0		--	Any	*	*	55	1	
1		--	Any	*	*	551	2	

'551' will never match because '55' matches every prefix that starts with '55'

# Numbers Notation for Routing and Manipulation

- Flexible numbers notations for describing the prefix and/or suffix source and/or destination phone numbers and SIP URI user names:
  - **Prefix [n-m] or Suffix (n-m)**
    - Represents a range of numbers
  - **Prefix [n,m,...] or Suffix (n,m,...)**
    - Represents multiple numbers
    - Multiple ranges such as [n-m,s-t] are also supported
    - Up to three digits can be used to denote each number
  - **x (letter 'x')**
    - Represents any single digit
  - **# (Pound symbol)**
    - Represents the end of a number
  - **\*** (asterisk symbol)
    - Represents any number

Destination Phone Prefix	Source Phone Prefix
1	9x*
2[2,6,7,9]	1xxx
2[1-4,7,9]	1xxx#
[100-150,222,244,300-499]	1*
6[100-300]	(99)
976(99)	2[1-4]
6[100-300]#	*
*	*

- Examples:
  - [5200-5300]#
    - represents all numbers from 5200 to 5300
  - [2,3,4]xxx#
    - represents four-digit numbers that start with 2, 3 or 4 (2000-4999)
  - 54324
    - represents any number that starts with 54324
  - 54324xx#
    - represents seven-digit numbers that start with 54324
  - 123[100-200]#
    - represents six-digit numbers that start with 123 (123100 to 123200)
  - (100)
    - represents any number that finishes with 100
  - (266[1-9])
    - represents any number that finishes with 2661 to 2669

# Assigning Rows from other Tables

- Tables may contain parameters assigned a value which is a row referenced from another table

Proxy Sets (5)

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	SIPInterface_0	--	60		Disable
1	Proxy_Group1	DefaultSRD (#0)	--	SBC Interface	50		Disable
2	Proxy_Group2	DefaultSRD (#0)	--	SBC Interface	50		Disable
3	Proxy_Group3	DefaultSRD (#0)	--	SBC Interface	50		Disable
4	Proxy_Group4	DefaultSRD (#0)	--	SBC Interface	50		Disable

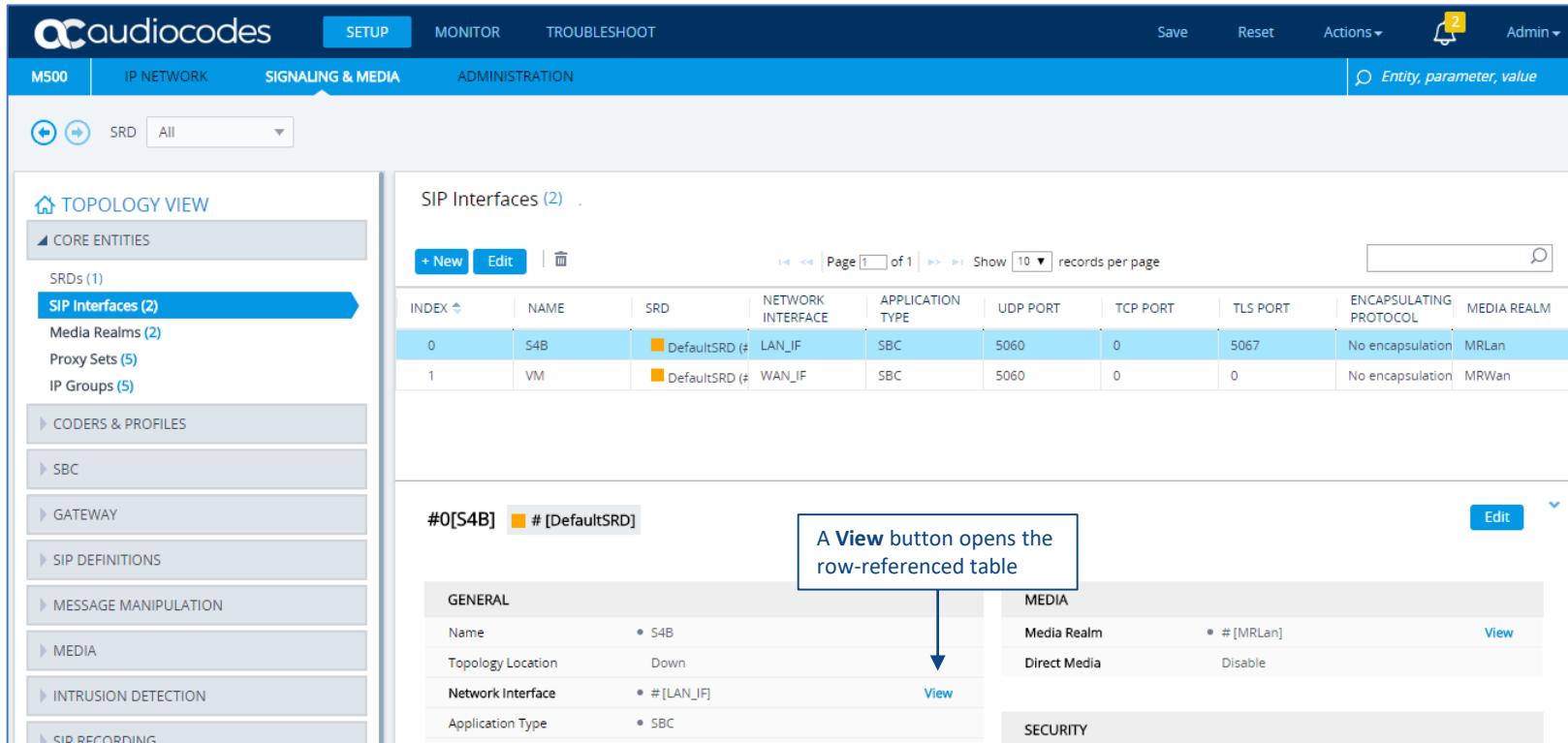
#4[Proxy\_Group4]    # [DefaultSRD]

A View button opens the row-referenced table

GENERAL		REDUNDANCY	
Name	* Proxy_Group4	Redundancy Mode	
Gateway IPv4 SIP Interface	# [-]	Proxy Hot Swap	Disable
SBC IPV4 SIP Interface	* # [SBC Interface]	Proxy Load Balancing Method	Disable
TLS Context Name	# [-]	Min. Active Servers for Lo...	1

# Assigning Rows from other Tables

- For example, after pressing the View button pointing to the Network Interface, the referenced table web page is opened



The screenshot shows the audiocodes M500 web interface. The top navigation bar includes tabs for SETUP, MONITOR, and TROUBLESHOOT, along with Save, Reset, Actions, and Admin buttons. A search bar on the right is set to "Entity, parameter, value".

The main content area has tabs for IP NETWORK, SIGNALING & MEDIA (which is selected), and ADMINISTRATION. On the left, a sidebar menu lists CORE ENTITIES (SRDs 1, SIP Interfaces 2, Media Realms 2, Proxy Sets 5, IP Groups 5), CODERS & PROFILES, SBC, GATEWAY, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, INTRUSION DETECTION, and SIP RECORDING.

The central panel displays the "SIP Interfaces (2)" table:

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	S4B	DefaultSRD (#)	LAN_IF	SBC	5060	0	5067	No encapsulation	MRLan
1	VM	DefaultSRD (#)	WAN_IF	SBC	5060	0	0	No encapsulation	MRWan

A callout box points to the "View" button in the bottom right corner of the S4B row's detail view, with the text: "A View button opens the row-referenced table".

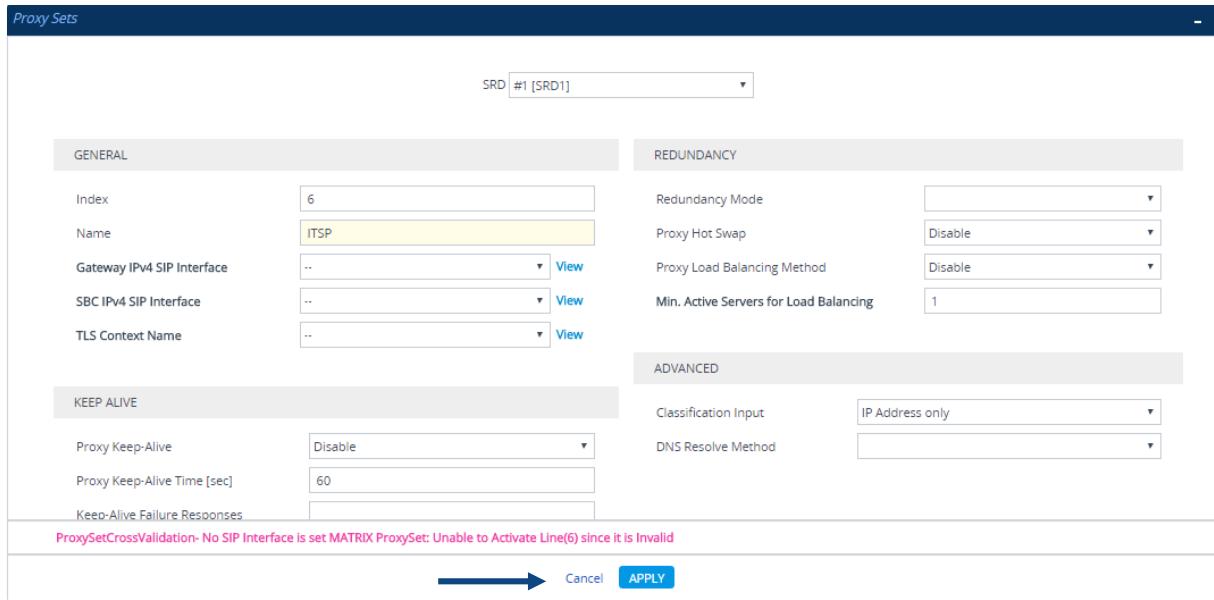
The detailed view for S4B shows:

GENERAL		MEDIA	
Name	S4B	Media Realm	# [MRLan]
Topology Location	Down	Direct Media	Disable
Network Interface	# [LAN_IF]	View	
Application Type	SBC	SECURITY	

# Table Parameters Invalid Values Indications

- When adding a row:

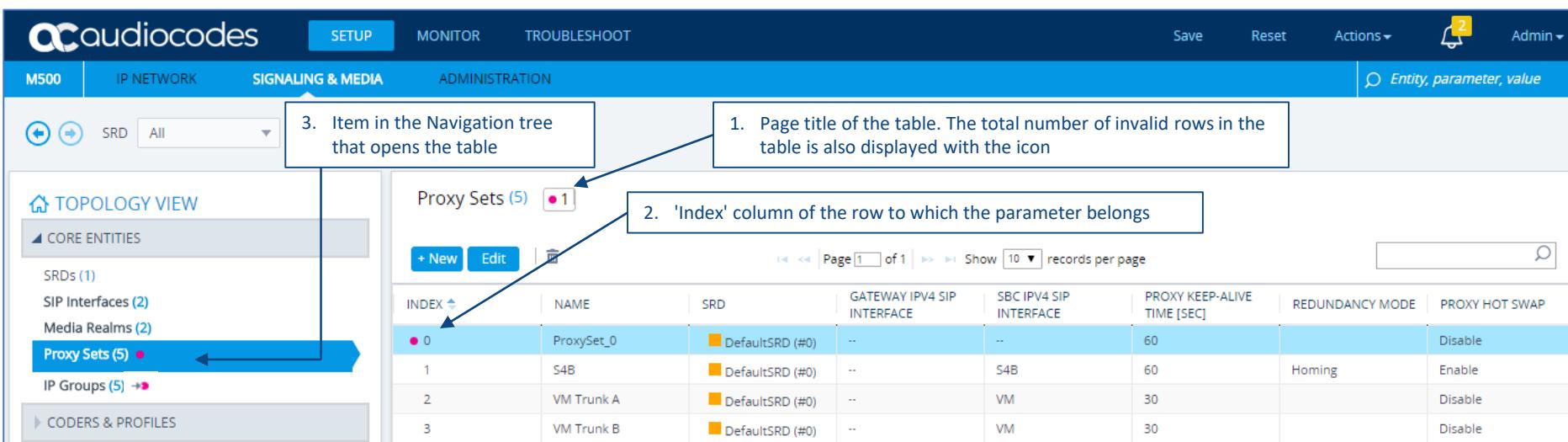
- If a mandatory parameter's value, which is a row referenced from another table is not assigned, after clicking Apply, an error message is displayed at the bottom of the dialog box
- Clicking Cancel closes the dialog box and the row is not added to the table
- To add the row, you must configure the parameter



# Table Parameters Invalid Values Indications

- When editing a row:

- If a parameter's configuration is changed so that it's no longer assigned with a referenced row from another table, when the dialog box is closed, the Invalid Line icon • appears for the table in which the parameter is configured, in the shown locations:



The screenshot shows the audiocodes M500 web interface. The top navigation bar includes tabs for SETUP, MONITOR, and TROUBLESHOOT, along with Save, Reset, Actions, and Admin buttons. The main content area is titled "SIGNALING & MEDIA". On the left, a navigation tree lists "TOPOLOGY VIEW", "CORE ENTITIES" (with "SRDs (1)", "SIP Interfaces (2)", "Media Realms (2)", and "Proxy Sets (5)" highlighted), and "IP Groups (5)". The "Proxy Sets" item is marked with a red dot and a question mark icon, indicating an invalid value. The main table, "Proxy Sets (5)", displays five rows of data. The first row is selected and highlighted in blue. The "INDEX" column of this row contains a red dot and a question mark icon, indicating an invalid value. Other columns include NAME, SRD, GATEWAY IPV4 SIP INTERFACE, SBC IPV4 SIP INTERFACE, PROXY KEEP-ALIVE TIME [SEC], REDUNDANCY MODE, and PROXY HOT SWAP. The table also includes pagination controls for page 1 of 1 and 10 records per page.

1. Page title of the table. The total number of invalid rows in the table is also displayed with the icon

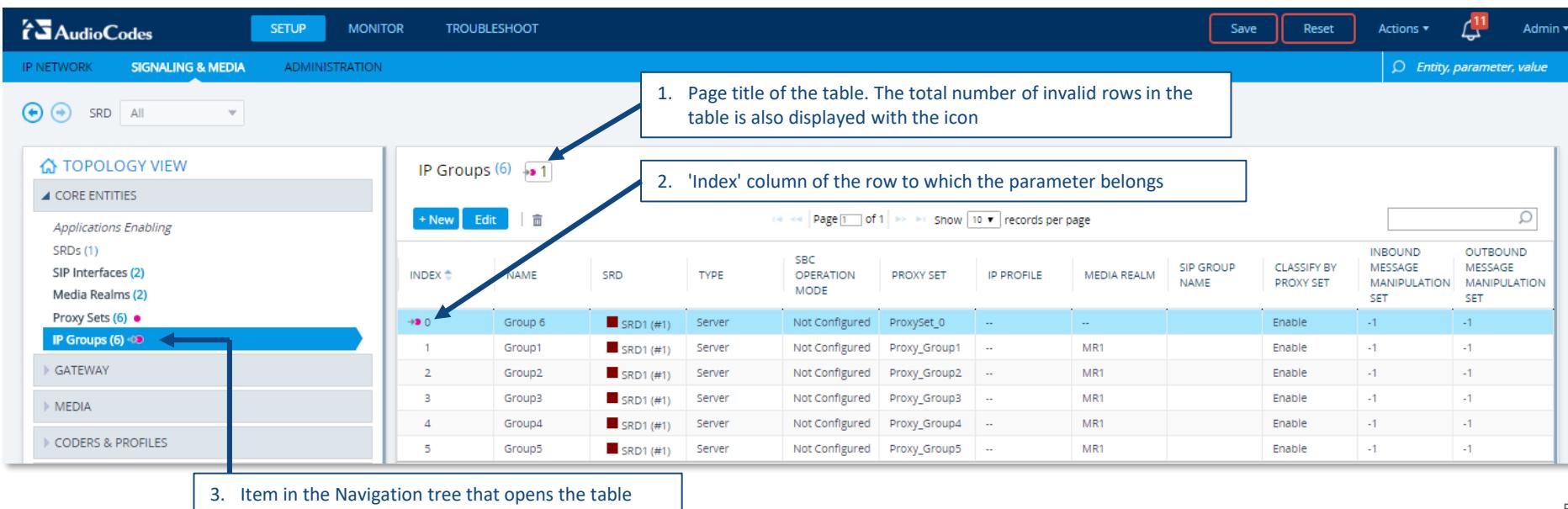
2. 'Index' column of the row to which the parameter belongs

3. Item in the Navigation tree that opens the table

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
• 0	ProxySet_0	DefaultSRD (#0)	--	--	60		Disable
1	S4B	DefaultSRD (#0)	--	S4B	60	Homing	Enable
2	VM Trunk A	DefaultSRD (#0)	--	VM	30		Disable
3	VM Trunk B	DefaultSRD (#0)	--	VM	30		Disable

# Table Parameters Invalid Values Indications

- When a parameter assigned a value which is an invalid row referenced from another
  - The Invalid Reference Line Icon  is displayed for the table in which the parameter is configured, in the shown locations



The screenshot shows the AudioCodes Management Interface with the following details:

- Page Title:** IP Groups (6) 
- Table Headers:** INDEX, NAME, SRD, TYPE, SBC OPERATION MODE, PROXY SET, IP PROFILE, MEDIA REALM, SIP GROUP NAME, CLASSIFY BY PROXY SET, INBOUND MESSAGE MANIPULATION SET, OUTBOUND MESSAGE MANIPULATION SET.
- Data Rows:** The first row (INDEX 0) has an invalid reference icon  in the INDEX column. The remaining rows (1-5) have valid data.
- Navigation:** The left sidebar shows "TOPOLOGY VIEW" and "CORE ENTITIES". Under "CORE ENTITIES", "IP Groups (6)" is highlighted with a blue arrow, and the "IP Groups (6)" item in the navigation tree is also highlighted with a blue arrow.
- Table Row Labels:** 1. Page title of the table. The total number of invalid rows in the table is also displayed with the icon. 2. 'Index' column of the row to which the parameter belongs. 3. Item in the Navigation tree that opens the table.

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Group 6	SRD1 (#1)	Server	Not Configured	ProxySet_0	--	--		Enable	-1	-1
1	Group1	SRD1 (#1)	Server	Not Configured	Proxy_Group1	--	MR1		Enable	-1	-1
2	Group2	SRD1 (#1)	Server	Not Configured	Proxy_Group2	--	MR1		Enable	-1	-1
3	Group3	SRD1 (#1)	Server	Not Configured	Proxy_Group3	--	MR1		Enable	-1	-1
4	Group4	SRD1 (#1)	Server	Not Configured	Proxy_Group4	--	MR1		Enable	-1	-1
5	Group5	SRD1 (#1)	Server	Not Configured	Proxy_Group5	--	MR1		Enable	-1	-1

- Parameter names (standalone or table) and values can be searched in the Web interface
  - The search key can include the full parameter name (Web or ini file name) or a substring of it
  - For a substring, all parameters containing the substring in their names are listed in the search result
  - The search key for a parameter value can include alphanumeric and certain characters
    - The key can be a complete value or a partial value
- When the device completes the search, it displays a list of found results based on the search key
  - Each possible result, when clicked, opens the page on which the parameter or value is located

# Searching for Configuration Parameters

Search results for: SBC

Search by name:

Page	Parameter	Value	Description
<a href="#">Signaling &amp; Media-&gt;CORE ENTITIES-&gt;IP Groups</a>	SBC Client Forking Mode		0 - Sequential route to all contacts who registered with same AOR. 1 - Fork INVITE messages in parallel to all registered contacts (up to 5). 2 - Sequential route only to available contacts
<a href="#">Signaling &amp; Media-&gt;CORE ENTITIES-&gt;IP Groups</a>	SBC PSAP Mode		SBC PSAP Mode
<a href="#">Signaling &amp; Media-&gt;CORE ENTITIES-&gt;IP Groups</a>	SBC Operation Mode		Overrides the same parameter in the SRD, when configured
<a href="#">Signaling &amp; Media-&gt;CODERS &amp; PROFILES-&gt;IP Profiles</a>	SBC Media Security Mode		Determines the transcoding method between SRTP and RTP.
<a href="#">Signaling &amp; Media-&gt;CODERS &amp; PROFILES-&gt;IP Profiles</a>	SBC Enforce MKI Size		SBC Enforce MKI Size
<a href="#">Signaling &amp; Media-&gt;CODERS &amp; PROFILES-&gt;IP Profiles</a>	SBC Remove Crypto Lifetime in SDP		SBC SDP Remove Crypto Lifetime
<a href="#">Signaling &amp; Media-&gt;CODERS &amp; PROFILES-&gt;IP Profiles</a>	SBC Media Security Method		Determines the SRTP method SDES/DTLS.
<a href="#">Signaling &amp; Media-&gt;CORE ENTITIES-&gt;SRDs</a>	SBC Operation Mode		For Call Stateful Proxy, the SBC uses the same Call-Id and From tag for both sides of calls and dialogs. For B2BUA it changes them
<a href="#">Signaling &amp; Media-&gt;CORE ENTITIES-&gt;SRDs</a>	SBC Routing Policy		SBCRoutingPolicy Name
<a href="#">Signaling &amp; Media-&gt;CORE ENTITIES-&gt;Proxy Sets</a>	SBC IPv4 SIP Interface		SBCIPv4 SIPInterface Name
<a href="#">Signaling &amp; Media-&gt;CORE ENTITIES-&gt;Proxy Sets</a>	SBC IPv6 SIP Interface		SBCIPv6 SIPInterface Name

Search by value:

Page	Parameter	Value	Description
<a href="#">Signaling &amp; Media-&gt;SBC-&gt;Routing-&gt;Routing Policies</a>	Name	Default_SBCRoutingPolicy	Name

Save    Reset    Actions ▾    Admin ▾

2

Search can be by name or by value

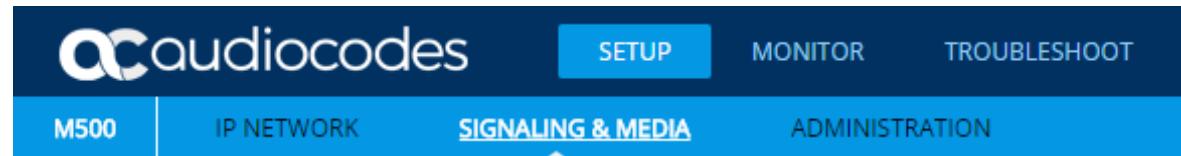
# Setup Menu

- 3 Options:

- IP Network



- Signaling & Media



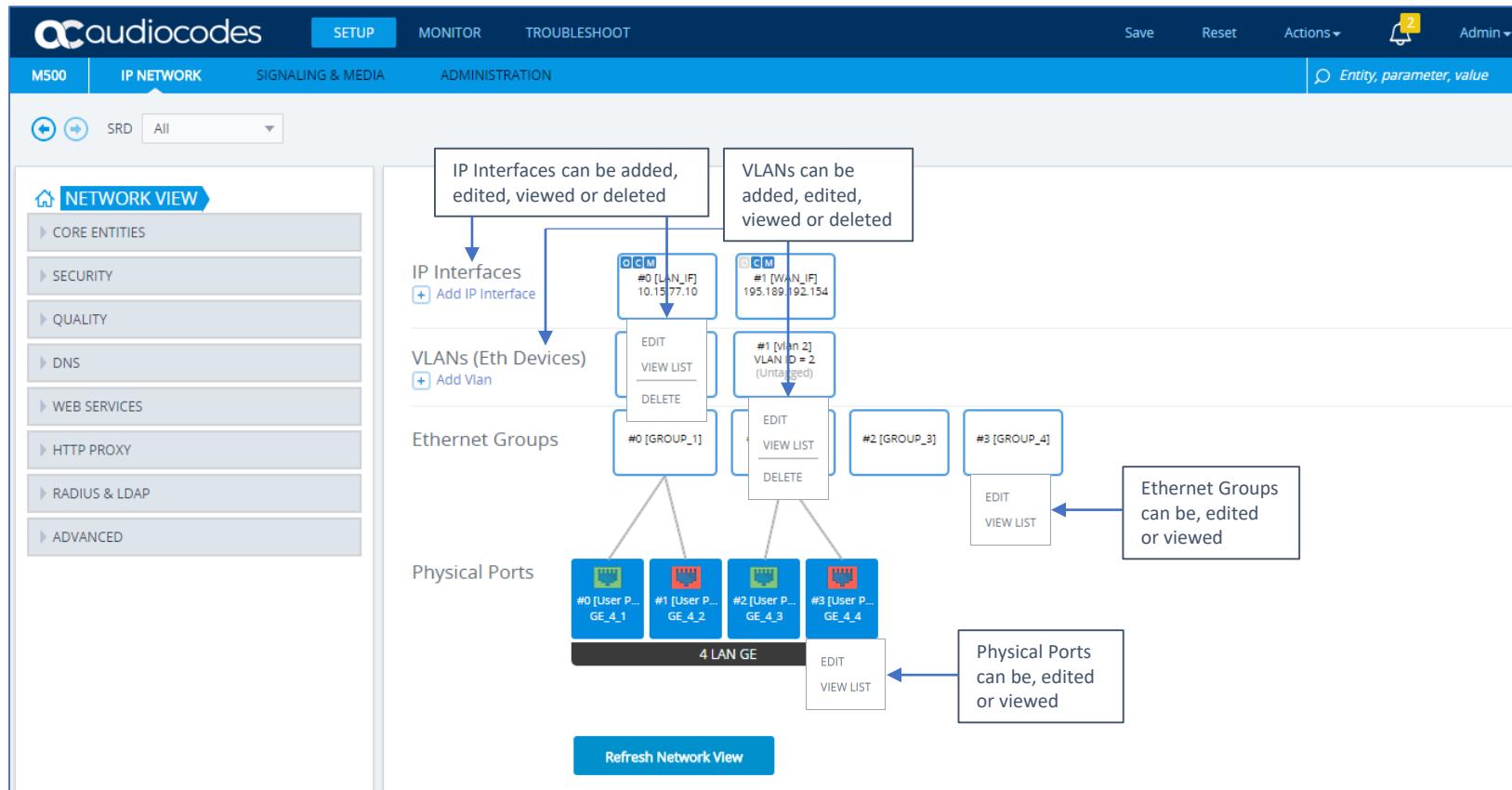
- Administration



- Home Page: NETWORK VIEW
  - Shows a graphical display of the core networking entities
    - IP interfaces
    - VLANs (Ethernet Devices)
    - Ethernet Groups
    - Physical Ethernet ports
  - Enables the administrator to easily build and view the main network topology
- Other Pages
  - Networking Core Entities
  - Security
  - Quality
  - DNS
  - WEB Services
  - HTTP Proxy
  - Radius & LDAP
  - Advanced

# Setup Menu: IP Network Option

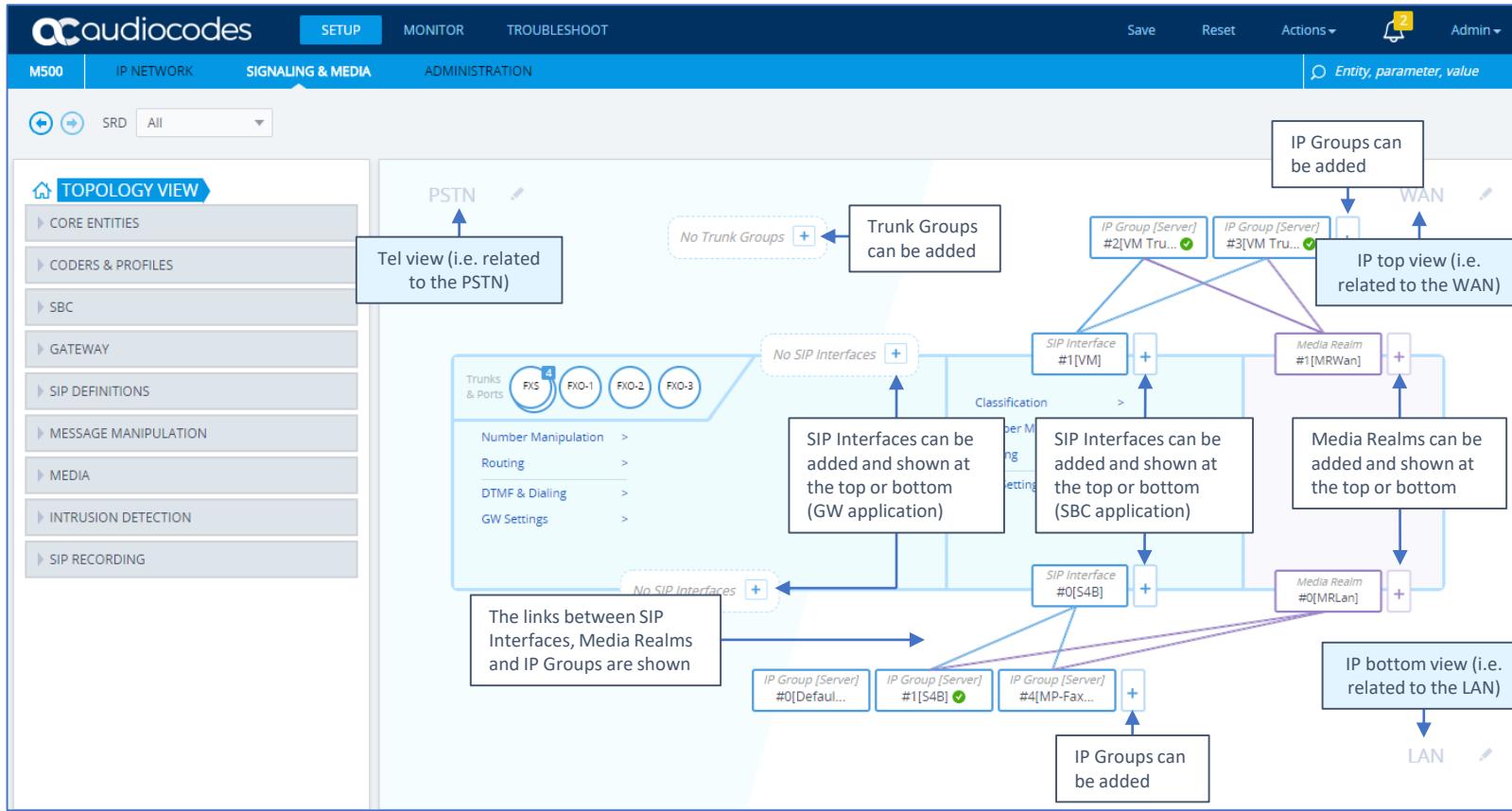
- Home Page: NETWORK VIEW



- Home Page: **TOPOLOGY VIEW**
  - Shows a graphical display of the core SIP configuration entities
    - IP Groups
    - SIP Interfaces
    - Media Realms
  - Enables the administrator to easily build and view the SIP topology
- Other Pages
  - Signaling and Media Core Entities
  - Gateway
  - Media
  - Coders and Profiles
  - SBC
  - SIP Definition
  - Message Manipulation
  - Intrusion Detection
  - SIP Recording

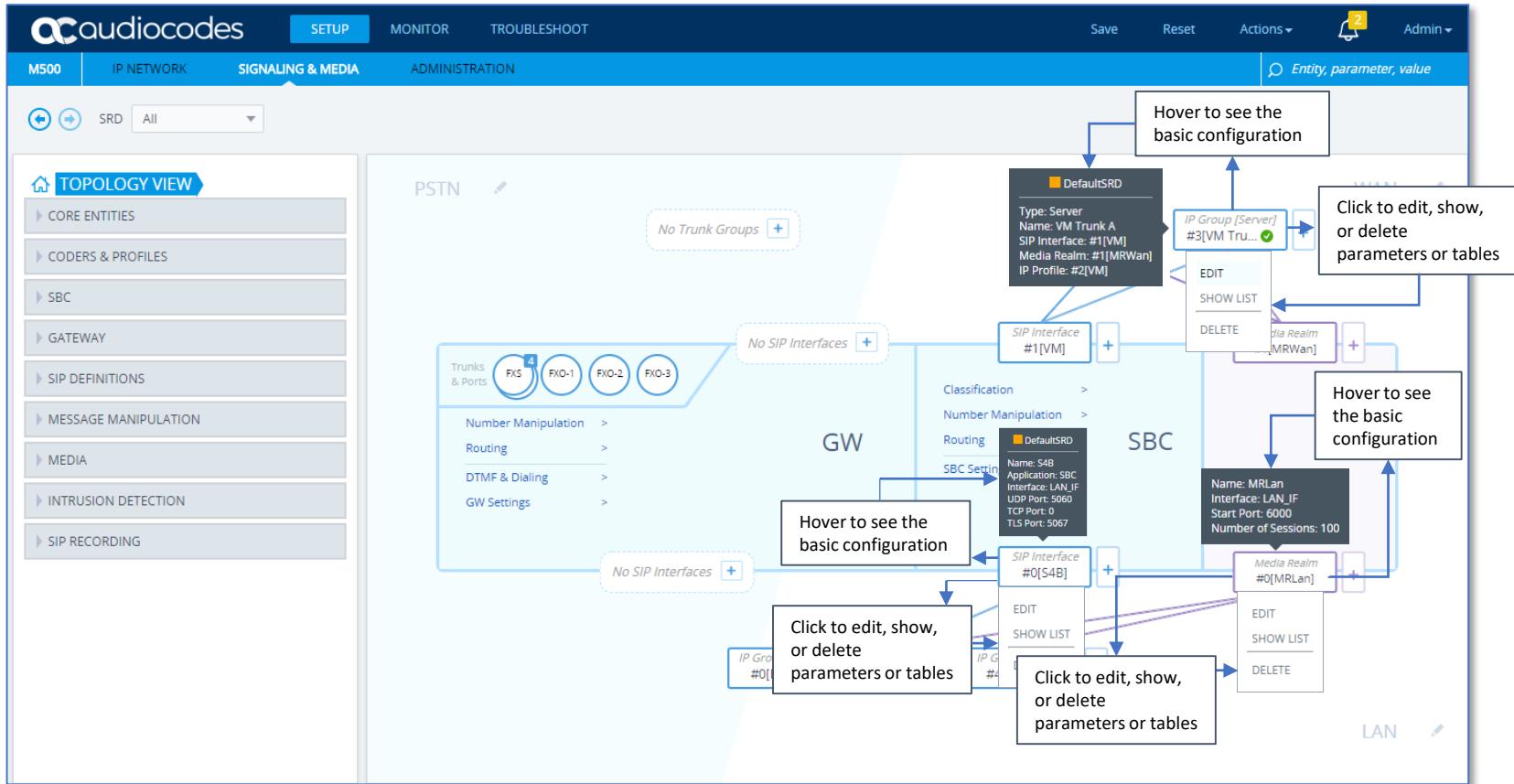
# Setup Menu: Signaling & Media Option

- Home Page: TOPOLOGY VIEW



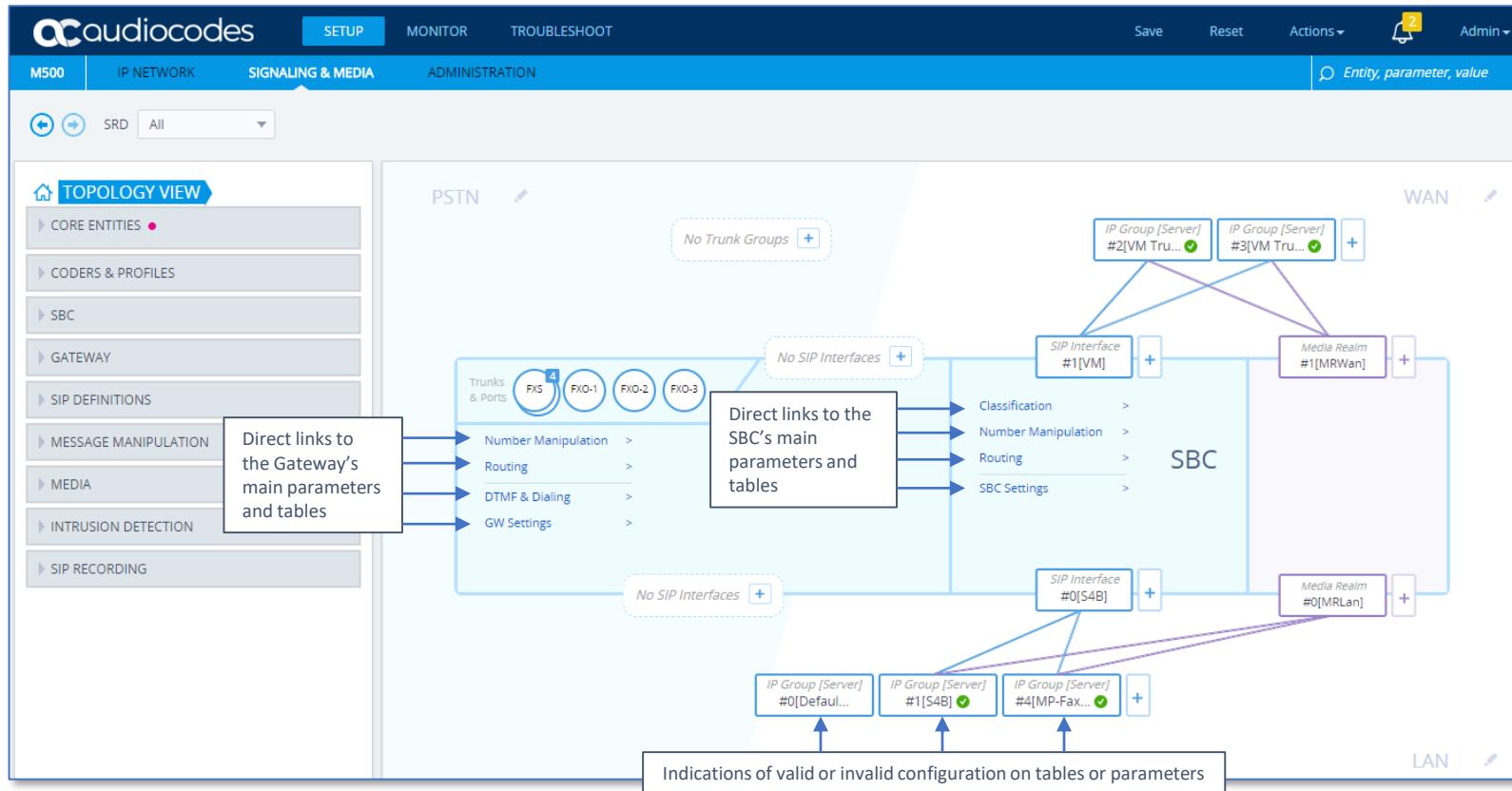
# Setup Menu: Signaling & Media Option

- Home Page: TOPOLOGY VIEW



# Setup Menu: Signaling & Media Option

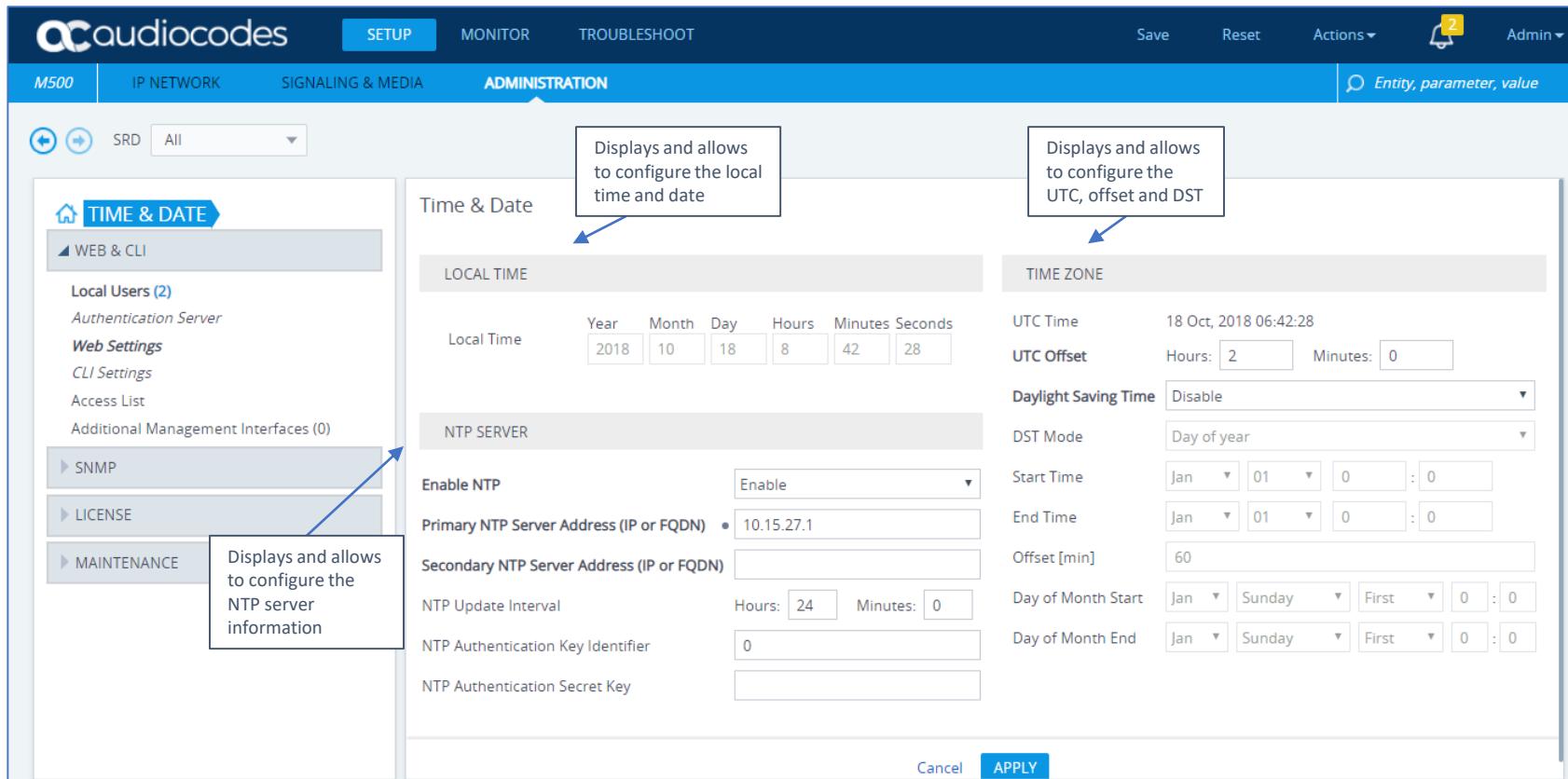
- Home Page: TOPOLOGY VIEW



- Home Page: TIME & DATE
  - Shows and allows to configure parameters related to:
    - Local Time
    - NTP Information
    - Time Zone
- Other Pages
  - WEB & CLI pages
  - SNMP Pages
  - Maintenance

# Setup Menu: Administration Option

- Home Page: TIME & DATE



The screenshot shows the audiocodes M500 web interface with the following navigation path:

- Home
- IP NETWORK
- SIGNALING & MEDIA
- ADMINISTRATION** (highlighted)
- Entity, parameter, value

The main content area displays the **TIME & DATE** configuration page. Key sections include:

- LOCAL TIME**: Displays and allows to configure the local time and date.
- NTP SERVER**: Displays and allows to configure the NTP server information.
- TIME ZONE**: Displays and allows to configure the UTC, offset and DST.

Configuration fields shown in the LOCAL TIME section:

Local Time	Year	Month	Day	Hours	Minutes	Seconds
Local Time	2018	10	18	8	42	28

Configuration fields shown in the NTP SERVER section:

- Enable NTP: Enable (dropdown menu)
- Primary NTP Server Address (IP or FQDN): 10.15.27.1
- Secondary NTP Server Address (IP or FQDN): (empty input field)
- NTP Update Interval: Hours: 24 Minutes: 0
- NTP Authentication Key Identifier: 0
- NTP Authentication Secret Key: (empty input field)

Configuration fields shown in the TIME ZONE section:

- UTC Time: 18 Oct, 2018 06:42:28
- UTC Offset: Hours: 2 Minutes: 0
- Daylight Saving Time: Disable (dropdown menu)
- DST Mode: Day of year (dropdown menu)
- Start Time: Jan 01 0 0 : 0
- End Time: Jan 01 0 0 : 0
- Offset [min]: 60
- Day of Month Start: Jan Sunday First 0 : 0
- Day of Month End: Jan Sunday First 0 : 0

Buttons at the bottom:

- Cancel
- APPLY

A callout box in the sidebar indicates that the **LICENSE** section displays and allows to configure the NTP server information.

# Web Local Users Table

Main ITSP    SETUP    MONITOR    TROUBLESHOOT

MEDIANT 1000    IP NETWORK    SIGNALING & MEDIA    ADMINISTRATION    Entity, parameter, value

Save    Reset    Actions ▾    Admin ▾

SRD All

**TIME & DATE**

WEB & CLI

**Local Users (2)**

Authentication Server  
Web Settings  
CLI Settings  
Access List  
Additional Management Interfaces (0)

SNMP

MAINTENANCE

User levels:  
• End User  
• Monitor  
• Administrator  
• Security Administrator  
• Master

**Local Users (2)**

+ New    Edit   

Page 1 of 1 Show 10 records per page

INDEX	USERNAME	PASSWORD	STATUS	PASSWORD AGE	WEB SESSION LIMIT	CLI SESSION LIMIT	WEB SESSION TIMEOUT	BLOCK DURATION	USER LEVEL
0	Admin	*	Valid	0	2	-1	15	60	Security Administrat
1	User	*	Valid	0	2	-1	15	60	Monitor

#0 **Username & Password**

GENERAL

Username: Admin

Password: \*

User Level: Security Administrator

SSH Public Key: .d

Status: Valid

SECURITY

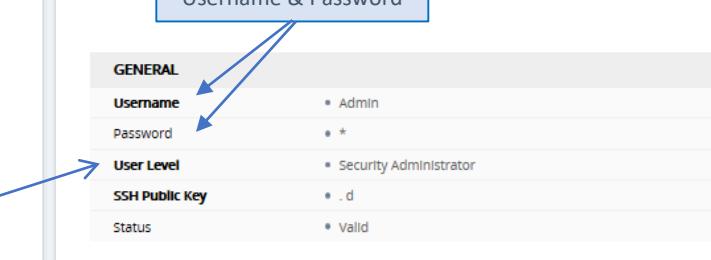
Password Age: 0

Web Session Limit: 2

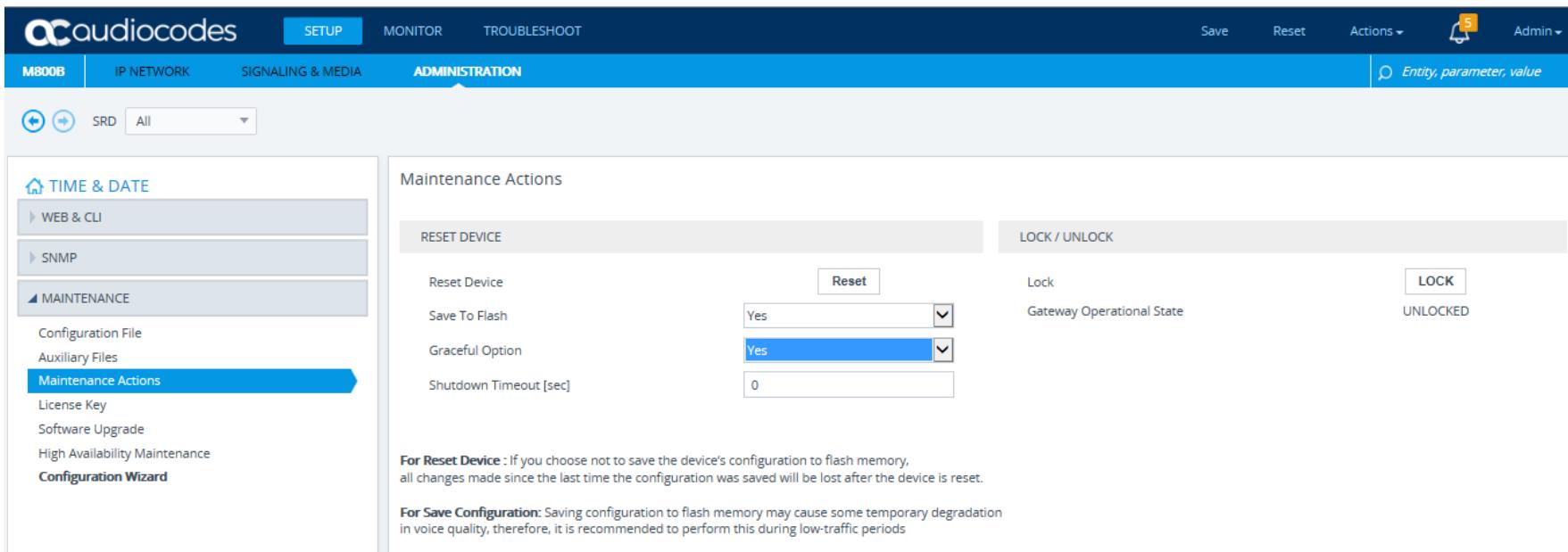
CLI Session Limit: -1

Web Session Timeout: 15

Block Duration: 60



- **Reset Device:** After a Web reset, the device starts from Flash
- **Lock:** The device doesn't accept any new incoming calls
- **Save to Flash:** Save the running configuration to the memory
- **Graceful Option:** Shutdown will perform only after X configured sec. or no more active traffic



The screenshot shows the audiocodes M800B web interface. The top navigation bar includes links for SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, Admin, and Entity, parameter, value. The left sidebar has sections for TIME & DATE, WEB & CLI, SNMP, MAINTENANCE (which is selected), Configuration File, Auxiliary Files, Maintenance Actions (highlighted with a blue arrow), License Key, Software Upgrade, High Availability Maintenance, and Configuration Wizard.

The main content area is titled "Maintenance Actions". It contains two main sections: "RESET DEVICE" and "LOCK / UNLOCK".

**RESET DEVICE:**

- Reset Device: A button labeled "Reset".
- Save To Flash: A dropdown menu set to "Yes".
- Graceful Option: A dropdown menu set to "Yes".
- Shutdown Timeout [sec]: An input field containing "0".

**LOCK / UNLOCK:**

- Lock: A button labeled "LOCK".
- Gateway Operational State: A status indicator showing "UNLOCKED".

**Textual Notes:**

- For Reset Device:** If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset.
- For Save Configuration:** Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods.

# Maintenance: Configuration File

The screenshot shows the audiocodes web interface for the MB00B device. The navigation bar includes links for SETUP, MONITOR, TROUBLESHOOT, ADMINISTRATION, and various system status indicators. The left sidebar has sections for TIME & DATE, WEB & CLI, SNMP, MAINTENANCE, and Configuration File, with Configuration File selected. The main content area is titled 'Configuration File' and contains three sections: 'INI FILE', 'CLI SCRIPT', and 'CONFIGURATION PACKAGE'. The 'INI FILE' section includes 'Save INI file to the PC.' and 'Load INI file to the device.' buttons. The 'CLI SCRIPT' section includes 'Save CLI Script file to the PC.', 'Load CLI Script file to the device.', and 'Load CLI Startup Script to the device.' buttons. The 'CONFIGURATION PACKAGE' section includes 'Save Configuration Package to the PC.' and 'Load Configuration Package to the device.' buttons. A callout box highlights the 'Restore Factory Defaults' button and the 'Preserve Network and Users configuration.' checkbox. Another callout box explains how to restore defaults using an empty ini file or the 'Restore Defaults' option. A final callout box describes the Configuration Package feature for backup and restore operations.

audiocodes

SETUP MONITOR TROUBLESHOOT

MB00B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions Admin

Entity, parameter, value

SRD All

TIME & DATE

WEB & CLI

SNMP

MAINTENANCE

Configuration File

Auxiliary Files  
Maintenance Actions  
License Key  
Software Upgrade  
High Availability Maintenance  
Configuration Wizard

INI FILE

Save INI file to the PC.

Load INI file to the device.

Save INI File

Load INI File

The device will perform a reset after loading the INI file.

CLI SCRIPT

Save CLI Script file to the PC.

Load CLI Script file to the device.

Load CLI Startup Script to the device.

Save CLI Script File

Load CLI Script File

Load CLI Startup Script

CONFIGURATION PACKAGE

Save Configuration Package to the PC.

Load Configuration Package to the device.

Save Configuration Package

Load Configuration Package

RESTORE THE DEFAULT CONFIGURATION OF THE DEVICE.

Restore Factory Defaults

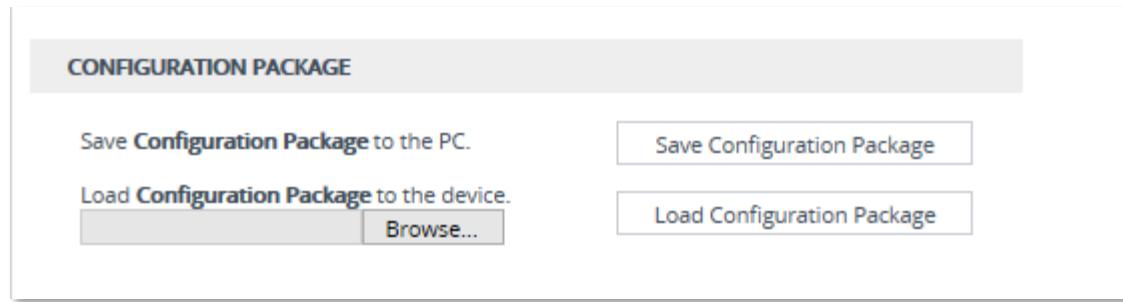
Preserve Network and Users configuration.

To restore the defaults, use an *empty ini file* (except for the incremental option via the Auxiliary Files page – later more on this) or '*Restore Defaults*' with checked '**'Preserve Network and users Configuration'** (option supported only on Mediant Family Devices)

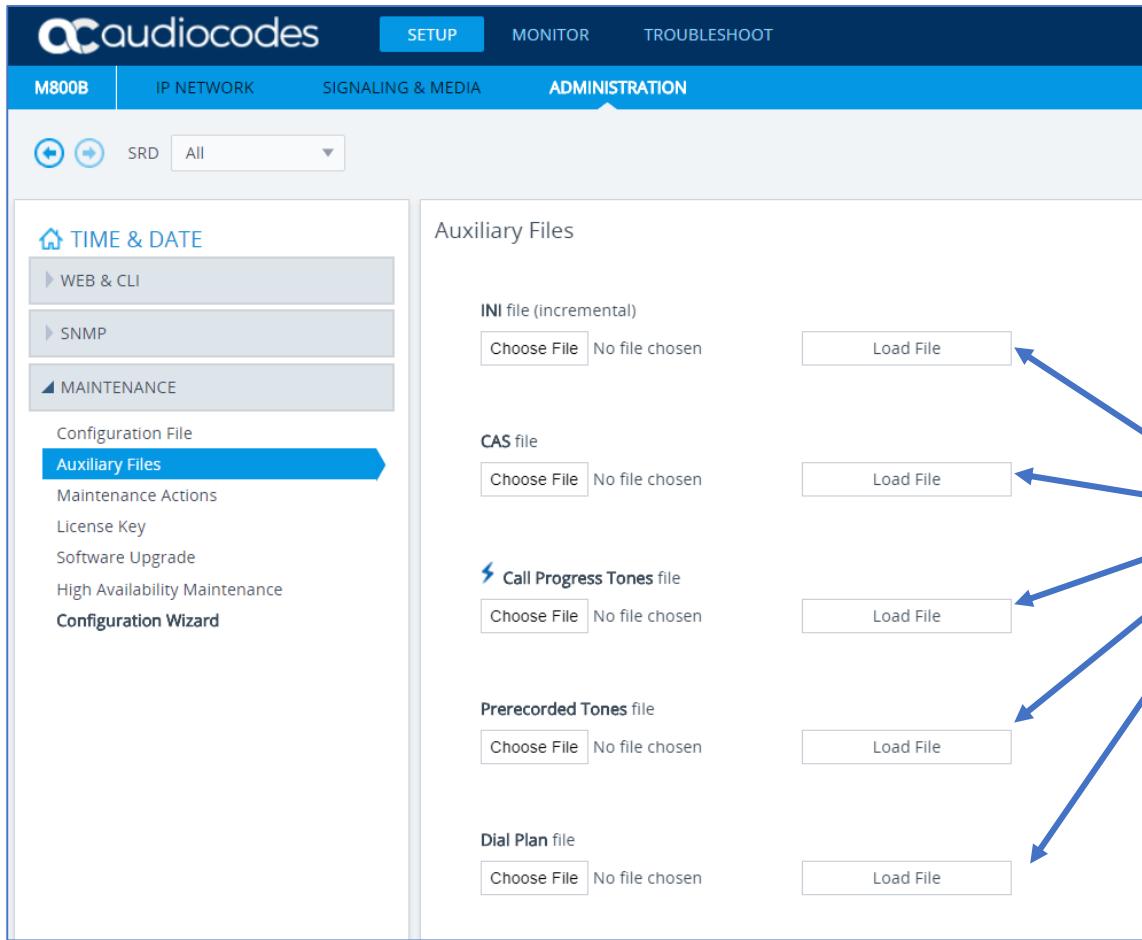
Configuration, Auxiliary and Certificate files can be loaded to and saved from the device as a single, packaged file. The feature is typically used for backup and loading the backup to other devices.

# Configuration Package Files

- INI.ini
- LOGO.dat
- FAVICON.dat
- CPT.dat
- PRT.dat
- AMD.dat
- SBC\_Wizard.dat
- CAS.dat
- DPLN.dat (Dial Plan)
- Certificate files
- DialPlanRule.csv (import only - can load any CSV file. For example, User-Info Table)



# Maintenance: Auxiliary Files



The screenshot shows the audiocodes M800B web interface. The navigation bar includes SETUP, MONITOR, TROUBLESHOOT, M800B, IP NETWORK, SIGNALING & MEDIA, and ADMINISTRATION. The ADMINISTRATION tab is selected. On the left, a sidebar under MAINTENANCE lists Configuration File, Auxiliary Files (which is selected and highlighted in blue), Maintenance Actions, License Key, Software Upgrade, High Availability Maintenance, and Configuration Wizard.

The main content area is titled "Auxiliary Files" and contains five sections:

- INI file (incremental)**: Includes "Choose File" and "Load File" buttons.
- CAS file**: Includes "Choose File" and "Load File" buttons.
- Call Progress Tones file**: Includes "Choose File" and "Load File" buttons.
- Prerecorded Tones file**: Includes "Choose File" and "Load File" buttons.
- Dial Plan file**: Includes "Choose File" and "Load File" buttons.

A callout box on the right side of the interface states: "Various auxiliary files can be loaded to the device".

# Maintenance: Upgrading & Downgrading Software



- The device can be updated with software (cmp file), configuration (ini file), auxiliary files and license key using:
  - Web interface
  - BootP/TFTP utility
  - Automatic Update Mechanism

The screenshot shows the audiocodes M800B web interface. The top navigation bar includes links for SETUP, MONITOR, TROUBLESHOOT, and ADMINISTRATION. The ADMINISTRATION tab is selected. On the left sidebar under MAINTENANCE, the Software Upgrade option is highlighted. The main content area displays the "Software Upgrade" page with a large blue arrow pointing to the "Start Software Upgrade" button. A warning message below the button states: "In case of an upgrade failure, the device will reset and the previous configuration saved to flash will be lost." The left sidebar also lists Configuration File, Auxiliary Files, Maintenance Actions, License Key, and Configuration Wizard.

The screenshot shows the "Software Upgrade Wizard - Google Chrome" window. The URL is 10.15.11.11/SoftwareUpdateIndex. The left sidebar lists file types: CMP file, INI file, CPT file, PRT file, CAS file, USRINF file, AMD file, and FINISH. The main panel has a "Choose File" button with the message "No file chosen" and a warning: "Warning: Once you load the CMP file, you must complete the upgrade process." A "Load File" button is also present. At the bottom are Back, Next, Cancel, and Reset buttons.

- Supplied with digital gateways (not relevant for MP-1xx)
- Determines features, capabilities and available resources
- Provided in string format or in a txt file to be loaded to the device
- Stored in the device's non-volatile flash memory
- After loading the new key, the device must be reset

# Maintenance: License Key

audiocodes

SETUP MONITOR TROUBLESHOOT

Save Reset Actions ▾ Entity, parameter, value

M500 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

TIME & DATE

WEB & CLI

SNMP

MAINTENANCE

Configuration File

Auxiliary Files

Maintenance Actions

**License Key**

Floating License

Software Upgrade

High Availability Maintenance

Configuration Wizard

License Key

Product Key	Local License Key	Serial Number	Device Type
	4965606		77

GENERAL		VOIP SIGNALING PROTOCOLS		SBC CAPACITY	
High Availability (HA)	30	SIP	MGCP	SBC Sessions	Local Actual
DSP Channels	30			Far End Users (FEU)	100 100
IPMedia DSP Channels	30				100 600

SKYPE FOR BUSINESS		VOIP FEATURES		CODERS	
MSFT	30	Voice Quality Monitoring	100	G.723 NETCODER AMR G.729 G.727 G.786	
		Test Call		GSM-EFR GSM-FR EVRC QCELP ILBC EVRC-B	
		RTCP-XR		AMR-WB G.722 Enhanced G.711 MS RTA-NB	
		Media Enhancement		MS RTA-WB SILK-NB SILK-WB Speex-NB	
				Speex-WB Opus-NB Opus-WB	

TELEPHONY INTERFACES		SECURITY FEATURES		IP MEDIA FEATURES	
FXS Ports	3	IPSec		VXML	
FXO Ports	1	Media Encryption			
		Strong Encryption			
		Encrypt Control Protocol			

Floating License Load File Load String

Screenshot of the audiocodes M800B web interface showing the High Availability Maintenance page.

The top navigation bar includes: SETUP (selected), MONITOR, TROUBLESHOOT, Save, Reset, Actions (with a notification count of 4), and Admin.

The left sidebar shows: TIME & DATE, WEB & CLI, SNMP, MAINTENANCE (selected), Configuration File, Auxiliary Files, Maintenance Actions, License Key, Software Upgrade, High Availability Maintenance (selected), and Configuration Wizard.

The main content area is titled "High Availability Maintenance". It contains two sections: "SWITCH OVER" and "REDUNDANT OPTIONS".

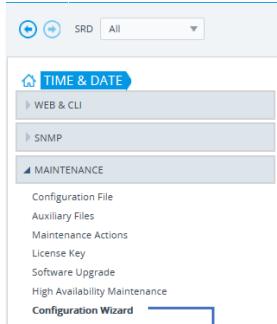
**SWITCH OVER:** Contains the action "Switch Between Active And Redundant Boards" with a "Switch Over" button. A blue arrow points from this section to the "Switch Over" button.

**REDUNDANT OPTIONS:** Contains the action "Reset The Redundant Board" with a "Reset" button. A blue arrow points from this section to the "Reset" button.

**Note:** These operations will result with no high availability for a period of time.

# Maintenance: Configuration Wizard

- **The SBC configuration wizard** provides fast SBC configuration
- Based on a large set of tested interoperability configurations
- User selects a PBX type and service provider SIP trunk type from a list of over 30 PBX models and 100 SIP trunks
- Data base updates automatically with new PBX models and SIP trunks from the cloud
- Available in both standalone windows app and embedded on the SBC web GUI



Welcome to SBC configuration wizard

**INTRODUCTION**

This wizard will assist you with initial device configuration. You will be asked to select configuration template and network topology. Once done, you will be prompted to fill a short questionnaire to describe your setup details. The wizard will conclude by generating new device configuration based on all provided input.

Template pack version: 2.16

**USAGE STATISTICS**

Report usage statistics

End Customer

Country  Select a country

Integrator

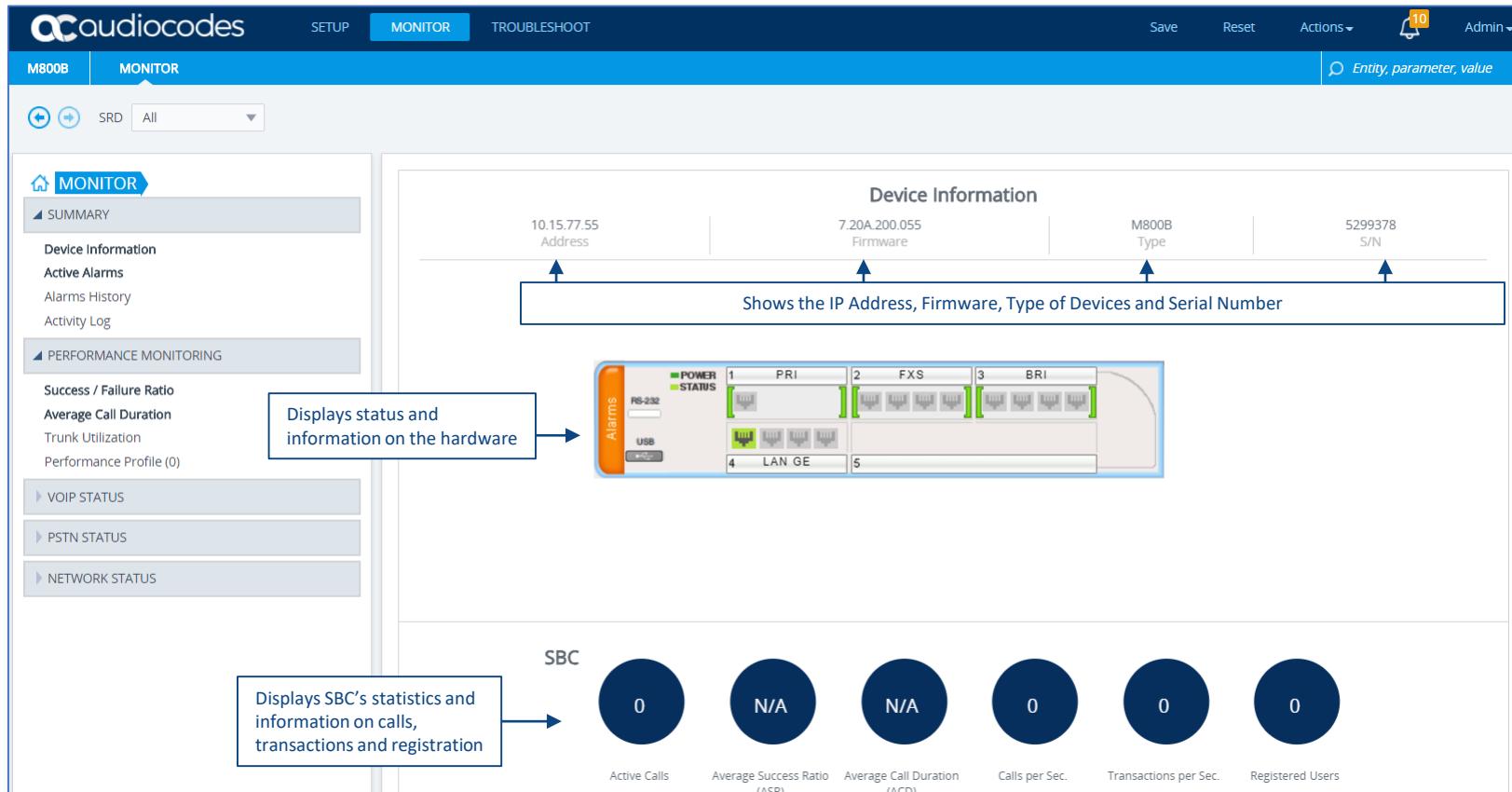
Installer

**WARNING:** Please note that when configuration wizard is completed it will overwrite all of the existing device configuration

- One Option: Monitor
- Home Page: MONITOR
  - Shows a graphical display of the Device
    - Device Information
    - Alarms Status
    - Activity Log
  - Enables the administrator to easily view the device's main information and statuses
- Other Pages
  - Performance Monitoring
  - VoIP Status
  - PSTN Status
  - Network Status

# Monitor Menu

- Home Page: MONITOR



The screenshot shows the audiocodes M800B monitor interface. The top navigation bar includes links for SETUP, MONITOR (which is selected), and TROUBLESHOOT, along with Save, Reset, Actions (with a notification count of 10), and Admin.

The left sidebar contains sections for MONITOR (SUMMARY, Device Information, Active Alarms, Alarms History, Activity Log), PERFORMANCE MONITORING (Success / Failure Ratio, Average Call Duration, Trunk Utilization, Performance Profile (0)), VOIP STATUS, PSTN STATUS, and NETWORK STATUS.

The main content area is divided into two main sections:

- Device Information:** Displays the IP Address (10.15.77.55), Firmware (7.20A.200.055), Type (M800B), and Serial Number (5299378). A callout notes: "Shows the IP Address, Firmware, Type of Devices and Serial Number".
- SBC:** Displays SBC's statistics and information on calls, transactions and registration. It includes circular indicators for Active Calls (0), Average Success Ratio (N/A), Average Call Duration (ACD) (N/A), Calls per Sec. (0), Transactions per Sec. (0), and Registered Users (0).

A central box labeled "Displays status and information on the hardware" points to a diagram of the M800B hardware board, which shows slots for PRI, FXS, BRI, LAN GE, and RS-232/USB ports, each with a green power LED and a green status LED.

A callout for the SBC section notes: "Displays SBC's statistics and information on calls, transactions and registration".

# Device Information



audiocodes

SETUP MONITOR TROUBLESHOOT

Save Reset Actions ▾ Admin ▾

Entity, parameter, value

M800B MONITOR SRD All

MONITOR SUMMARY Device Information Active Alarms Alarms History Activity Log PERFORMANCE MONITORING VOIP STATUS PSTN STATUS NETWORK STATUS

Device Information

GENERAL SETTINGS

MAC Address:	00908f5e85ba	←
Serial Number:	6194618	
Product Key:		
Board Type:	72	
Device Up Time:	0d:23h:6m:40s:99th	
Device Administrative State:	Unlocked	
Device Operational State:	Enabled	←
Flash Size [Mbytes]:	64	
RAM Size [Mbytes]:	512	
CPU Speed [MHz]:	500	

LOADED FILES

Call Progress Tones File Name:	usa_tones_13.dat	←
		Delete

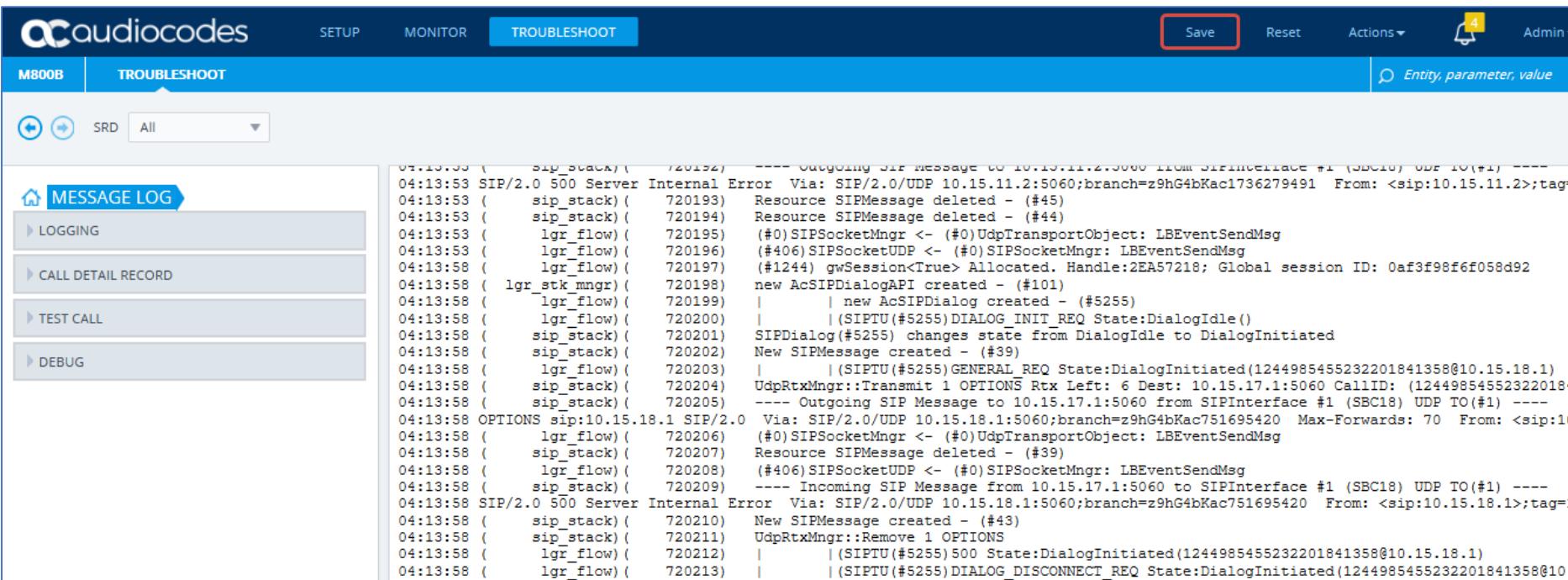
VERSIONS

Version ID:	7.20A.200.016	←
DSP Type:	1	
DSP Software Version:	72162	
DSP Software Name:	5014AE3_R	
Flash Version:	0	

- One Option: TROUBLESHOOT
- Home Page: Message Log
  - If logging is active, it shows the device's activity
- Other Pages
  - Logging configuration
  - Call Detail Record
  - Test Calls
  - Debug

# Troubleshoot Menu

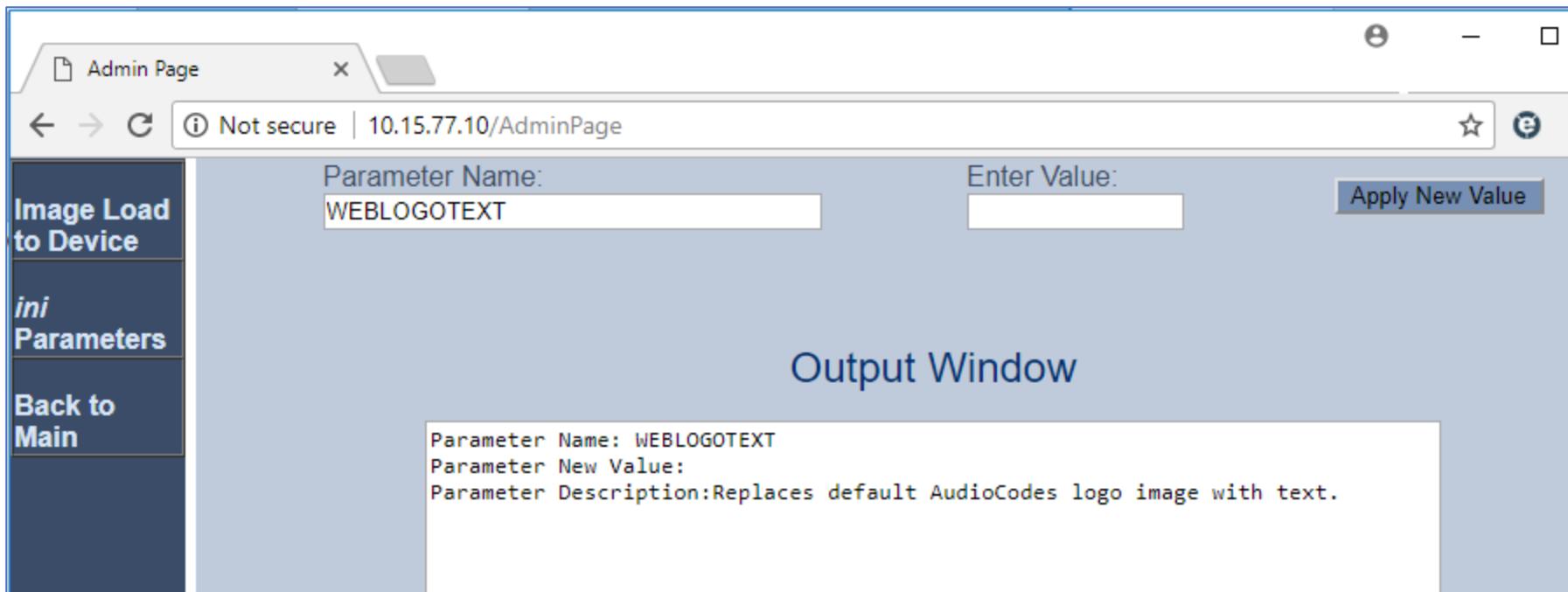
- Home Page: MESSAGE LOG



The screenshot shows the audiocodes M800B Troubleshoot interface. The left sidebar has tabs for MESSAGE LOG (selected), LOGGING, CALL DETAIL RECORD, TEST CALL, and DEBUG. The main area is titled "MESSAGE LOG" and displays a log of SIP messages and system events. The log entries are as follows:

```
04:13:53 ( sip_stack)( 720192) ---- Outgoing SIP Message to 10.15.11.2:5060 from SIPInterface #1 (SBC18) UDP TO(#1) ----
04:13:53 SIP/2.0 500 Server Internal Error Via: SIP/2.0/UDP 10.15.11.2:5060;branch=z9hG4bKac1736279491 From: <sip:10.15.11.2>;tag=#
04:13:53 ( sip_stack)( 720193) Resource SIPMessage deleted - (#45)
04:13:53 ( sip_stack)( 720194) Resource SIPMessage deleted - (#44)
04:13:53 ( lgr_flow)( 720195) (#0)SIPSocketMngr <- (#0)UdpTransportObject: LBEventSendMsg
04:13:53 ( lgr_flow)( 720196) (#406)SIPSockeUDP <- (#0)SIPSocketMngr: LBEventSendMsg
04:13:58 ( lgr_flow)( 720197) (#1244) gwSession<True> Allocated. Handle:2EA57218; Global session ID: 0af3f98f6f058d92
04:13:58 ( lgr_stk_mngr)( 720198) new AcSIPDialogAPI created - (#101)
04:13:58 ( lgr_flow)( 720199) |       | new AcSIPDialog created - (#5255)
04:13:58 ( lgr_flow)( 720200) |       | (SIPTU(#5255)DIALOG_INIT_REQ State:DialogIdle())
04:13:58 ( sip_stack)( 720201) SIPDialog(#5255) changes state from DialogIdle to DialogInitiated
04:13:58 ( sip_stack)( 720202) New SIPMessage created - (#39)
04:13:58 ( lgr_flow)( 720203) |       | (SIPTU(#5255)GENERAL_REQ State:DialogInitiated(1244985455232201841358@10.15.18.1)
04:13:58 ( sip_stack)( 720204) UdpRtxMngr::Transmit 1 OPTIONS Rtx Left: 6 Dest: 10.15.17.1:5060 CallID: (1244985455232201841358@10.15.18.1)
04:13:58 ( sip_stack)( 720205) ---- Outgoing SIP Message to 10.15.17.1:5060 from SIPInterface #1 (SBC18) UDP TO(#1) ----
04:13:58 OPTIONS sip:10.15.18.1 SIP/2.0 Via: SIP/2.0/UDP 10.15.18.1:5060;branch=z9hG4bKac751695420 Max-Forwards: 70 From: <sip:10.15.18.1>;tag=#
04:13:58 ( lgr_flow)( 720206) (#0)SIPSocketMngr <- (#0)UdpTransportObject: LBEventSendMsg
04:13:58 ( sip_stack)( 720207) Resource SIPMessage deleted - (#39)
04:13:58 ( lgr_flow)( 720208) (#406)SIPSockeUDP <- (#0)SIPSocketMngr: LBEventSendMsg
04:13:58 ( sip_stack)( 720209) ---- Incoming SIP Message from 10.15.17.1:5060 to SIPInterface #1 (SBC18) UDP TO(#1) ----
04:13:58 SIP/2.0 500 Server Internal Error Via: SIP/2.0/UDP 10.15.18.1:5060;branch=z9hG4bKac751695420 From: <sip:10.15.18.1>;tag=#
04:13:58 ( sip_stack)( 720210) New SIPMessage created - (#43)
04:13:58 ( sip_stack)( 720211) UdpRtxMngr::Remove 1 OPTIONS
04:13:58 ( lgr_flow)( 720212) |       | (SIPTU(#5255)500 State:DialogInitiated(1244985455232201841358@10.15.18.1)
04:13:58 ( lgr_flow)( 720213) |       | (SIPTU(#5255)DIALOG_DISCONNECT_REQ State:DialogInitiated(1244985455232201841358@10.15.18.1)
```

- Used to configure parameters that don't appear in the Web interface



The screenshot shows a web browser window titled "Admin Page" with the URL "Not secure | 10.15.77.10/AdminPage". On the left, a sidebar menu includes "Image Load to Device", "ini Parameters", and "Back to Main". The main content area has a form for configuring a parameter:

Parameter Name: **WEBLOGOTEXT** Enter Value:

**Output Window**

```
Parameter Name: WEBLOGOTEXT
Parameter New Value:
Parameter Description:Replaces default AudioCodes logo image with text.
```

Which of the following is **false**?

- A. License key doesn't apply to the MP-11x
- B. License key can limit the number of trunks that can be used on the Mediant 1000
- C. License key can be defined for the SBC application on a Mediant 1000
- D. To enable the coder G.711 the required License key should be loaded

How can I assign networking parameters to a Mediant SBC?

- A. Only via DHCP
- B. Only using the CLI interface
- C. Only via HTTP using web browser
- D. Via DHCP, CLI or HTTP using web browser



Configuring the Mediant IP address is done in the:

- A. IP Interfaces table
- B. VLAN table
- C. SIP Definitions General Settings
- D. None of the above

The Call Progress Tone file can be uploaded as:

- A. A Configuration file
- B. An Auxiliary file
- C. SIP Definitions General Settings
- D. None of the above



Which of the following is **true** in the structure of the ini file?

- A. The subsection names have to be written specifically in uppercase
- B. Parameters must be placed in the relevant section in the ini file
- C. When a parameter is missing the assumed value will be 0 (zero)
- D. None of the above

When dot appears in the Web Interface next to parameters it means that:

- A. That is a significant parameter
- B. The value was changed from its default value
- C. Need to perform a device reset for parameter value change to take effect
- D. It doesn't mean a thing





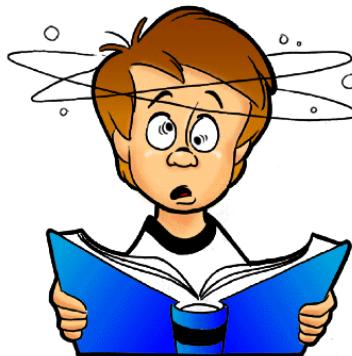
## Lesson 3

# AudioCodes Documentation



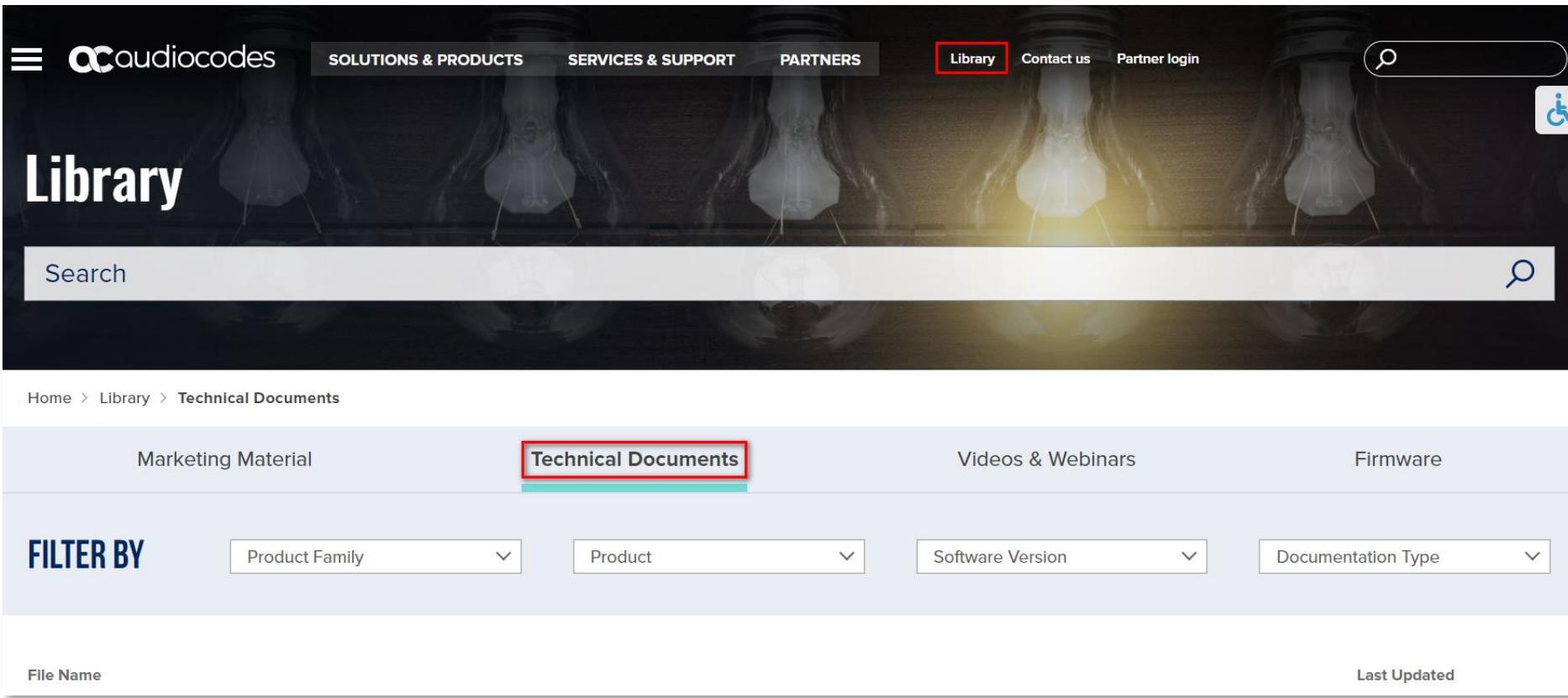
- After completing this lesson, you will:

- Understand how to obtain technical documentation from AudioCodes' Web site
- Be familiar with the different documents that AudioCodes publishes regularly for its' products
- Understand how to use the documents for configuration and maintenances purposes



- You can access all AudioCodes' documentation from AudioCodes Web site
- This includes:
  - Technical documentation (user manuals, hardware installation manuals, configuration and release notes)
  - Homologation material (regulatory information)
  - Partner/channel material (interoperability guides etc.)
  - Marketing material (white papers, application notes, product notices, etc.)

# Obtaining Document



SOLUTIONS & PRODUCTS SERVICES & SUPPORT PARTNERS

Library Contact us Partner login

Search

Marketing Material

Technical Documents

Videos & Webinars

Firmware

**FILTER BY**

Product Family

Product

Software Version

Documentation Type

File Name

Last Updated

- Use the following filters to search for your document:
  - Product Family: Choose the family to which the product belongs
  - Product: Choose the required product
  - Software Version: Choose an option that is displayed in the format Version <version> (e.g. Version 7.2)
  - Documentation Type: Choose the type of document (e.g. User Manuals)

- Analog Gateways (MediaPack family):
  - MP-11x & MP-124, MP-1288
- Digital Gateways and/or SBCs (Mediant family):
  - Mediant 500L/500, 800, 1000B, 2600, 3000, 4000, 9000, SW Virtual/Server/Cloud Edition
- For each product, the following documents are published per release:
  - User's Manual
  - Hardware Installation Manual

- Main document for configuration and maintenance
  - Divided into parts, such as:
    - Overview of the product
    - Getting started
    - Management tools
    - General System Settings
    - General Configuration
    - Specific applications' description and configuration
    - Maintenance
    - Status, Performance Monitoring and Reporting
    - Diagnostics
    - Appendixes
  - Identified by software release version



- **Hardware description and step-by-step procedures for installing and cabling the device**
  - Divided into chapters, such as:
    - Overview of the product
    - Unpacking the device
    - Physical description
    - Mounting the device
    - Cabling the device
    - Hardware maintenance

## Hardware Installation Manual

*AudioCodes Mediant™ Family of Enterprise Session Border Controllers (E-SBC)*

### Mediant 500 E-SBC



- Besides the previous manuals there are other useful documents

- Release Notes
  - One per software release
  - Includes:
    - New features
    - Updates
    - Bugs fixing
    - Workarounds on existing constraints
    - Others

## Release Notes

*AudioCodes Gateways, Session Border Controllers (SBC) & Multi-Service Business Routers (MSBR)*

**Session Border Controllers  
Multi-Service Business Routers  
Analog & Digital Media Gateways**

Version 7.2

- Complementary Guides

- Includes

- Reference Guides
- Design Guides
- Security Guidelines
- Utilities Guides
- Others

- Identified by software release version

 Reference Guide

*AudioCodes Family of Media Gateways and Session Border Controllers (SBCs)*

## Security Guidelines

SIP Media Gateways and SBCs

Version 7.2

- **Configuration Notes**

- Document providing a detailed description on how to configure a specific feature/function/application for a product
- Normally referenced by the User's Manual

Configuration Note

*AudioCodes Mediant™ Series of Session Border Controllers (SBC)*

## SBC Configuration Examples for Mediant SBC

Version 7.2



## Hands-on Lab 1

## Management Interface Usage





## Lesson 4

# Gateways and SBC Product Line



- After completing this lesson you'll be able to:
  - Identify AudioCodes analog and digital gateways
  - Identify AudioCodes products that support SBC
  - Know entities physical description

- Analog FXS and FXO VoIP gateways
- Available configurations:
  - MP-112 featuring 2 FXS ports
  - MP-114 featuring 4 FXS / FXO / Mixed FXS + FXO ports
  - MP-118 featuring 8 FXS / FXO / Mixed FXS + FXO ports
  - MP-124 featuring 24 FXS ports
  - MP-1288 featuring up to 288 FXS ports
- Firmware file:
  - MP-11x gateways (FXS and FXO) use the same firmware (.cmp) file \*
  - MP-124 gateway requires its own firmware file \*
  - MP-1288 gateway requires its own firmware file

*Note: The latest maintenance firmware version for MP-11x and MP-124 is 6.6*

# Analog Gateways Portfolio



	<b>MP-112</b>	<b>MP-114</b>	<b>MP-118</b>	<b>MP-124</b>	<b>MP-1288</b>
<b>Number of analog ports</b>	2	4	8	24	288
<b>FXS / FXO</b>	FXS	FXS / FXO	FXS / FXO	FXS	FXS
<b>Power Supply</b>	AC	AC	AC	AC / DC	AC / DC



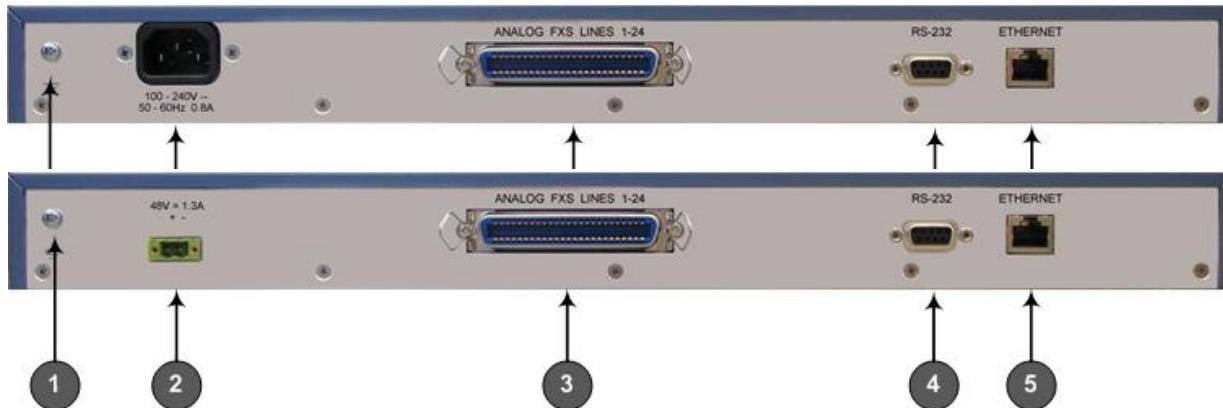
LED	Description		
Channel Status	<span style="color: green;">●</span> <b>Green On:</b> Off-hook <b>Slow Flash:</b> Ringing <b>Fast Flash:</b> Malfunction	<b>Off:</b> On-hook	
Uplink	<span style="color: green;">●</span> <b>Green On:</b> Ethernet up	<b>Off:</b> No Ethernet Link	
Fail	<span style="color: red;">●</span> <b>Red On:</b> Failure or initializing	<b>Off:</b> Normal	
Ready	<span style="color: green;">●</span> <b>Green On:</b> Operational	<b>Off:</b> Loading software or failure	
Power	<span style="color: green;">●</span> <b>Green On:</b> Power on	<b>Off:</b> No power	



<b>1</b>	AC Power Socket
<b>2</b>	RJ-45 10/100BaseTX Ethernet Port
<b>3</b>	Serial RS-232 6-Pin Mini-DIN Female (PS/2) Port
<b>4</b>	RJ-11 FXS Ports
<b>5</b>	Reset Button
<b>6</b>	RJ-11 FXO Ports



LED	Description		
Channels	<span style="color: green;">●</span> <b>Green On:</b> Off-hook <span style="color: red;">●</span> <b>Red On:</b> Line malfunction or unavailable due to SRTP enabled <span style="color: black;">●</span> <b>Off:</b> On-hook		
Data	<span style="color: green;">●</span> <b>Green Flash:</b> Transmitting RTP <span style="color: red;">●</span> <b>Red Flash:</b> Receiving RTP		<span style="color: black;">●</span> <b>Off:</b> No traffic
Control	<span style="color: green;">●</span> <b>Green On:</b> Sending/receiving SIP messages		<span style="color: black;">●</span> <b>Off:</b> No traffic
Lan	<span style="color: green;">●</span> <b>Green On:</b> 10/100BaseTX link		<span style="color: red;">●</span> <b>Red On:</b> Malfunction
Ready	<span style="color: green;">●</span> <b>Green On:</b> Power on <span style="color: yellow;">●</span> <b>Amber Flash:</b> Initializing		<span style="color: red;">●</span> <b>Red On:</b> Malfunction <span style="color: black;">●</span> <b>Off:</b> No power

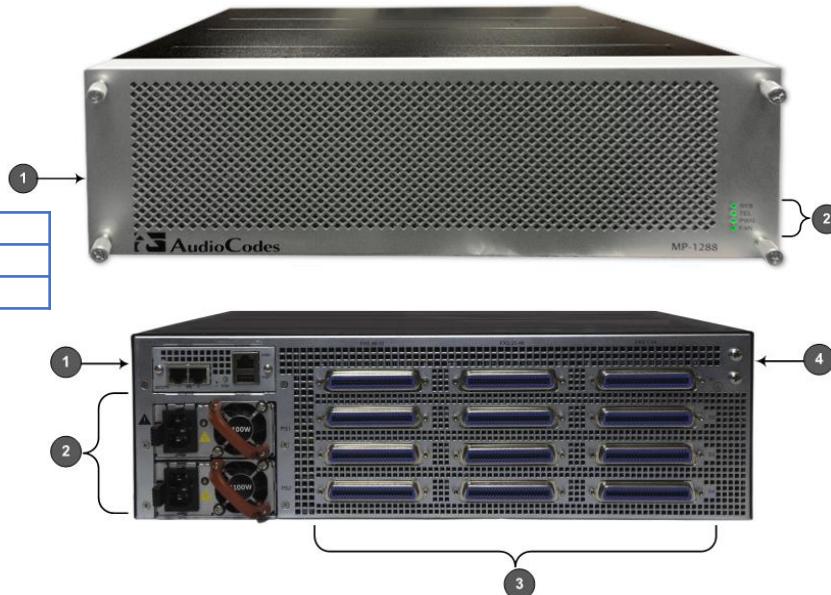


Item	Label	Component Description
1		Protective earthing screw
2	100-240 V~ / 50 - 60Hz 0.8A	AC power supply socket. <i>Note:</i> Applicable only to the AC-powered model.
	48V 1.3A	DC inlet for a DC terminal block. <i>Note:</i> Applicable only to the DC-powered model.
3	ANALOG FXS LINES 1-24	50-pin Telco connector, providing up to 24 analog lines.
4	RS-232	DB-9-pin male port for serial (RS-232) communication.
5	ETHERNET	RJ-45 port for 10/100Base-TX Ethernet interface.

# MP-1288 Overview

- 19" x 3U Chassis
- Single CPU module
- 4 Analog blades, each supporting 72 ports
- 1+1 AC Power Supplies
- Front to Rear Cooling
- Extractable fan tray
- 1+1 Gig ETH connection
- DSPs on each Blade
- Hot-swappable
- Supports short and long haul up to 7.5 Km
- SBC functionality

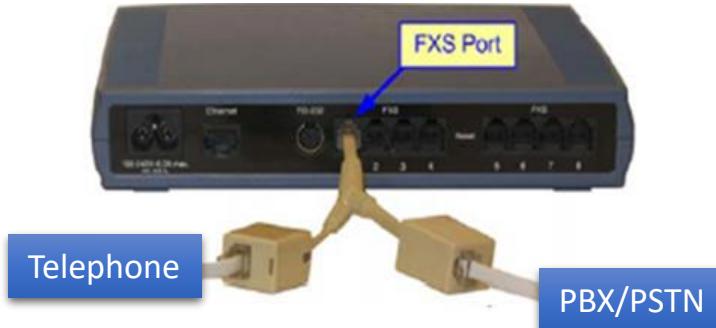
Item #	Label	Description
1	-	Fan Tray cover
2	SYS / TEL / PWR / FAN	Front-panel LEDs



Item #	Label	Description
1	CPU	CPU module providing the central processing unit and various network port interfaces
2	PS1 / PS2	Power Supply modules
3	Blades: S1 / S2 / S3 / S4 FXS Ports: FXS 1-24 / FXS 25-48 / FXS 49-72	FXS blades providing FXS port interfaces
4		Protective grounding for connecting a grounding lug for chassis ground connection for ESD-preventive equipment or a grounding wire

# Analog Lifeline Support

- Provides a wired analog POTS connection to any PSTN or PBX FXS port when power fails or when the network connection fails
- Available configurations:
  - FXS only: A single Lifeline connected to Port #1 using a splitter
  - Mixed FXS and FXO: Splitter not required - all FXS ports automatically connected to FXO ports (e.g., FXS Port 1 to FXO Port 5)
  - FXO only: Lifeline not available
- Activated by parameter *LifeLineType*



# Digital Gateways Overview

- Digital PRI and BRI VoIP gateways
- SBC capability (some of them)
- Up to 16,000 simultaneous calls (M8000)
- Gateway types:
  - Small: Mediant 500L, Mediant 500, Mediant 800B
  - Medium: Mediant 1000B
  - Large: Mediant 3000, Mediant 5000, Mediant 8000
- Note:
  - The latest maintenance firmware version for Mediant 5000 and 8000 is 6.6
  - The latest maintenance firmware version for Mediant 3000 is 7.0



Mediant 500L



Mediant 500



Mediant 800B



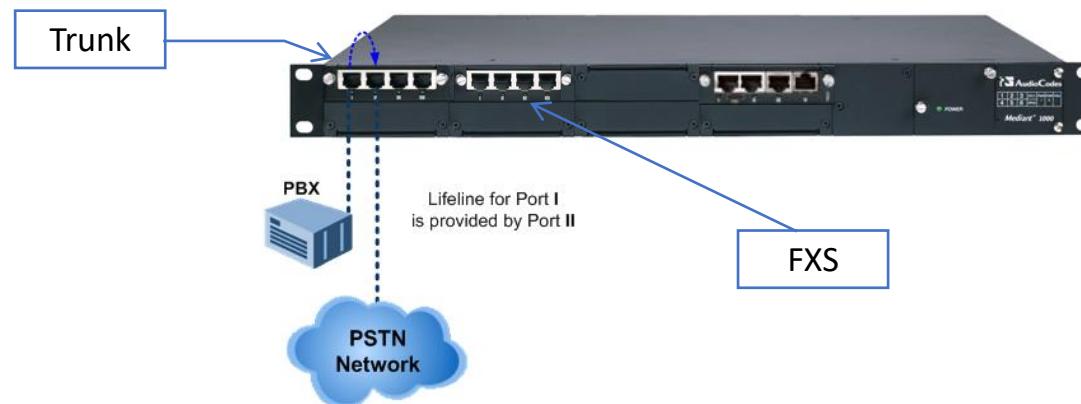
Mediant 1000B



Mediant 3000

- **PSTN Fallback (Digital):**

- If power fails or there is a loss of IP network connectivity, a relay connects trunks 1 to 2 and/or 3 to 4 in the same module
- To provide the link, a metallic switch inside the module closes so that the trunk from the PBX is routed from the module to the PSTN



- **Lifeline (Analog):**

- Lifeline is provided only by Port 1 on an FXS module

## Pure SBC



Mediant 2600



Mediant 4000/B

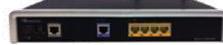


Mediant 90xx



Mediant SE Software Edition

## Hybrid SBC/Gateway



Mediant 500/L



Mediant 800/B/C



Mediant 1000B



Mediant 3000\*

## Virtual & Cloud SBC



vmware



Microsoft® Hyper-V®



Mediant VE (Virtual Edition)

Microsoft  
Azureamazon  
web services™

Mediant CE (Cloud Edition)

**Note:** The latest maintenance firmware version for Mediant 3000 is 7.0

# Pure SBC Portfolio



	<b>Mediant 2600 SBC</b>	<b>Mediant 4000/B SBC</b>	<b>Mediant 9030/9080 SBC</b>	<b>Mediant SE</b>
End customer	Enterprise and Contact Center	Large Enterprise, Service Providers, Contact Centers	Large Enterprise, Service Providers, Contact Centers	Service Providers, OEM
Application	SIP trunking	SIP trunking, Service Provider Access SBC	SIP trunking, SP Access SBC	SIP trunking, SP Access SBC
Sessions	Up to 600	Up to 5,000	30,000/70,000	Up to 55,000
SRTP-RTP	600	3,000/5,000	30,000/Up to 40,000	Up to 40,000
Transcoding	Up to 600 (with MPM4)	Up to 2,400 (with MPM8) / 5,000 (with MPM12B)	9080 only - up to 30,000 w/Media Component (MC)	Up to 25,000 w/MTC
Registers	Up to 8,000	Up to 20,000	200,000/Up to 500,000	Up to 300,000

# Hybrid SBC portfolio



	<b>Mediant 500L E-SBC</b>	<b>Mediant 500 E-SBC</b>	<b>Mediant 800B/C E-SBC</b>	<b>Mediant 1000B E-SBC</b>	<b>Mediant 3000 SBC (7.0)</b>
End customer	Small enterprise, branch	SMB	SMB, branch	SMB, SME, branch	Enterprise, Service Providers
Application	Demarcation device, SIP trunking	SIP trunk, survivability, TDM trunking	SIP trunk, survivability, TDM trunking	SIP and TDM trunking	SIP and TDM trunking
Sessions	60	Up to 250	Up to 400	150	1,008
SRTP-RTP	60	Up to 200	Up to 250	120	1,008
Transcoding	N/A	N/A	Up to 114	96	1,008
Registers	200	Up to 1,500	Up to 2,000	600	3,000
MSBR/MGW	✓ Analog, Up to 4 BRI	✓ Analog, 1 E1/T1	✓ Analog, BRI, 2/4 E1/T1	✓ 6E1/8T1	✓ OC3/STM1/DS3

# Virtual & Cloud SBC Portfolio



	Mediant VE	Mediant CE
End customer	Enterprise, ISVs & OEMs, Service Providers	Enterprise, Service Providers
Application	SIP trunking, SP Access SBC	SIP trunking, SP Access SBC
Sessions	Up to 24,000	Up to 40,000
SRTP to RTP	Up to 10,000	Up to 40,000
Transcoding	Up to 12,000 w/MTC	Up to 30,000 w/Media Component (MC)
Registers	Up to 75,000	Up to 130,000

# Mediant 500L Physical Interfaces

- **LAN Ethernet ports:**
  - Four Gigabit Ethernet (10/100/1000Base-T) LAN ports
- **Optional PSTN interfaces:**
  - Up to 4 BRI
  - Up to 4 FXS/FXO
- **High-Availability 1+1**
- **OAM&P**
  - Embedded HTTP/S-based Web Server
  - Command Line Interface (CLI)
  - Configuration *ini* file
  - SNMP
  - REST API



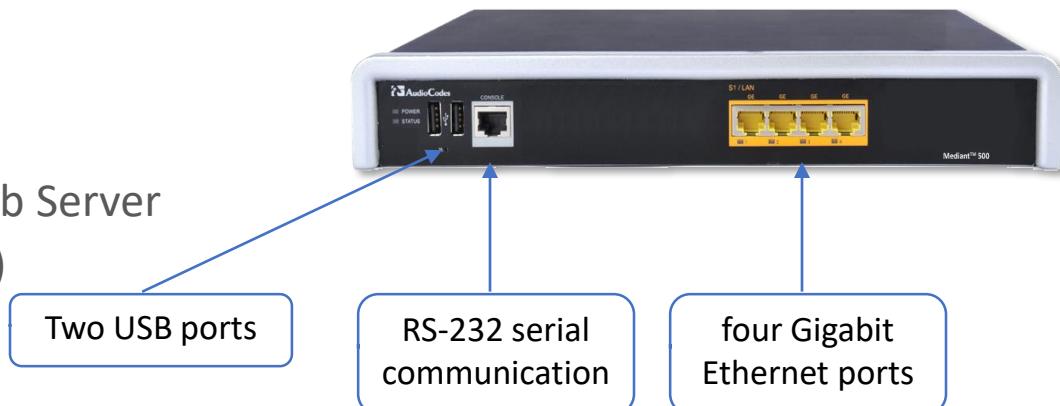
RS-232 serial communication

USB port

Four Gigabit Ethernet ports

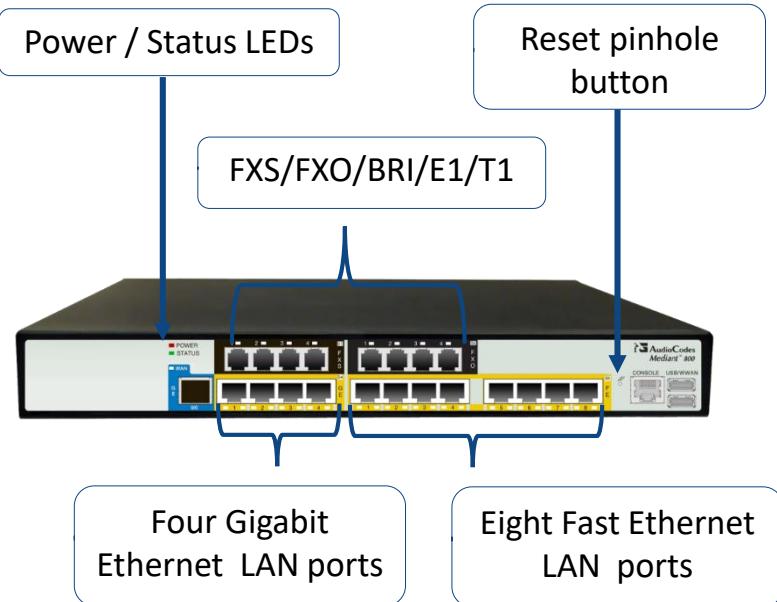
# Mediant 500 Physical Interfaces

- **LAN Ethernet ports :**
  - Four Gigabit Ethernet (10/100/1000Base-T) LAN ports
- **PSTN connectivity**
  - Up to 1 E1/T1/J1 trunk
- **High-Availability 1+1**
- **OAM&P**
  - Embedded HTTP/S-based Web Server
  - Command Line Interface (CLI)
  - Configuration *ini* file
  - SNMP
  - REST API

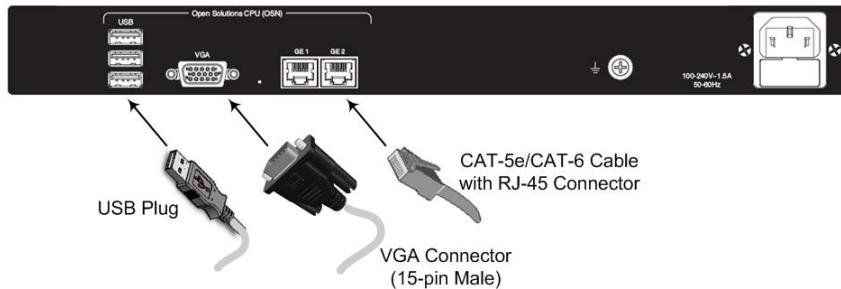


# Mediant 800B Physical Interfaces

- LAN Ethernet ports:
  - Up to 4 Gigabit Ethernet
  - Up to 8 Fast Ethernet
- Integrated PSTN connectivity
  - Up to 2 E1/T1/J1 trunks
  - 8 BRI ports (16 calls)
  - Up to 12 analog FXS/FXO ports
- High-Availability 1+1
- OAM&P:
  - Embedded HTTP/S-based Web Server
  - Command Line Interface (CLI)
  - Configuration *ini* file
  - SNMP
  - REST API
- Integrated Open Solutions Network (OSN) server platform



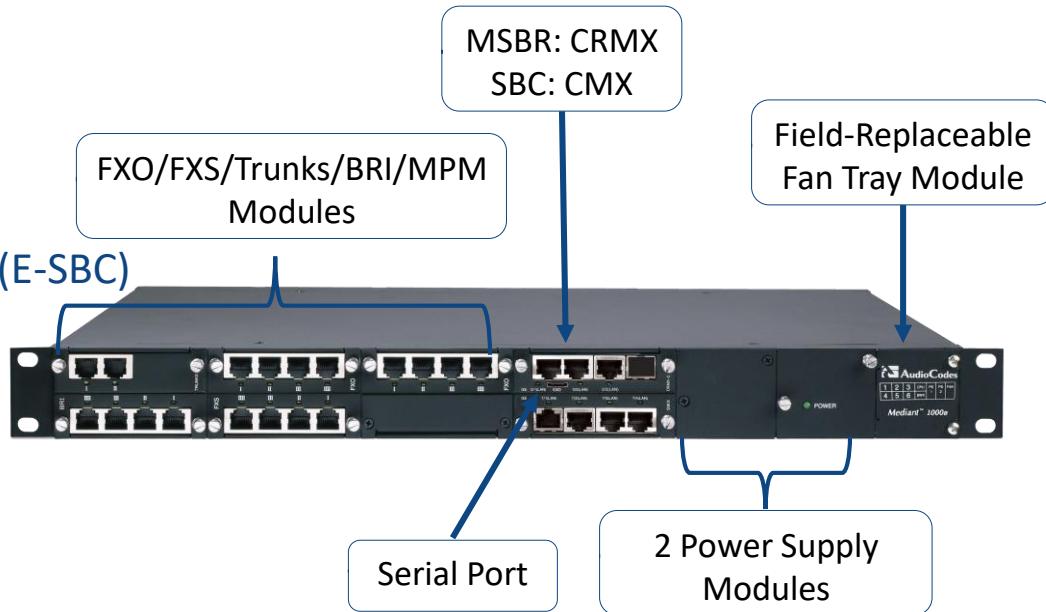
- Up to 4 x E1/T1
- Dual flash memory, allowing the user to revert to the previous software version after a software upgrade failure
- Dual power supply – in addition to the AC power supply supplied by default, the chassis can be ordered with an option DC power supply inlet
- Increased Gateway and SBC session capacity due to powerful CPU



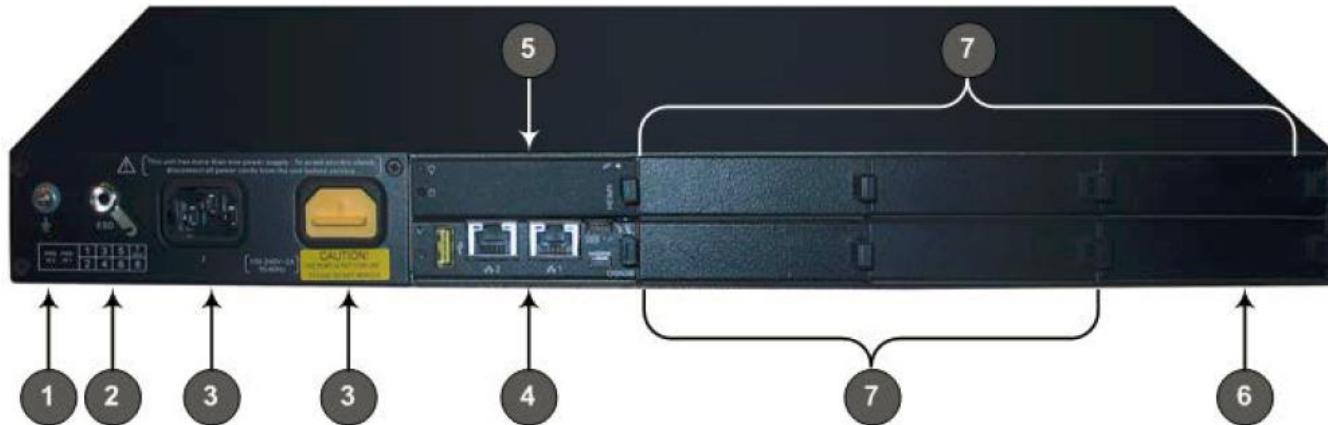
Parameter	OSN6	OSN7
CPU	Intel® Core™ i7-5850EQ Processor <i>4 Cores, 6M Cache, 2.7 GHz</i>	Intel® Pentium® Processor D Series <i>2 Cores, 3M Cache, 2.60 GHz</i>
Memory	32 GB	16 GB
Hard Drives	128 GB SSD (or higher, for special request)	
Interfaces	<ul style="list-style-type: none"><li>• 2 Gigabit Ethernet external (rear panel)</li><li>• 1 Gigabit Ethernet internal bus, connected to the Mediant</li><li>• 3 USB 2.0</li><li>• VGA</li></ul>	

# Mediant 1000B

- LAN Ethernet ports
  - Up to 3 Pairs of 1+1 LAN interfaces
- Modular – can host a variety of interfaces
  - 1 to 6 E1/8T1/ trunks (up to 192 channels)
  - 4 to 20 BRI ports (40 calls)
  - 4 to 24 analog (FXS/FXO) ports
  - Up to 4 MPMs for media processing
- Enterprise Class Session Border Controller (E-SBC)
- Single or Dual Power Supply
- 2 OSN servers (Optional)
- OAM&P:
  - Embedded HTTP/S-based Web Server
  - Command Line Interface (CLI)
  - Configuration *ini* file
  - SNMP
  - REST API



# Mediant 1000B – Rear Panel



Item #	Label	Description
1	⏚	Protective earthing screw.
2	ESD	Electrostatic Discharge (ESD) socket.
3	100-240V~1A	Dual AC Power Supply Entries.
4	OSN3C or OSN4B	OSN3C or OSN4B AMC module.
5	HDMX	Main hard-disk drive (HDD) AMC module for OSN server platform.
6	HDMX	Slot for second (optional) HDD for OSN server platform.
7	-	Unused and covered AMC module slots.



Parameter	OSN3C	OSN4B
CPU	Intel® Pentium® Processor D1508 <i>2 Cores, 3M Cache, 2.20 GHz</i>	Intel® Xeon® Processor D-1527 <i>4 Cores , 6M Cache, 2.20 GHz</i>
RAM Memory	8 GB	16 GB
Hard Drives	Up to 2 hard drives (HDMX modules) 500 GB HDD or 120GB SSD (2 HDD can work in Raid1)	
Interfaces	<ul style="list-style-type: none"><li>• 2 Gigabit Ethernet external (rear panel)</li><li>• 1 Gigabit Ethernet internal bus, connected to the Mediant</li><li>• USB 2.0</li><li>• RS-232</li><li>• Graphics</li></ul>	

- Dual Processors (CMX & RMX)
- WAN port – WAN Gigabit Ethernet, T1 WAN, SHDSL, ADSL/VDSL
- Strong CLI management
- Data Routing capabilities by providing static routing and dynamic routing protocols such as RIP/OSPF and BGP
- Supports a selection of WAN interfaces providing flexibility connecting to Service Providers
- Firewall
- QoS
- Mediant 500L/500 and 800 only: 3G connection (using USB 3G stick) used as primary WAN interface or as optional/backup when primary WAN fails



**Note:** The latest maintenance firmware version for Mediant 1000B MSBR is 7.0

- Operation modes:
  - Simplex operation
  - High-Availability 2 x cPCI
- LAN ports:
  - Dual redundant 10/100/1000 Base-T (6310)
  - 2nd dual redundant 10/100/1000 Base-T (8410)
- Integrated PSTN connectivity
  - 63 – E1, 84 – T1, 3 X DS-3 (T3), 1 X STM-1 or 1 X OC3

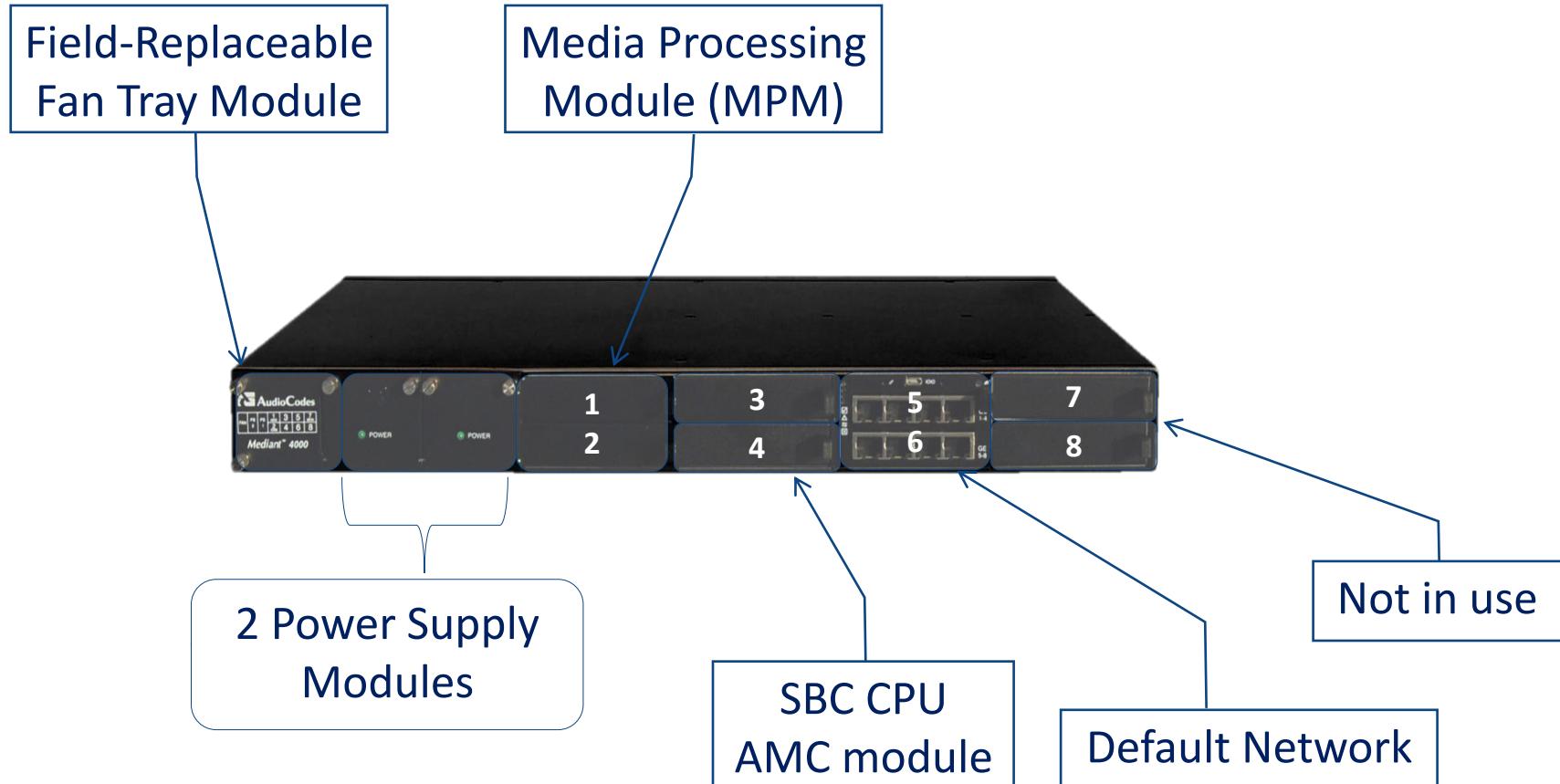




Mediant  
2600

Mediant  
4000

- Scalable from 100 up to 600 Sessions
- High-Availability 1+1
- Max. 600 simultaneous calls
- Scalable from 50 up to 5,000 Sessions
- Max. 5,000 simultaneous calls





## Mediant 4000B

- Scalable from 50 up to 5,000 Sessions
- High-Availability 1+1
- Max. 5,000 simultaneous calls

# Mediant 4000B – Optional HW Configurations



SBC CPU Only		CPU		
SBC CPU + 1 x MPM	MPM	CPU		
SBC CPU + 2 x MPMs	MPM	CPU	MPM	
SBC CPU + 3 x MPMs	MPM	CPU	MPM	MPM
SBC CPU + OSN		CPU	OSN	
			HDMX	
SBC CPU + 1 x MPM + OSN	MPM	CPU	OSN	
			HDMX	
SBC CPU + 2 x MPMs + OSN	MPM	CPU	OSN	MPM
			HDMX	
SBC CPU + 2 x MPMs + OSN with 2 x HDMX	MPM	CPU	OSN	HDMX
			HDMX	

## Optional Hardware Configurations

### Notes:

- OSN = OSN4B
- Same types as in Mediant 1000B
- Mediant 2600B offer OSN4B for SBA solution only

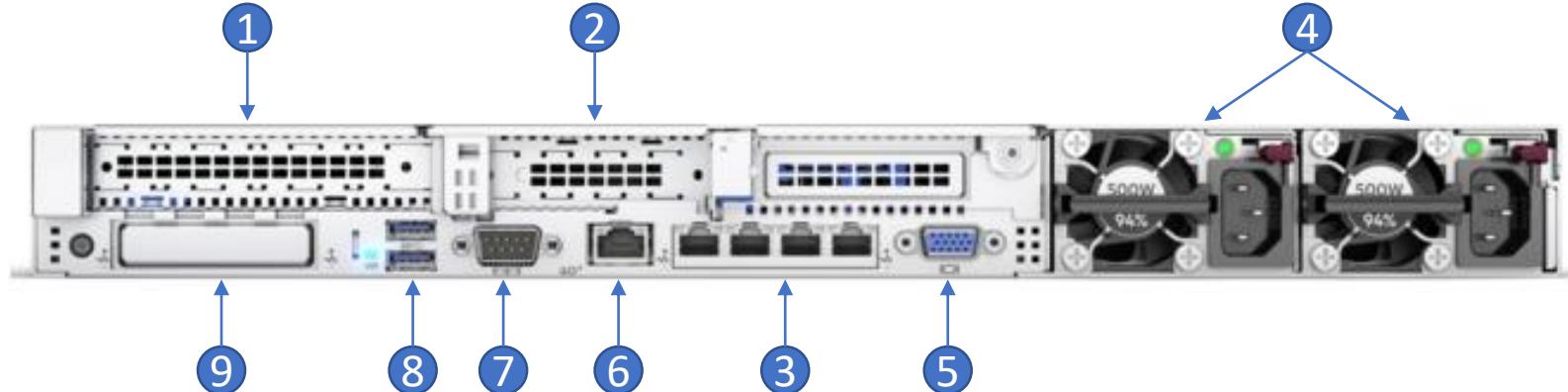
- Optional, customer-ordered AMC-based module
- Provides additional Digital Signaling Resources (DSP) required for transcoding call sessions
- Up to three MPM modules can be installed
- Two different MPM module types are available:
  - MPM8B module, providing 8 DSPs (up to 2400 sessions)
  - MPM12B module, providing 12 DSPs (up to 3250 sessions)
- Both module types can be installed in the same chassis



## Specification (Based on HP Server Hardware)

Resource	Mediant 9030	Mediant 9080 (Mediant 9000 Rev. B)
CPU	2 x 8 cores, 2.1 GHz, 11MB Cache	2 x 12 cores, 2.6 GHz, 19.25MB Cache
Memory	32 GB, DDR4-2666/PC4-21300	96 GB, DDR4-2666/PC4-21300
Network Cards	<ul style="list-style-type: none"><li>• 12x 1-GbE ports or</li><li>• 8 x 1-GbE ports and 4 x 10-GbE (SFP+) ports</li></ul>	
Disk	Mechanical hard drive, 1 TB SATA	Mechanical hard drive, SAS 600 GB
CD/DVD	SATA CD/DVD R/W	
Installation Interface	VGA Monitor and Keyboard	
High-Availability 1+1		
Max. 70,000 simultaneous calls		

# Mediant 9030/9080 – Rear Panel

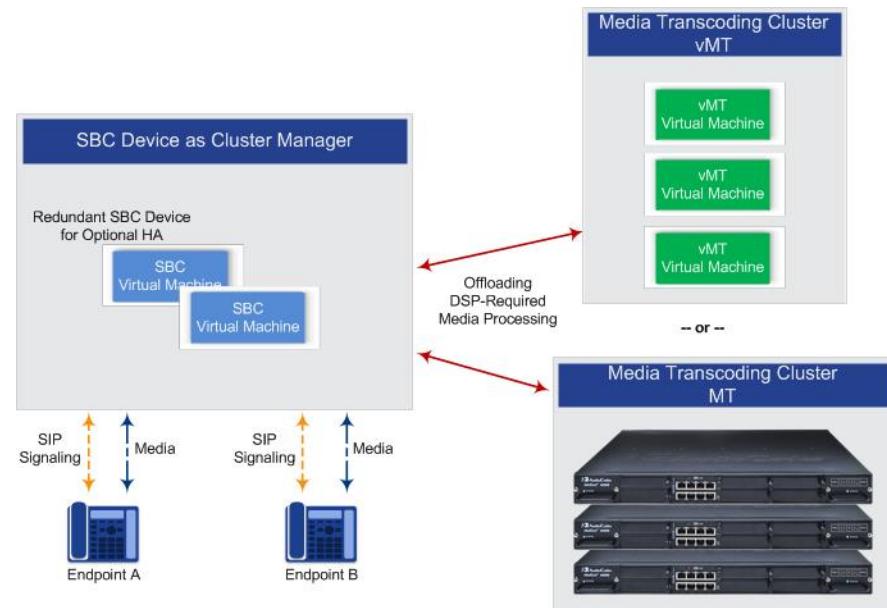
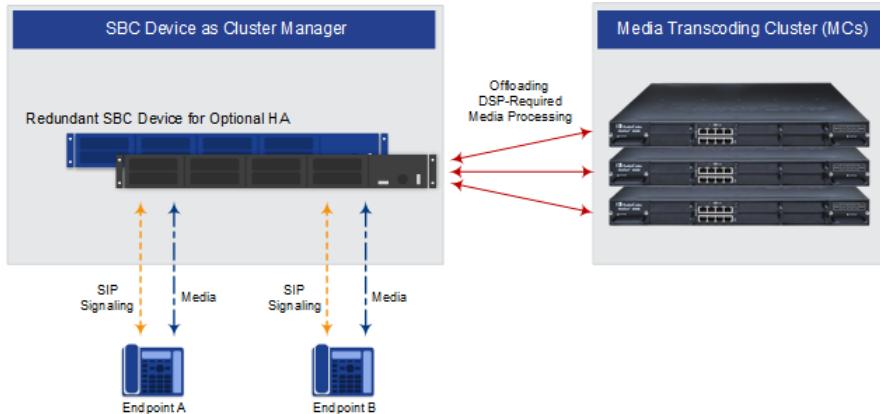


Item #	Mediant 9030	Mediant 9080 / Mediant 9000 Rev. B
1	Slot 1: Quad 1-GbE copper ports or Quad 10-GbE SFP+ ports	Slot 1: Quad 1-GbE copper ports
2	Slot 2: Not used	Slot 2: Quad 1-GbE copper ports or Quad 10-GbE SFP+ ports
3	Unsupported NIC ports (dust covered)	Embedded Quad 1-GbE copper ports (These ports must <b>not</b> be used for media (RTP/SRTP) traffic)
4	Power Supply (active and redundant)	
5	Video port	
6	iLO (Integrated Lights Out) Management Port	
7	Serial port	
8	USB 3.0 ports	
9	Quad 1-GbE copper ports	

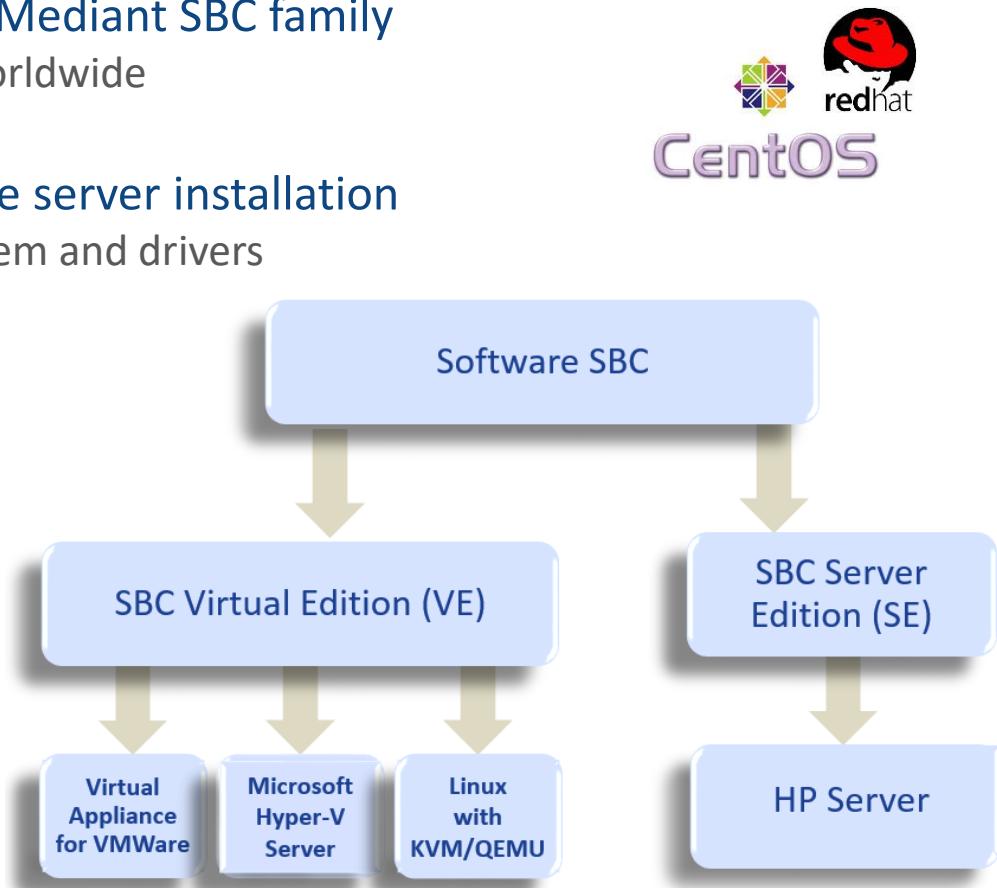
- External DSP resources for media-related features requiring DSPs
- 2 types of deployment:
  - Hardware based on the Mediant 4000 chassis and MPM8 or/and MPM12 modules
  - Virtual based on Mediant VE platform and virtual DSPs
- Supported only by **Mediant 9080** and **SW-SBC VE**
- Each MC device support up to 5000 media session
- As transcoding needs increase, multiple MC devices can be configured as farm (cluster)
  - Up to 8 MTs for hardware based appliance
  - Up to 5 MTs for virtual based appliance
  - Provides load-sharing and cluster redundancy
- MC cannot be shared by multiple SBC devices

# Media Transcoding Cluster (MC)

- The Media Transcoding Clusters are "hidden" from the endpoints being serviced by the SBC
- Requires a suitable License Key



- Same robust SBC software stack of the Mediant SBC family
  - Runs on thousands of deployed SBCs worldwide
  - Same GUI for short learning curve
- SBC software image includes a complete server installation
  - Includes SBC application, operating system and drivers
  - Assures SBC robustness
- Operating System
  - CentOS (Community Enterprise OS) 6.0
  - Binary Compatible with Red Hat Enterprise Linux (RHEL)
  - Built from the same sources but without RedHat trademarks
- Available on two formats:
  - Dedicated Server (SE)
  - Virtualized Machine (VE)

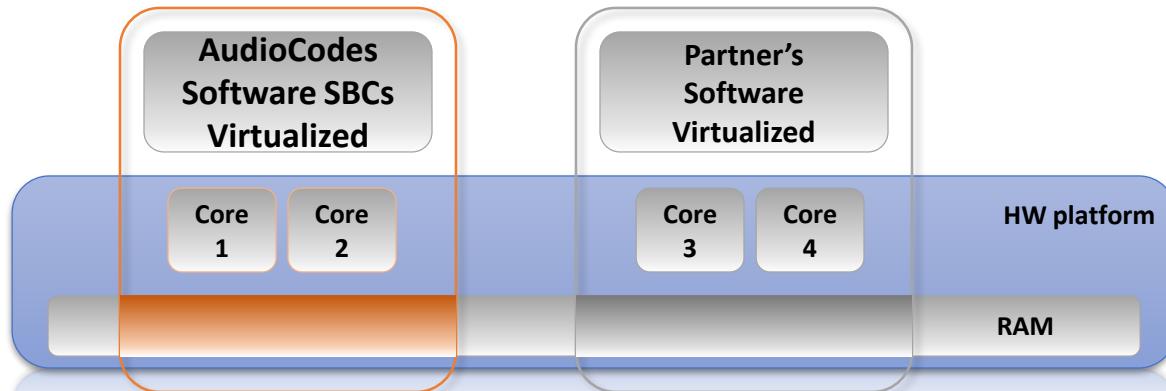


CentOS

- Targets SBC applications that require high performance and heavy load of SIP registrations/subscribes/notifies
- Runs on common off-the-shelf Intel based servers
- Server image includes a complete server installation including OS and drivers
- Two pairs of GE interfaces for WAN and LAN separation
- 1+1 High Availability configuration
- Two HP ProLiant certified servers models:

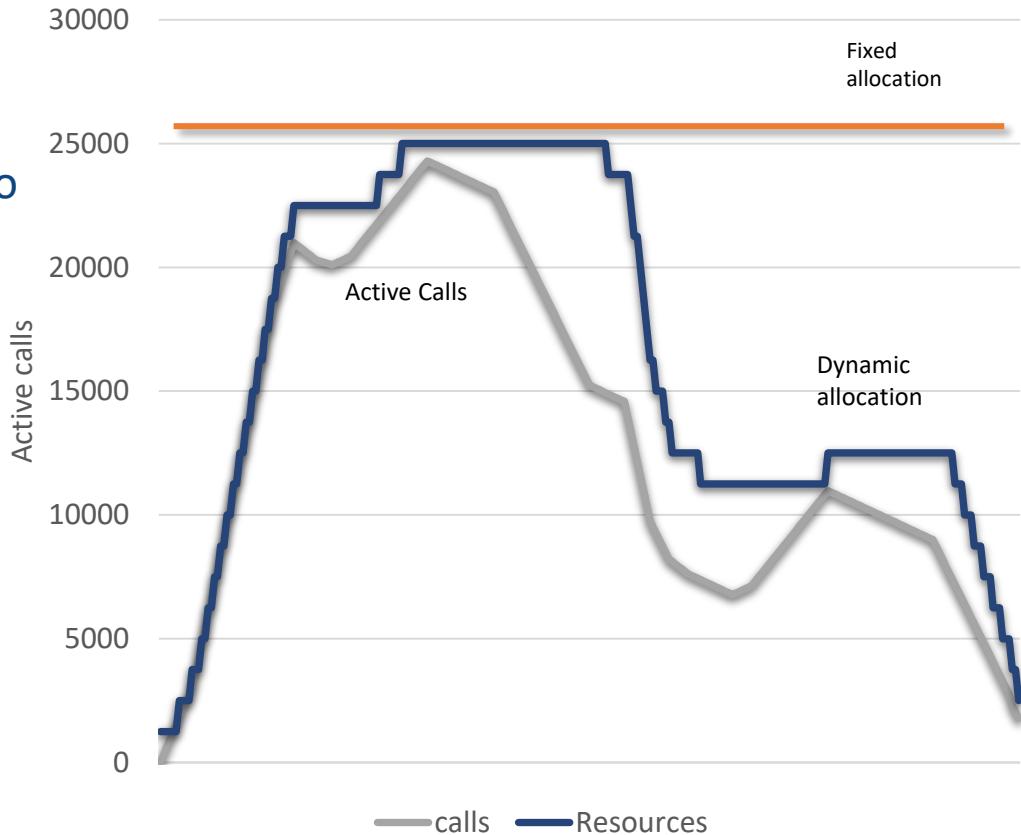
Product		Signaling Capacity		Media Sessions			
		SIP Sessions	Registered Users	Session Type	RTP	SRTP	Detailed Media Capabilities
Mediant SE	DL360p G8 20-cores 2.8 GHz 64-GB RAM - or - DL360 G9 8-cores 2.6 GHz 32-GB RAM	24,000	120,000	SBC-Only	16,000	14,000	-
		24,000	0	SBC-Only	24,000	14,000	-

- Target applications:
  - Enterprises and Service Providers who prefer to virtualize their entire Data Center
  - Software vendors looking to integrate their application with an SBC on a single physical server
- Available for VMware, OpenStack KVM and Hyper-V hypervisors
- Designed for consistent performance (without overbooking) with additional VMs running on same machine



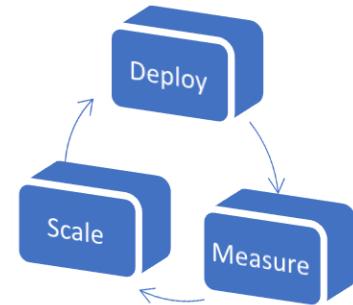
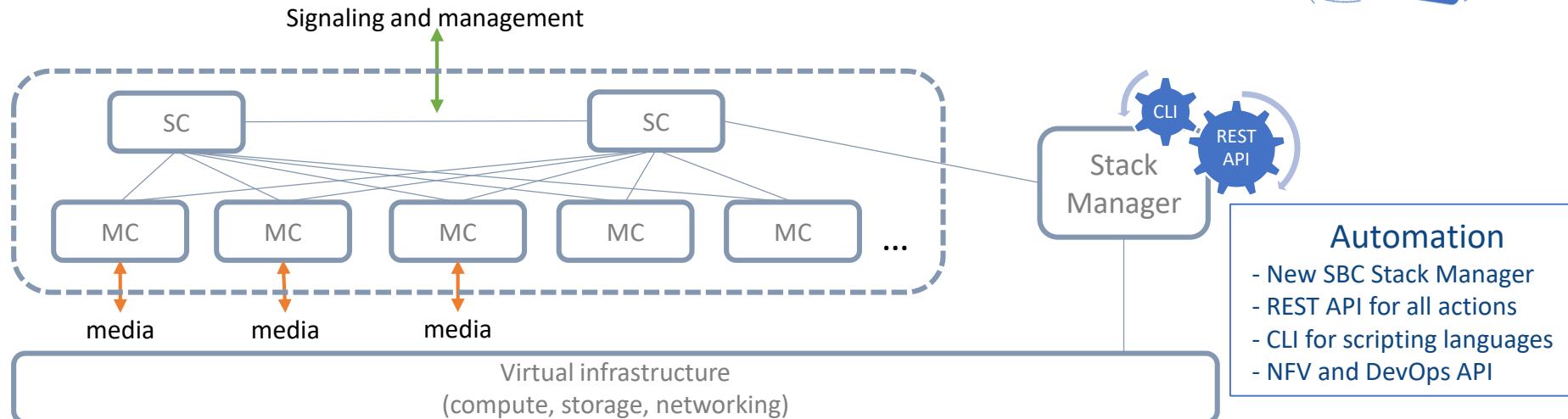
# SBCs journey to the cloud

- SBC traffic demands are dynamic
- Sizing an SBC for worst-case scenario is cost prohibitive
- SBC elasticity is key for resource optimization – you can start small and grow as needed



# Mediant Cloud Edition SBC (Mediant CE)

- Separated signaling and media processing (built out of dedicated functional blocks)
- Elastic Media Cluster (traffic based scalability)
- Full SBC functionality
- Single management point
- Multi Cloud (Amazon AWS and Microsoft Azure)
- Built-in HA



Which of the following is **false**?

- A. Mediant 2600 is an hybrid SBC
- B. Six E1's is the max. capacity of Mediant 1000B
- C. Mediant 800B can be ordered with an integrated OSN
- D. High Availability configuration is supported on Mediant 4000

Media Transcoding Cluster is:

- A. Internal source of DSP resources
- B. External source of DSP resources
- C. Group of SBC's
- D. None of the above



The Media Transcoding Cluster Provides:

- A. SBC functionality only
- B. SBC and DSP functionality
- C. DSP functionality Only
- D. None of the above

In Mediant 4000B chassis you can install:

- A. Only MPM8B
- B. Only MPM12B
- C. Both MPM types
- D. None of the above





## Lesson 5

# SBC Application Description



- After completing this lesson you'll know:

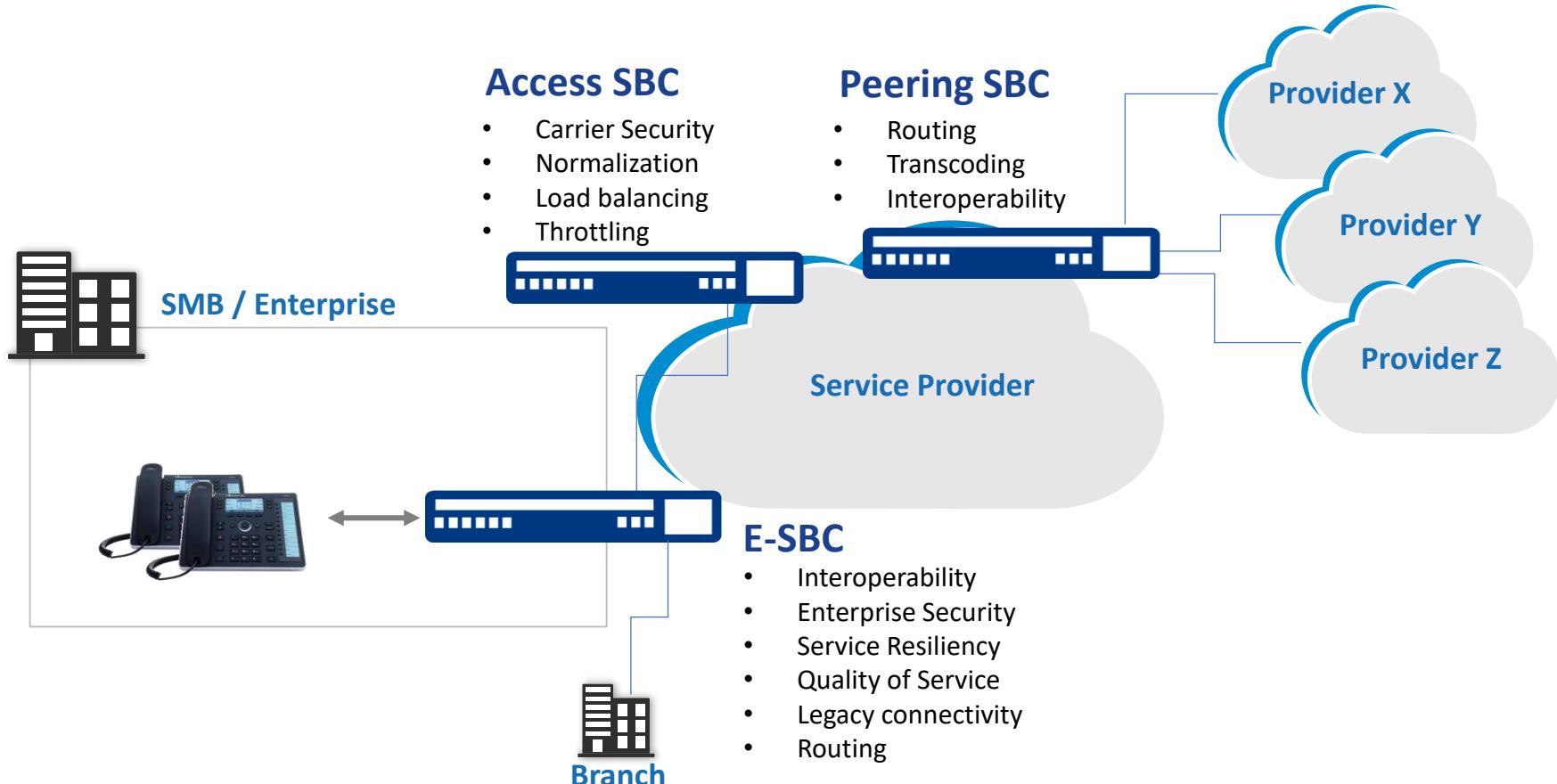
- Where and How to have the SBC located
- SBC functions

- A device/application which:
  - Manages a VoIP session by performing:
    - Session setup
    - Call conducting
    - Session tear down
  - Enforces Security, QoS and Call Admission Control (CAC)
- Often installed at a demarcation point between one network segment (Un-Trusted) and another (Trusted)

# What are Session Border Controllers For?

- Connectivity
- Security
- Quality Assurance
- Regulatory Compliance (Emergency calls, lawful interception)
- Media Services
- Statistics and Billing information





## Security

- DDoS
- Call theft
- Eavesdropping

## Connectivity

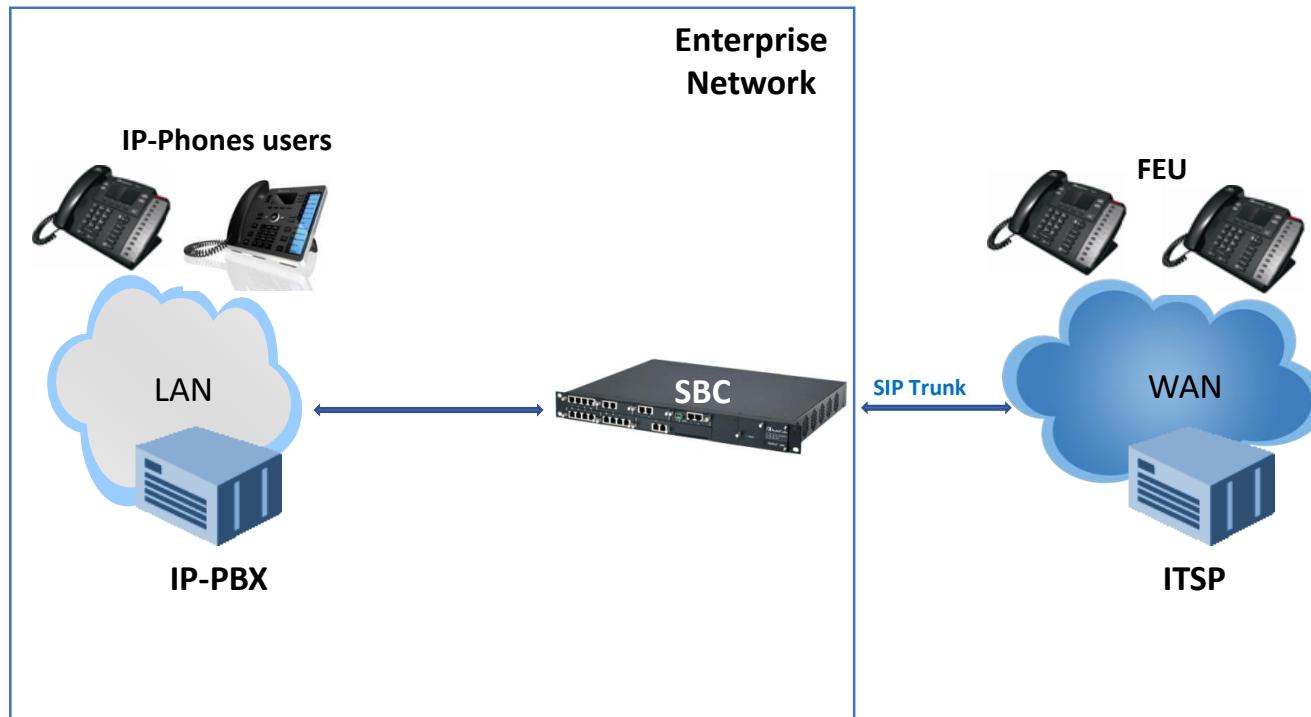
- Connect between any PBX to any SIP Trunk
- Connect between PBXs
- Connect remote workers to the enterprise

## Quality of Service and SLA

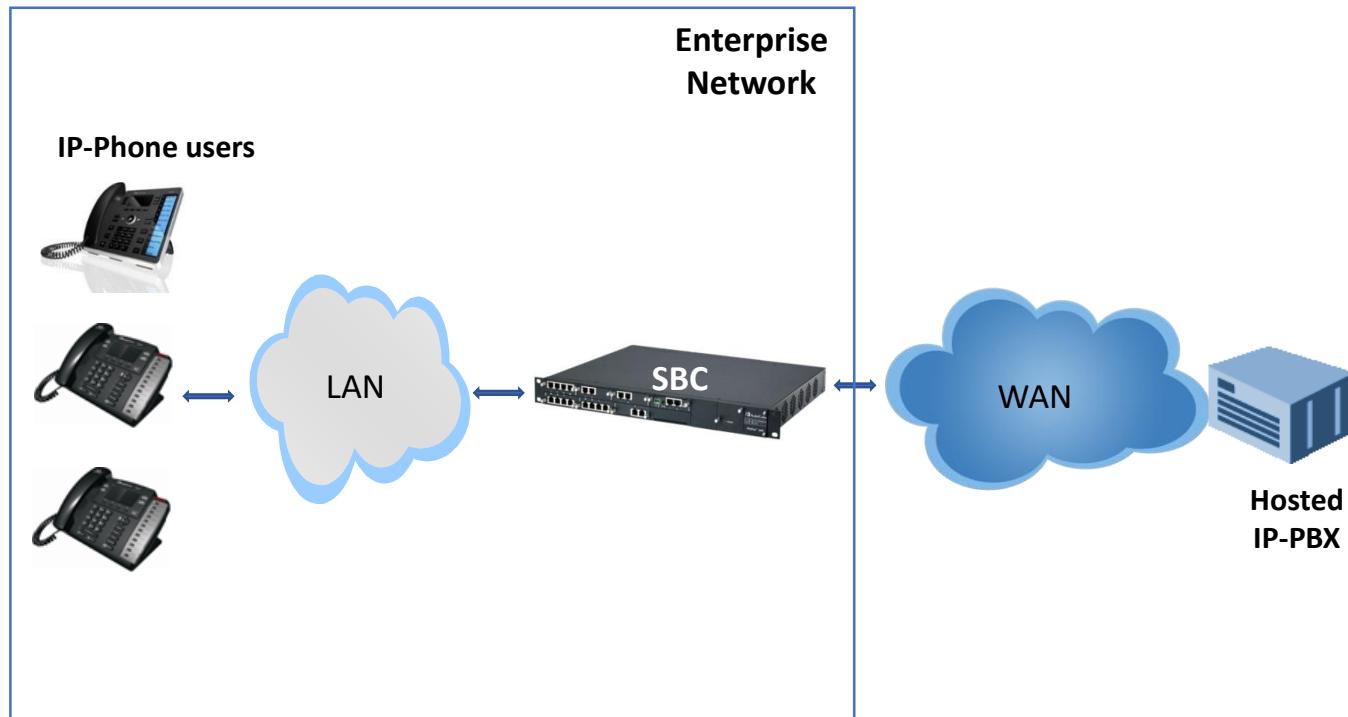
- Monitor call quality
- Report on quality issues
- Quality enhancements
- Call recording

- Three options:
  - Local IP-PBX with SIP Trunk by ITSP
  - Hosted IP-PBX
  - Two Local IP-PBXs

- Local IP-PBX with SIP Trunk by ITSP

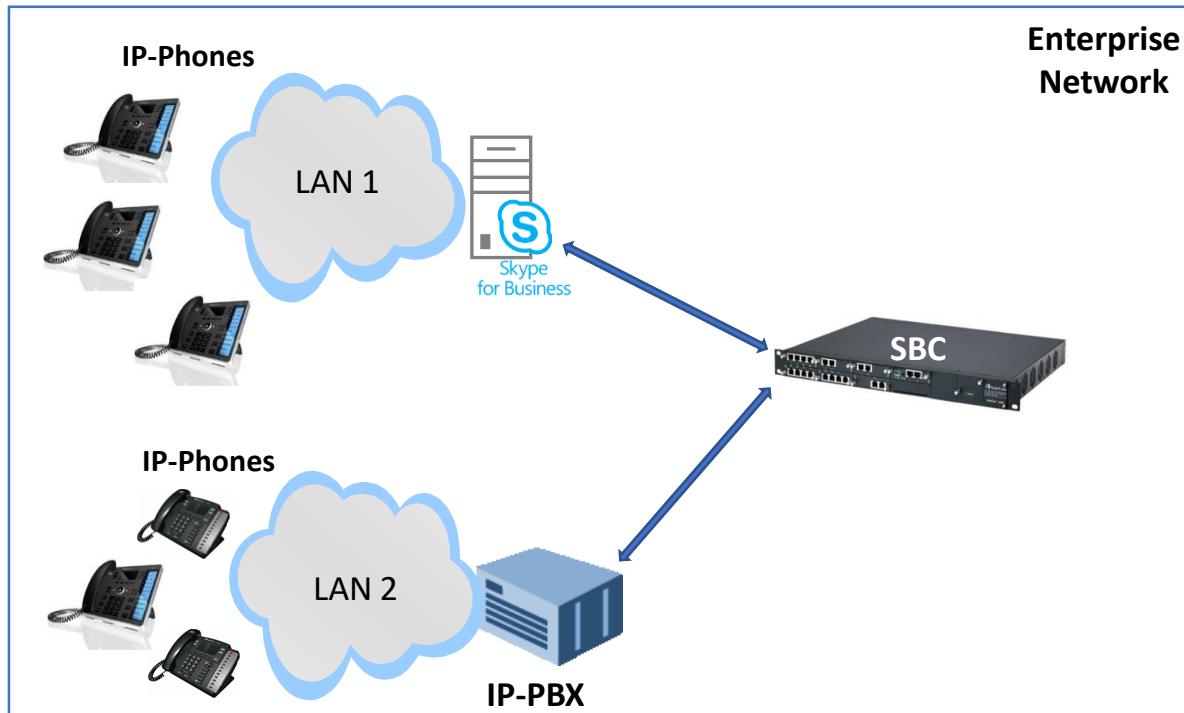


- Hosted IP-PBX



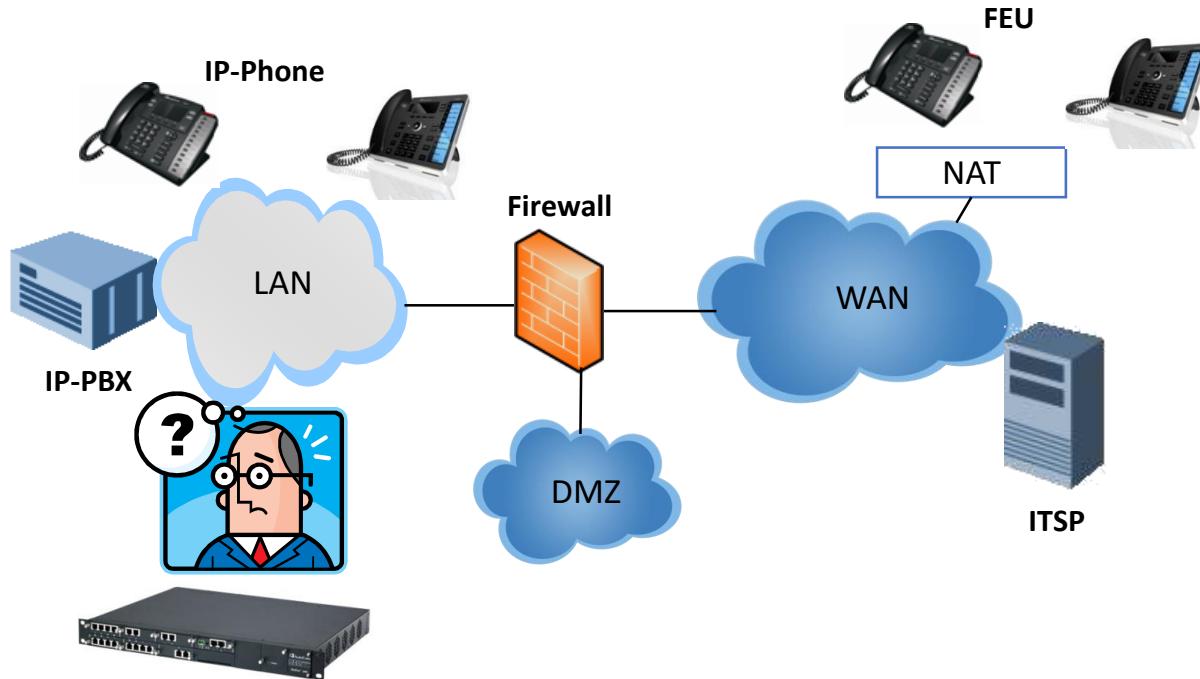
# Applications / Topologies

- Two Local IP-PBXs (SIP Normalization)

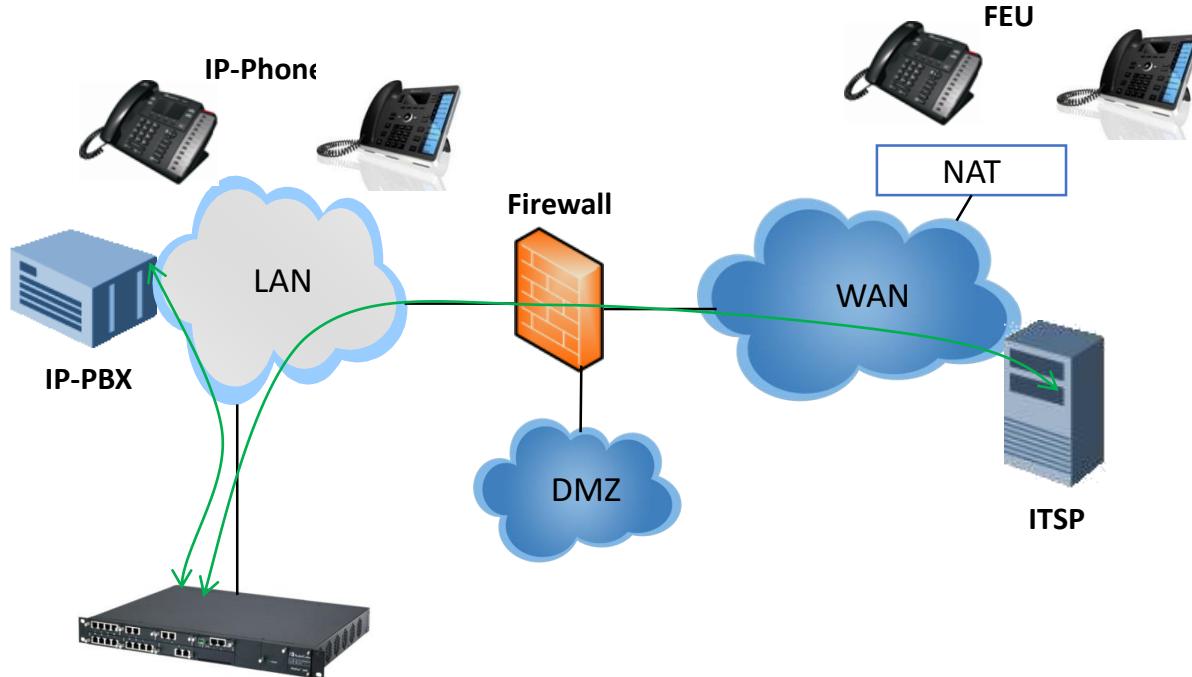


- Three options:
  - SBC connected with one leg to LAN
  - SBC connected with one leg to DMZ
  - SBC connected with one leg to DMZ and another leg to LAN
- Physical SBC Connections with the Enterprise
  - # of ports used for each logical connection, with or without 1+1 port redundancy

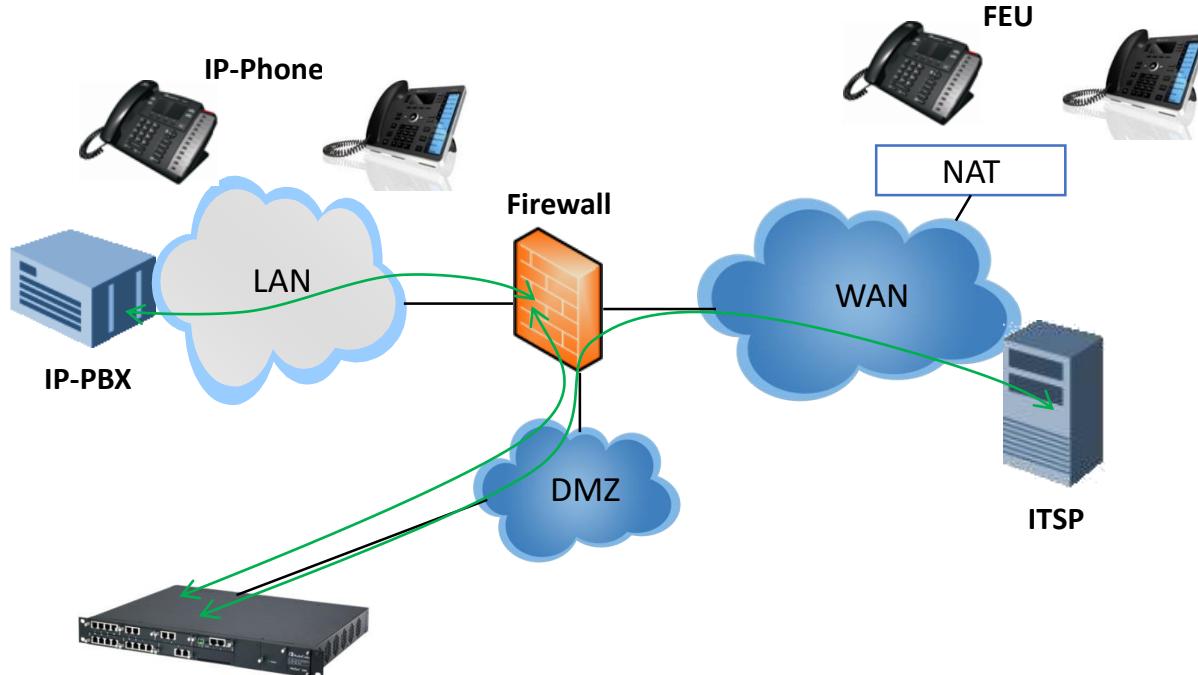
# Logical SBC Connections – Locating the SBC

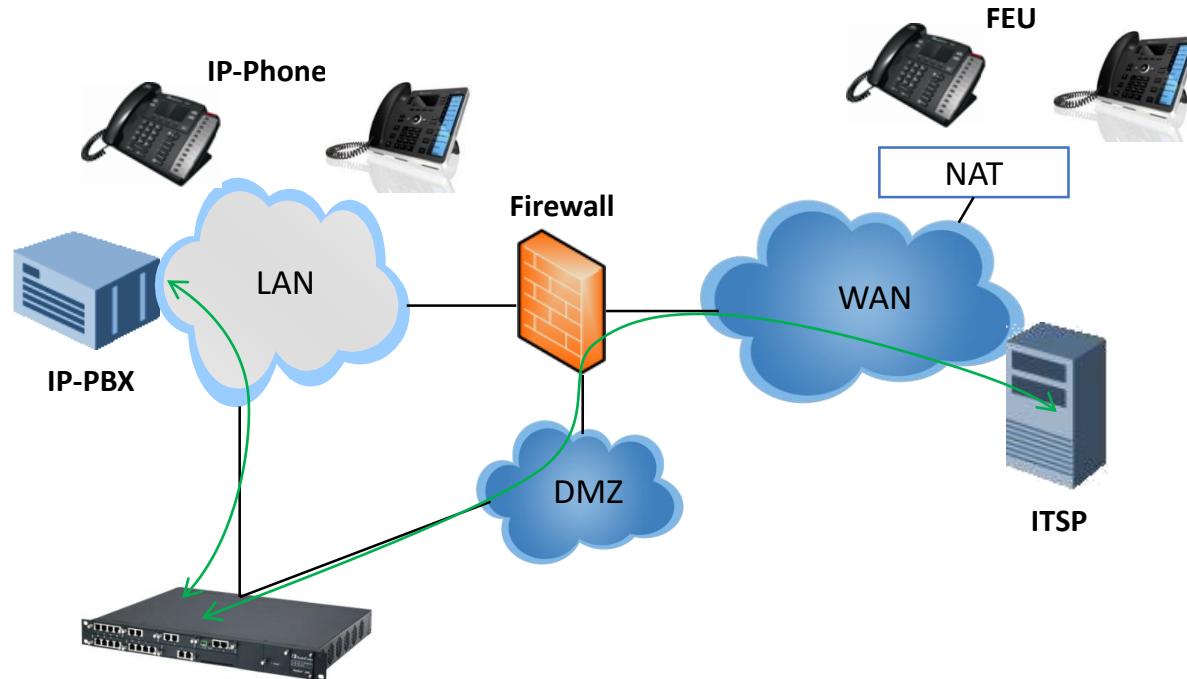


# Logical SBC Connections – One Leg LAN



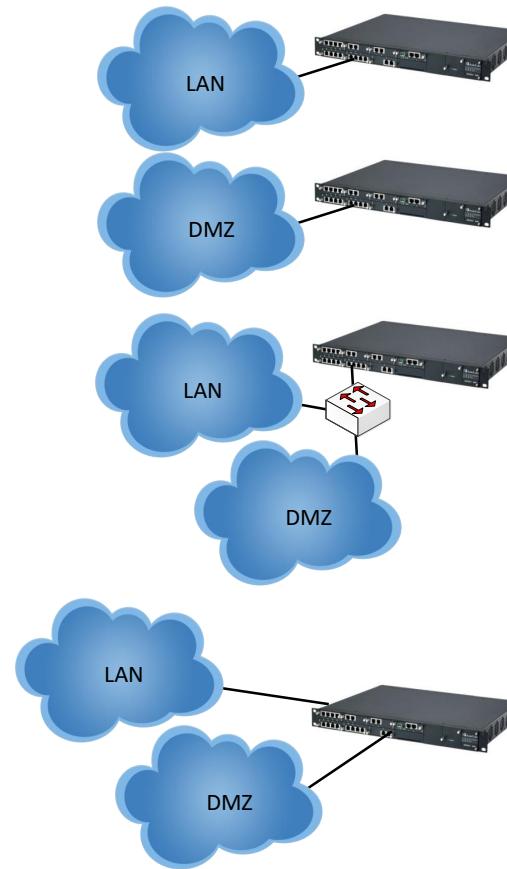
# Logical SBC Connections – One Leg DMZ





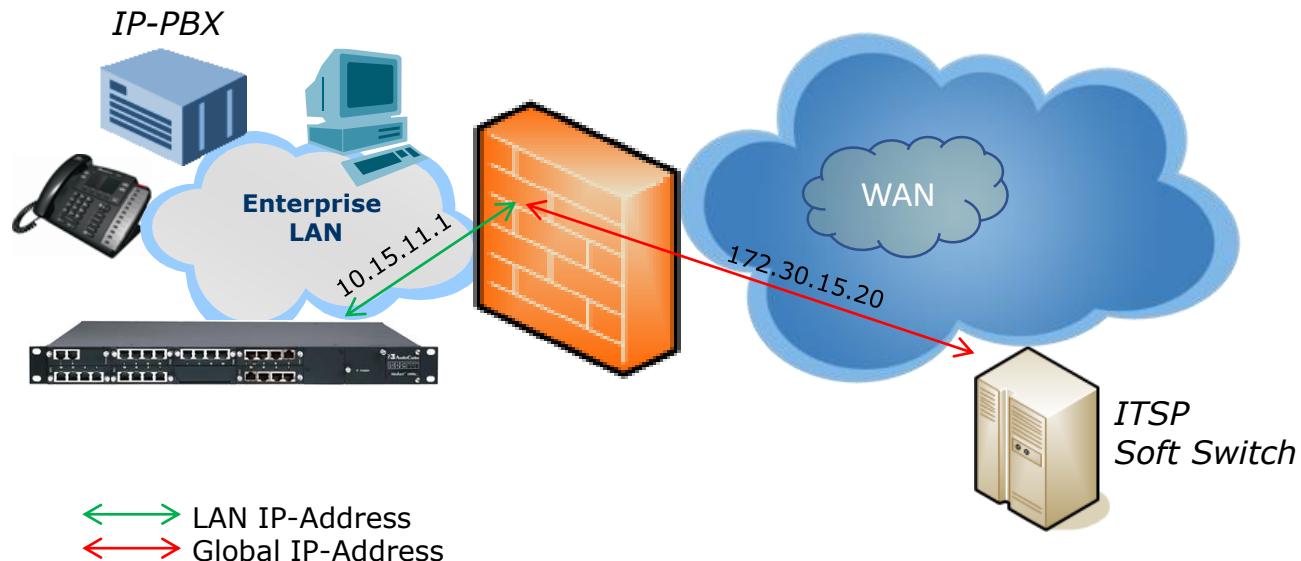
# Physical SBC Connections

- One-Leg (DMZ or LAN)
- Only 1 port required (1 cable)
- Optional: 2 ports, 1+1 redundancy (2 cables)
  
- VLAN-Aware Switch
- Only 1 port required (1 cable)
- Optional: 2 ports, 1+1 redundancy (2 cables)
  
- Two-Legs (LAN and DMZ)
- 2 ports used (2 cables)
- 4 ports used, 1+1 redundancy (4 cables)
- LAN Expansion Module required on M1000

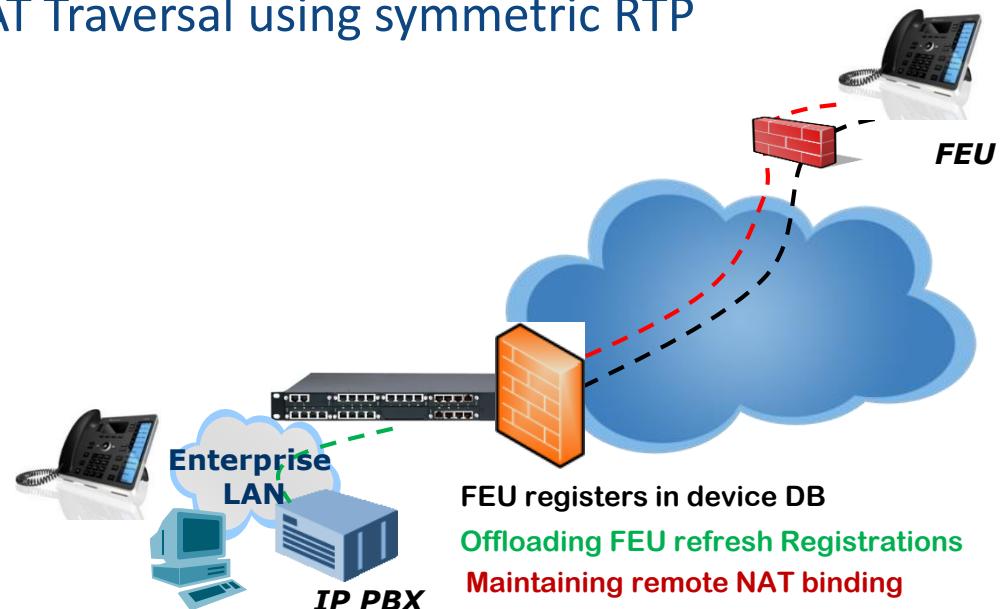


- NAT Traversal
- Transcoding
- Topology Hiding
- VoIP Firewall
- SIP Routing
- SIP Normalization
- Survivability

- Enables communication with ITSP/SIP Trunk using globally unique IP addresses



- SBC supported Far End Users (FEU)
- Maintaining remote NAT binding state by frequent FEU registration time
- First incoming RTP Packet for NAT Traversal using symmetric RTP
- Protocols that can traverse SBC:
  - Audio
  - Video
  - Application
  - Text

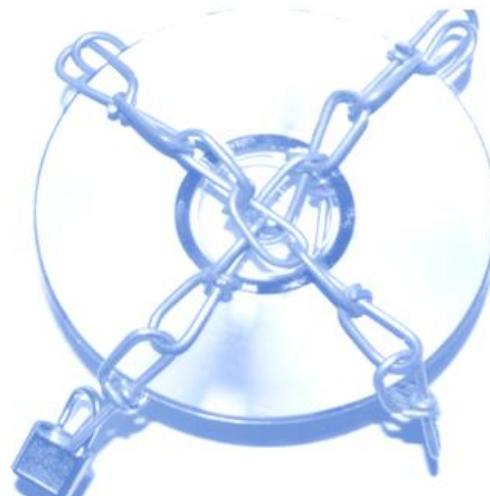


# SBC Transcoding

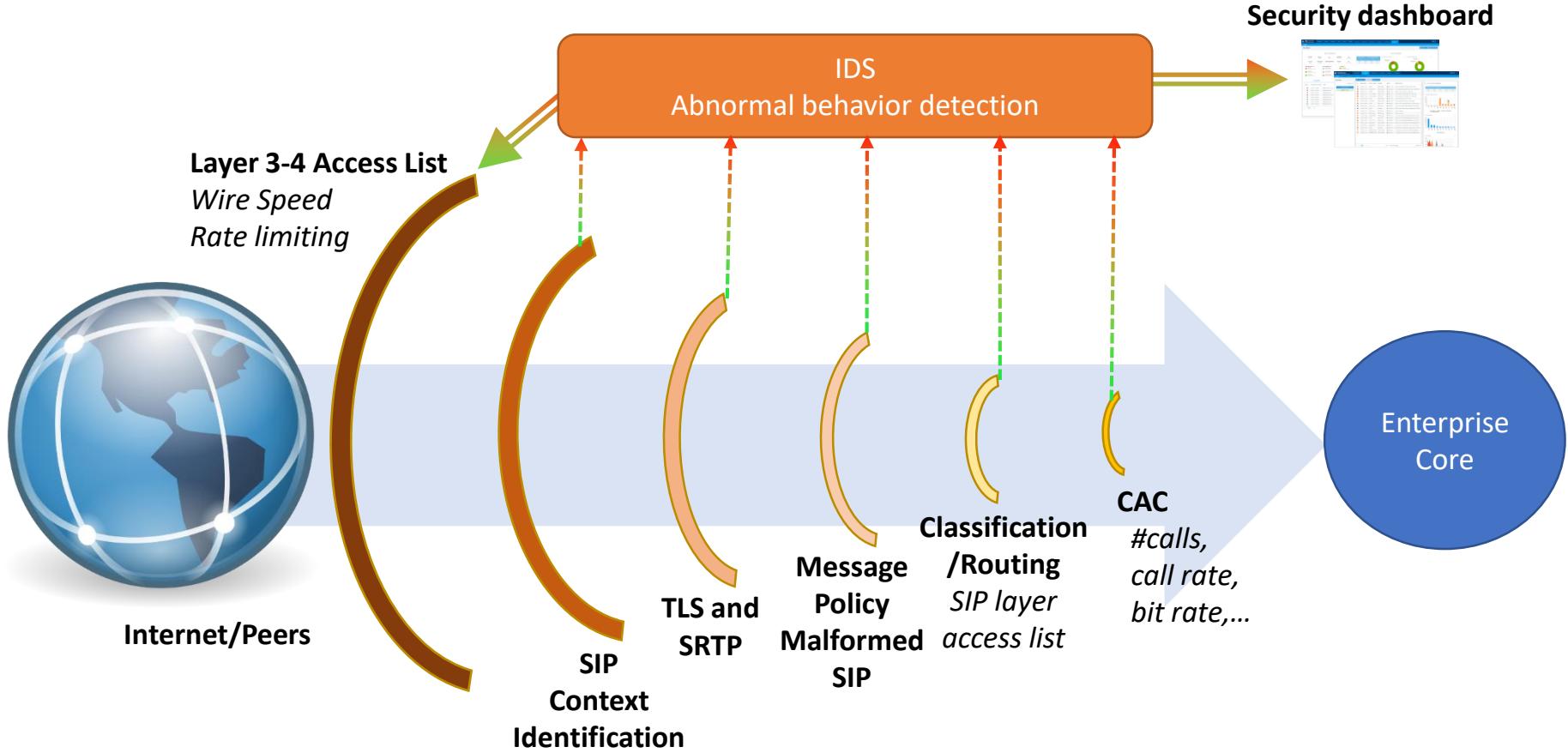
- Coder Transcoding
- RTP <-> SRTP
- Fax/Modem translations
- Transrating
- Voice gain adjustments
- RFC 2833 <-> Transparent DTMF <-> SIP INFO



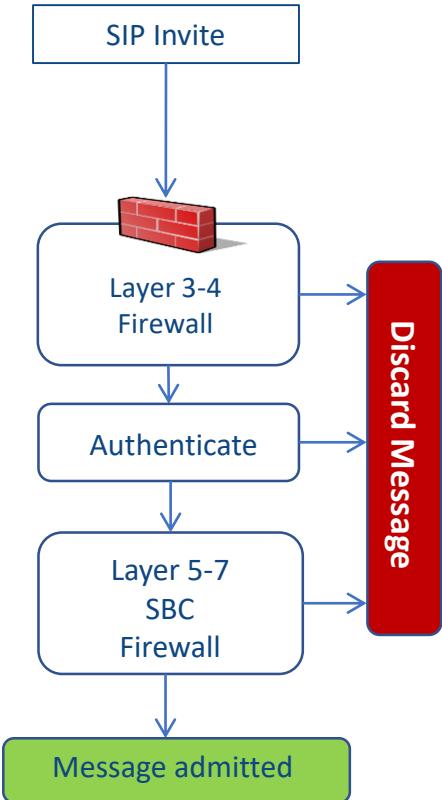
- Hides the Internal Network
- SBC implements back-to-back user agent (B2BUA):
  - VIA stripping
  - Independent Route/Record Route per leg
  - Use SBC Contact info
  - Change Call-ID per leg
  - Restrict Caller-ID
  - Host Name modification



# Comprehensive Security

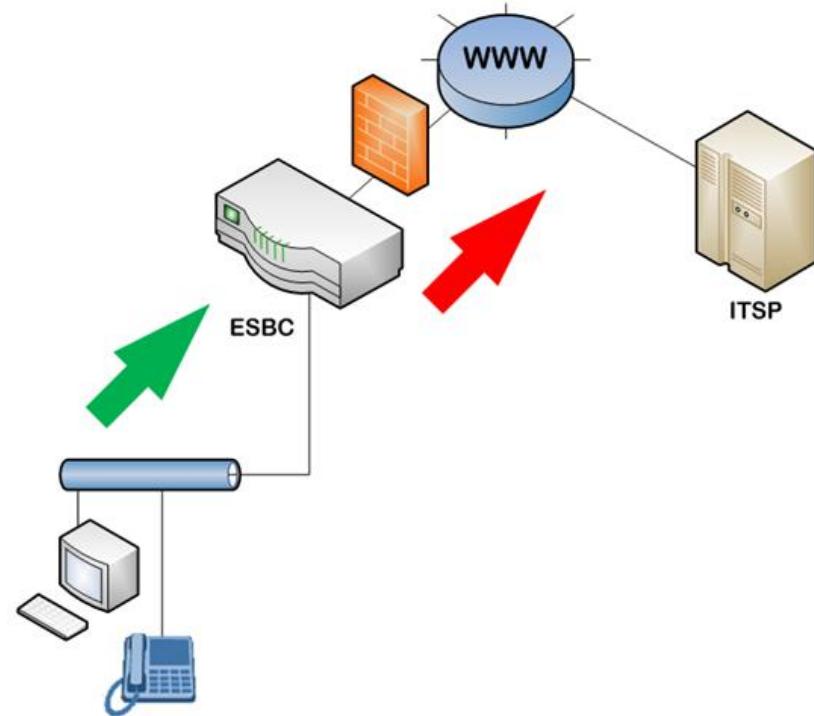


- **SIP Signaling**
  - Deep Stateful Packet Inspection (SPI) of all SIP signaling packets
  - SIP classification
  - Packets not belonging to a valid SIP dialog are discarded
- **RTP**
  - Opening pin holes according to Offer/Answer negotiation
  - DPI of all RTP packets





- Solves interoperability issues between SIP user agents
  - Manipulation of SIP URI user and host
  - SIP Header Manipulations
  - P-Asserted-ID conversions
  - Session timer conversions
  - Early media conversions
  - Register to ITSP on behalf of the IP-PBX
  - Flexible REFER and Forward handling
  - And more



# SIP Normalization – Example



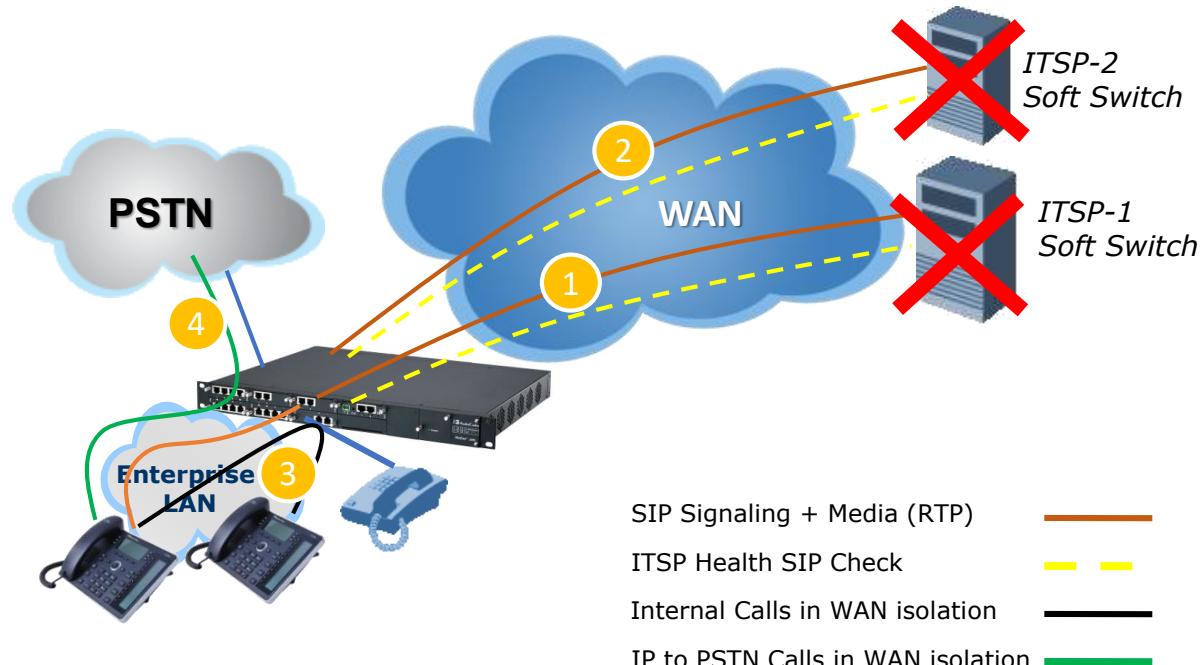
INVITE sip:5550000@10.15.5.1;user=phone SIP/2.0  
Via: SIP/2.0/TCP 10.15.5.5:5050;branch=z9hG4ac8071985;alias  
Max-Forwards: 70  
From: <sip:4000@10.15.5.5>;tag=1c1218068773  
To: <sip:5550000@10.15.5.1;user=phone>  
Call-ID: 121806822010120101484@10.15.5.5  
CSeq: 1 INVITE  
Contact: <sip:4000@10.15.5.5:5050;transport=tcp>  
Privacy: none  
P-Asserted-Identity: <sip:4000@10.15.5.5>

INVITE sip:5550000@**ITSP.com**;user=phone SIP/2.0  
Via: **SIP/2.0/UDP 200.100.10.2;branch=z9hG4ac463637**  
Max-Forwards: 10  
From: <sip:**9764000@audiocodes.com**>;tag=1c456353708  
To: <sip:5550000@**ITSP.com**;user=phone>  
Call-ID: **4563049822722010203627@200.100.10.2**  
CSeq: 1 INVITE  
Contact: <sip:4000@**200.100.10.2:5060**>  
Privacy: **session**  
P-Asserted-Identity: <**sip:9764000@audiocodes.com**>  
**Priority: emergency**

- 3 survivability features:
  - Routing calls to alternative routes such as:
    - ITSP
    - IP-PBX
  - Routing calls between user agents in the local network using a dynamic DB (built according to registrations of SIP user agents)
  - Fallback to the PSTN based on E1/T1 connection (Hybrid devices)

# SBC Survability

- Continuous VoIP service for enterprise users on WAN isolation



The SBC can be connected in the following way:

- A. 1 leg to the LAN only
- B. 1 leg to the DMZ only
- C. 2 legs to the LAN and DMZ
- D. Any one of the above

The SBC:

- A. Tracks the state of network connections traveling across it
- B. Determines legitimate packets for different connection types
- C. Only allows packets matching a known active connection and rejects others
- D. All of the above



SBC call can be handed over to the Gateway from the:

- A. IP to Tel Routing table
- B. IP to IP Routing table
- C. Tel to IP Routing table
- D. None of the above

Which of the following is **not** correct?

- A. The SBC can terminate SIP Messages
- B. The SBC can manipulate SIP URI user and host
- C. The SBC can't perform routing based on external server response
- D. Survivability feature is supported by the SBC



IDS is:

- A. A Routing mechanism
- B. A VoIP quality mechanism
- C. A security mechanism
- D. None of the above





## Lesson 6

# SBC Basic Terminology



- After completing this lesson you will:
  - Be familiar with the SBC terminology
  - Know what is an SRD/Tenant, SIP Interface and Media Realm
  - How this is associated to IP Groups and Proxy Sets

## 1. B2BUA

- Maintains independent sessions toward the endpoints
- Processing an incoming request as a User Agent Server (UAS) on the inbound leg
- Processing the outgoing request as a User Agent Client (UAC) on the outbound leg
- SIP messages are modified regarding headers between the legs
- The device's interworking features may be applied



## 2. Stateful Proxy Server

- SIP messages traverse the device transparently (with minimal interference) between the inbound and outbound legs
- No topology hiding

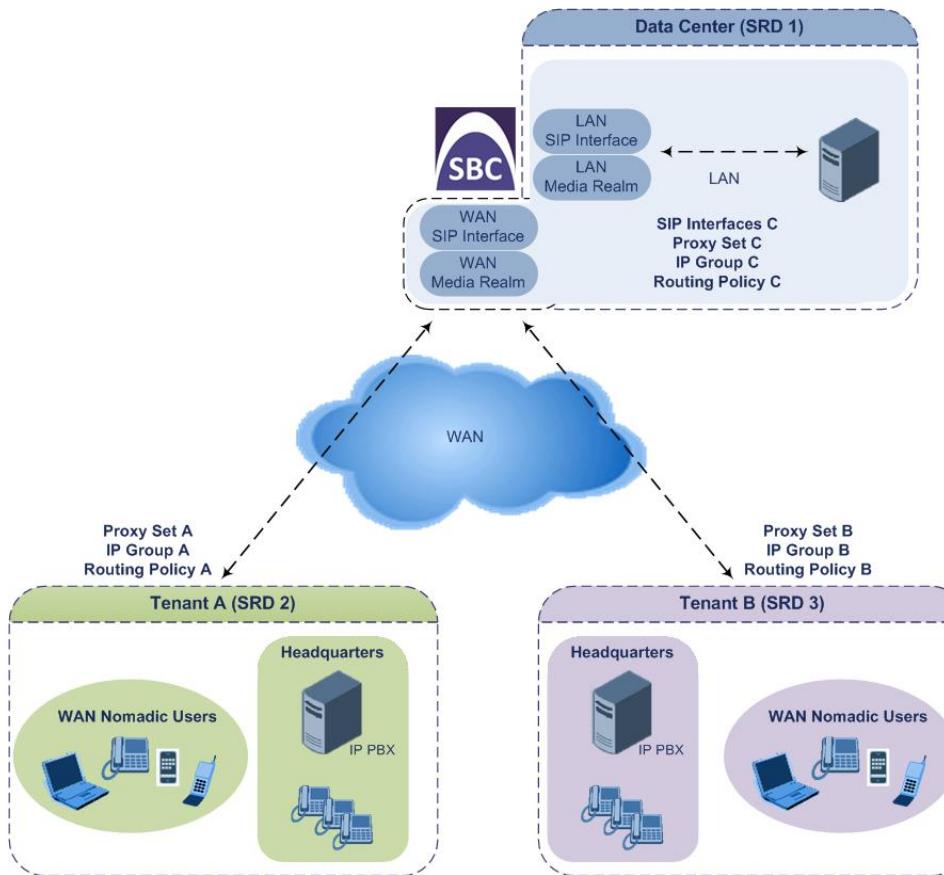
## 3. Microsoft Server

- Operating mode for the One-Voice Resiliency (OVR) feature

- Logical representation of the entire SIP-based VoIP network (Layer 5) containing groups of SIP users and servers
- Not bounded to any layer 3 network
- Typically, only a single SRD is required and this is the recommended configuration topology
- Multiple SRDs are required only for multi-tenant deployments, where it "splits" the device into multiple logical devices
- SRD contains:
  - Single/Multiple SIP Interface/s
  - Single/Multiple Media Realms

- SBC device serves a large number of enterprises/branches
- Support and secure the IP communications requirements of multiple enterprises simultaneously
- Full logical separation, on the SIP application layer, between tenants is achieved by SRD
- Provides per tenant configuration:
  - SIP Interfaces
  - IP Groups
  - Proxy Sets
  - Classification rules
  - IP-to-IP Routing rules
  - Least Cost Routing (LCR)
  - LDAP

# Multi-Tenant Architecture – Example



- Range of UDP ports associated with an IP network interface
- Used by SBC to perform media (Audio, Video, Fax) anchoring functionality
- Defines maximum number of sessions (based on the ports range)
- Can be assigned to the SIP Interface and/or the IP Group

- The SIP Interface represents a Layer-3 network (Bounded)
- It defines a local listening port for SIP signaling traffic on a local, logical IP Network Interface
- SIP Interface is associated with one and only one SRD
- Defines the application, SBC or GW (relevant just for Hybrid devices)
- The SIP Interface is used to receive and send SIP messages with a specific SIP entity (IP Group)
- Multiple SIP Interfaces may represent multiple SIP entities in the VoIP network:
  - SIP Trunk
  - LAN IP-PBX
  - Remote WAN users

- An entity with a set of definitions and behaviors which represents a SIP Group in the IP Network
- Used to classify incoming SIP dialog-initiating requests to a source IP Group, based on Proxy Set ID
- Used in IP-to-IP routing rules to denote the source and destination of the call
- **3 Types of IP Group:**
  - **Server:** Used when the destination address is known
  - **User:** Represents a group of users where their location is dynamically obtained by the device when REGISTER
  - **Gateway:** Applicable where the SBC receives requests to and from a gateway representing multiple users
- **It is highly recommended that you do not configure IP Group ID 0**
  - The only time that you should configure this specific IP Group is when it is used for the Gateway Interface (e.g., PSTN fallback)

- A Proxy Set is a group of Proxy servers defined by IP address or Fully Qualified Domain Name (FQDN)
- Represents the destination (address) of the Server-type IP Group
- Each Proxy server address can define:
  - Destination SIP port
  - Transport type
  - Load balancing
  - Redundancy mechanisms
- Can be used for message classification
- Keep alive mechanism can be implemented

- An optional configuration entity that defines a wide range of call settings for a specific SIP entity (IP Group)
- Includes signaling and media related settings
- The IP Profile is the interoperability “machine” of the device, enabling communication between SIP endpoints that “speak” different call “languages”
- The IP Profile is associated with the SIP entity by assigning the IP Profile to the IP Group of the SIP entity

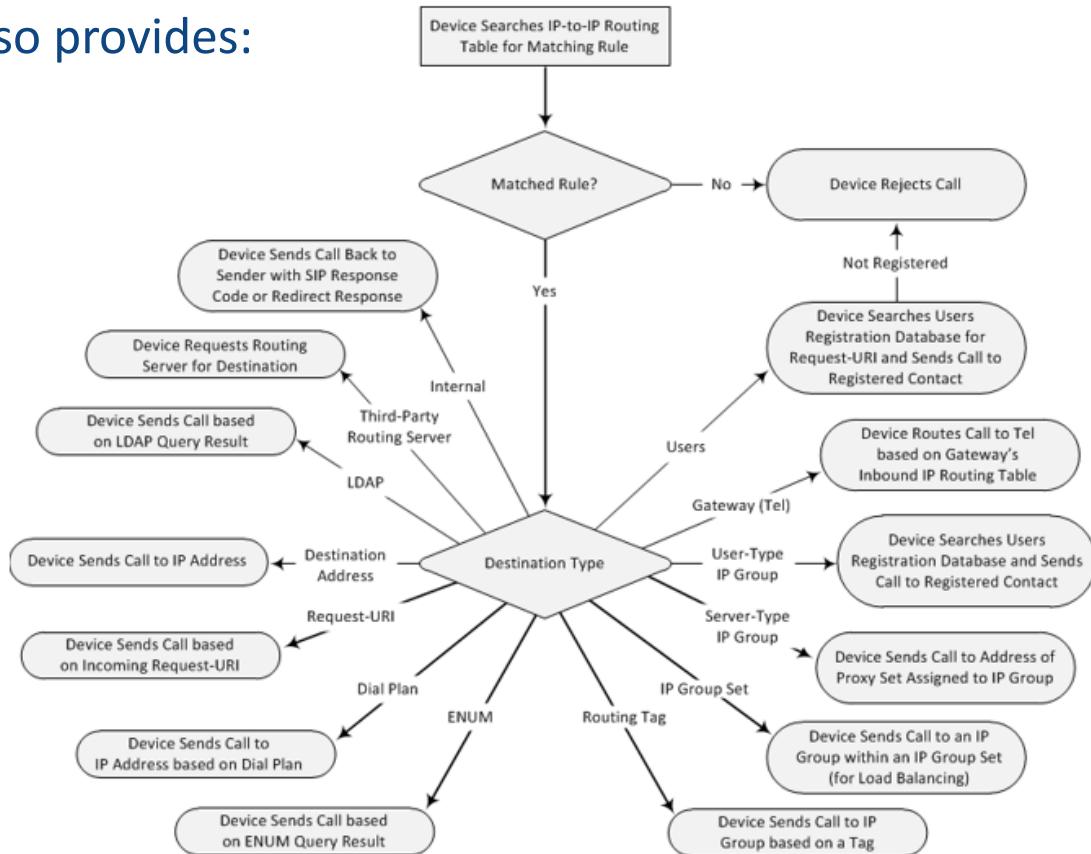
- A process that identifies the incoming call (SIP dialog request) as belonging to a specific SIP entity (IP Group)
- There are four chronological classification stages:  
*(each stage is done only if the previous stage fails)*
  - Classify the incoming SIP message by checking if it belongs to a user that is already registered in the device's registration database
  - Classify the incoming SIP message by Proxy Set Table
  - Classify the incoming SIP message using the Classification Table
  - Classify the incoming SIP message using the Reject or Allow 'Unclassified Calls' parameter
- If the SBC doesn't find a matching rule (i.e., classification fails), the dialog is rejected

- IP-to-IP routing rules define the routes for routing calls between SIP entities
- The routing rules typically employ IP Groups to denote the source and destination of the call
- Various other source and destination methods can be used
  - For example, the source can be a source host name while the destination can be an IP address or based on an LDAP query

# SBC IP-to-IP Routing

- The IP-to-IP Routing Table also provides:

- Alternative routing
- Re-routing of SIP requests
- Least Cost Routing (LCR)
- Call Forking

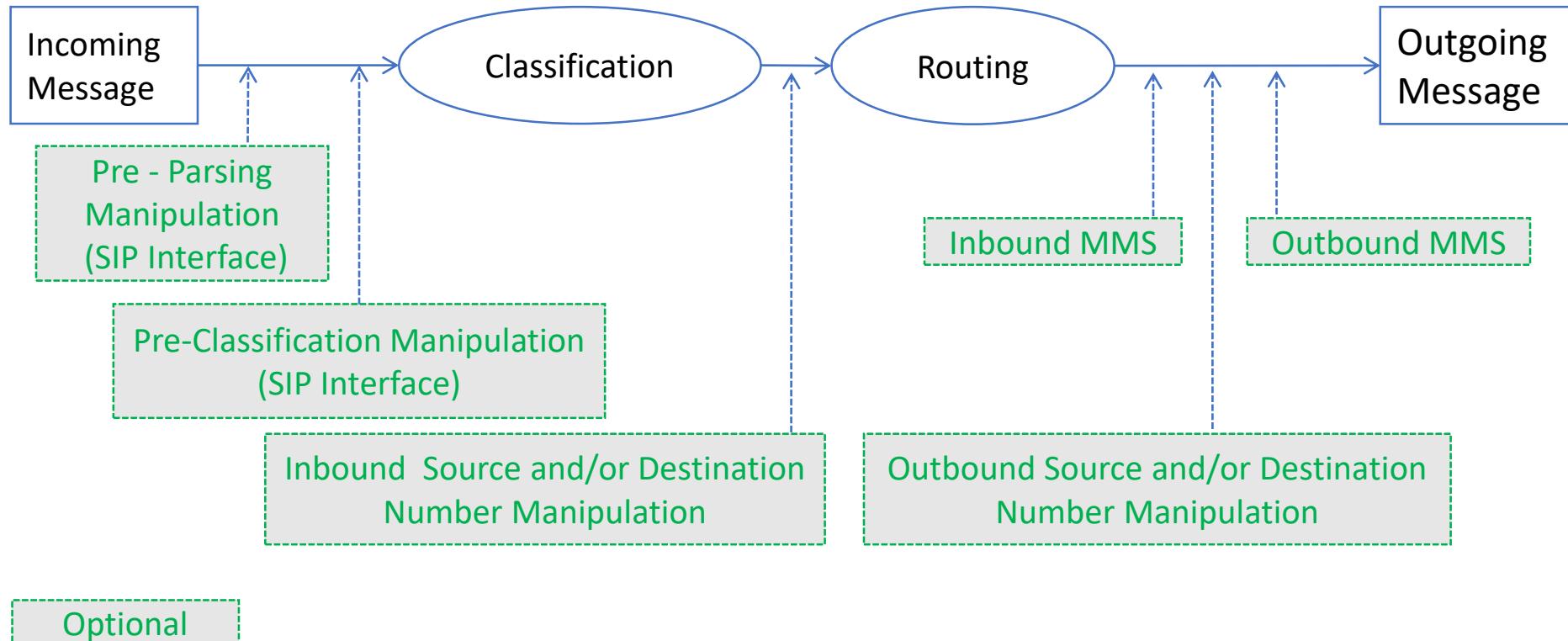


- IP-to-IP Inbound and Outbound manipulation lets you manipulate the user part of the SIP URI in the SIP message for a specific entity
- Inbound manipulation is done on messages received from the SIP entity
- Outbound manipulation is done on messages sent to the SIP entity

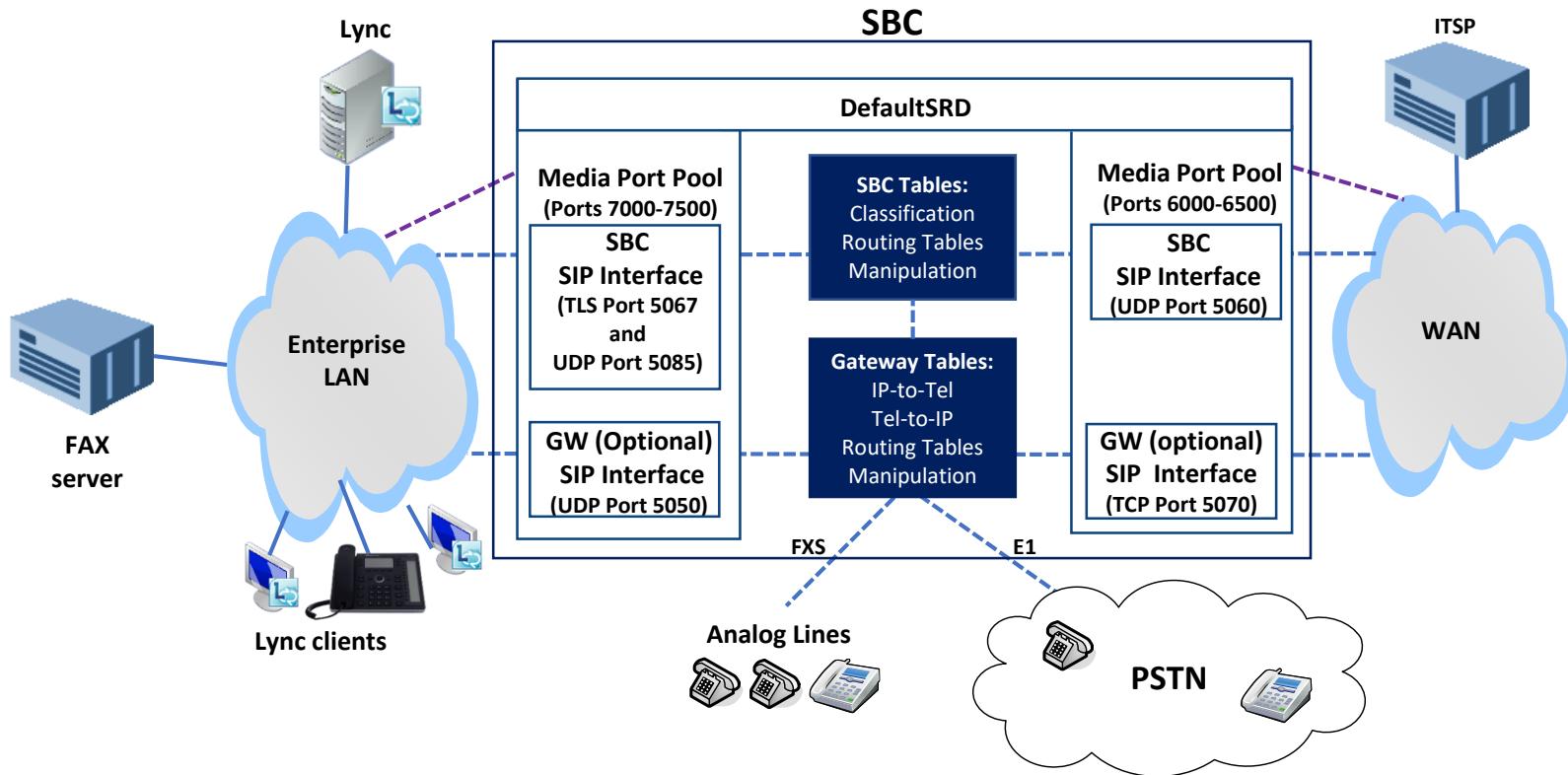
- A combination of rules, specified as a set or group of actions, to be attached to IP Group
- IP Group page display 2 fields:
  - Inbound Message Manipulation Set
    - Set of rules applied on incoming messages (received from the SIP entity)
  - Outbound Message Manipulation Set
    - Set of rules applied on outgoing messages (sent to the SIP entity)

- SBC Routing Policy logically groups routing and manipulation (inbound and outbound) rules to a specific SRD
- For most deployments only a single Routing Policy is required
- A default Routing Policy is provided which is automatically associated with all relevant configuration entities
- Enables Least Cost Routing (LCR) for routing rules and associates an LDAP server for LDAP-based routing

- Call Admission Control (CAC) limits the maximum number of permitted concurrent calls (SIP dialogs) per:
  - SRD
  - SIP Interface
  - IP Group
  - User

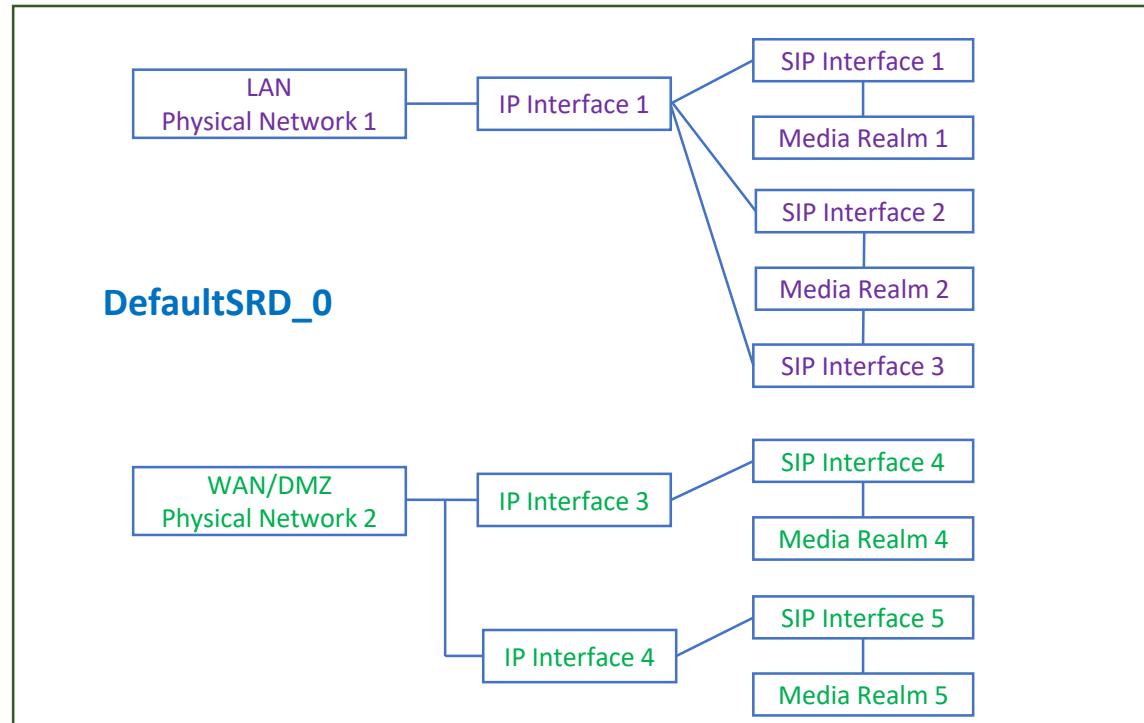


# SIP Trunk Example



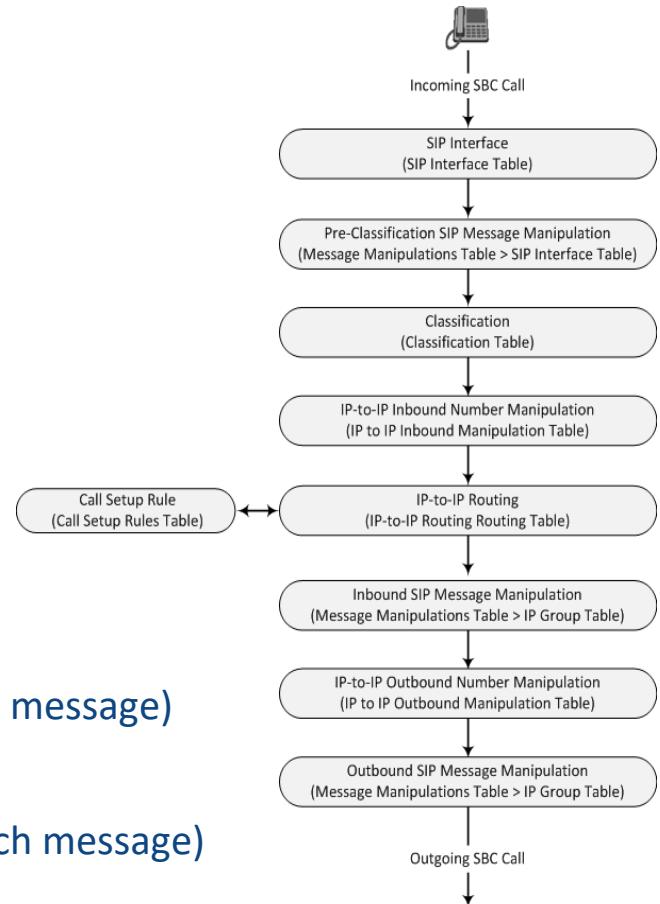
# SIP Trunk Example

- SRD represents the entire SIP-based VoIP network (Layer 5)
- Multiple SIP Interfaces represent Multiple Layer 3 Networks



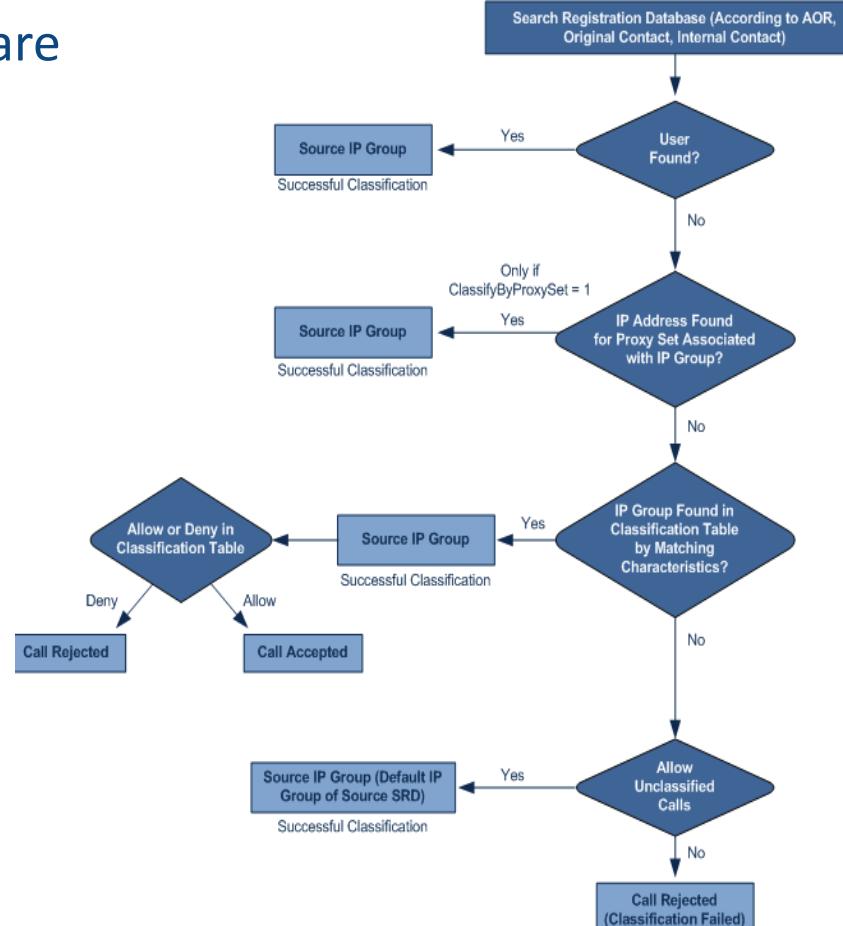
# SIP Dialog Initiation Process

- SIP dialog requests such as:
  - INVITE, SUBSCRIBE, OPTIONS, REFER, INFO, NOTIFY, REGISTER
- Determining Source and Destination URL
- Determining SIP Interface
- Applying SIP Message Manipulation (Optional)
- Classifying to an IP Group
- Applying IP-to-IP Inbound Manipulation (Optional)
- SBC IP-to-IP Routing
- Applying Inbound SIP Message Manipulation (Optional – For each message)
- Applying IP-to-IP Outbound Manipulation (Optional)
- Applying Outbound SIP Message Manipulation (Optional – For each message)



# Classification Process

- Occurs after Source and Destination URL are extracted
- Identifies Source IP Group stages by:
  - Device's registration database
  - Proxy Set
  - Classification Table
  - Reject or Allow unclassified calls



- **If the IP address of the IP Group entity is known**, it is recommended to employ the classification based on Classification Table, where the rule is configured with not only the IP address, but also with SIP message characteristics to increase the strictness of the classification process
- **If the IP address is unknown**, meaning the Proxy Set associated with the IP Group is configured with an FQDN, it is recommended to employ the classification based on Proxy Set
  - This allows the SBC to classify the incoming message based on the DNS-resolved IP address
  - The reason for classifying by Proxy Set is that IP address forgery (commonly known as IP spoofing) is more difficult than malicious SIP message tampering and therefore, using a classification rule without an IP address offers a weaker form of security

An IP Profile is associated to:

- A. An IP Group from Gateway type
- B. An IP Group from Server type
- C. An IP Group from User type
- D. An IP Group from any type

Proxy Sets can be associated to:

- A. An IP Group from Server type only
- B. An IP Group from User type only
- C. An IP Group from Gateway type only
- D. An IP Group from any type



**Classify by Proxy Set means:**

- A. Identify the source by it's Address of Record in the Data Base
- B. Identify the source by it's IP destination address
- C. Identify the source by it's IP address
- D. Identify the source by it's URI





Lesson 7

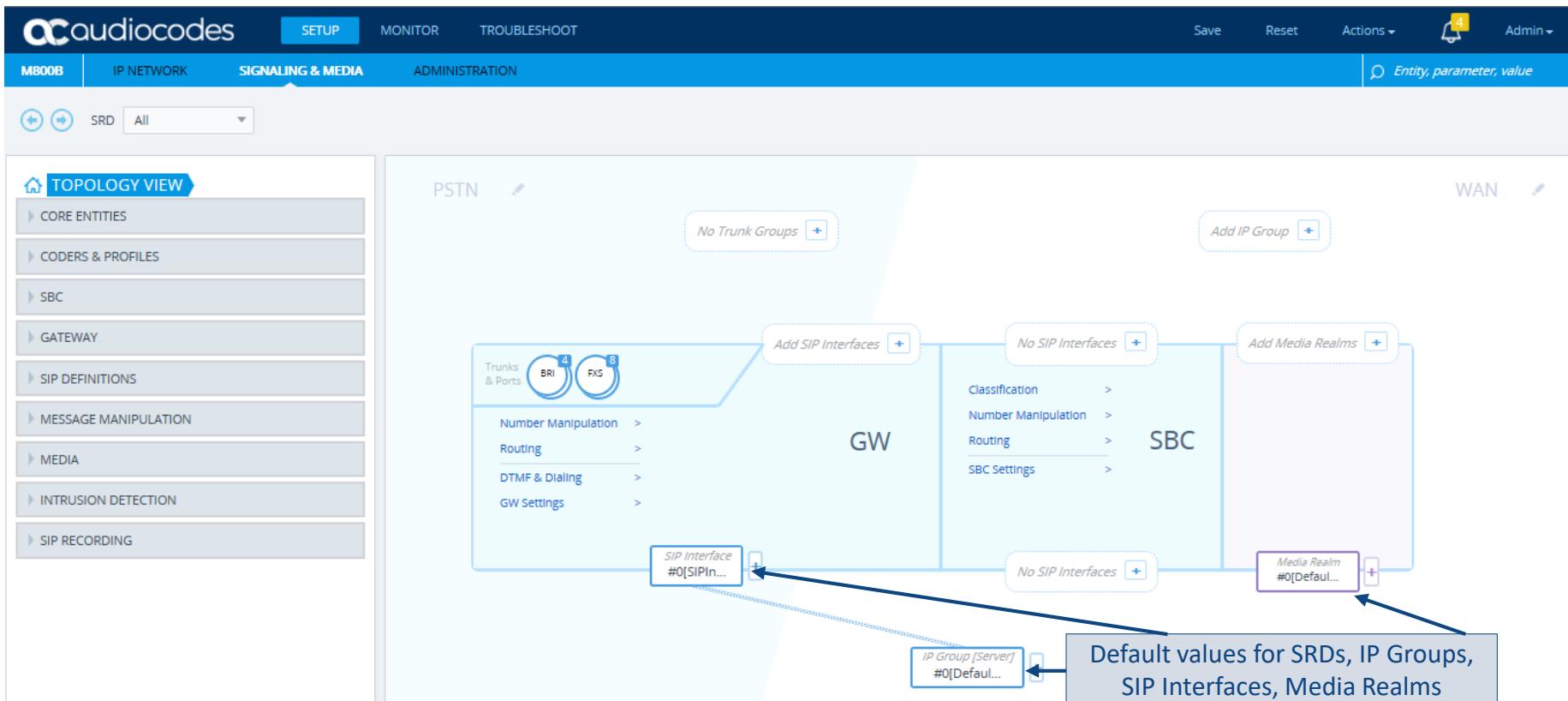
## SBC Configuration



- After completing this lesson you'll know how to:
  - Configure the parameters required by the SBC
  - Configure SBC IP to IP Routing

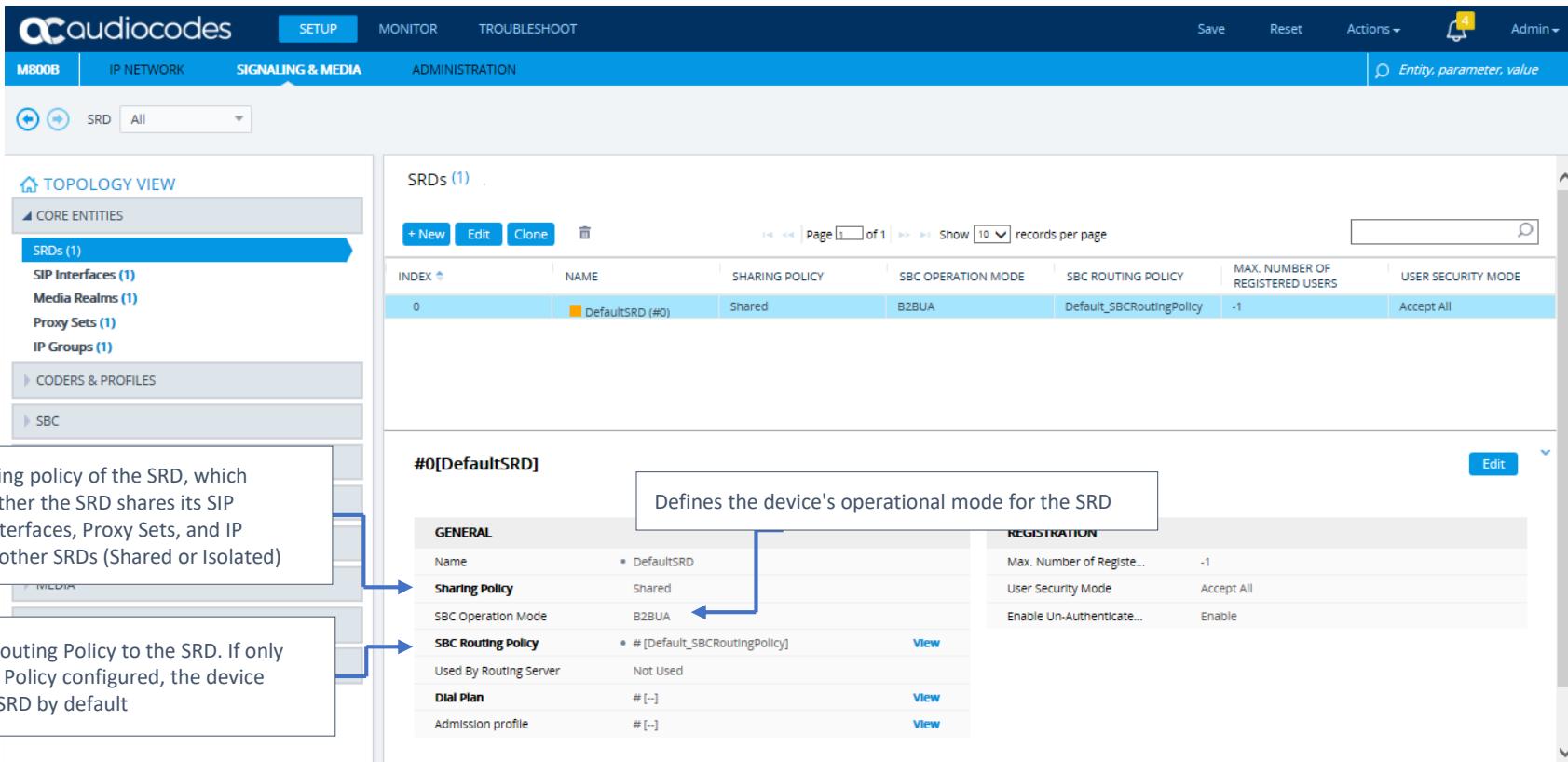
# Initial Topology View

- SBC application is enabled by default



# SRD Table

- Default SRD is already pre-configured



TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (1)
- Media Realms (1)
- Proxy Sets (1)
- IP Groups (1)

CODERS & PROFILES

SBC

Defines the sharing policy of the SRD, which determines whether the SRD shares its SIP resources (SIP Interfaces, Proxy Sets, and IP Groups) with all other SRDs (Shared or Isolated)

Assigns an SBC Routing Policy to the SRD. If only one SBC Routing Policy configured, the device assigns it to the SRD by default

SRDs (1)

INDEX	NAME	SHARING POLICY	SBC OPERATION MODE	SBC ROUTING POLICY	MAX. NUMBER OF REGISTERED USERS	USER SECURITY MODE
0	DefaultSRD (#0)	Shared	B2BUA	Default_SBCRoutingPolicy	-1	Accept All

#0[DefaultSRD]

GENERAL

Name: DefaultSRD

Sharing Policy: Shared

SBC Operation Mode: B2BUA

SBC Routing Policy: # [Default\_SBCRoutingPolicy]

Used By Routing Server: Not Used

Dial Plan: # [-]

Admission profile: # [-]

REGISTRATION

Max. Number of Registrations: -1

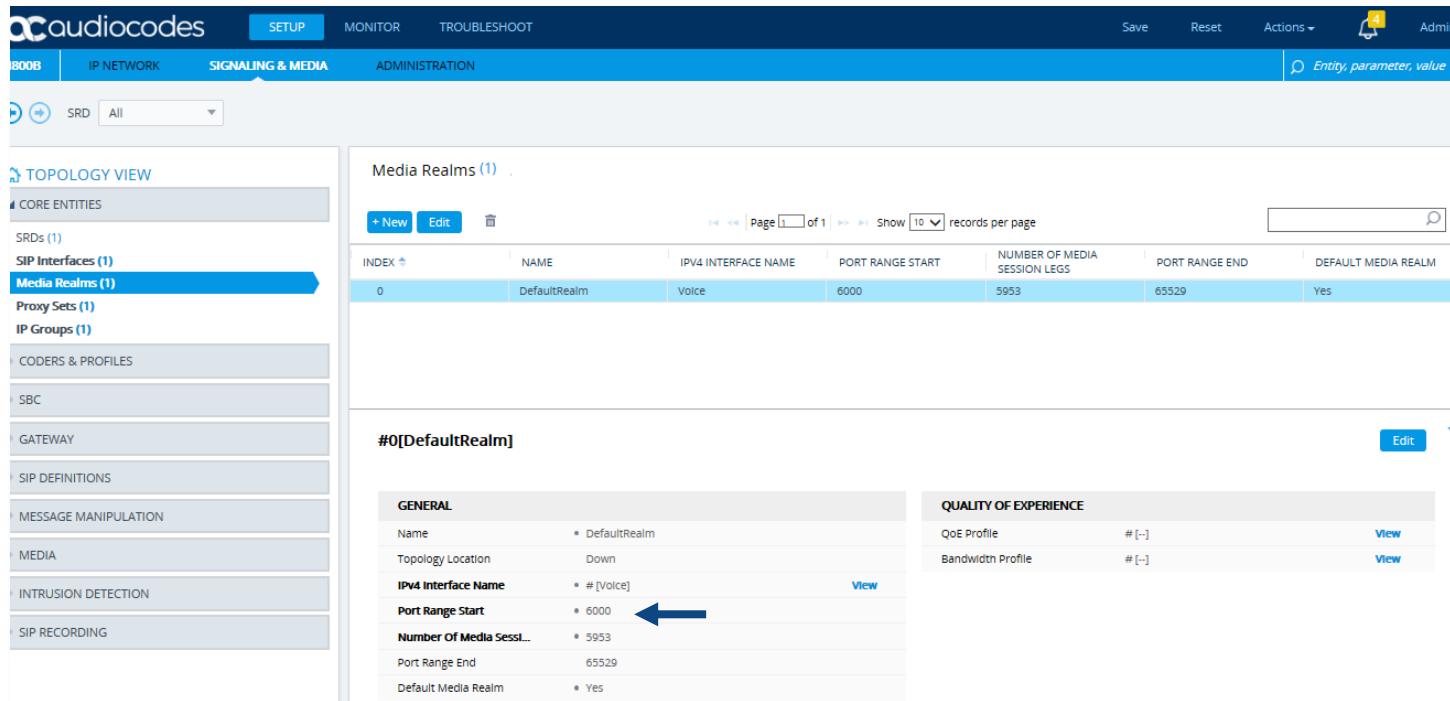
User Security Mode: Accept All

Enable Un-Authenticate: Enable

Defines the device's operational mode for the SRD

# Media Realm Table

- The default Media Realm is used for SIP Interfaces and IP Groups for which you have not assigned a Media Realm
- Ports are allocated in chunks of 4, 5 or 10 (device dependent) called media session legs



The screenshot shows the audiocodes web interface with the following details:

**Top Navigation:** SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, Admin.

**Left Sidebar:** CORE ENTITIES (SRDs 1), SIP Interfaces 1, **Media Realms 1** (highlighted in blue), Proxy Sets 1, IP Groups 1. CODERS & PROFILES, SBC, GATEWAY, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, INTRUSION DETECTION, SIP RECORDING.

**Main Content - Media Realms Table:**

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	DefaultRealm	Voice	6000	5953	65529	Yes

**Bottom Content - #0[DefaultRealm] Details:**

**GENERAL**

- Name: DefaultRealm
- Topology Location: Down
- IPv4 Interface Name:** # [Voice] View
- Port Range Start:** 6000 ←
- Number Of Media Ses...**: 5953
- Port Range End: 65529
- Default Media Realm: Yes

**QUALITY OF EXPERIENCE**

- QoE Profile: # [-] View
- Bandwidth Profile: # [-] View

- Media Realm Extensions let you configure a Media Realm with different port ranges or/and different interfaces
- This means that the Media Realm is distributed across multiple interfaces
- The number of Media Realm Extensions that can be configured depend from the platform

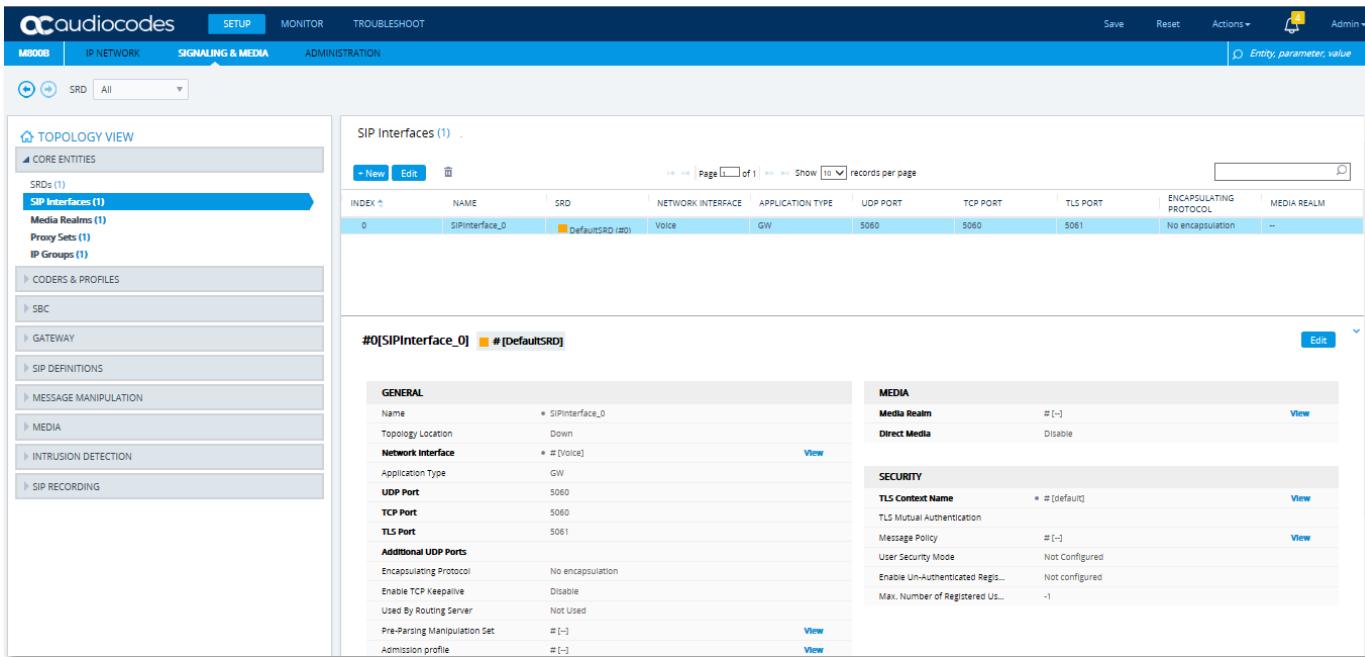
#0[DefaultRealm]

GENERAL	
Name	* DefaultRealm
Topology Location	Down
IPv4 Interface Name	* # [Voice] <a href="#">View</a>
Port Range Start	* 6000
Number Of Media Session...	* 5953
Port Range End	65529
Default Media Realm	* Yes

[Media Realm Extension 0 items >>](#)  [Remote Media Subnet 0 items >>](#)

# SIP Interface Table

- Default SIP Interface is already pre-configured and assigned to the default SRD
- Bounded to Layer-3 network
- Defines a local listening port for SIP signaling traffic on a local logical IP network



The screenshot shows the audiocodes M800 web interface. The top navigation bar includes tabs for SETUP, MONITOR, TROUBLESHOOT, and several others like SIGNALING & MEDIA and ADMINISTRATION. The main content area is titled "SIP Interfaces (1)" and displays a table with one row. The table columns are INDEX, NAME, SRD, NETWORK INTERFACE, APPLICATION TYPE, UDP PORT, TCP PORT, TLS PORT, ENCAPSULATING PROTOCOL, and MEDIA REALM. The single entry is #0[SIPInterface\_0] with SRD DefaultSRD (#0). Below the table, there are two tabs: GENERAL and MEDIA, each containing various configuration parameters.

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SIPInterface_0	DefaultSRD (#0)	Voice	GW	5060	5060	5061	No encapsulation	--

#0[SIPInterface\_0]    # {DefaultSRD}

GENERAL		MEDIA	
Name	# {SIPInterface_0}	Media Realm	# {-}
Topology Location	Down	Direct Media	Disable
Network Interface	# {Voice}	View	
Application Type	GW		
UDP Port	5060		
TCP Port	5060		
TLS Port	5061		
Additional UDP Ports			
Encapsulating Protocol	No encapsulation		
Enable TCP Keepalive	Disable		
Used By Routing Server	Not Used		
Pre-Parsing Manipulation Set	# {-}	View	View
Admission profile	# {-}	View	View
SECURITY			
TLS Context Name	# {default}	View	
TLS Mutual Authentication	# {-}	View	
Message Policy	# {-}	View	
User Security Mode	Not Configured	View	
Enable Un-Authenticated Regis...	Not configured	View	
Max. Number of Registered Us...	-1	View	

# SIP Interface Table Record

#1[SIP Trunk] # [DefaultSRD]		<p>By default, if you do not configure a name, the device automatically assigns the name</p>																																		
<table border="1"><tr><td colspan="2"><b>GENERAL</b></td></tr><tr><td>Name</td><td>* SIP Trunk</td></tr><tr><td>Topology Location</td><td>Down</td></tr><tr><td><b>Network Interface</b></td><td>* # [Voice]</td></tr><tr><td>Application Type</td><td>* SBC</td></tr><tr><td><b>UDP Port</b></td><td>* 5070</td></tr><tr><td><b>TCP Port</b></td><td>* 5070</td></tr><tr><td><b>TLS Port</b></td><td>* 5071</td></tr><tr><td><b>Additional UDP Ports</b></td><td></td></tr><tr><td>Encapsulating Protocol</td><td>No encapsulation</td></tr><tr><td>Enable TCP Keepalive</td><td>Disable</td></tr><tr><td>Used By Routing Server</td><td>Not Used</td></tr><tr><td>Pre-Parsing Manipulation Set</td><td># [-]</td></tr><tr><td>Admission profile</td><td># [-]</td></tr><tr><td colspan="2"><b>CLASSIFICATION</b></td></tr><tr><td>Classification Failure Response...</td><td>500</td></tr><tr><td>Pre-classification Manipulation...</td><td>-1</td></tr></table>			<b>GENERAL</b>		Name	* SIP Trunk	Topology Location	Down	<b>Network Interface</b>	* # [Voice]	Application Type	* SBC	<b>UDP Port</b>	* 5070	<b>TCP Port</b>	* 5070	<b>TLS Port</b>	* 5071	<b>Additional UDP Ports</b>		Encapsulating Protocol	No encapsulation	Enable TCP Keepalive	Disable	Used By Routing Server	Not Used	Pre-Parsing Manipulation Set	# [-]	Admission profile	# [-]	<b>CLASSIFICATION</b>		Classification Failure Response...	500	Pre-classification Manipulation...	-1
<b>GENERAL</b>																																				
Name	* SIP Trunk																																			
Topology Location	Down																																			
<b>Network Interface</b>	* # [Voice]																																			
Application Type	* SBC																																			
<b>UDP Port</b>	* 5070																																			
<b>TCP Port</b>	* 5070																																			
<b>TLS Port</b>	* 5071																																			
<b>Additional UDP Ports</b>																																				
Encapsulating Protocol	No encapsulation																																			
Enable TCP Keepalive	Disable																																			
Used By Routing Server	Not Used																																			
Pre-Parsing Manipulation Set	# [-]																																			
Admission profile	# [-]																																			
<b>CLASSIFICATION</b>																																				
Classification Failure Response...	500																																			
Pre-classification Manipulation...	-1																																			
<p>Select Network interface</p> <p>Select SBC or GW application</p> <p>Select UDP, TCP and/or TLS port/s</p> <p>Enables the SIP Interface to be used by a third-party routing server for call routing decisions</p>																																				
<table border="1"><tr><td colspan="2"><b>MEDIA</b></td></tr><tr><td>Media Realm</td><td>* # [DefaultRealm]</td></tr><tr><td>Direct Media</td><td>Disable</td></tr><tr><td colspan="2"><b>SECURITY</b></td></tr><tr><td>TLS Context Name</td><td>* # [default]</td></tr><tr><td>TLS Mutual Authentication</td><td></td></tr><tr><td>Message Policy</td><td># [-]</td></tr><tr><td>User Security Mode</td><td>Not Configured</td></tr><tr><td>Enable Un-Authenticated Regis...</td><td>Not configured</td></tr><tr><td>Max. Number of Registered Us...</td><td>-1</td></tr></table>			<b>MEDIA</b>		Media Realm	* # [DefaultRealm]	Direct Media	Disable	<b>SECURITY</b>		TLS Context Name	* # [default]	TLS Mutual Authentication		Message Policy	# [-]	User Security Mode	Not Configured	Enable Un-Authenticated Regis...	Not configured	Max. Number of Registered Us...	-1														
<b>MEDIA</b>																																				
Media Realm	* # [DefaultRealm]																																			
Direct Media	Disable																																			
<b>SECURITY</b>																																				
TLS Context Name	* # [default]																																			
TLS Mutual Authentication																																				
Message Policy	# [-]																																			
User Security Mode	Not Configured																																			
Enable Un-Authenticated Regis...	Not configured																																			
Max. Number of Registered Us...	-1																																			
<p>Defines the SIP response code that the device sends if a received SIP request (OPTIONS, REGISTER, or INVITE) fails the SBC Classification process.</p> <p>The valid value can be a SIP response code from 400 through 699, or it can be set to 0 to not send any response at all (recommended for security reasons).</p> <p>The default response code is 500 (Server Internal Error)</p>																																				

# Proxy Sets Table



audiocodes

SETUP MONITOR TROUBLESHOOT

MSOOL IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions 4 Admin Entity, parameter, value

SRD All

### TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)**
- IP Groups (2)

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

### Proxy Sets (2)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	IP-PBX	DefaultSRD (#0)	..	IP-PBX	60		Disable
1	ITSP	DefaultSRD (#0)	..	ITSP	60		Disable

#0[IP-PBX] # [DefaultSRD] Edit

**GENERAL**

Name	IP-PBX
Gateway IPv4 SIP Interface	# [-]
SBC IPv4 SIP Interface	# [IP-PBX]
TLS Context Name	# [-]

**REDUNDANCY**

Redundancy Mode	Proxy Hot Swap	Disable
Proxy Load Balancing Method		Disable
Min. Active Servers for Load B...	1	

**KEEP ALIVE**

Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Keep-Alive Failure Responses	
Success Detection Retries	1
Success Detection Interval	10
Failure Detection Retransmissio...	-1

**ADVANCED**

Classification Input	IP Address only
DNS Resolve Method	

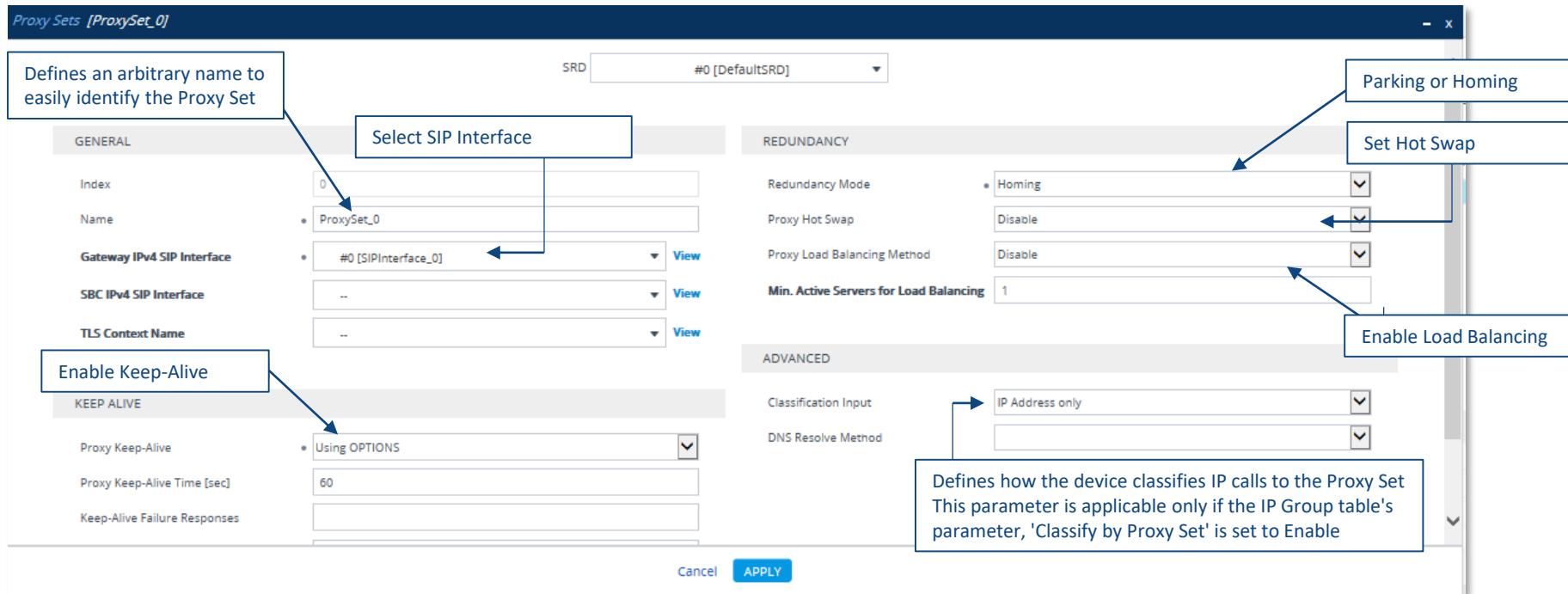
**PROXY ADDRESS**

10.15.77.144:5060	UDP
-------------------	-----

Proxy Address 1 items >>

# Proxy Sets Table

- Define the Proxy Set Name
- Select Redundancy mechanisms



Proxy Sets [ProxySet\_0]

SRD #0 [DefaultSRD]

GENERAL

Defines an arbitrary name to easily identify the Proxy Set

Select SIP Interface

Name: ProxySet\_0

Gateway IPv4 SIP Interface: #0 [SIPInterface\_0]

SBC IPv4 SIP Interface: --

TLS Context Name: --

KEEP ALIVE

Enable Keep-Alive

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time [sec]: 60

Keep-Alive Failure Responses: --

REDUNDANCY

Parking or Homing

Set Hot Swap

Redundancy Mode: Homing

Proxy Hot Swap: Disable

Proxy Load Balancing Method: Disable

Min. Active Servers for Load Balancing: 1

ADVANCED

Classification Input: IP Address only

DNS Resolve Method: None

Defines how the device classifies IP calls to the Proxy Set  
This parameter is applicable only if the IP Group table's parameter, 'Classify by Proxy Set' is set to Enable

Cancel **APPLY**

# Proxy Address Child Table

- Enter Proxy IP address or FQDN
- Enter Destination SIP port & Transport type

#0[ProxySet\_0] # [DefaultSRD]

GENERAL	
Name	* ProxySet_0
Gateway IPv4 SIP Interface	* #[SIPInterface_0] <a href="#">View</a>
SBC IPv4 SIP Interface	#[--] <a href="#">View</a>
TLS Context Name	#[--] <a href="#">View</a>

KEEP ALIVE	
Proxy Keep-Alive	* Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Keep-Alive Failure Responses	
Success Detection Retries	1
Success Detection Interval	10
Failure Detection Retransmissions	-1

[Proxy Address 0 Items >>](#)

Proxy Sets [#0] > Proxy Address (1)

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	10.15.12.2:5070	TCP

#0

GENERAL	
Proxy Address	* 10.15.12.2:5070
Transport Type	* TCP

# IP Group Table

audiocodes

SETUP MONITOR TROUBLESHOOT

M800 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions ▾ 6 Admin ▾

Entity, parameter, value

SRD All

TOPLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (3)
- Media Realms (2)
- Proxy Sets (3)
- IP Groups (3)**

CODERS & PROFILES

SBC

IP Groups (3) .

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPG	DefaultSRD	Server	Not Configured	ProxySet_0	--	--		Disable	-1	-1
1	PBX	DefaultSRD	Server	Not Configured	PBX	--	--		Enable	-1	-1
2	ITSP	DefaultSRD	Server	Not Configured	ITSP	--	--		Enable	-1	-1

# IP Group Table – General Parameters

**GENERAL**

Index	1
Name	PBX
Topology Location	Down
Type	Server
Proxy Set	#1 [PBX]
IP Profile	..
Media Realm	..
Contact User	
SIP Group Name	
Created By Routing Server	No
Used By Routing Server	Not Used
Proxy Set Connectivity	Connected

**IP Group Name**  
Defines the display location of the IP Group in the Topology view

**3 types: Server, User, Gateway**

**View**  
Proxy Set Name associated with the Server IP Group

**View**  
IP Profile, assigned to the IP Group. The default is 'None'

**View**  
Media Realm, assigned to the IP Group. Choose the name defined in the Media Realm Table from the drop-down list

**Read-only field.** Displays the connectivity status with Server-type IP Groups. As the Proxy Set defines the address of the IP Group, the connectivity check (keep-alive) by the device is done to this address.  
Values: **NA, Not Connected, Connected**  
This is also displayed in the Topology View page

**Defines the user part of the From, To, and Contact headers of SIP REGISTER messages, and the user part of the Contact header of INVITE messages received from this IP Group and forwarded by the device to another IP Group**

**The Request-URI host name used in INVITE and REGISTER messages sent to this IP Group, or the host name in the From header of INVITE messages received from this IP Group**

# IP Group Table – SBC General Parameters

SBC GENERAL	
Classify By Proxy Set	<input type="checkbox"/> Enable
SBC Operation Mode	<input type="checkbox"/> Not Configured
SBC Client Forking Mode	<input type="checkbox"/> Sequential
Admission profile	<input type="checkbox"/> --

Enables classification of incoming SIP dialogs (INVITEs) to the IP Group, based on the Proxy Set assigned to the IP Group (Applicable only to Server-type IP Groups)

Defines the device's operational mode for the IP Group  
Options:

- Not Configured = (Default)
- B2BUA
- Call Stateful Proxy
- Microsoft Server (for One-Voice Resiliency feature)

Defines call forking of INVITE messages to up to five separate SIP outgoing legs for User-type IP Groups

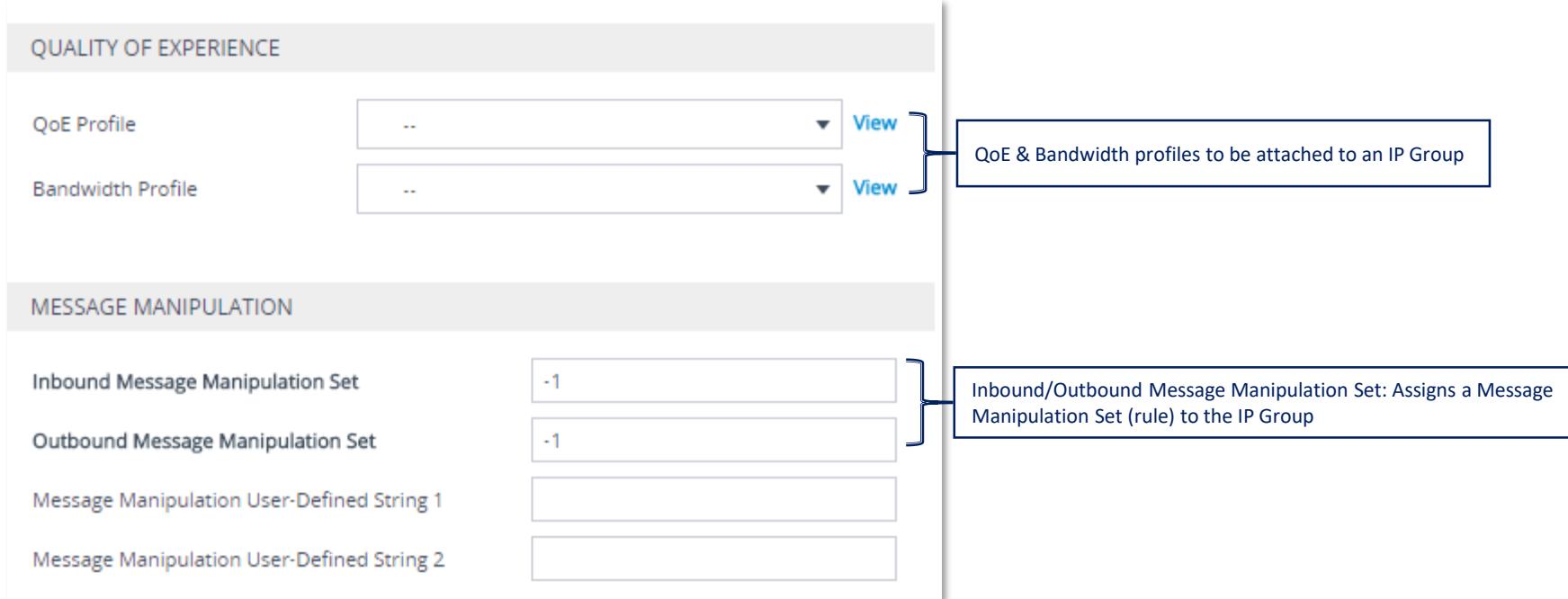
This occurs if multiple contacts are registered under the same AOR in the device's registration database

Options:

- Sequential = (Default)
- Parallel
- Sequential Available Only

Call Admission Profile, assigned to the IP Group. The default is 'None'

# IP Group Table – SBC Other Tabs



The screenshot shows the 'IP Group Table – SBC Other Tabs' interface. It has two main sections: 'QUALITY OF EXPERIENCE' and 'MESSAGE MANIPULATION'. In the 'QUALITY OF EXPERIENCE' section, there are dropdown menus for 'QoE Profile' and 'Bandwidth Profile', each with a 'View' button. In the 'MESSAGE MANIPULATION' section, there are dropdown menus for 'Inbound Message Manipulation Set' and 'Outbound Message Manipulation Set', each with a value '-1'. There are also two empty input fields for 'Message Manipulation User-Defined String 1' and 'Message Manipulation User-Defined String 2'. A callout box points to the 'QoE Profile' and 'Bandwidth Profile' sections with the text: 'QoE & Bandwidth profiles to be attached to an IP Group'. Another callout box points to the 'Inbound Message Manipulation Set' and 'Outbound Message Manipulation Set' sections with the text: 'Inbound/Outbound Message Manipulation Set: Assigns a Message Manipulation Set (rule) to the IP Group'.

QUALITY OF EXPERIENCE

QoE Profile

Bandwidth Profile

View

View

QoE & Bandwidth profiles to be attached to an IP Group

MESSAGE MANIPULATION

Inbound Message Manipulation Set

-1

Outbound Message Manipulation Set

-1

Message Manipulation User-Defined String 1

Message Manipulation User-Defined String 2

Inbound/Outbound Message Manipulation Set: Assigns a Message Manipulation Set (rule) to the IP Group

# IP Group Table – SBC Registration Tab

SBC REGISTRATION AND AUTHENTICATION

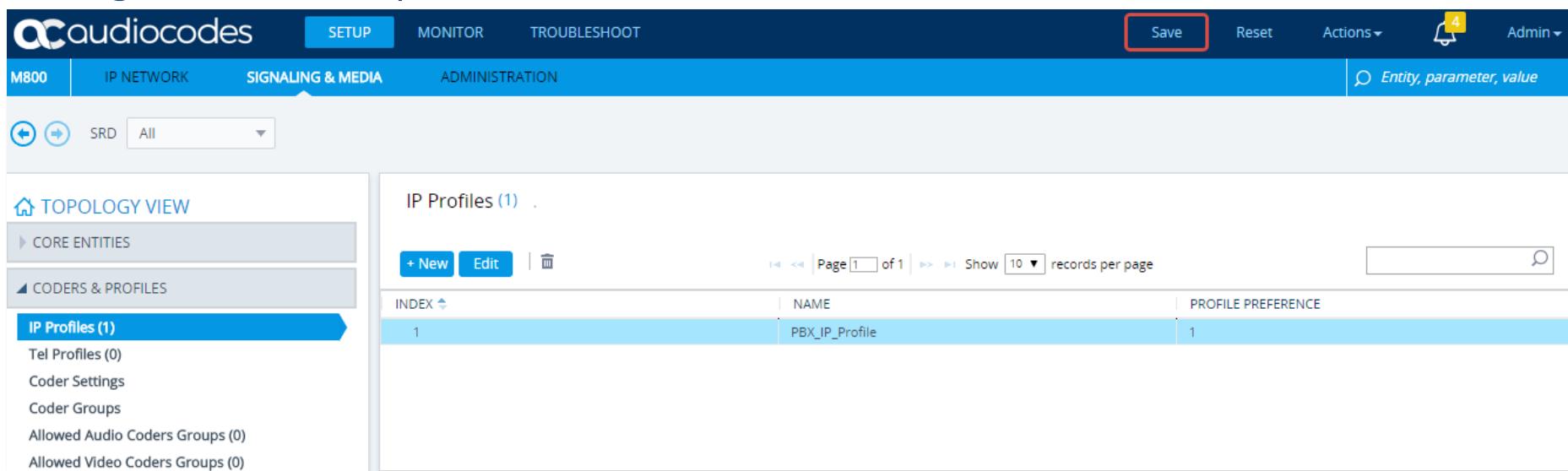
Max. Number of Registered Users	<input type="text" value="-1"/>
Registration Mode	User Initiates Registration
User Stickiness	Disable
User UDP Port Assignment	Disable
Authentication Mode	User Authenticates
Authentication Method List	
Username	• Admin
Password	• .....

This feature provides support for configuring the device to always route SIP requests of a user (belonging to a User-type IP Group) to the same registrar server in a Proxy Set (associated with a Server-type IP Group) to where the last successful REGISTER request was routed

Defines the authentication mode.  
**User Authenticates** = (Default) The device does not handle the authentication  
**SBC as Client** = The device authenticates as a client  
**SBC as Server** = The device acts as an Authentication server

Defines the shared username and password for authenticating the IP Group, when the device acts as an Authentication server

- A set of configuration parameters
- Provides high-level adaptation when connected to a variety of equipment, each of which requires different system behavior
- Assigned to IP Groups



The screenshot shows the audiocodes M800 web interface. The top navigation bar includes links for SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, and Admin. The main menu on the left has sections for CORE ENTITIES, CODERS & PROFILES, and IP Profiles (1). The IP Profiles section is currently selected. The central content area displays the 'IP Profiles (1)' page with a table showing one profile: INDEX 1, NAME PBX\_IP\_Profile, and PROFILE PREFERENCE 1. There are buttons for + New, Edit, and Delete.

INDEX	NAME	PROFILE PREFERENCE
1	PBX_IP_Profile	1

- The configurable parameters for the IP Profile are divided into sections:

- General parameters
- Media Security parameters
- SBC Signaling parameters
- SBC Early Media parameters
- SBC Registration parameters
- SBC Forward and Transfer parameters
- SBC Hold parameters
- SBC Media parameters
- SBC Fax parameters
- Media parameters
- Quality of Service parameters
- Jitter Buffer parameters
- Gateway General parameters
- Gateway DTMF parameters
- Gateway Fax and Modem parameters
- Answer Machine Detection parameters
- Local Tones parameters



# IP to IP Routing Table

audiocodes

SETUP MONITOR TROUBLESHOOT

M800 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions ▾ 4 Admin ▾ Entity, parameter, value

SRD All

**TOPOLOGY VIEW**

- CORE ENTITIES
- GATEWAY
- MEDIA
- CODERS & PROFILES
- SBC
  - Classification (0)
  - Routing
    - Routing Policies (1)
    - IP-to-IP Routing (2)**
  - Alternative Reasons (0)

**IP-to-IP Routing (2)**

New Edit Insert ⌂ ⌂ Page 1 of 1 Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	IP-PBX-ITSP	Default_SBCRoutingP	Route Row	IP-PBX	All	+	+	IP Group	ITSP	--	
1	ITSP-IP-PBX	Default_SBCRoutingP	Route Row	ITSP	All	+	+	IP Group	IP-PBX	--	

#1[ITSP-IP-PBX] #0 [Default\_SBCRoutingPolicy] Edit

**GENERAL**

Name	ITSP-IP-PBX
Alternative Route Options	Route Row

**MATCH**

Source IP Group	#1[ITSP]
Request Type	All
Source Username Prefix	+
Source Host	+
Source Tag	
Destination Username Prefix	+
Destination Host	+
Destination Tag	
Message Condition	--
Call Trigger	Any
reRoute IP Group	Any

**ACTION**

Destination Type	IP Group
Destination IP Group	#2[IP-PBX]
Destination SIP Interface	--
Destination Address	
Destination Port	0
Destination Transport Type	
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	--

# IP to IP Routing Table – General and Match Sections

## GENERAL

Index

0

Name

Alternative Route Options

Route Row

Route Row / Alternative Route / Forking Group

## MATCH

Source IP Group

Any

View

Request Type

All

View

Source Username Pattern

\*

Source Host

\*

Source Tag

Destination Username Pattern

\*

Destination Host

\*

Destination Tag

Message Condition

--

From Message Condition Table

Call Trigger

Any

Defines the reason for re-routing the SIP request : Any/3xx/Refer

ReRoute IP Group

Any

Defines the IP Group that initiated (sent) the SIP redirect response 3xx or REFER

Defines the SIP dialog request type:

- All (default)
- INVITE
- REGISTER
- SUBSCRIBE
- INVITE and REGISTER
- INVITE and SUBSCRIBE
- OPTIONS

# IP to IP Routing Table – Action Section

ACTION	
Destination Type	IP Group
Destination IP Group	--
Destination SIP Interface	--
Destination Address	
Destination Port	0
Destination Transport Type	
IP Group Set	--
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	--
Routing Tag Name	default
Internal Action	Reply(Response='200')

Determines the destination type to which the outgoing SIP dialog is sent. This can be: IP Group, Destination Address, ENUM, LDAP, Request URI, Gateway, etc.

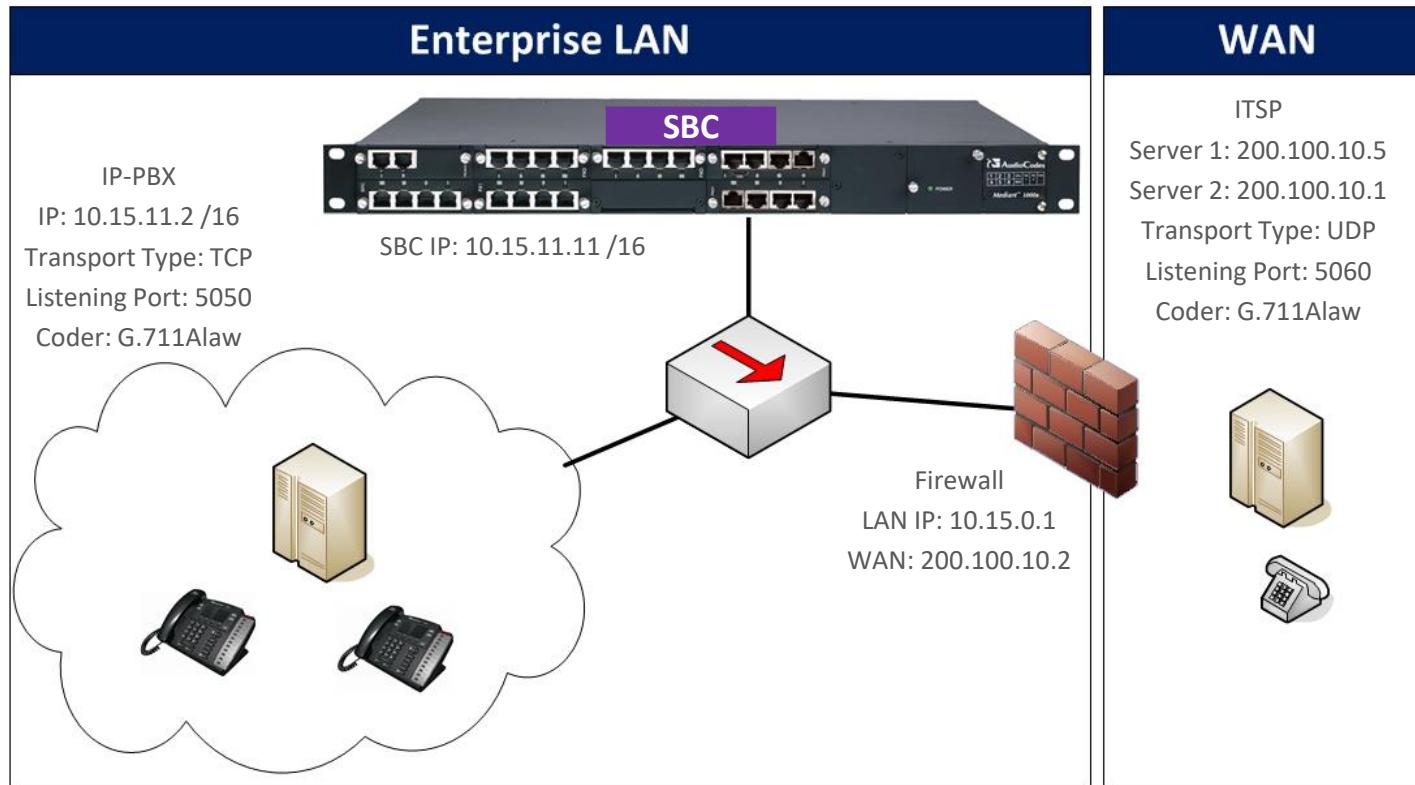
Assigns a Call Setup Rule ID to the routing rule. The device performs the Call Setup rules of this Set if the incoming call matches the characteristics of this routing rule

Defines whether the routing rule includes call forking

Defines the destination Dial Plan tag, which is used to determine the destination IP Group.

Defines a SIP response code (e.g., 200 OK) or a redirection response. The parameter is applicable only when the 'Destination Type' parameter in this table is configured to Internal

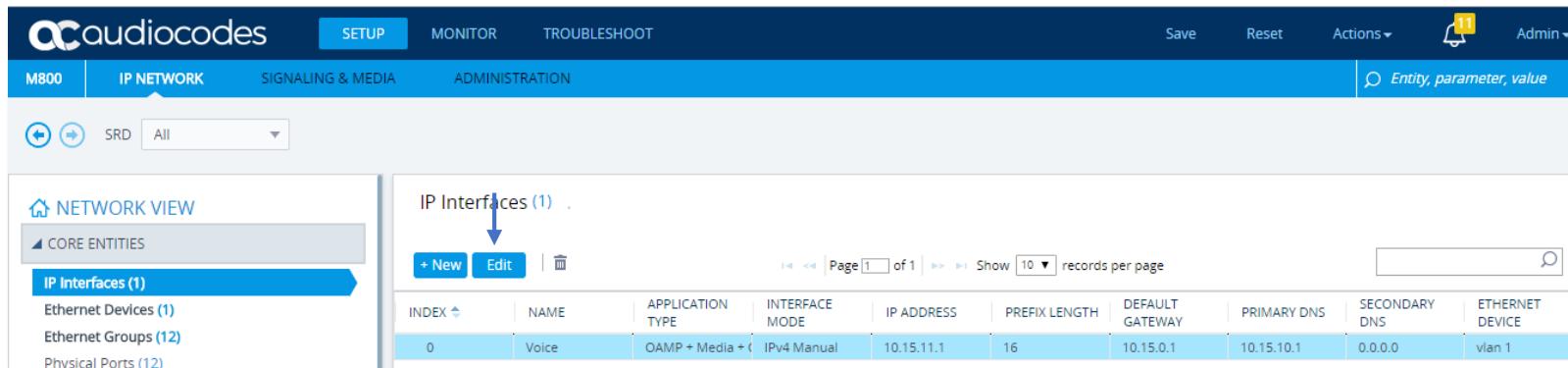
# Topology Configuration Example – One Leg LAN



- General Parameters Settings
- LAN IP Setting
- SIP Media Realm Table
- SIP Interface Table
- Proxy Sets Table
- IP Group Table
- Classification Table
- IP to IP Routing Table

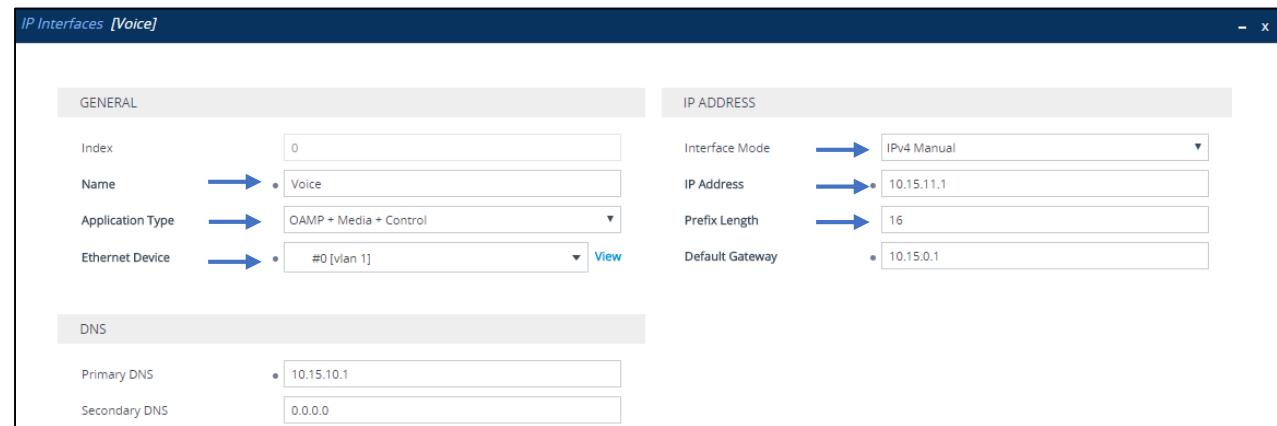
# Configure IP Addresses

- IP Interface Table



The screenshot shows the audiocodes M800 web interface. The top navigation bar includes SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, Admin, and a notification icon with 11 alerts. The main menu tabs are M800, IP NETWORK, SIGNALING & MEDIA, and ADMINISTRATION. The IP NETWORK tab is selected. On the left, the NETWORK VIEW sidebar shows CORE ENTITIES with IP Interfaces (1) selected, and lists Ethernet Devices (1), Ethernet Groups (12), and Physical Ports (12). The central content area displays the IP Interfaces table with one entry:

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	Voice	OAMP + Media + Control	IPv4 Manual	10.15.11.1	16	10.15.0.1	10.15.10.1	0.0.0.0	vlan 1



The screenshot shows the IP Interfaces [Voice] configuration dialog. It has two main sections: GENERAL and IP ADDRESS.

**GENERAL**

- Index: 0
- Name: Voice
- Application Type: OAMP + Media + Control
- Ethernet Device: #0 [vlan 1]

**IP ADDRESS**

- Interface Mode: IPv4 Manual
- IP Address: 10.15.11.1
- Prefix Length: 16
- Default Gateway: 10.15.0.1

**DNS**

- Primary DNS: 10.15.10.1
- Secondary DNS: 0.0.0.0

# IP Address – Physical to Interface

## Ethernet Devices (1)

+ New Edit

Page 1 of 1 Show 10 records per page



INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING	MTU
0	1	GROUP_1	vlan 1	Untagged	1500

## Ethernet Groups (12)

Edit

Page 1 of 2 Show 10 records per page



INDEX	NAME	MODE	MEMBER 1	MEMBER 2
0	GROUP_1	REDUN_1RX_1TX	GE_4_1	GE_4_2
1	GROUP_2	NONE	--	--
2	GROUP_3	NONE	--	--
3	GROUP_4	NONE	--	--

## NETWORK VIEW

### CORE ENTITIES

#### IP Interfaces (1)

#### Ethernet Devices (1)

#### Ethernet Groups (12)

#### Physical Ports (12)

#### Static Routes (0)

#### HA Settings

#### HA Network Monitor (0)

#### NAT Translation (0)

## Physical Ports (12)

Edit

Page 1 of 2 Show 10 records per page



INDEX	NAME	MODE	SPEED AND DUPLEX	DESCRIPTION	MEMBER OF ETHERNET GROUP	GROUP STATUS
0	GE_4_1	Enable	Auto Negotiation	User Port #0	GROUP_1	Active
1	GE_4_2	Disable	Auto Negotiation	User Port #1	None	
2	GE_4_3	Disable	Auto Negotiation	User Port #2	None	
3	GE_4_4	Disable	Auto Negotiation	User Port #3	None	
4	FE_5_1	Disable	Auto Negotiation	User Port #4	None	

- **SIP Interface IP-PBX:**
  - SIP signaling interface port 5050, protocol TCP
  - RTP port range start 7000
  - Number of media legs 50
- **SIP Interface ITSP:**
  - SIP signaling interface port 5060, protocol UDP
  - RTP port range start 8000
  - Number of media legs 50

# Configuring Media Realms



audiocodes

SETUP MONITOR TROUBLESHOOT Save Reset Actions ▾ Admin ▾

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

TOPLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (1)
- Media Realms (2)**
- Proxy Sets (1)
- IP Groups (1)

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

Media Realms (2)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MR_IP-PBX	Voice	7000	50	7499	No
1	MR_ITSP	Voice	8000	50	8499	No

#0[MR\_IP-PBX]

Edit

GENERAL

Name	MR_IP-PBX
Topology Location	Down
IPv4 Interface Name	# [Voice]
Port Range Start	7000
Number Of Media Ses...	50
Port Range End	7499
Default Media Realm	No

QUALITY OF EXPERIENCE

QoE Profile	# [-]	View
Bandwidth Profile	# [-]	View

227

# Configure SIP Interface Table

SIP Interfaces (2)

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	IP-PBX	DefaultSRD (# [DefaultSRD])	Voice	SBC	0	5050	0	No encapsulation	MR_IP-PBX
1	ITSP	DefaultSRD (# [DefaultSRD])	Voice	SBC	5060	0	0	No encapsulation	MR_ITSP

#0[IP-PBX] # [DefaultSRD]

GENERAL

Name	• IP-PBX	←
Topology Location	Down	
Network Interface	• # [Voice]	←
Application Type	• SBC	←
UDP Port	• 0	
TCP Port	• 5050	←
TLS Port	• 0	

MEDIA

Media Realm	• # [MR_IP-PBX]	←
Direct Media	Disable	

SECURITY

TLS Context Name	• # [default]	View
TLS Mutual Authentic...		
Message Policy	• # [-]	View

Save    Reset    Actions ▾    Admin ▾

TOPLOGY VIEW

CORE ENTITIES

SRDs (1)

SIP Interfaces (2)

Media Realms (2)

Proxy Sets (3)

IP Groups (3)

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

# Define Proxy Set IP-PBX

audiocodes

SETUP MONITOR TROUBLESHOOT

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions Admin

SRD All

TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (3)**
- IP Groups (3)

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

Proxy Sets (3) .

+ New Edit | Delete

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	--	IP-PBX	60		Disable
1	IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Disable
2	ITSP	DefaultSRD (#0)	--	ITSP	60	Homing	Enable

#1[IP-PBX] # [DefaultSRD] Edit

**GENERAL**

Name	• IP-PBX	<span style="color: blue; font-size: 2em;">←</span>
Gateway IPv4 SIP Interf...	# [-]	<span style="color: blue; font-size: 0.8em;">View</span>
SBC IPv4 SIP Interface	• # [IP-PBX]	<span style="color: blue; font-size: 0.8em;">View</span>
TLS Context Name	# [-]	<span style="color: blue; font-size: 0.8em;">View</span>

**REDUNDANCY**

Redundancy Mode	Disable
Proxy Hot Swap	Disable
Proxy Load Balancing ...	Disable
Min. Active Servers for...	1

**KEEP ALIVE**

Proxy Keep-Alive	• Using OPTIONS	<span style="color: blue; font-size: 0.8em;">←</span>
Proxy Keep-Alive Time [...]	60	<span style="color: blue; font-size: 0.8em;">←</span>
Keep-Alive Failure Resp...		
Success Detection Retri...	1	
Success Detection Inter...	10	
Failure Detection Retra...	-1	

**ADVANCED**

Classification Input	IP Address only
DNS Resolve Method	

**PROXY ADDRESS**

TYPE		
10.15.11.2:5050	TCP	<span style="color: blue; font-size: 2em;">←</span>

# Define Proxy Set ITSP

audiocodes

SETUP MONITOR TROUBLESHOOT

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions Admin

SRD All

TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (3)**
- IP Groups (3)

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

Proxy Sets (3)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	--	IP-PBX	60		Disable
1	IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Disable
2	ITSP	DefaultSRD (#0)	--	ITSP	60	Homing	Enable

#2[ITSP] # [DefaultSRD]

Edit

GENERAL

Name: ITSP

Gateway IPv4 SIP Interface: # [-]

SBC IPv4 SIP Interface: # [ITSP]

TLS Context Name: # [-]

REDUNDANCY

Redundancy Mode: Homing

Proxy Hot Swap: Enable

Proxy Load Balancing: Round Robin

Min. Active Servers for...: 1

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time: 60

Keep-Alive Failure Response:

Success Detection Retries: 1

Success Detection Interval: 10

Failure Detection Retries: -1

ADVANCED

Classification Input: IP Address only

DNS Resolve Method:

PROXY ADDRESS TYPE

200.100.10.5:5060 UDP

200.100.10.1:5060 UDP

# Define IP Group 1 (IP-PBX)

audiocodes

SETUP MONITOR TROUBLESHOOT Save Reset Actions ▾ Admin ▾

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

TOPLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (3)
- IP Groups (3)**

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

IP Groups (3) .

+ New Edit | Delete

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATI SET	OUTBOUND MESSAGE MANIPULATI SET
0	Default_IPG	DefaultSRD	Server	Not Configure	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	DefaultSRD	Server	Not Configure	IP-PBX	--	--		Enable	-1	-1
2	ITSP	DefaultSRD	Server	Not Configure	ITSP	--	--		Enable	-1	-1

#1[IP-PBX] # [DefaultSRD]

Edit

GENERAL

Name	• IP-PBX	←
Topology Location	Down	
Type	Server	
Proxy Set	• # [IP-PBX]	←
IP Profile	# [-]	<a href="#">View</a>
Media Realm	# [-]	<a href="#">View</a>

QUALITY OF EXPERIENCE

QoE Profile	# [-]	<a href="#">View</a>
Bandwidth Profile	# [-]	<a href="#">View</a>

MESSAGE MANIPULATION

Inbound Message Ma...	-1
Outbound Message ...	-1

# Define IP Group 2 (ITSP)

audiocodes

SETUP MONITOR TROUBLESHOOT Save Reset Actions ▾ Admin ▾

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (3)
- IP Groups (3)**

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

IP Groups (3) .

+ New Edit | # [DefaultSRD]

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATISET	OUTBOUND MESSAGE MANIPULATISET
0	Default_IPG	DefaultSRD	Server	Not Configure	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	DefaultSRD	Server	Not Configure	IP-PBX	--	--		Enable	-1	-1
2	ITSP	DefaultSRD	Server	Not Configure	ITSP	--	--		Enable	-1	-1

#2[ITSP] # [DefaultSRD]

Edit

GENERAL

Name	• ITSP	
Topology Location	• Up	
Type	Server	
Proxy Set	• # [ITSP]	
IP Profile	# [-]	<a href="#">View</a>
Media Realm	# [-]	<a href="#">View</a>

QUALITY OF EXPERIENCE

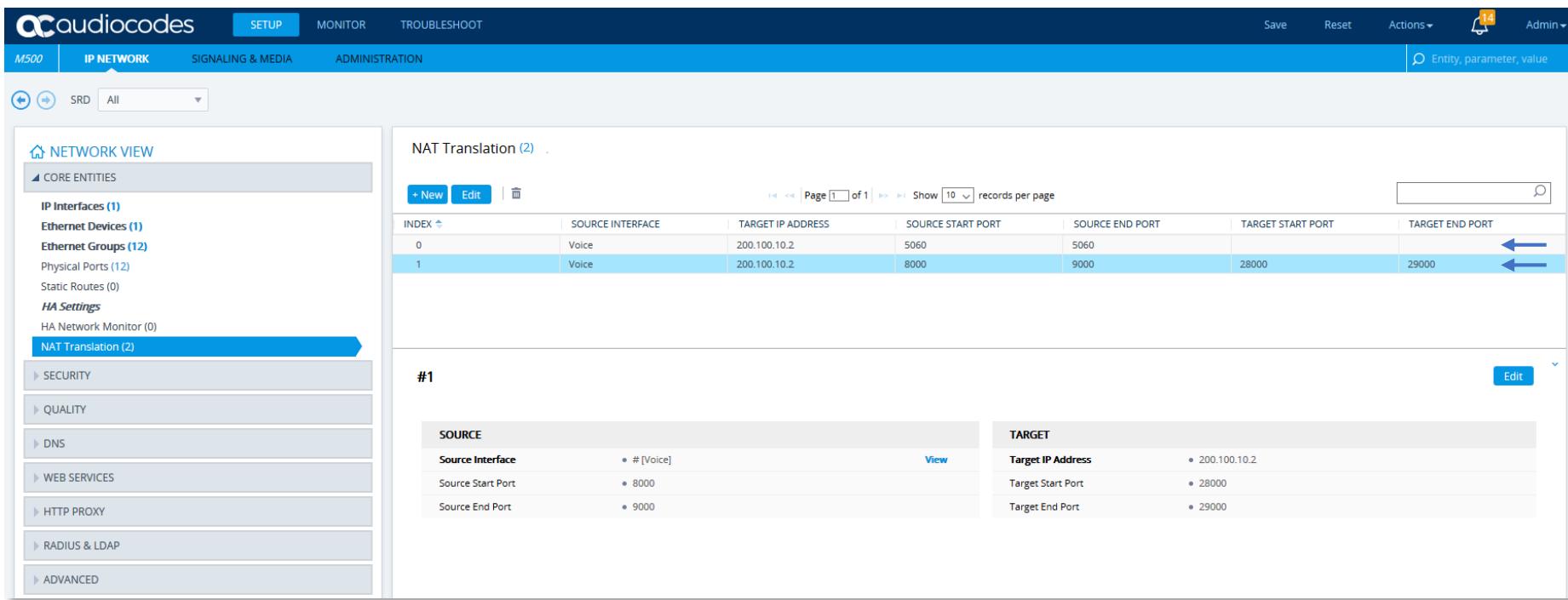
QoE Profile	# [-]	<a href="#">View</a>
Bandwidth Profile	# [-]	<a href="#">View</a>

MESSAGE MANIPULATION

Inbound Message Ma...	-1
Outbound Message ...	-1

# Define NAT Translation

- NAT rules for translating source IP addresses per VoIP interface:
  - SIP Control
  - Media Traffic



The screenshot shows the audiocodes M500 web interface with the following details:

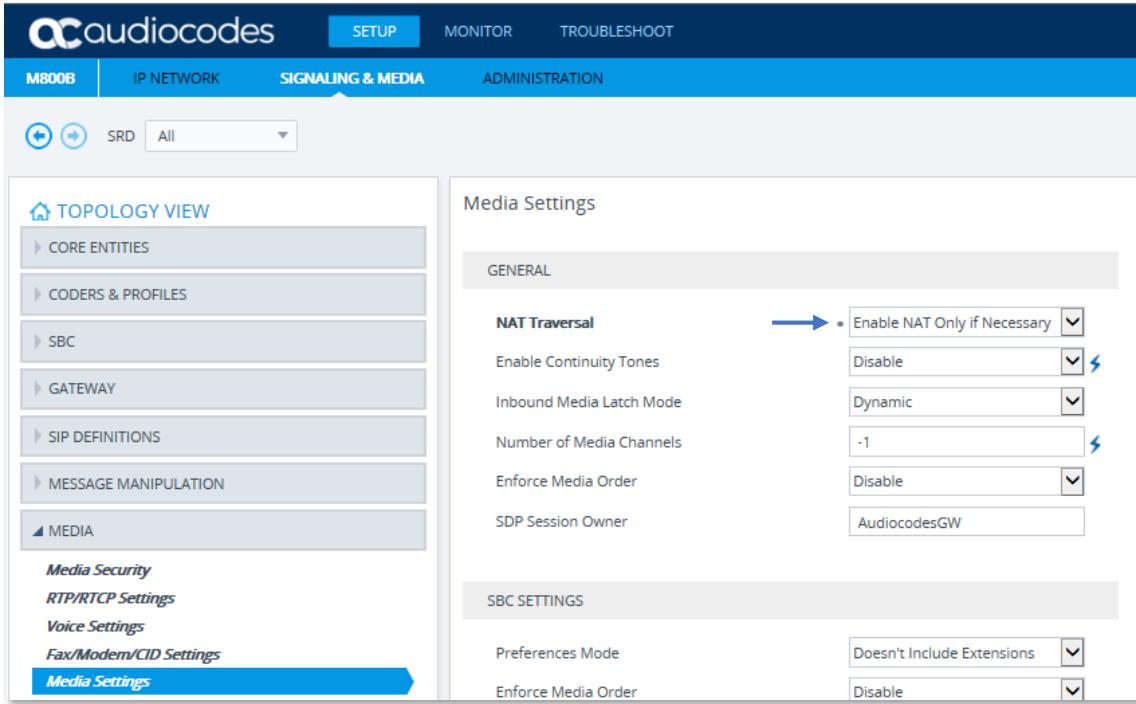
- Header:** audiocodes M500, SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, Admin.
- Left Sidebar:** NETWORK VIEW, CORE ENTITIES, IP Interfaces (1), Ethernet Devices (1), Ethernet Groups (12), Physical Ports (12), Static Routes (0), HA Settings, HA Network Monitor (0), NAT Translation (2) (selected).
- Top Bar:** IP NETWORK (selected), SIGNALING & MEDIA, ADMINISTRATION, Entity, parameter, value.
- Table:** NAT Translation (2).

INDEX	SOURCE INTERFACE	TARGET IP ADDRESS	SOURCE START PORT	SOURCE END PORT	TARGET START PORT	TARGET END PORT
0	Voice	200.100.10.2	5060	5060		
1	Voice	200.100.10.2	8000	9000	28000	29000
- Detail View:** #1, Edit.

SOURCE		TARGET	
Source Interface	# [Voice]	Target IP Address	200.100.10.2
Source Start Port	8000	Target Start Port	28000
Source End Port	9000	Target End Port	29000

# First Incoming Packet Mechanism

- The device identifies whether the UA is located behind NAT by comparing the source IP address of the first received media packet with the IP address and UDP port of the first received SIP message (INVITE) when the SIP session was started
- To enable the option via Web GUI:



The screenshot shows the audiocodes M800B Web GUI interface. The top navigation bar includes the audiocodes logo, SETUP, MONITOR, and TROUBLESHOOT buttons. Below the bar, there are tabs for M800B, IP NETWORK, SIGNALING & MEDIA (which is selected), and ADMINISTRATION. On the left, a sidebar menu lists TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, SIP DEFINITIONS, MESSAGE MANIPULATION, and MEDIA. Under MEDIA, sub-options include Media Security, RTP/RTCP Settings, Voice Settings, Fax/Modem/CID Settings, and Media Settings (which is highlighted with a blue arrow). The main content area is titled "Media Settings" and contains two sections: GENERAL and SBC SETTINGS. In the GENERAL section, under NAT Traversal, there is a dropdown menu with an arrow pointing to "Enable NAT Only if Necessary". Other settings in this section include Enable Continuity Tones (Disable/Dynamic), Inbound Media Latch Mode (Dynamic/-1), Number of Media Channels (Disable/AudiocodesGW), Enforce Media Order (Disable), and SDP Session Owner (AudiocodesGW). The SBC SETTINGS section includes Preferences Mode (Doesn't Include Extensions) and Enforce Media Order (Disable).

# Configuring IP-to-IP Call Routing Rules



SERIALIZED BY: [object Object]

8 Admin ▾

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

TOPOLOGY VIEW

CORE ENTITIES

CODERS & PROFILES

SBC

Classification (1)

Routing Policies (1)

Routing (1)

IP-to-IP Routing (3)

Alternative Reasons (1)

IP Group Set (0)

Manipulation

SBC General Settings

Call Admission Control Profile (0)

Malicious Signature (12)

External Media Source (0)

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

SETUP MONITOR TROUBLESHOOT

Save Reset Actions ▾

IP-to-IP Routing (3)

+ New Edit Insert Page 1 of 1 Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Options	Default_SBCRouting	Route Row	Any	OPTIONS	*	*	Internal	--	--	
1	IP-PBX to ITSP	Default_SBCRouting	Route Row	IP-PBX	All	*	*	IP Group	ITSP	--	
2	ITSP to IP-PBX	Default_SBCRouting	Route Row	ITSP	All	*	*	IP Group	IP-PBX	--	

#0[Options] # [Default\_SBCRoutingPolicy]

GENERAL

Name: Options

Alternative Route Options: Route Row

MATCH

Source IP Group: # [Any]

Request Type: OPTIONS

Source Username Pattern: \*

Source Host: \*

Source Tag: \*

Destination Username Pattern: \*

Destination Host: \*

Destination Tag: \*

Message Condition: # [-]

Call Trigger: Any

ReRoute IP Group: # [Any]

ACTION

Destination Type: Internal

Destination IP Group: # [-]

Destination SIP Interface: # [-]

Destination Address:

Destination Port: 0

Destination Transport Type:

IP Group Set: # [-]

Call Setup Rules Set ID: -1

Group Policy: Sequential

Cost Group: # [-]

Routing Tag Name: default

Internal Action: Reply(Response='200')

View View

235

# Define Classification Rules (Optional)

SERIALIZED BY: [object Object]

audiocodes

SETUP MONITOR TROUBLESHOOT

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

TOPLOGY VIEW

- CORE ENTITIES
- CODERS & PROFILES
- SBC
- Classification (2)**
  - Routing
  - Manipulation
  - SBC General Settings
  - Call Admission Control Profile (0)
  - Malicious Signature (12)
  - External Media Source (0)
- GATEWAY
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- MEDIA
- INTRUSION DETECTION
- SIP RECORDING

Classification (2) .

+ New Edit Insert ↑ ↓ | Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	SOURCE SIP INTERFACE	SOURCE USERNAME PATTERN	SOURCE HOST	DESTINATION USERNAME PATTERN	DESTINATION HOST	ACTION TYPE	SOURCE IP GROUP
0	ITSP	DefaultSRD (#0)	ITSP	*	ITSP.com	*	*	Allow	ITSP
1	ITSP2	DefaultSRD (#0)	ITSP	*	ITSP.com	*	*	Allow	ITSP

#0[ITSP] # [DefaultSRD]

Edit

**MATCH**

Name	• ITSP	←
Source SIP Interface	• # [ITSP]	View
Source IP Address	• 200.100.10.5	←
Source Transport Type	• UDP	←
Source Port	• 5060	←
Source Username Pattern	*	
Source Host	• ITSP.com	←
Destination Username Pattern	*	
Destination Host	*	
Message Condition	• # [ITSP]	←

**ACTION**

Action Type	Allow	←
Destination Routing Policy	# [-]	View
Source IP Group	• # [ITSP]	←
IP Profile	# [-]	View

# Message Conditions (Optional)

audiocodes

SETUP MONITOR TROUBLESHOOT

M500 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions ▾ Entity, parameter, value Admin ▾

SRD All

TOPLOGY VIEW

- CORE ENTITIES
- CODERS & PROFILES
- SBC
- GATEWAY
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- Message Manipulations (0)
- Message Conditions (1) **Selected**
- Message Policies (1)
- Pre-Parsing Manipulation Sets (0)

MEDIA

INTRUSION DETECTION

SIP RECORDING

Message Conditions (1) .

+ New Edit | Delete

Page 1 of 1 Show 10 records per page

INDEX	NAME	CONDITION
0	ITSP	Header.User-Agent==‘ITSP Server name and version’

#0[ITSP] Edit

**GENERAL**

Name	• ITSP
Condition	• Header.User-Agent==‘ITSP Server name and version’

Two blue arrows point to the 'Condition' row in the GENERAL table.

What of the following statements is **false**:

- A. The SBC can be operational as Stateful Proxy Server
- B. The SBC can be operational as B2BUA
- C. The SBC can be operational as Stateful Proxy Server and B2BUA at the same time
- D. None of the above

What of the following statements is **false**:

- A. Destination IP address can be configured in the IP2IP routing table
- B. Destination IP address can be configured in the proxy set child table
- C. Destination port is configured by default
- D. The default destination IP address can't be override



**What of the following statements is **false**:**

- A. Media Realm Extensions let you configure a Media Realm with different port ranges
- B. Media Realm Extensions let you configure a Media Realm with different interfaces
- C. Up to 4 Media Realm Extensions can be configured
- D. Media Realm is distributed across multiple interfaces

**Media Realm is:**

- A. Bulk of TCP ports for the signaling
- B. Bulk of TCP ports for the Media
- C. Bulk of UDP ports for the Media
- D. Bulk of UDP ports for the signaling





Lesson 8

SBC Wizard



- User-friendly online tool designed to get AudioCodes Mediant SBC up and running quickly and easily
- Step-by-step setup process, presenting the configuration options in a clear way
- Eliminates configuration errors and troubleshooting
- Easy to install Windows-based application
- Includes predefined configurations for a wide range SBC deployments (SIP trunk, hosting etc.) with a variety of service providers and IP-PBXs
- Automatic software updates
- Built-in online help
- Available as web built-in and stand-alone application

# Configuration Wizard

audiocodes

SETUP MONITOR TROUBLESHOOT

M800 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

 TIME & DATE

WEB & CLI

SNMP

MAINTENANCE

Configuration File

Auxiliary Files

Maintenance Actions

License Key

Software Upgrade

High Availability Maintenance

Configuration Wizard

TIME & DATE

LOCAL TIME

Local Time Year Month Day Hours Minutes Seconds  
2018 3 11 10 31 6

NTP SERVER

Primary NTP Server Address (IP or FQDN) • 10.15.45.80

Secondary NTP Server Address (IP or FQDN)

NTP Update Interval Hours: 24 Minutes: 0

NTP Authentication Key Identifier 0

NTP Authentication Secret Key

WELCOME

GENERAL SETUP

SYSTEM

INTERFACES

IP-PBX

SIP TRUNK

NUMBER MANIPULATION

SUMMARY

FINISH

INTRODUCTION

USAGE STATISTICS

This wizard will assist you with initial device configuration. You will be asked to select configuration template and network topology. Once done, you will be prompted to fill a short questionnaire to describe your setup details. The wizard will conclude by generating new device configuration based on all provided input.

Template pack version: 2.26

WARNING: Please note that when configuration wizard is completed it will overwrite all of the existing device configuration

Report usage statistics

End Customer → New

Country →  United Kingdom

Integrator → Test

Installer → John

Back Next Cancel



# SIP Trunk Configuration

WELCOME

GENERAL SETUP

SYSTEM

INTERFACES

IP-PBX

SIP TRUNK

NUMBER MANIPULATION

SUMMARY

FINISH

Choose application type and configuration

PRE-DEFINED TEMPLATES

ARCHITECTURE DIAGRAM

- SIP Trunk (IP-PBX with ITSP)
- SIP Normalization (two IP-PBX's)
- Hosted IP-PBX (IP-PBX with Users)
- Remote users (IP-PBX with remote Users)

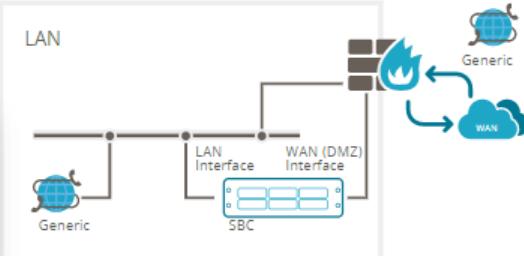
Select an IP-PBX

Alcatel-Lucent OXE

Generic SIP Trunk

- 8x8 SIP Trunk
- AAPT SIP Trunk
- AireSpring SIP Trunk
- Alphalink SIP Trunk
- Alteva SIP Trunk
- Amcom SIP Trunk

AT&T Enhanced IP Flexible Reach



Back < Next >

Cancel

# System Parameters

WELCOME

GENERAL SETUP

SYSTEM

INTERFACES

IP-PBX

SIP TRUNK

NUMBER MANIPULATION

SUMMARY

FINISH

## Configure system parameters

### MANAGEMENT

Web Interface

Enable



CLI Interface

Enable Syslog



Syslog IP

### TIME AND DATE

Time Zone

Primary NTP Server

Secondary NTP Server



Back

Next

Cancel

WELCOME

GENERAL SETUP

SYSTEM

**INTERFACES**

IP-PBX

SIP TRUNK

NUMBER MANIPULATION

SUMMARY

FINISH

## Configure interfaces

LAN INTERFACE

Physical Port: GROUP\_1 (GE\_4\_1,GE\_4\_2)

VLAN Tagging:

VLAN ID: Untagged

IP Address: 10.15.18.1

Subnet Mask: 255.255.0.0

Default Gateway: 10.15.0.1

NAT Public IP: 0.0.0.0

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

MANAGEMENT INTERFACE

OAM Interface: LAN

?

Back Next Cancel



# IP-PBX Parameters

WELCOME

GENERAL SETUP

SYSTEM

INTERFACES

IP-PBX

SIP TRUNK

NUMBER MANIPULATION

SUMMARY

FINISH

## NETWORK INTERFACE

Network Type

LAN



## IP-PBX

Address

10.15.10.2

Backup Address

0.0.0.0 or domain.com

SIP Domain

0.0.0.0 or domain.com

Keep Alive



## SIP INTERFACE

Transport Type

UDP

Destination Port

5060

Listening Port

5060

## MEDIA PORTS (REALM)

Media Protocol

RTP

Base Port

6000

Number Of Sessions

100



Back

Next

Cancel

# ITSP Parameters

WELCOME

GENERAL SETUP

SYSTEM

INTERFACES

IP-PBX

**SIP TRUNK**

NUMBER MANIPULATION

SUMMARY

FINISH

**NETWORK INTERFACE**

Network Type

**NAT**

NAT Public IP

**SIP TRUNK**

Address

Backup Address

SIP Domain

Keep Alive

**SIP INTERFACE**

Transport Type

Destination Port

Listening Port

**SIP ACCOUNT**

Account Type

Trunk Main Line

Username

**MEDIA PORTS (REALM)**

Media Protocol

Base Port

Number Of Sessions



**Back** **Next** **Cancel**

# Number Manipulation

WELCOME

GENERAL SETUP

SYSTEM

INTERFACES

IP-PBX

SIP TRUNK

NUMBER MANIPULATION

SUMMARY

FINISH

## Number Manipulation configuration

### OUTBOUND CALLS (IP-PBX → SIP TRUNK)

Destination Number  
Manipulation



Prefix

Remove

Add

Source Number  
Manipulation



### ADVANCED ROUTING MANAGER

Use ARM for call routing

### INBOUND CALLS (SIP TRUNK → IP-PBX)

Destination Number  
Manipulation



Prefix

Remove

Add

Source Number  
Manipulation



Back

Next

Cancel

WELCOME

GENERAL SETUP

SYSTEM

INTERFACES

IP-PBX

SIP TRUNK

NUMBER MANIPULATION

**SUMMARY**

FINISH

## Conclusion & INI

Configuration Summary

INI file

**Welcome**  
Report usage statistics: Yes  
End Customer: ss  
Country: DZ  
Integrator: sss  
Installer: sss

**General Setup**  
Network setup: One port: LAN  
Application: ITSP  
IP-PBX: Alcatel-Lucent OXE  
SIP-Trunk: AAPT SIP Trunk

**System**  
Web Interface: HTTP  
CLI Interface: SSH  
Syslog IP: 0.0.0  
Primary NTP Server: 10.1.1.11

**Interfaces**  
Physical Port: GROUP\_1 (GE\_4\_1,GE\_4\_2)  
OAM Interface: LAN  
VLAN Tagging: No  
IP Address: 10.15.18.1  
Subnet Mask: 255.255.0.0  
Default Gateway: 10.15.0.1

**IP-PBX**  
Media Protocol: RTP

Back

Next

Save INI file

Cancel

WELCOME

GENERAL SETUP

SYSTEM

INTERFACES

IP-PBX

SIP TRUNK

NUMBER MANIPULATION

SUMMARY

**FINISH**

## Congratulations!

You have successfully completed the SBC Configuration wizard.

Click "Apply & Reset" button to activate the new configuration. Note that device will be restarted and it may take up to 4 minutes before it completes activation.

The generated configuration file is a good "starting point" that enables successful establishment of basic calls.

For complete device configuration you may need to configure additional functionality.

For example, you may need to add security configuration (e.g. Firewalls, IDS) to ensure that SBC is protected from malicious user activity and DoS attacks.

Refer to the User Manual for more information.

WARNING: Applying this configuration will overwrite all of the existing device configuration.

Apply & Reset



Back

Next

Save INI file

Cancel



## Lesson 9

# Debugging Tools



- Understanding the problem
  - What are the expected results?
  - What are the actual results?
- Collecting data
  - Use the relevant data collection tools for problem investigation

- When reporting a problem, provide AudioCodes Support with:
  - Accurate, clear and detailed problem description
  - Test setup (network diagram, call direction, etc.)
  - Uploaded ini file
  - Syslog trace (without missing messages)
  - Unfiltered Wireshark
  - Advanced (per request):
    - PSTN traces for PSTN problems
    - DSP traces for problems related to voice quality, Modem/Fax, DTMF detection, etc.

# What is Syslog?

- Standard for forwarding log messages in an IP network
- A Syslog server is used to remotely record logging information
- Syslog information sent by the gateway is a collection of error, warning and system messages that record every internal operation of the gateway
- Syslog messages are marked with a sequential number
- A Syslog server usually adds the time the message was received and the source IP address

# Syslog Message Format - Example

```
08:59:10.239 10.15.11.1 local0.notice [S=1974] [SID=a929c9:21:24] ( lgr_sbc)( 1773) Classification Succeeded - Source IP Group #2 (ITSP), - Dest Routing Policy #0
08:59:10.239 10.15.11.1 local0.notice [S=1975] [SID=a929c9:21:24] ( lgr_flow)( 1774) (#3091)SBCRoutesIterator::Change State From: InitialCSRRouting To : InitialRouting
08:59:10.240 10.15.11.1 local0.notice [S=1976] [SID=a929c9:21:24] ( lgr_flow)( 1775) (#3091)SBCRoutesIterator::Change State From: InitialRouting To : AlternativeRouting
08:59:10.241 10.15.11.1 syslog.error 4 packets missing
08:59:10.241 10.15.11.1 local0.notice [S=1981] [SID=a929c9:21:24] ( media_service)( 1780) ServicesMngr: Allocate SBC leg. current active: 1 and max is: 120
08:59:10.242 10.15.11.1 local0.notice [S=1982] [SID=a929c9:21:24] ( lgr_flow)( 1781) (#3091)SBCRoutesIterator::Next route found: Rule #1, Route by: IPGroup , IP Group ID: 1 (SfB), Live:True
08:59:10.242 10.15.11.1 local0.notice [S=1983] [SID=a929c9:21:24] ( lgr_sbc)( 1782) Routing Succeeded -IP2IPRouting Rule #1
```

Timestamp and IP Address

Message Sequence Number  
In this example 4 messages were lost

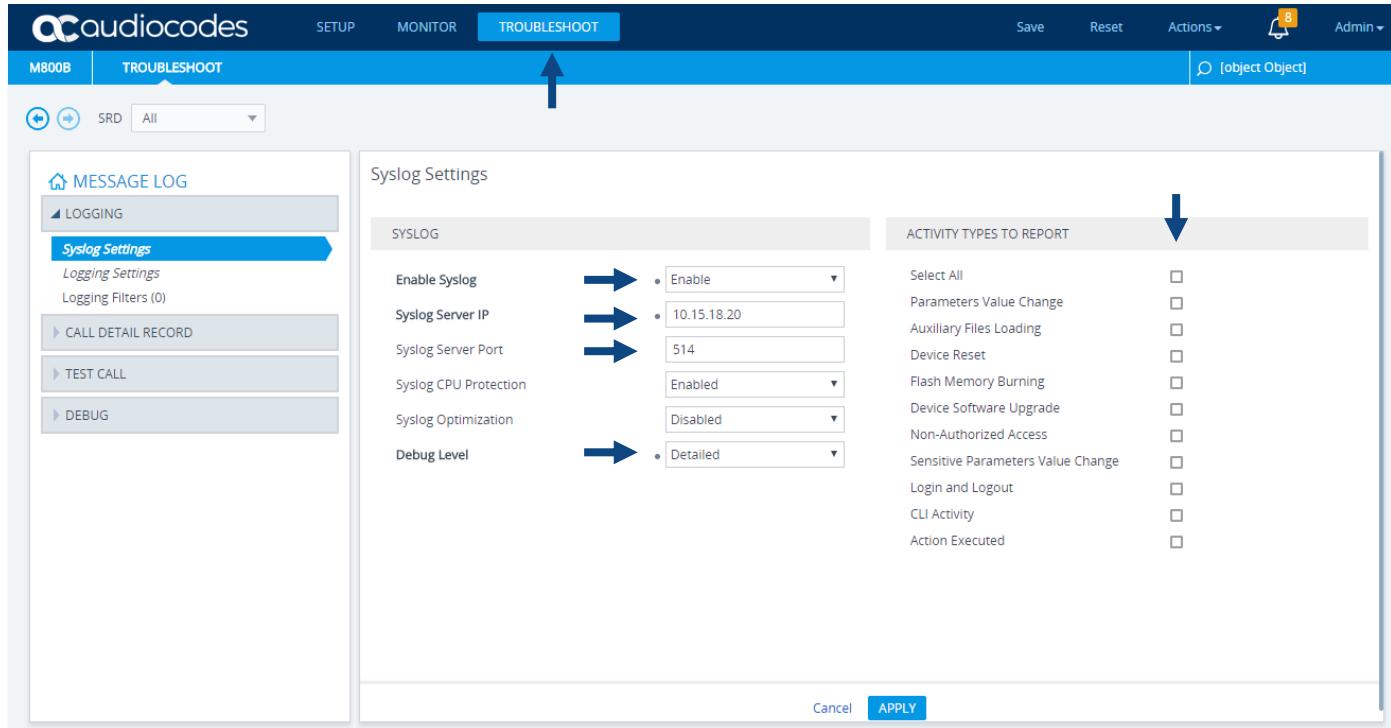
Type of Message

Unique SIP call session and device identifier, SID =  
<last 6 characters of device's MAC address>  
<number of times device has reset>  
<unique SID counter indicating the call session (increments consecutively for each new session; resets to 1 after a device reset)>  
**SID=47ecef:94:69**

- **Syslog generates the following types of messages:**
  - **error:** Indicates that a problem has been identified that requires immediate handling
  - **warning:** Indicates an error that might occur if measures are not taken to prevent it
  - **notice:** Indicates that an unusual event has occurred
  - **info:** Indicates an operational message
  - **debug:** Messages used for debugging

# Enabling Syslog

- Enable Syslog
- Set Syslog Server IP address and port
- Select the Syslog level (recommended 'Detailed')



The screenshot shows the audiocodes M800B web interface. The top navigation bar includes tabs for SETUP, MONITOR, and TROUBLESHOOT, with TROUBLESHOOT currently selected. Below the tabs are buttons for Save, Reset, Actions, and Admin. A search bar and a notifications icon (8) are also present.

The main content area has a left sidebar with links for MESSAGE LOG, LOGGING (selected), Syslog Settings (highlighted with a blue arrow), Logging Filters (0), CALL DETAIL RECORD, TEST CALL, and DEBUG.

The central panel displays the "Syslog Settings" configuration page. It contains several configuration fields:

- Enable Syslog: Set to Enabled (radio button selected).
- Syslog Server IP: Set to 10.15.18.20.
- Syslog Server Port: Set to 514.
- Syslog CPU Protection: Set to Enabled.
- Syslog Optimization: Set to Disabled.
- Debug Level: Set to Detailed.

To the right of these settings is a "ACTIVITY TYPES TO REPORT" section containing a list of 15 activity types, each with a checkbox. Most checkboxes are unselected, except for "Select All".

At the bottom of the page are "Cancel" and "APPLY" buttons.

# Message Log



- View the Syslog messages sent by the device

The screenshot shows the audiocodes M800B web interface with the 'TROUBLESHOOT' tab selected. On the left, a sidebar menu includes 'MESSAGE LOG' (which is active), 'LOGGING', 'CALL DETAIL RECORD', 'TEST CALL', and 'DEBUG'. The main content area is titled 'Message Log' and displays a list of syslog messages. At the bottom of the log area are three buttons: 'Start', 'Stop', and 'Clear'. An upward-pointing arrow is overlaid on the bottom right corner of the interface.

Message Log

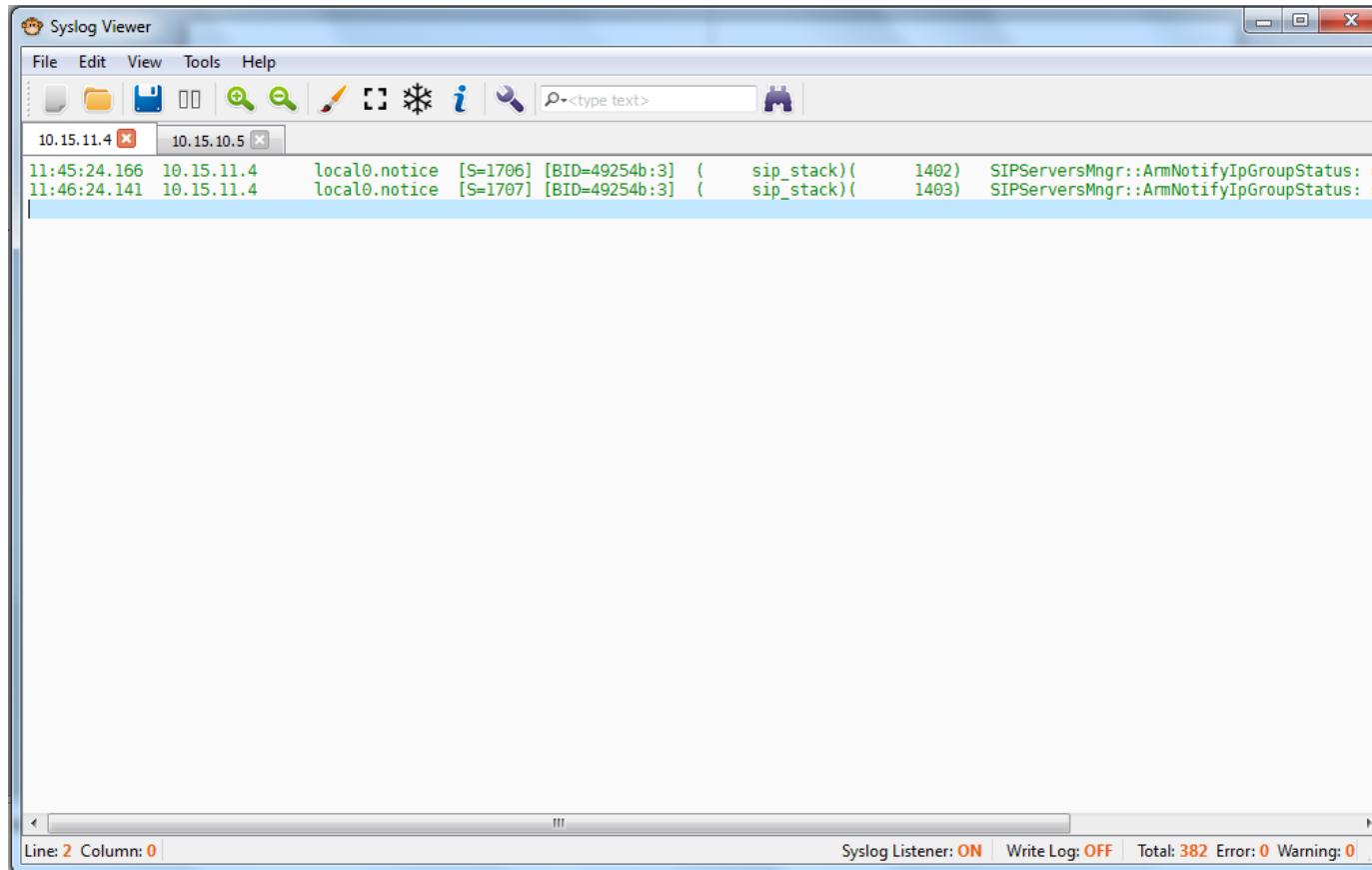
```
Jan 16 16:07:15 local0.notice [S=6520733] [SID=50dcbb2:247:166520] ( 6261280) (#1975)gwSession[Deallocated] [Time:16-01@16:07:14.848]
Jan 16 16:07:15 local0.notice [S=6520732] [SID=50dcbb2:247:166520] ( 6261279) States: (#2523)AcSIPDialog[Deallocated]
(#2523)AcSIPDialog[DialogDisconnected->DialogIdle] [Time:16-01@16:07:14.848]
Jan 16 16:07:15 local0.notice [S=6520731] [SID=50dcbb2:247:166520] ( 6261278) SIPAppMngr::FreeDialogAPI - (#162) [Time:16-01@16:07:14.848]
Jan 16 16:07:15 local0.notice [S=6520730] [SID=50dcbb2:247:166520] ( 6261277) States: (#2523)AcSIPDialog[DialogConnected->DialogDisconnected] [Time:16-01@16:07:14.847]
Jan 16 16:07:15 local0.notice [S=6520729] [SID=50dcbb2:247:166520] ( 6261276) AcSIPDialog(#2523): Handling DIALOG_DISCONNECT_REQ in state DialogConnected [Time:16-01@16:07:14.847]
Jan 16 16:07:14 local0.notice [S=6520728] [SID=50dcbb2:247:166520] ( 6261275) SIPServer::SetOnline - Server: 52.114.132.46:5061 server is now ONLINE [Time:16-01@16:07:14.847]
Jan 16 16:07:14 local0.notice [S=6520727] [SID=50dcbb2:247:166520] ( 6261274) SIPServersMngr::UpdateSetWithOnlineServer - Added server 52.114.132.46 to balancing cycle [Time:16-01@16:07:14.847]
Jan 16 16:07:14 local0.notice [S=6520726] [SID=50dcbb2:247:166520] ( 6261273) States: (#2523)AcSIPDialog[DialogInitiated->DialogConnected] [Time:16-01@16:07:14.847]
Jan 16 16:07:14 local0.notice [S=6520725] [SID=50dcbb2:247:166520] ( 6261272) AcSIPDialog(#2523): Handling 200 OK in state DialogInitiated [Time:16-01@16:07:14.846]
Jan 16 16:07:14 local0.notice [S=6520724] [SID=50dcbb2:247:166520] SIP/2.0 200 OK
FROM: <sip:195.189.192.157>;tag=lc356776830
TO: <sip:195.189.192.157>
CSEQ: 1 OPTIONS
CALL-ID: 1483860605161201916713@int-sbc2.audctrunk.aceducation.info
VIA: SIP/2.0/TLS int-sbc2.audctrunk.aceducation.info:5061;branch=z9hG4bKac1511935915;alias
CONTENT-LENGTH: 0
ALLOW: TINVITE
```

Start Stop Clear

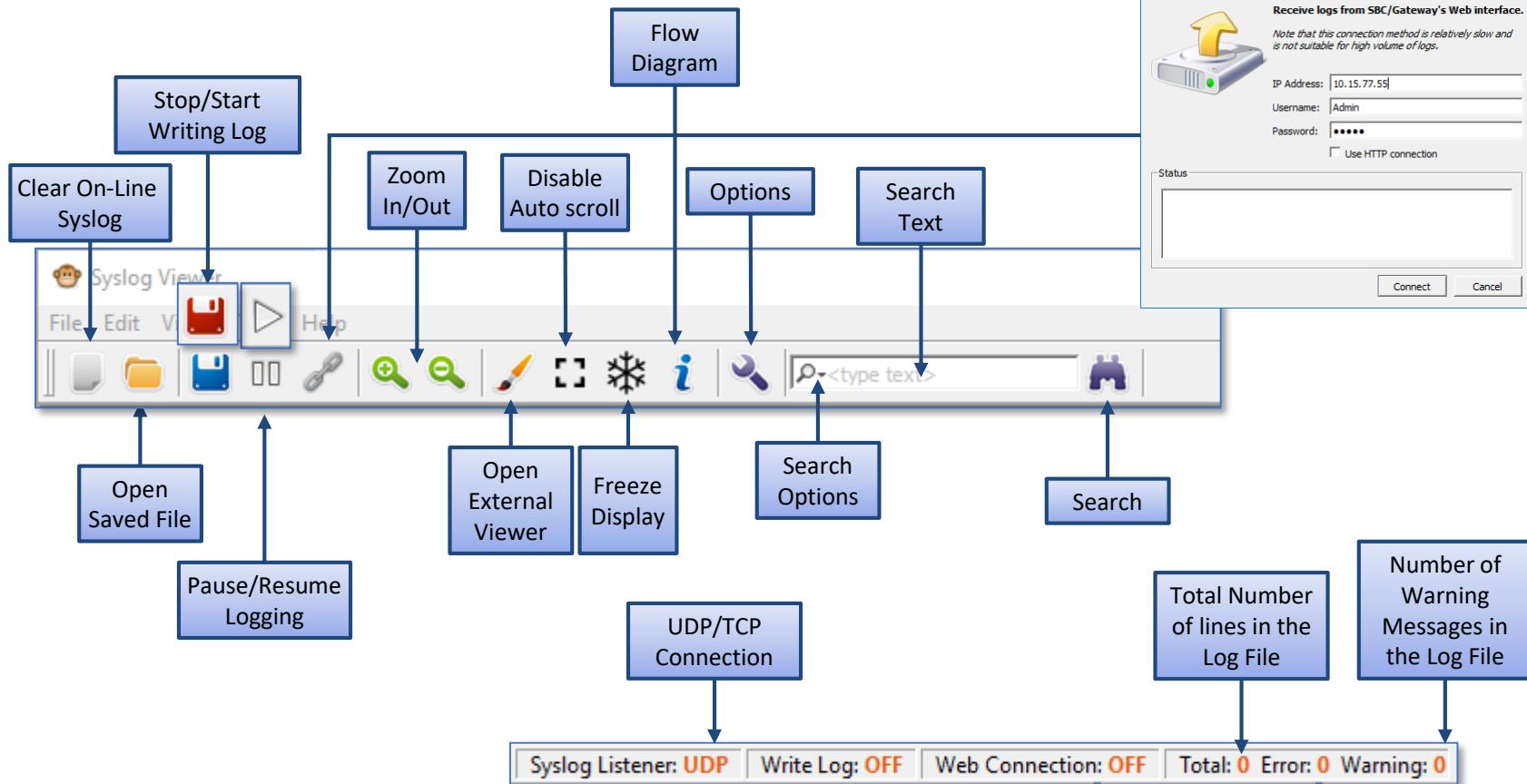
# AudioCodes Syslog Viewer



- A newer Syslog application provided with the student utilities kit



# AudioCodes Syslog Viewer



# AudioCodes Syslog Viewer



- Syslog can be enabled simultaneously in several devices, reporting to the same Syslog Server

Syslog form different IP Addresses can be viewed

The screenshot shows the 'Syslog Viewer' application interface. At the top, there's a menu bar with File, Edit, View, Tools, and Help. Below the menu is a toolbar with icons for file operations like Open, Save, and Print, along with search and filter tools. Two tabs are open: '10.15.77.14' and '10.15.77.55'. The main window displays a list of syslog messages. A blue box highlights the text 'Syslog form different IP Addresses can be viewed'.

Time	IP Address	Facility	Severity	Message
17:10:15.904	10.15.77.14	local0	notice	[S=438] [SID:297606343] (lgr_digitmap_mngr)(23638) #0:Activate DigitMapMngr pattern:[(
17:10:15.905	10.15.77.14	local0	notice	[S=439] [SID:297606343] ( lgr_psbrdif)(23639) ) #0:PSOSBoardInterface::StopPlayTone-(
17:10:15.906	10.15.77.14	local0	notice	[S=440] [SID:297606343] ( lgr_psbrdex)(23640) ) PCIIFChangeChannelParams failed ECCNC
17:10:15.909	10.15.77.14	local0	notice	[S=441] [SID:297606343] ( lgr_psbrdif)(23641) ) Changed ECNlpMode to: 1
17:10:15.910	10.15.77.14	local0	notice	[S=442] [SID:297606343] ( lgr_psbrdif)(23642) ) #0:PSOSBoardInterface::PlayTone - Call
17:10:17.595	10.15.77.14	local0	notice	[S=443] [SID:297606343] ( lgr_psbrdex)(23643) ) recv <- ON HOOK Ch:0
17:10:17.596	10.15.77.14	local0	notice	[S=444] [SID:297606343] ( lgr_flow)(23644) ) #0:ON_HOOK_EV
17:10:17.597	10.15.77.14	local0	notice	[S=445] [SID:297606343] ( lgr_flow)(23645) )   #0:ON_HOOK_EV State:COLLECT_DI
17:10:17.598	10.15.77.14	local0	notice	[S=446] [SID:297606343] ( lgr_psbrdif)(23646) ) #0:PSOSBoardInterface::StopPlayTone-(
17:10:17.598	10.15.77.14	local0	notice	[S=447] [SID:297606343] ( lgr_psbrdex)(23647) ) #0:cpDigitMapHndl_Stop - Stopped (0)
17:10:17.600	10.15.77.14	local0	notice	[S=448] [SID:297606343] (lgr_digitmap_mngr)(23648) ) #0:DigitMapMngr::Deactivated!
17:10:17.601	10.15.77.14	local0	notice	[S=449] [SID:297606343] ( lgr_psbrdif)(23649) ) #0:cpDigitMapHndl_Stop - Stopped (0)
17:10:17.601	10.15.77.14	local0	notice	[S=450] [SID:297606343] ( lgr_psbrdif)(23650) ) #0:CloseChannel: ChannelNum=0
17:10:17.603	10.15.77.14	local0	notice	[S=451] ( lgr_psbrdif)(23651) ) Open channel: IsVoiceOn: 1, IsT38On: 0, IsVbdOn: 0, Is
17:10:17.604	10.15.77.14	local0	notice	[S=452] ( lgr_psbrdif)(23652) ) #0:OpenChannelon Trunk -1 BChannel:0 CID=0 with Voice
17:10:17.604	10.15.77.14	local0	notice	[S=453] ( lgr_psbrdex)(23653) ) #0:OpenChannel VoiceVolume = 0, DTMFVolume = -11, Input
17:10:17.605	10.15.77.14	local0	notice	[S=454] ( lgr_psbrdif)(23654) ) RFC2833RTPPayloadType: Rx=96 Tx=96
17:10:17.606	10.15.77.14	local0	notice	[S=455] ( lgr_psbrdif)(23655) ) OpenChannel, CoderType = 16, Interval = 0, M = 1
17:10:17.606	10.15.77.14	local0	notice	[S=456] ( lgr_psbrdif)(23656) ) ConfigureVbdAndT38:FAXTransportType:1 T38Version:0 Fa:
17:10:17.607	10.15.77.14	local0	notice	[S=457] ( lgr_psbrdif)(23657) ) #0:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=0
17:10:17.608	10.15.77.14	local0	notice	[S=458] ( lgr_psbrdif)(23658) ) #0:FAXTransportType = 1
17:10:17.609	10.15.77.14	local0	notice	[S=459] ( lgr_psbrdex)(23659) ) Detectors: Amd:On=0,Direction=0, Ans:On=0,Direction=0
17:10:17.610	10.15.77.14	local0	notice	[S=460] ( lgr_psbrdif)(23660) ) #0:Channel will be open WITH DSP
17:10:17.613	10.15.77.14	local0	notice	[S=461] [SID:297606343] ( lgr_flow)(23661) ) #0:LOCAL_END_PLAYING_CALL_PROGRESS_TON
17:10:17.614	10.15.77.14	local0	notice	[S=462] [SID:297606343] ( lgr_flow)(23662) )   #0:LOCAL END_PLAYING CALL PRO

Line: 44 Column: 0      Syslog Listener: UDP Write Log: OFF Web Connection: OFF Total: 100 Error: 0 Warning: 0

# AudioCodes Syslog Viewer



- SIP/SDP messages are properly arranged to be easily identified for analysis

Syslog Viewer - [D:\WorkArea\Docs\#Courses\#Training Modules\MS Direct Routing\Lab-related\Lab3-Traces\Teams-to-PSTN-MB-disabled.log]

File Edit View Tools Help

File Explorer Search Filter Options Zoom Text Input

11:45:50.734 10.15.11.1 local0.notice [S=32760] [SID=4bfc38:23:1377] ( 29980) (#4817)gwSession[Allocated]. Handle:2C255788; Global session ID: 6c8df61045e724b3 [Time:31-12@13:35:24.710] 11:45:50.736 10.15.11.1 local0.notice [S=32761] [SID=4bfc38:23:1377] ( 29981) Condition Table matched on condition Index 0 [Time:31-12@13:35:24.710] 11:45:50.736 10.15.11.1 local0.notice [S=32762] [SID=4bfc38:23:1377] ( 29982) Classification Succeeded - Source IP Group #2 (Teams) [Time:31-12@13:35:24.710] 11:45:50.736 10.15.11.1 local0.notice [S=32763] [SID=4bfc38:23:1377] ( 29983) IP2IPInboundManipulation Rule #0 [Time:31-12@13:35:24.711] 11:45:50.738 10.15.11.1 local0.notice [S=32764] [SID=4bfc38:23:1377] ( 29984) SBCRoutingMngr::InboundManipulate: Destination username was manipulated from +1111555: 11:45:50.738 10.15.11.1 local0.notice [S=32765] [SID=4bfc38:23:1377] ( 29985) States: (#109)SBCRoutesIterator[InitialRouting->AlternativeRouting] [Time:31-12@13:35:24.711] 11:45:50.738 10.15.11.1 local0.notice [S=32766] [SID=4bfc38:23:1377] ( 29986) SBC\_ADMIN\_DIALOGS\_EV: (#109)SBCRoutesIterator -> (#-1)SBCAdmissionControlMngr [Time:31-12@13:35:24.711] 11:45:50.739 10.15.11.1 local0.notice [S=32767] [SID=4bfc38:23:1377] ( 29987) CAC: Add SBC Incoming INVITE, IPG 2 (Teams): 1, SRD 0 (DefaultSRD): 1, SipIF 1 (Teams) 11:45:50.739 10.15.11.1 local0.notice [S=32768] [SID=4bfc38:23:1377] ( 29988) ResourceCounter: SBC leg +1 [1/200] [Time:31-12@13:35:24.713] 11:45:50.740 10.15.11.1 local0.notice [S=32769] [SID=4bfc38:23:1377] ( 29989) CAC: Add SBC Outgoing INVITE, IPG 1 (ITSP): 1, SRD 0 (DefaultSRD): 1, SipIF 0 (ITSP): 11:45:50.740 10.15.11.1 local0.notice [S=32770] [SID=4bfc38:23:1377] ( 29990) ResourceCounter: SBC leg +1 [2/200] [Time:31-12@13:35:24.713] 11:45:50.741 10.15.11.1 local0.notice [S=32771] [SID=4bfc38:23:1377] ( 29991) (#109)Route found (2), Route by IPGroup, IP Group 2 -> 1 (Teams -> ITSP) [Time:31-12@13:35:24.713] 11:45:50.742 10.15.11.1 local0.notice [S=32772] [SID=4bfc38:23:1377] ( 29992) --- Incoming SIP Message from 52.114.76.1920 to SIPInterface #1 (Teams) TLS TO:#1 11:45:50.742 10.15.11.1 local0.notice [S=32773] [SID=4bfc38:23:1377] INVITE sip:+11115551201@tr-sbc1.audctrunk.aceducation.info:5061;user=phone;transport=tls SIP/2.0 FROM: Interop1<sip:+11115551005@ip.pstnhub.microsoft.com:5061;user=phone>;tag=7b2f533fcf474222a6: TO: <sip:+11115551201@tr-sbc1.audctrunk.aceducation.info:5061;user=phone> CSEQ: 1 INVITE CALL-ID: 8c44407eb2f75c579cccc065f3d33e12 MAX-FORWARDS: 70 VIA: SIP/2.0/TLS 52.114.76.76:5061;branch=z9hG4bKd14c6339 RECORD-ROUTE: <sip:sip-du-a-eu.pstnhub.microsoft.com:5061;transport=tls;lr> CONTACT: <sip:api-du-a-euwe.pstnhub.microsoft.com:8000;transport=tls;x-i=ac7e7clc-140a-429c-902b-15> CONTENT-LENGTH: 1115 USER-AGENT: Microsoft.PSTNHub.SIPPProxy v.2019.1.24.1 i.EUNO.0 CONTENT-TYPE: application/sdp ALLOW: INVITE ALLOW: ACK ALLOW: OPTIONS ALLOW: CANCEL ALLOW: BYE ALLOW: NOTIFY v=0 o=- 56290 0 IN IP4 127.0.0.1 s=session c=IN IP4 52.114.116.48 b=CT:10000000 t=0 m=audio 53064 RTP/SAVP 104 117 9 103 111 18 0 8 97 101 13 118 c=IN IP4 52.114.116.48 a=rtpc:53065 a=ice-ufrag:Kb7F a=ice-pwd:qrIN9V1ITVbBLcUsVczu5X62

Line: 13 Column: 49

Syslog Listener: OFF Write Log: OFF Web Connection: OFF Total: 1274 Error: 0 Warning: 1

# AudioCodes Syslog Viewer



- The SIP/SDP flow diagram can be viewed and exported

Syslog Viewer - [D:\WorkArea\Docs\#Courses\#Training Modules\MS Direct Routing\Lab-related\Lab3-Traces\Teams-to-PSTN-MB-disabled.log]

File Edit View Tools Help

SIP Flow Diagram - 4bf38:23:1377

11:45:50.734 10.15.11.1 local0.notice [S=32] [60] [SID=4bf38:23:1377] ( 29980) (#4817)gwSession[Allocated]. Handle:2C255788; Global session ID: 6c8df61045e724b3 [Ti...  
11:45:50.736 10.15.11.1 local0.notice [S=32] [61] [SID=4bf38:23:1377] ( 29981) Condition Table matched on condition Index 0 [Time:31-12@13:35:24.710]  
11:45:50.736 10.15.11.1 local0.notice [S=32] [62] [SID=4bf38:23:1377] ( 29982) Classification Succeeded - Source IP Group #2 (Teams) [Time:31-12@13:35:24.710]

11:45:50.736 10.15.11.1 local0.notice [S=32] [63] [SID=4bf38:23:1377] ( 29983) SIP Flow Diagram - 4bf38:23:1377  
11:45:50.736 10.15.11.1 local0.notice [S=32] [64] [SID=4bf38:23:1377] ( 29984)  
11:45:50.738 10.15.11.1 local0.notice [S=32] [65] [SID=4bf38:23:1377] ( 29985)  
11:45:50.738 10.15.11.1 local0.notice [S=32] [66] [SID=4bf38:23:1377] ( 29986)  
11:45:50.739 10.15.11.1 local0.notice [S=32] [67] [SID=4bf38:23:1377] ( 29987)  
11:45:50.739 10.15.11.1 local0.notice [S=32] [68] [SID=4bf38:23:1377] ( 29988)  
11:45:50.740 10.15.11.1 local0.notice [S=32] [69] [SID=4bf38:23:1377] ( 29989)  
11:45:50.740 10.15.11.1 local0.notice [S=32] [70] [SID=4bf38:23:1377] ( 29990)  
11:45:50.741 10.15.11.1 local0.notice [S=32] [71] [SID=4bf38:23:1377] ( 29991)  
11:45:50.742 10.15.11.1 local0.notice [S=32] [72] [SID=4bf38:23:1377] ( 29992)  
11:45:50.742 10.15.11.1 local0.notice [S=32] [73] [SID=4bf38:23:1377] ( 29993) INVITE s  
FROM: In  
TO: <sip:  
CSEQ: 1  
CALL-ID:  
MAX-FORW:  
VIA: SIP  
RECORD-R:  
CONTACT:  
CONTENT-  
USER-AGE:  
CONTENT-  
ALLOW: I  
ALLOW: A  
ALLOW: O  
ALLOW: C  
ALLOW: B  
ALLOW: N  
  
v=0  
o=- 5629  
s=session  
c=IN IP4  
b=CT:100  
t=0 0  
m=audio  
c=IN IP4  
a=rtpc:5  
a=ice-uf  
a=ice-pw

SIP Flow Diagram

```
graph TD; S1[52.114.76.76] -- "INVITE (SDP)" --> S2[Device]; S2 -- "100 Trying" --> S3[10.15.10.5]; S3 -- "INVITE (SDP)" --> S4[Device]; S4 -- "100 Trying" --> S5[10.15.10.5]; S5 -- "180 Ringing" --> S6[Device]; S6 -- "200 OK (SDP)" --> S7[10.15.10.5]; S7 -- "ACK" --> S8[Device]; S8 -- "ACK" --> S9[10.15.10.5]; S9 -- "INVITE (SDP)" --> S10[Device]; S10 -- "INVITE (SDP)" --> S11[10.15.10.5]; S11 -- "200 OK (SDP)" --> S12[Device]; S12 -- "200 OK (SDP)" --> S13[10.15.10.5]; S13 -- "ACK" --> S14[Device]; S14 -- "ACK" --> S15[10.15.10.5]; S15 -- "BYE" --> S16[Device]; S16 -- "200 OK" --> S17[10.15.10.5]; S17 -- "200 OK" --> S18[Device];
```

11:45:50 11:45:55 11:46:23

# SID Type Time From To Term F  
1 4bf38:23:1377 INVITE 11:45:50 +11115551005@tr-sbc1.audctrunk.aced... NORMAL

<> Prev Find Next >> Export Show calls only Calls: 1 Other: 8  
Message CDR  
Export sessions Export flow diagram

11:45:50.742 .... Incoming SIP Message from 52.114.76.56:5061  
INVITE sip:+11115551201@tr-sbc1.audctrunk.aced... SIP/2.0  
FROM: Interop111<sip:+11115551005@sp.pstnhub.microsoft.com:5061>;user=phone>;tag=7b2f53fc47  
TO: <sip:+11115551201@tr-sbc1.audctrunk.aced...>;user=phone>  
CSEQ: 1 INVITE  
CALL-ID: 8c44407eb2f75c579ccc065f3d33e12  
MAX-FORWARDS: 70  
VIA: SIP/2.0/TLS 52.114.76.56:5061;branch=z9hG4bKd14e6339  
RECORD-ROUTE: <>;sp.du-a.eu.pstnhub.microsoft.com:5061;transport=tls;lr>  
CONTACT: <sip:sp.du-a.eu.pstnhub.microsoft.com:8000;transport=tls;x-ac7e7c1c-140a-429c-902b:  
CONTENT-LENGTH: 111  
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2019.1.24.1.i.EUNO.0  
CONTENT-TYPE: application/sdp  
ALLOW: INVITE  
ALLOW: ACK  
ALLOW: OPTIONS  
ALLOW: CANCEL  
ALLOW: BYE  
ALLOW: NOTIFY  
v=0

# AudioCodes Syslog Viewer



- The SIP/SDP <-> ISDN flow diagram can be viewed

SIP Flow Diagram - [SID:1546847905]

Trunk:0      Device      10.220.33.65

INCOMING\_CALL  
ISDNSendSetupAcknowledge  
ISDNCallProceeding  
INVITE  
100 Trying  
407 Proxy Authentication R...  
ACK  
INVITE  
100 Trying  
180 Ringing  
200 OK  
ACK  
PSTNAnswerCall  
CALL\_CONNECTED  
CALL\_DISCONNECTED  
psPSTNReleaseCall  
CALL\_RELEASED

# SID Time From To

1	1546847905	13:24:21	0049211100001@s1.e1.sp...	0049211100002
2	1546847910	13:24:26	0211100001@s1.e1.sp1.w...	0049211100002@s1....
3	1546847911	13:26:48	0049211100001@s1.e1.sp...	00431101191@s1.e1...
4	1546847913	13:29:15	0049211100001@s1.e1.sp...	00431101191@s1.e1...
5	1546847914	13:38:52	0049211100001@s1.e1.sp...	0049211100002
6	1546847915	13:38:57	0211100001@s1.e1.sp1.w...	0049211100002@s1....
7	1546847923	13:52:57	0049211100001@s1.e1.sp...	0049211100002@s1....
8	1546847925	13:53:02	0211100001@s1.e1.sp1.w...	0049211100002@s1....
9	1546847924	14:15:34	787a78fb877d14d3@s1.e...	787a78fb877d14d3...

13:24:21.366 ---- Incoming Message  
pstn recv <-- INCOMING\_CALL (src:100001 dst:100002 redirect1:  
redirect2:) Trunk:0 Conn:255 BChannel:1 OffhookInd:0 MoreDigits:1  
ReverseCh:0

# AudioCodes Syslog Viewer



- Each arrow on the SIP/SDP flow diagram points to the right place in the trace

Syslog Viewer - [D:\WorkArea\Docs\#Courses\#Training Modules\MS Direct Routing\Lab-related\Lab3-Traces\Teams-to-PSTN-MB-disabled.log]

File Edit View Tools Help

SIP Flow Diagram

Highlighted

11:45:50.734 10.15.11.1 local0.notice [S=32] [60] [SID=4bfc38:23:1377] ( 29980 ) (#4817)gwSession[Allocated]. Handle:2C255788; Global session ID: 6c8df61045e724b3 [Time:31-12@13:35:24.710]  
11:45:50.736 10.15.11.1 local0.notice [S=32] [61] [SID=4bfc38:23:1377] ( 29981 ) Condition Table matched on condition Index 0 [Time:31-12@13:35:24.710]  
- Source IP Group #2 (Teams) [Time:31-12@13:35:24.710]

11:45:50.736 10.15.11.1 local0.notice [S=32] [62] [SID=4bfc38:23:1377] ( 29982 ) C  
11:45:50.736 10.15.11.1 local0.notice [S=32] [63] [SID=4bfc38:23:1377] ( 29983 ) C  
11:45:50.736 10.15.11.1 local0.notice [S=32] [64] [SID=4bfc38:23:1377] ( 29984 ) C  
11:45:50.738 10.15.11.1 local0.notice [S=32] [65] [SID=4bfc38:23:1377] ( 29985 ) C  
11:45:50.738 10.15.11.1 local0.notice [S=32] [66] [SID=4bfc38:23:1377] ( 29986 ) C  
11:45:50.739 10.15.11.1 local0.notice [S=32] [67] [SID=4bfc38:23:1377] ( 29987 ) C  
11:45:50.739 10.15.11.1 local0.notice [S=32] [68] [SID=4bfc38:23:1377] ( 29988 ) C  
11:45:50.740 10.15.11.1 local0.notice [S=32] [69] [SID=4bfc38:23:1377] ( 29989 ) C  
11:45:50.740 10.15.11.1 local0.notice [S=32] [70] [SID=4bfc38:23:1377] ( 29990 ) C  
11:45:50.741 10.15.11.1 local0.notice [S=32] [71] [SID=4bfc38:23:1377] ( 29991 ) C  
11:45:50.742 10.15.11.1 local0.notice [S=32] [72] [SID=4bfc38:23:1377] ( 29992 ) C  
11:45:50.742 10.15.11.1 local0.notice [S=32] [73] [SID=4bfc38:23:1377] ( 29993 ) C

11:45:50 52.114.76.76 Device 10.15.10.5

INVITE (SDP)  
100 Trying  
INVITE (SDP)  
100 Trying  
180 Ringing  
200 OK (SDP)  
200 OK (SDP)  
ACK  
INVITE (SDP)  
INVITE (SDP)  
200 OK (SDP)  
200 OK (SDP)  
ACK  
ACK  
BYE  
200 OK  
200 OK

# SID Type Time From To Term F

1 4bfc38:23:1377 INVITE 11:45:50 +11115551005@tr-sbc1.audctrunk.ac... +11115551201@tr-sbc1.audctrunk.ac... NORMAL

<> Prev Find Next >> Export Show calls only Calls: 1 Other: 8

Message CDR

11:45:50.742 ---- Incoming SIP Message from 52.114.76.76:1920 to SIPInterface #1 (Teams) TLS TO #1  
INVITE sip:+11115551201@tr-sbc1.audctrunk.aceducation.info:5061;user=phone;transport=tls SIP/2.0  
FROM: Interop111<sip:+11115551005@ip.psrbhub.microsoft.com:5061;user=phone>;tag=7b2f533fc4f;  
TO: <sip:+11115551201@tr-sbc1.audctrunk.aceducation.info:5061;user=phone>  
CSEQ: 1 INVITE  
CALL-ID: 8c44407eb2f75c579ccc065f3d33e12  
MAX-FORWARDS: 70  
VIA: SIP/2.0/TLS 52.114.76.76:5061;brANCH=z9Hg4bKd14c6339  
RECORD-ROUTE: <>sip:du-a-eu.psrbhub.microsoft.com:5061;transport=tls;lr>  
CONTACT: <>sip:du-a-eu.ee.psrbhub.microsoft.com:8000;transport=tls;x-ac7e7c1c-140-a429c-902b;  
USER-LENGTH: 111  
USER-AGENT: Microsoft.PSTNHub.SIPPProxy v.2019.1.24.1.i.EUNO.0  
CONTENT-TYPE: application/sdp  
ALLOW: INVITE  
ALLOW: ACK  
ALLOW: OPTIONS  
ALLOW: CANCEL  
ALLOW: BYE  
ALLOW: NOTIFY

v=0  
o=- 5629  
s=session  
c=IN IP4  
b=CT:100  
t=0 0  
m=audio  
c=IN IP4  
a=rtpc:5  
a=ice-uf  
a=ice-pw

Line: 13 Column: 49

# AudioCodes Syslog Viewer



- CDR info

Syslog Viewer - [D:\WorkArea\Docs\#Courses\#Training Modules\MS Direct Routing\Lab-related\Lab3-Traces\Teams-to-PSTN-MB-disabled.log]

File Edit View Tools Help

<type text>

11:45:50.734 10.15.11.1 local0.notice [S=32760] [SID=4bf38:23:1377] (11:45:50.736 10.15.11.1 local0.notice [S=32761] [SID=4bf38:23:1377] (11:45:50.736 10.15.11.1 local0.notice [S=32762] [SID=4bf38:23:1377] (11:45:50.736 10.15.11.1 local0.notice [S=32763] [SID=4bf38:23:1377] (11:45:50.738 10.15.11.1 local0.notice [S=32764] [SID=4bf38:23:1377] (11:45:50.738 10.15.11.1 local0.notice [S=32765] [SID=4bf38:23:1377] (11:45:50.738 10.15.11.1 local0.notice [S=32766] [SID=4bf38:23:1377] (11:45:50.739 10.15.11.1 local0.notice [S=32767] [SID=4bf38:23:1377] (11:45:50.739 10.15.11.1 local0.notice [S=32768] [SID=4bf38:23:1377] (11:45:50.740 10.15.11.1 local0.notice [S=32769] [SID=4bf38:23:1377] (11:45:50.740 10.15.11.1 local0.notice [S=32770] [SID=4bf38:23:1377] (11:45:50.741 10.15.11.1 local0.notice [S=32771] [SID=4bf38:23:1377] (11:45:50.742 10.15.11.1 local0.notice [S=32772] [SID=4bf38:23:1377] (11:45:50.742 10.15.11.1 local0.notice [S=32773] [SID=4bf38:23:1377] INVITE (SDP) FROM: TO: CSEQ: CALL-ID: MAX-FR: VIA: RECORD-ROUTE: CONTACT: CONTENT-TYPE: USER-AGENT: ALLOW: ALLOW: ALLOW: ALLOW: ALLOW: ALLOW: ALLOW: v=0 o=- S=- s=- c=IN b=CT t=0 m=audio c=IN a=rtp a=ice a=ice a=ice

11:45:50 52.114.76.76 Device 10.15.10.5 INVITE (SDP) 100 Trying INVITE (SDP) 100 Trying 180 Ringing 180 Ringing 200 OK (SDP) 200 OK (SDP) ACK ACK INVITE (SDP) INVITE (SDP) 200 OK (SDP) 200 OK (SDP) ACK ACK BYE BYE 200 OK 200 OK

# SID Type Time From To Term F  
1 4bf38:23:1377 INVITE 11:45:50 +11115551005@tr-sbc1.audctrunk.a... +11115551201@tr-sbc1.audctrunk.a... NORMAL\_C

<< Prev Find Next >> Export Show calls only Calls: 1 Other: 8

Message CDR

CALL DETAIL RECORD (CDR)  
Leg: local (2)  
Call ID: 45768921131122018133524@10.15.11.1  
Source URI: +11115551005@elip.pstnhub.microsoft.com  
Dest URI: 11115551201@tr-sbc1.audctrunk.aceduation.info  
Duration: 28 sec  
Term Reason: NORMAL\_CALL\_CLEAR  
Term Side: remote  
Direct Media: no  
Setup Time: 13:35:24.730 UTC Mon Dec 31 2018  
Connect Time: 13:35:29.144 UTC Mon Dec 31 2018  
Release Time: 13:35:57.874 UTC Mon Dec 31 2018  
IP Group: ITSP  
SRD: DefaultSRD  
SIP Interface: ITSP  
Proxy Set: ITSP  
IP Profile: ITSP  
Media Realm: MR-ITSP

Line: 13 Column: 49

# AudioCodes Syslog Viewer



- Extracting Single Call

```
( lgr_psbrdif)( 4822) PS0SBoardInterface::DiscoverLocalWanIPAddress
[SID:1546] Copy Ctrl+C 3) pstn recv <-- INCOMING_CALL (
[SID:1546] Select All Ctrl+A 4) #30:LOCAL_INCOMING_CALL_EV(Tr
[SID:1546] | #30:LOCAL_INCOMING_CA
[SID:1546] 5) pstn send --> ISDNSendSetupAc
[SID:1546] 6) MscmlSignalFeature Allocated
[SID:1546] 7) EndPoint channel# 30 ::Active
[SID:1546] 8) (#20) CALL Allocated.
[SID:1546] 9) | #30:NEW_CALL_EV (send
[SID:1546] 10) | | (#20):NEW_CAL
[SID:1546] Filter CDRs 11) Resource StackSession (#28) A
[SID:1546] 12) | | | (#20):Call ch
[SID:1546] Filter line 13) | | | | (#28)
[SID:1546] Mark line Ctrl+F2 14) | | | | (to 100002)
[SID:1546] 15) | | | | #30:SETUP_EV (send)
[SID:1546847905] ( lgr_flow)( 4836) |
```

FILTER#1 X						
192.168.0.1	local0.notice	[S=5114]	[SID:1546847905]	( lgr_psbrdex)(	4823)	pstn recv <-- INCOMING_CALL (src:100001
192.168.0.1	local0.notice	[S=5115]	[SID:1546847905]	( lgr_flow)(	4824)	#30:LOCAL_INCOMING_CALL_EV(Trunk:0 Conn:
192.168.0.1	local0.notice	[S=5116]	[SID:1546847905]	( lgr_flow)(	4825)	#30:LOCAL_INCOMING_CALL_EV State
192.168.0.1	local0.notice	[S=5117]	[SID:1546847905]	( lgr_psbrdif)(	4826)	pstn send --> ISDNSendSetupAcknowledge()
192.168.0.1	local0.notice	[S=5118]	[SID:1546847905]	( media_service)(	4827)	MscmlSignalFeature Allocated ResourceID:
192.168.0.1	local0.notice	[S=5119]	[SID:1546847905]	( lgr_flow)(	4828)	EndPoint channel# 30 ::Active DSP Channe
192.168.0.1	local0.notice	[S=5120]	[SID:1546847905]	( lgr_call)(	4829)	#(20) CALL Allocated.
192.168.0.1	local0.notice	[S=5121]	[SID:1546847905]	( lgr_flow)(	4830)	#30:NEW_CALL_EV (send) : (Unkn
192.168.0.1	local0.notice	[S=5122]	[SID:1546847905]	( lgr_flow)(	4831)	(#20):NEW_CALL_EV: (Unkn
192.168.0.1	local0.notice	[S=5123]	[SID:1546847905]	( lgr_stk_mngr)(	4832)	Resource StackSession (#28) Allocated
192.168.0.1	local0.notice	[S=5124]	[SID:1546847905]	( lgr_flow)(	4833)	(#20):Call changing stat

# AudioCodes Syslog Viewer



Syslog Viewer - [D:\WorkArea\Docs\#Courses\#Training Modules\MS Direct Routing\Lab-related\Lab3-Traces\Teams-to-PSTN-MB-disabled.log]

File Edit View Tools Help

Toolbar: Back, Forward, Stop, Refresh, Search, Filter, Options, Text Input, Zoom In/Out, Window Control.

Log Content:

```
11:45:50.734 10.15.11.1 local0.notice [S=32760] [SID=4bfc38:23:1377] ( 29980) (#4817)gwSession[All]
11:45:50.736 10.15.11.1 local0.notice [S=32761] [SID=4bfc38:23:1377] ( 29981) Condition Table match
11:45:50.736 10.15.11.1 local0.notice [S=32762] [SID=4bfc38:23:1377] ( 29982) Classification Success
11:45:50.736 10.15.11.1 local0.notice [S=32763] [SID=4bfc38:23:1377] ( 29983) IP2IPInboundManipula
11:45:50.738 10.15.11.1 local0.notice [S=32764] [SID=4bfc38:23:1377] ( 29984) SBCRoutingMngr:::Info
11:45:50.738 10.15.11.1 local0.notice [S=32765] [SID=4bfc38:23:1377] ( 29985) States: (#109)SBCRout
11:45:50.738 10.15.11.1 local0.notice [S=32766] [SID=4bfc38:23:1377] ( 29986) SBC ADMIT_DIALOGS_EV
11:45:50.739 10.15.11.1 local0.notice [S=32767] [SID=4bfc38:23:1377] ( 29987) CACI Add SBC Incoming
11:45:50.739 10.15.11.1 local0.notice [S=32768] [SID=4bfc38:23:1377] ( 29988) ResourceCounter: SBC
11:45:50.740 10.15.11.1 local0.notice [S=32769] [SID=4bfc38:23:1377] ( 29989) CAC: Add SBC Outgoing
11:45:50.740 10.15.11.1 local0.notice [S=32770] [SID=4bfc38:23:1377] ( 29990) ResourceCounter: SBC
11:45:50.741 10.15.11.1 local0.notice [S=32771] [SID=4bfc38:23:1377] ( 29991) (#109)Route found (2
11:45:50.742 10.15.11.1 local0.notice [S=32772] [SID=4bfc38:23:1377] ( 29992) ---- Incoming SIP Mes
11:45:50.742 10.15.11.1 local0.notice [S=32773] [SID=4bfc38:23:1377] INVITE sip:+1115551201@tr-sbc1.aud
  FROM: Interop11<sip:+1115551005@tr-sbc1.aud
  TO: <sip:+1115551201@tr-sbc1.aud
  CSEQ: 1 INVITE
  CALL-ID: 8c44407eb2f75c579cccc065f3
  MAX-FORWARDS: 70
  VIA: SIP/2.0/PCP 52.114.76.100:5060
  RECORD-ROUTE: <sip:sip-du-a-eu.pstn
  CONTACT: <sip:api-du-a-euwe.pstn
  CONTENT-LENGTH: 1115
  USER-AGENT: Microsoft.PSTNHub.SIP/1.0
  CONTENT-TYPE: application/sdp
  ALLOW: INVITE
  ALLOW: ACK
  ALLOW: OPTIONS
  ALLOW: CANCEL
  ALLOW: BYE
  ALLOW: NOTIFY

  v=0
  o=- 56290 0 IN IP4 127.0.0.1
  s=session
  c=IN IP4 52.114.116.48
  b=CT:10000000
  t=0
  m=audio 53064 RTP/SAVP 104 117 9 10
  c=IN IP4 52.114.116.48
  a=rtpc:53065
  a=ice-ufrag:kb7F
  a=ice-pwd:qrIN9V1ITVbBLcUsVczuX5X62
```

Line: 13 Column: 49

Syslog Listener

Options

Options Dialog (Open):

- Viewer**:
  - Font: Bitstream Vera Sans Mono
  - Size: 8
  - Lines of scrollback: 10000
  - Save window position
- Syslog**:
  - Syslog interface: Any
  - UDP port: 514
  - TCP port: 0
  - Compensate for packet reorder
  - Show syslog date
- Log File**:
  - File size (MBytes): 10
  - Number of files: 100
  - Start with new file
- IP Filter**:
  - Filter incoming traffic
  - Allowed IP addresses: [Text Box]
  - Blocked IP addresses: [Text Box]
- Content Filter**:
  - Receive filter
  - Display filter
- Multiple Devices**:
  - Use multiple tabs to separate between devices
  - Create separate log files for each device
  - Store logs of each device in separate directory
- SIP Flow Diagram**:
  - Group messages by: Call-ID + IP Address
  - Merge sessions with identical Call-ID
  - Parse CDR records
- Miscellaneous**:
  - External viewer: notepad.exe

OK Cancel

# Wireshark



- Freeware packet sniffer application enabling you to view traffic passed over the network
- Advantages:
  - Used for live/offline network troubleshooting and analysis
  - Strong filtering
  - SIP Call flow and Play sound
  - And more
- AudioCodes add advance filtering for DTM/DSP debug

# Capture Interfaces

- Capture > Options...
- Select the network interface currently used by the computer

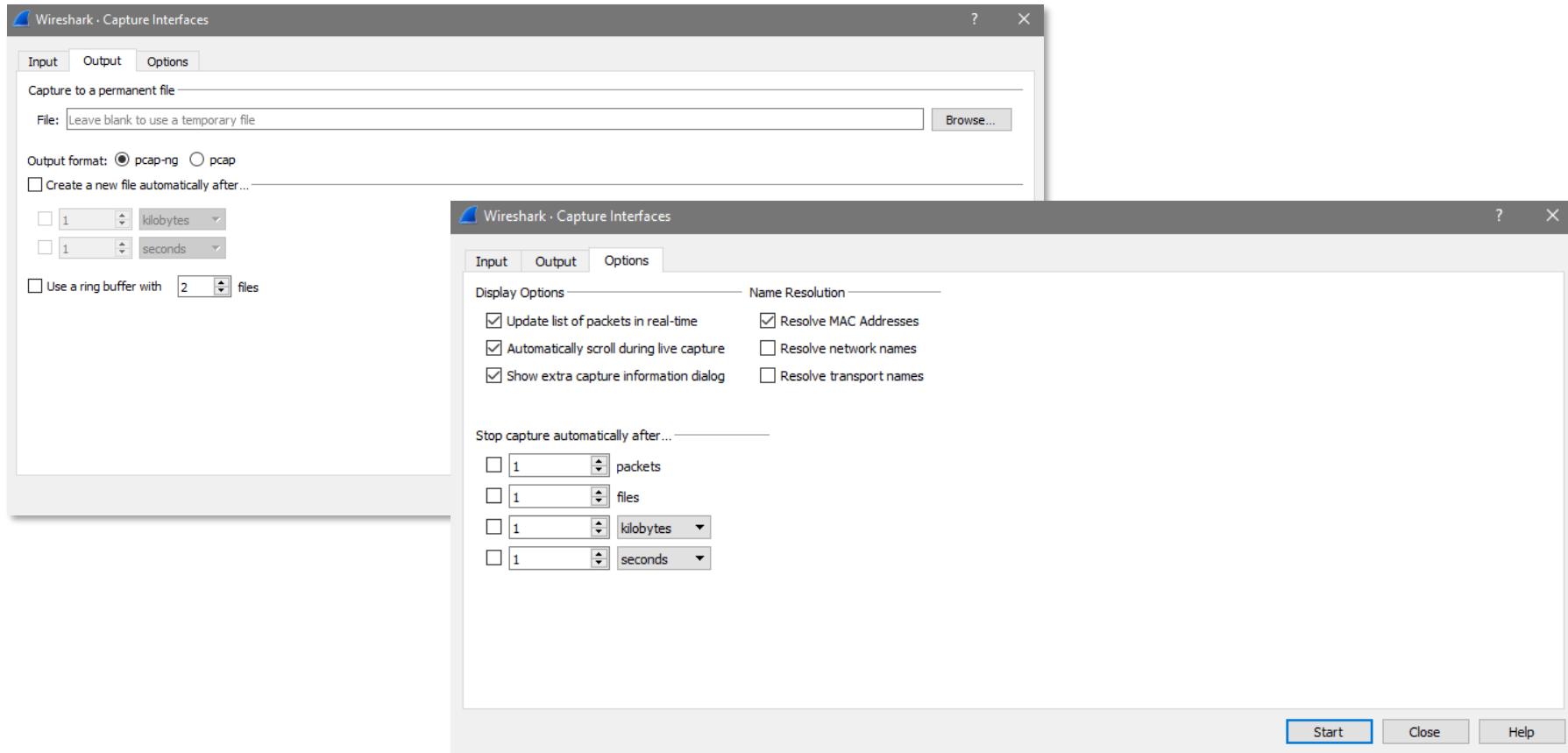
The screenshot shows the Wireshark application interface. On the left, the main window displays a file named "C:\Work\Trainings\Student Kit\Example Traces\Wireshark.pcap (242 KB)". Below it, the "Capture" pane shows a list of interfaces: Ethernet, Wi-Fi, Bluetooth Network Connection, USBPcap1, and USBPcap2. The "USBPcap1" interface is selected. On the right, a modal dialog titled "Wireshark - Capture Interfaces" lists the same interfaces with their current settings. The "Ethernet" interface is selected, and its row shows the following details:

Interface	Traffic	Link-layer Header	Promisc.	Snaplen	Buffer (MB)	Monitor Mode	Capture Filter
Ethernet	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	—
Wi-Fi	—	Ethernet	<input type="checkbox"/>	default	2	—	—
Bluetooth Network Connection	—	Ethernet	<input type="checkbox"/>	default	2	—	—
USBPcap1	—	USBPcap	<input type="checkbox"/>	—	—	—	—
USBPcap2	—	USBPcap	<input type="checkbox"/>	—	—	—	—

At the bottom of the dialog, there is a checkbox for "Enable promiscuous mode on all interfaces" and a "Start" button.

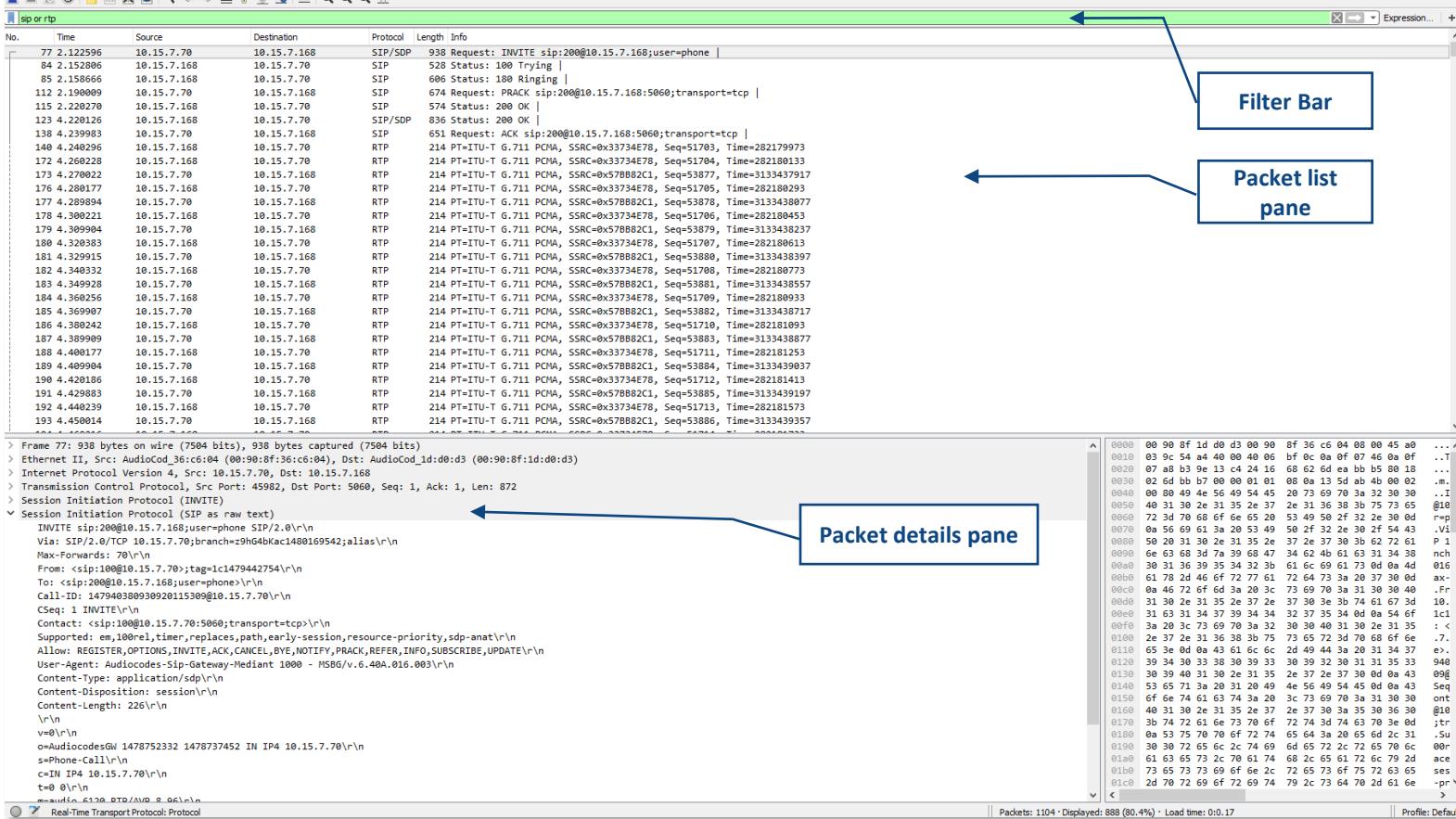
At the very bottom of the main Wireshark window, the status bar reads "Ready to load or capture" and "No Packets".

# Capture Output & Options



# Wireshark Main Window

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



The diagram illustrates the Wireshark main window interface. At the top is the **Filter Bar**, which contains a search field and a dropdown menu labeled "Expression...". Below it is the **Packet list pane**, displaying a list of network packets. Each packet row includes columns for No., Time, Source, Destination, Protocol, Length, and Info. A blue double-headed arrow connects the Filter Bar to the Packet list pane. To the right of the list pane is the **Packet details pane**, which shows detailed information for the selected packet. A blue double-headed arrow connects the Packet list pane to the Packet details pane. At the bottom right is the **Packet bytes pane**, showing the raw byte representation of the selected packet. A blue double-headed arrow connects the Packet details pane to the Packet bytes pane.

No. Time Source Destination Protocol Length Info

77 2.122596 10.15.7.70 10.15.7.168 SIP/SDP 938 Request: INVITE sip:200@10.15.7.168;user=phone |

84 2.152898 10.15.7.168 10.15.7.70 SIP 528 Status: 100 Trying |

85 2.158666 10.15.7.168 10.15.7.70 SIP 606 Status: 180 Ringing |

112 2.190099 10.15.7.70 10.15.7.168 SIP 674 Request: PRACK sip:200@10.15.7.168:5060;transport=tcp |

115 2.220270 10.15.7.168 10.15.7.70 SIP 574 Status: 200 OK |

123 4.220126 10.15.7.168 10.15.7.70 SIP/SDP 836 Status: 200 OK |

138 4.239983 10.15.7.70 10.15.7.168 SIP 651 Request: ACK sip:200@10.15.7.168:5060;transport=tcp |

140 4.240296 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51703, Time=282179973

172 4.269228 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51704, Time=282180133

173 4.270022 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53077, Time=3133437917

176 4.280177 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51705, Time=282180293

177 4.289894 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53087, Time=3133438087

178 4.308221 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51706, Time=282180453

179 4.309960 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53089, Time=3133438237

180 4.320833 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51707, Time=282180613

181 4.329915 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53088, Time=3133438397

182 4.340332 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51708, Time=282180773

183 4.349928 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53081, Time=3133438557

184 4.360256 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51709, Time=282180933

185 4.369907 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53082, Time=3133438717

186 4.380242 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51710, Time=282181093

187 4.389999 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53083, Time=3133438877

188 4.400177 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51711, Time=282181253

189 4.400904 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53084, Time=3133439037

190 4.420186 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51712, Time=282181413

191 4.429883 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53085, Time=3133439197

192 4.446239 10.15.7.168 10.15.7.70 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x33734E78, Seq=51713, Time=282181573

193 4.450014 10.15.7.70 10.15.7.168 RTP 214 PT=ITU-T G.711 PCMA, SSRC=0x57B882C1, Seq=53086, Time=3133439357

> Frame 77: 938 bytes on wire (7504 bits), 938 bytes captured (7504 bits)

> Ethernet II, Src: Audiocod\_id:d3:b3 (00:90:8f:3e:c6:04), Dst: AudioCod\_id:d0:d3 (00:90:8f:1d:d0:d3)

> Internet Protocol Version 4, Src: 10.15.7.70, Dst: 10.15.7.168

> Transmission Control Protocol, Src Port: 45982, Dst Port: 5060, Seq: 1, Ack: 1, Len: 872

> Session Initiation Protocol (INVITE)

> Session Initiation Protocol (SIP as raw text)

INVITE sip:200@10.15.7.168;user=phone;proxy=2.0;r=0.1\r\nVia: SIP/2.0/TCP 10.15.7.70;brANCH=z9hG4bKac1480169542;alias\r\nMax-Forwards: 70\r\nFrom: <sip:100@10.15.7.70;tag=1c1479442754>\r\nTo: <sip:200@10.15.7.168;user=phone>\r\nCall-ID: 14794438093020115309@10.15.7.70\r\nSeq: 1\r\nINVITE\r\nContact: <sip:100@10.15.7.70:5060;transport=tcp>\r\nSupported: em,100rel,timer,replaces,path,early-session,resource-priority,sdp-anat\r\nAllow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE\r\nUser-Agent: AudiocodesGw 1478752332 1478737452 IN IP4 10.15.7.70\r\nContent-Type: application/sdp\r\nContent-Disposition: session\r\nContent-Length: 226\r\n\r\n\r\no=AudiocodesGw 1478752332 1478737452 IN IP4 10.15.7.70\r\ns=Phone-Call\r\nn=c=IN IP4 10.15.7.70\r\nt=0\r\nm=audio 6139 RTP/Audio 8\_0\_64\r\n\r\nReal-Time Transport Protocol: Protocol

0000 00 90 8f 1d 0d d0 00 90 8f 36 c6 04 08 00 45 a9 ...^

0010 03 9c 54 ad 40 99 00 06 bf 0a 0f 07 46 0a 0f ..T

0020 07 a3 b3 9e 13 c4 24 16 68 62 6d ea bb b5 80 18 ..

0030 02 6d bb 7b 00 00 01 01 08 0a 13 5d ab 4b 00 02 ..m.

0040 00 88 49 4e 56 49 54 45 20 73 69 70 3a 32 30 30 ..I

0050 40 31 30 2e 31 35 2e 37 2e 31 36 38 3b 75 73 65 @10

0060 72 3d 70 68 6f 6e 65 20 53 49 50 2f 32 2e 30 0d r=p

0070 0a 56 69 61 3a 20 53 49 50 2f 32 2e 30 2f 54 43 .Vi

0080 50 20 31 30 2e 31 35 2e 37 37 27 37 30 3b 62 72 61 P 1

0090 6e 63 63 3d 7a 39 68 47 34 62 4b 61 63 31 34 nch

00a0 30 31 36 39 35 34 32 3b 61 66 69 61 73 0d 0a 4d 016

00b0 61 78 2d 46 6f 72 77 61 72 64 73 3a 23 37 30 0d ax-

00c0 04 46 72 6f 3a 20 3c 73 69 70 3a 31 30 30 40 .Fr

00d0 31 30 2e 31 35 2e 37 2e 37 30 3e 3b 74 61 67 3d 10.

00e0 31 63 31 35 2e 37 30 3e 3b 74 61 67 3d 1c1

00f0 73 69 70 3a 31 30 30 40 37 30 3e 3b 74 61 67 3d :;

0100 2e 37 2e 31 36 38 3b 75 73 65 72 3d 70 68 61 66 7e .,

0110 65 3e 0d 04 43 61 6c 6c 24 49 44 3a 20 31 34 37 >e,

0120 39 34 30 32 38 30 39 33 30 39 32 30 31 35 33 040

0130 30 39 40 31 30 2e 31 35 2e 37 37 30 38 0a 43 09g

0140 53 65 71 3a 28 31 20 49 4e 56 49 54 45 0d 0a 43 Seq

0150 6f 6e 74 61 63 74 3a 20 3c 73 69 70 3a 31 30 30 ont

0160 40 31 30 2e 31 35 2e 37 2e 37 30 3a 35 30 36 30 @10

0170 3b 74 72 61 63 73 70 69 6f 72 74 3d 74 63 70 3e 0d ;tr

0180 0a 53 75 70 6f 6f 72 74 65 64 3a 20 65 6d 2c 31 .Su

0190 30 38 72 65 6c 2c 74 69 6d 65 72 2c 72 65 70 6c 00r

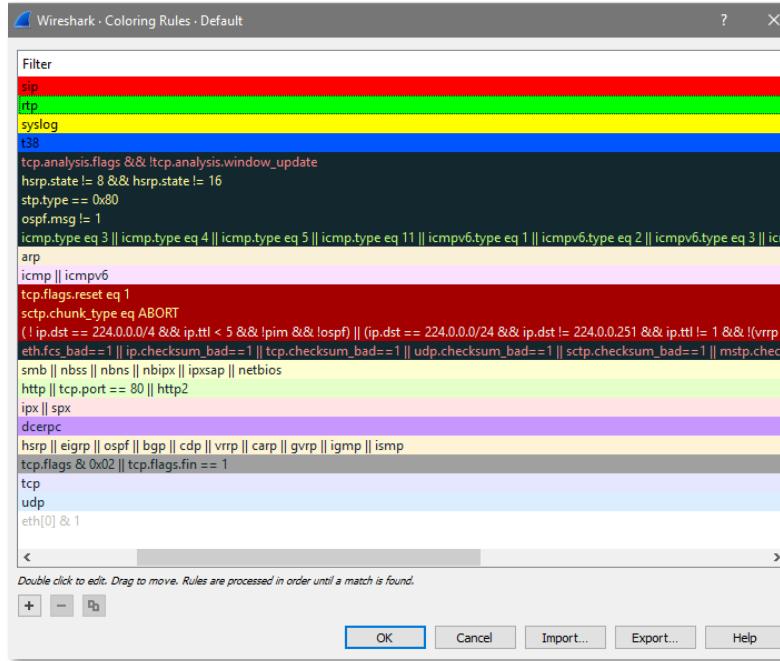
01a0 61 63 73 73 2c 70 61 74 68 2c 65 61 72 6c 79 2d ace

01b0 73 65 73 73 6f 6e 2c 72 65 73 6f 75 72 63 65 ses

01c0 2d 70 62 69 6f 72 69 74 79 2c 73 64 70 2d 61 6e -pr >

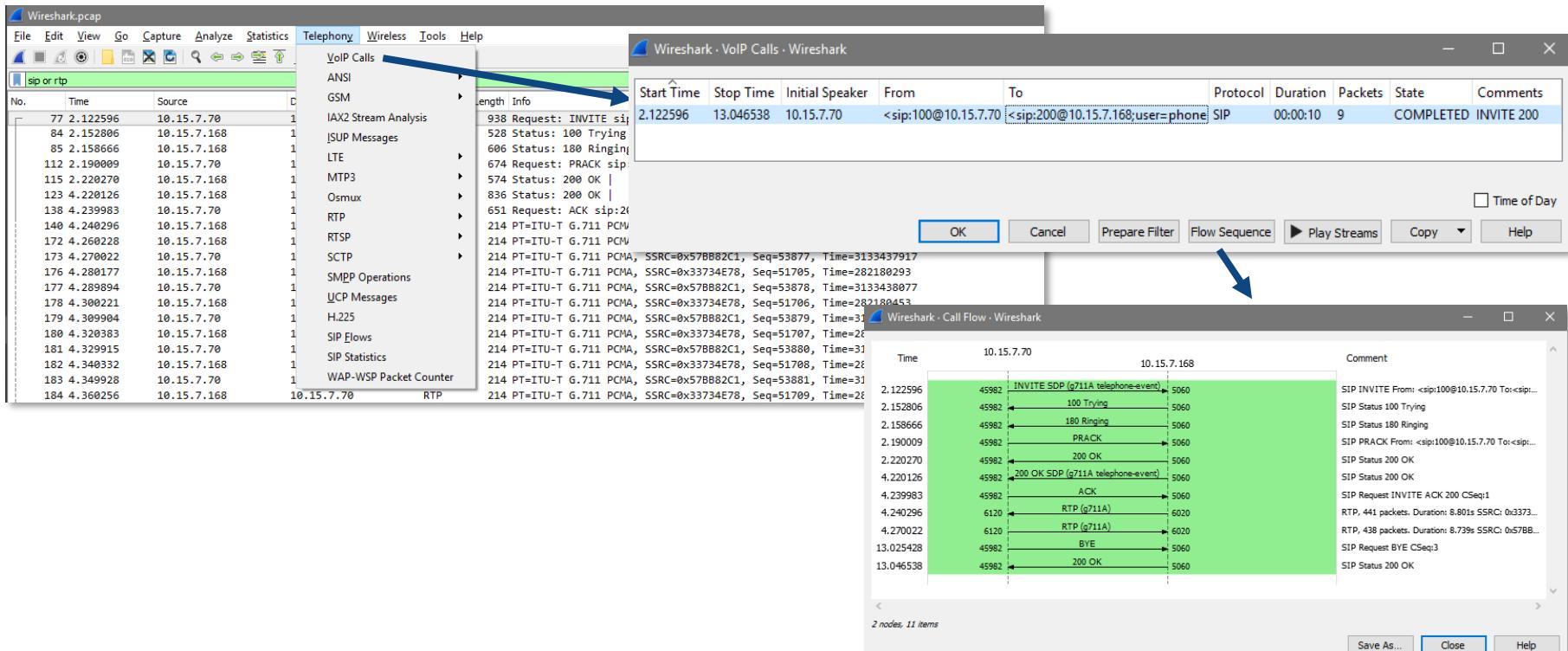
# Coloring Rules

- Assign a color to each protocol to facilitate quick analysis
- Define general rules e.g., TCP, UDP at the bottom of the coloring list because processing is from top to bottom until a match is found



# Generating Call Flow

- Visually represents entire call flow
- Telephony > VoIP Calls



The screenshot shows the Wireshark interface with three main windows:

- Wireshark - VoIP Calls**: A table view of VoIP calls. A blue arrow points from the "Telephony" menu to this table. One row is selected, showing a SIP INVITE from <sip:100@10.15.7.70> to <sip:200@10.15.7.168> with a duration of 00:00:10 and state COMPLETED.
- Wireshark - Call Flow - Wireshark**: A detailed call flow diagram. A blue arrow points from the "Call Flow" button in the top right of the VoIP Calls table to this window. It displays a sequence of SIP messages (INVITE, 100 Trying, 180 Ringing, PRACK, 200 OK) and RTP packets (g711A) between the two endpoints.
- Wireshark - Top Bar**: The main Wireshark window title bar.

The "Telephony" menu is open, showing various protocols and analysis options. The "Call Flow" button is highlighted in the top right corner of the VoIP Calls table.

# Playing G.711 RTP Stream

Wireshark.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

VoIP Calls

ANSI

GSM

IAX2 Stream Analysis

ISUP Messages

LTE

MTP3

RTP

RTSP

SCTP

SMP Operations

UCP Messages

H.225

SIP Flows

SIP Statistics

WAP-WSP Packet Counter

No. Time Source D

77 2.122596 10.15.7.70 1

84 2.152806 10.15.7.168 1

85 2.158666 10.15.7.168 1

112 2.190009 10.15.7.70 1

115 2.220270 10.15.7.168 1

123 4.228126 10.15.7.168 1

138 4.239983 10.15.7.70 1

140 4.240296 10.15.7.168 1

172 4.260228 10.15.7.168 1

173 4.270022 10.15.7.70 1

176 4.288177 10.15.7.168 1

177 4.289894 10.15.7.70 1

178 4.300221 10.15.7.168 1

179 4.309904 10.15.7.70 1

180 4.320383 10.15.7.168 1

181 4.329915 10.15.7.70 1

182 4.340332 10.15.7.168 1

183 4.349928 10.15.7.70 1

184 4.360256 10.15.7.168 10.15.7.70 RTP

Start Time: 2.122596 Stop Time: 13.046538 Initial Speaker: 10.15.7.70 From: <sip:100@10.15.7.70> To: <sip:200@10.15.7.168;user=phone> Protocol: SIP Duration: 00:00:10 Packets: 9 State: COMPLETED Comments: INVITE 200

OK Cancel Prepare Filter Flow Sequence Play Streams Copy Help

Time of Day

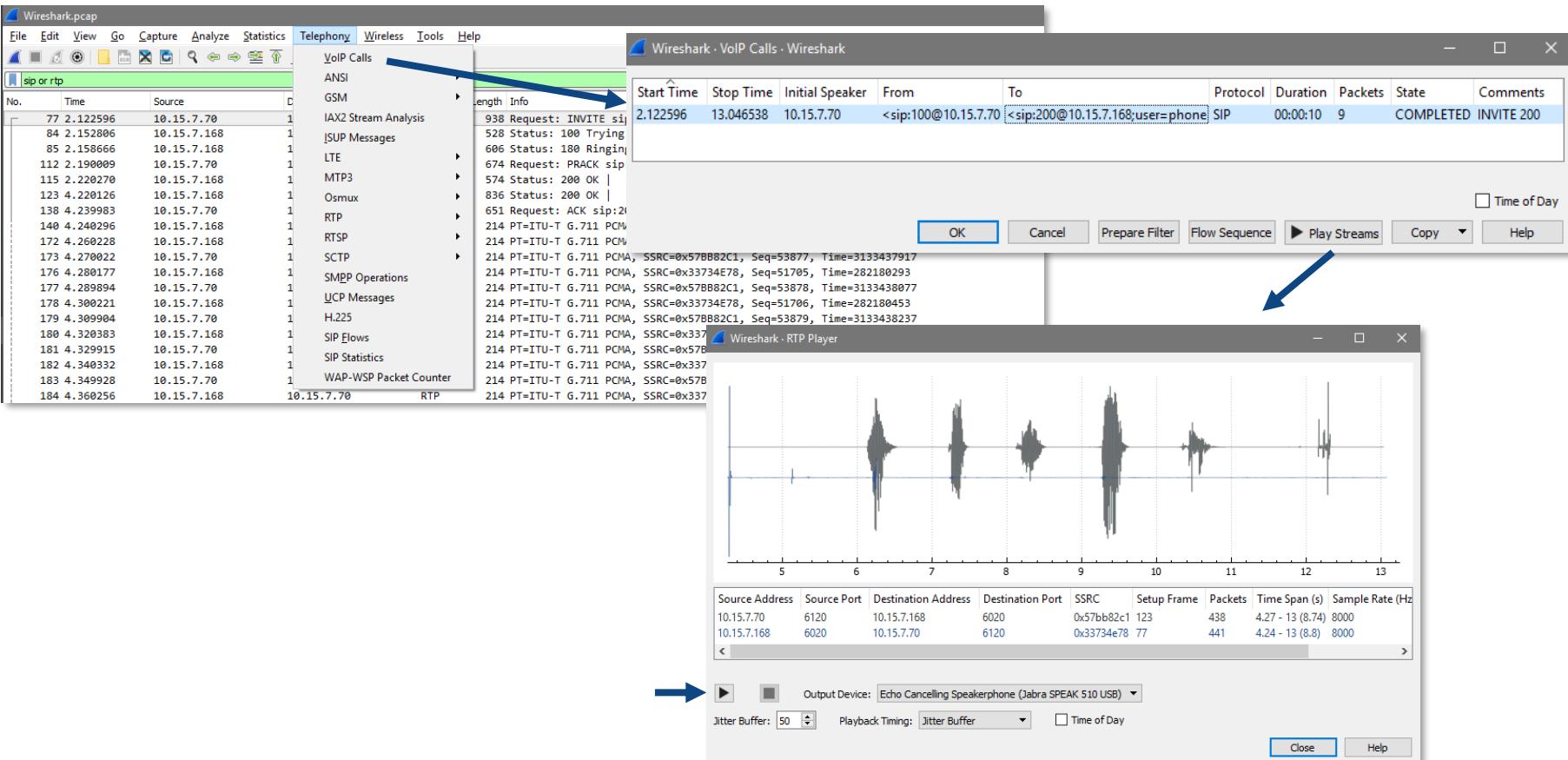
Wireshark - RTP Player

Source Address: 10.15.7.70 Source Port: 6120 Destination Address: 10.15.7.168 Destination Port: 6020 SSRC: 0x57bb82c1 Setup Frame: 123 Packets: 438 Time Span (s): 4.27 - 13 (8.74) Sample Rate (Hz): 8000

Output Device: Echo Cancelling Speakerphone (Jabra SPEAK 510 USB)

Jitter Buffer: 50 Playback Timing: Jitter Buffer Time of Day

Close Help



# Analyzing RTP Data Stream

- Extracts audio from data packets (G.711 only)

Wireshark.pcap

File Edit View Go Capture Analyze Statistics **Telephony** Wireless Tools Help

sip or rtp

No.	Time	Source	Destination	Length	Info
77	2.122596	10.15.7.70	10.15.7.168	1	IAX2 Stream Analysis
84	2.152806	10.15.7.168	10.15.7.168	1	ANSI
85	2.158666	10.15.7.168	10.15.7.168	1	GSM
112	2.190009	10.15.7.70	10.15.7.168	1	IAX2 Stream Analysis
115	2.220270	10.15.7.168	10.15.7.168	1	LTE
123	4.220126	10.15.7.168	10.15.7.168	1	MTP3
138	4.239983	10.15.7.70	10.15.7.168	1	Osmux
140	4.240296	10.15.7.168	10.15.7.168	1	RTP
172	4.260228	10.15.7.168	10.15.7.168	1	RTSP
173	4.270022	10.15.7.70	10.15.7.168	1	SCTP
176	4.288177	10.15.7.168	10.15.7.168	1	SMPP Operations
177	4.289894	10.15.7.70	10.15.7.168	1	UCP Messages
178	4.300221	10.15.7.168	10.15.7.168	1	H.225
179	4.309904	10.15.7.70	10.15.7.168	1	SIP Flows
180	4.320383	10.15.7.168	10.15.7.168	1	SIP Statistics
181	4.329915	10.15.7.70	10.15.7.168	1	
182	4.340332	10.15.7.168	10.15.7.168	1	
183	4.340332	10.15.7.168	10.15.7.168	1	Wireshark - RTP Streams - Wireshark
184	4.340332	10.15.7.168	10.15.7.168	1	

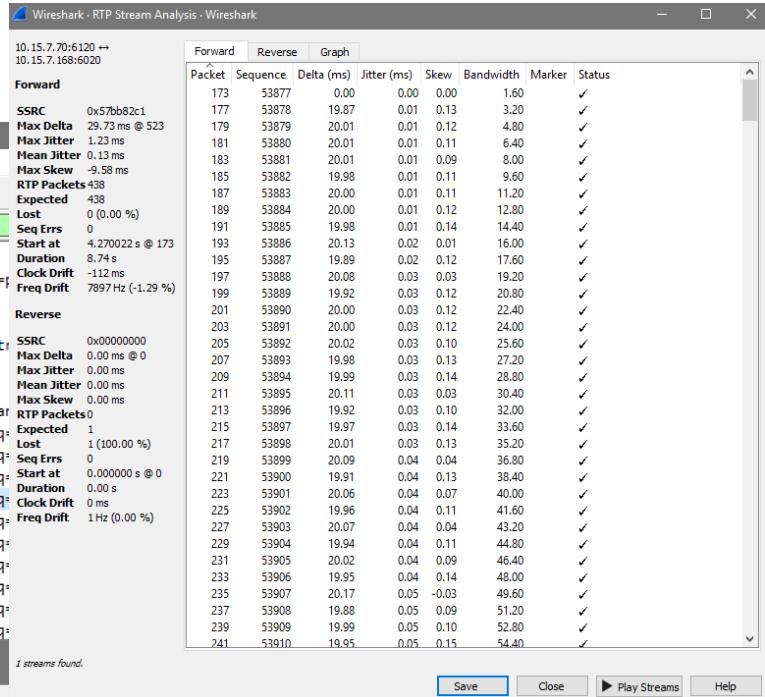
2 streams found.

Source Address | Source Port | Destination Address | Destination Port | SSRC | Payload | Packets | Lost | Max Delta (ms) | Max Jitter | Mean Jitter | Status

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
10.15.7.70	6120	10.15.7.168	6020	0x57bb82c1	g711A	438	0 (0.0%)	29.730	1.232	0.133	
10.15.7.168	6020	10.15.7.70	6120	0x33734e78	g711A	441	0 (0.0%)	21.094	0.128	0.056	

2 streams, 1 selected, 438 total packets. Right-click for more options.

Close Find Reverse Prepare Filter Export... Copy Analyze Help



# Debug Recording



# What is Debug Recording (DR)?



- A feature used to capture and record traffic sent and/or received by the device
- It is used for advanced debugging when you need to analyze internal messages and signals
- The device can send debug recording packets to a debug capturing server
- Can record different types of traffic such as
  - Media streams (RTP, T.38 and PCM)
  - PSTN signaling (ISDN, CAS, SS7)
  - Control messages (SIP, MGCP, MEGACO)
  - Networking streams (such as HTTP and SCTP)
  - Other internal information (such as DSP Events)

- Can record all IP traffic sent by/received from the device
- Can record actual voice signal arriving from the TDM (before it enters the DSP)
- Useful for recording network traffic in environments where hub or port mirroring is unavailable
- Useful for recording internal traffic between two endpoints on the same device
- Can include Syslog messages
- Debug Recording packets are captured using Wireshark or a similar tool (requires AudioCodes proprietary Plug-in)

# Installing AudioCodes' Proprietary Plug-in



- **Install Wireshark on your computer**
  - The Wireshark program can be downloaded from <http://www.wireshark.org>
- **Download the proprietary plug-in files from [www.audiocodes.com/downloads](http://www.audiocodes.com/downloads).**
- **Copy the plug-in files to the directory in which you installed Wireshark, as follows:**

Copy this file	To this folder on your PC
...\\dtds\\cdr.dtd	Wireshark\\dtds\\
...\\plugins\\<Wireshark ver.>\\*.dll	Wireshark\\plugins\\<Wireshark ver.>

- **Start Wireshark**
- In the Filter field, type "acdr" to view the debug recording messages
- Note that the source IP address of the messages is always the OAMP IP address of the device
- The device adds the header "AUDIODES DEBUG RECORDING" to each debug recording message

# Viewing DR Messages in Wireshark



ACDR Filter

Proprietary Header

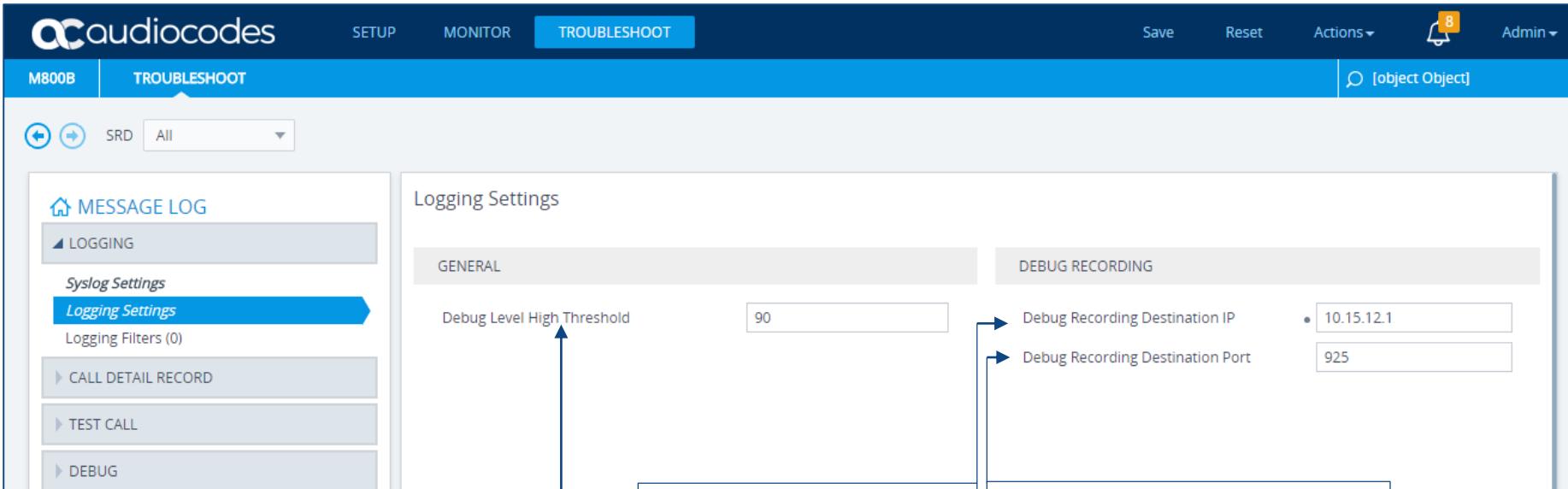
The screenshot shows the Wireshark interface with a list of captured frames. Frame 615 is selected, displaying its detailed structure:

- Frame 615: 1357 bytes on wire (10856 bits), 1357 bytes captured (10856 bits) on interface 0
- Ethernet II, Src: AudioCodes\_5f:d9:5a (00:90:8f:5f:d9:5a), Dst: Portwell\_4e:ed:ab (00:90:fb:4e:ed:ab)
- Internet Protocol Version 4, Src: 134.99.217.167, Dst: 134.99.217.168
- User Datagram Protocol, Src Port: 926, Dst Port: 925
- AUDIOCODES DEBUG RECORDING
  - Version: 0x07
  - Time Stamp: 513f778f (1363.113871 sec)
  - Sequence Number: 220
  - Source ID: 7
  - Dest ID: 7
  - Extra Data: 0x00
  - Trace Point: Dsp -> Tdm (9)
  - Media Type: PCM (15)
  - Header Extension Len: 0
  - Full Session ID: 5fd95a:21:382
    - Board ID: 0x5fd95a
    - Reset Counter: 21
    - Session ID: 382
  - Real-Time Transport Protocol
  - Data (1315 bytes)

Packets: 3938 · Displayed: 1752 (44.5%) · Load time: 0:0.76 · Profile: Default

# Activating the DR through the WEB Interface

- To set the address/port of the debug recording server:



The screenshot shows the audiocodes M800B TROUBLESHOOT interface. In the left sidebar, under the **MESSAGE LOG** section, the **Logging Settings** item is selected. On the right, the **Logging Settings** page is displayed with two main tabs: **GENERAL** and **DEBUG RECORDING**. The **GENERAL** tab contains the **Debug Level High Threshold** field set to 90. The **DEBUG RECORDING** tab contains the **Debug Recording Destination IP** field set to 10.15.12.1 and the **Debug Recording Destination Port** field set to 925. Callouts provide detailed descriptions for each highlighted parameter.

**GENERAL**

Defines the threshold (in percentage) for automatically switching to a different debug level, depending on CPU usage  
The parameter is applicable only if the 'Syslog CPU Protection' parameter is enabled

**DEBUG RECORDING**

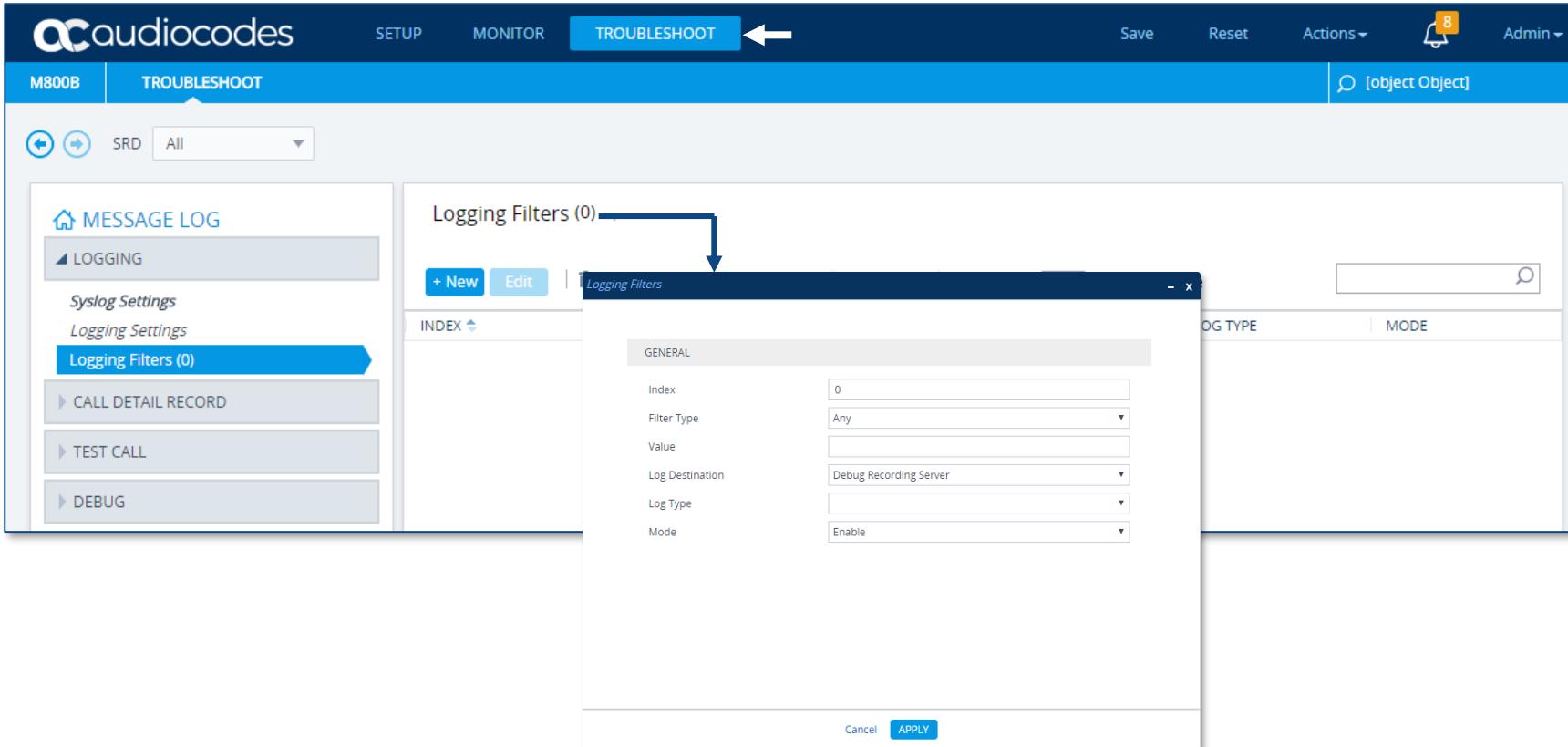
Defines the IP address of the server for capturing debug recording

Defines the port of the server for capturing debug recording. The default is 925

- The Logging Filters table lets you configure rules for filtering debug recording packets, Syslog messages, and Call Detail Records (CDR)
  - Example:
    - A rule to generate Syslog messages only for calls belonging to IP Groups 2 and 4, or for calls belonging to all IP Groups except IP Group 3
- Debug recording log filters can include:
  - Signaling information (such as SIP messages)
  - Syslog messages
  - PSTN traces (ISDN and CAS)
  - CDRs
  - Media (RTP, RTCP, and T.38)
  - Pulse-code modulation (PCM) of voice signals from and to the TDM
- Log Filters can be enabled or disabled

# Configuring filtering rules

- To configure logging filtering rules:

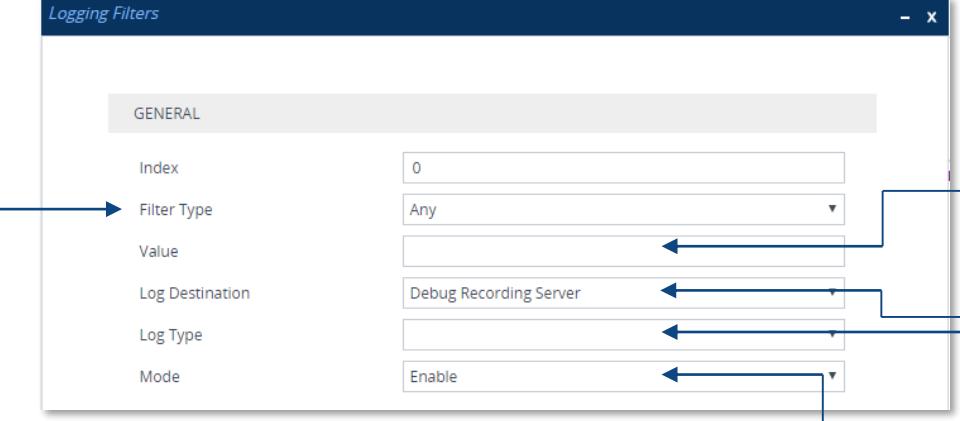


The screenshot shows the audiocodes M800B web interface with the TROUBLESHOOT tab selected. In the left sidebar under MESSAGE LOG, the Logging Filters (0) option is highlighted. A modal window titled "Logging Filters (0)" is open, showing a form with the following fields:

GENERAL	
Index	0
Filter Type	Any
Value	(empty)
Log Destination	Debug Recording Server
Log Type	(empty)
Mode	Enable

At the bottom of the modal are "Cancel" and "APPLY" buttons.

# Configuring filtering rules



The screenshot shows the 'Logging Filters' configuration window with the following fields:

- Index:** 0
- Filter Type:** Any
- Value:** (empty)
- Log Destination:** Debug Recording Server
- Log Type:** (empty)
- Mode:** Enable

Annotations explain the purpose of each field:

- Filter Type:** Defines the value for the selected Filtering Type.
- Log Destination:** Defines where the device sends the log file.
  - 0. Syslog Server
  - 1. Debug Recording Server (Default)
  - 2. Local Storage
  - 3. Call Flow Server (i.e., OVOC)
- Log Type:** Defines the type of messages to include in the log file.
  - 0. (Default) Not configured
  - 1. Signaling (only Debug Recording)
  - 2. Signaling & Media (only Debug Recording)
  - 3. Signaling & Media & PCM (only Debug Recording)
  - 4. PSTN Trace (only Debug Recording)
  - 5. CDR Only (applicable only if the 'Log Destination' parameter is configured to Syslog Server or Local Storage)
  - 6. Call Flow (the device sends SIP messages in XML format to OVOC)
- Mode:** Enables (default) or disables the rule.

**Defines the filter criteria:**

1. Any (default)
2. Trunk ID = Filters log by Trunk ID (only Gateway application)
3. Trunk Group ID = Filters log by Trunk Group ID (only Gateway application)
4. Trunk & B-channel = (only Gateway application)
5. FXS or FXO = (only Gateway application)
6. Tel-to-IP = Filters log by Tel-to-IP routing rule (only Gateway application)
7. IP-to-Tel = Filters log by IP-to-Tel routing rule (only Gateway application)
8. IP Group = Filters log by IP Group
9. SRD = Filters log by SRD
10. Classification = Filters log by Classification rule (only SBC application)
11. IP-to-IP Routing = Filters log by IP-to-IP routing rule (only SBC application)
12. User = Filters log by user
13. IP Trace = Filters log by an IP network trace, Wireshark-like expression
14. SIP Interface = Filters log by SIP Interface



Hands-on Lab 2

SBC Routing





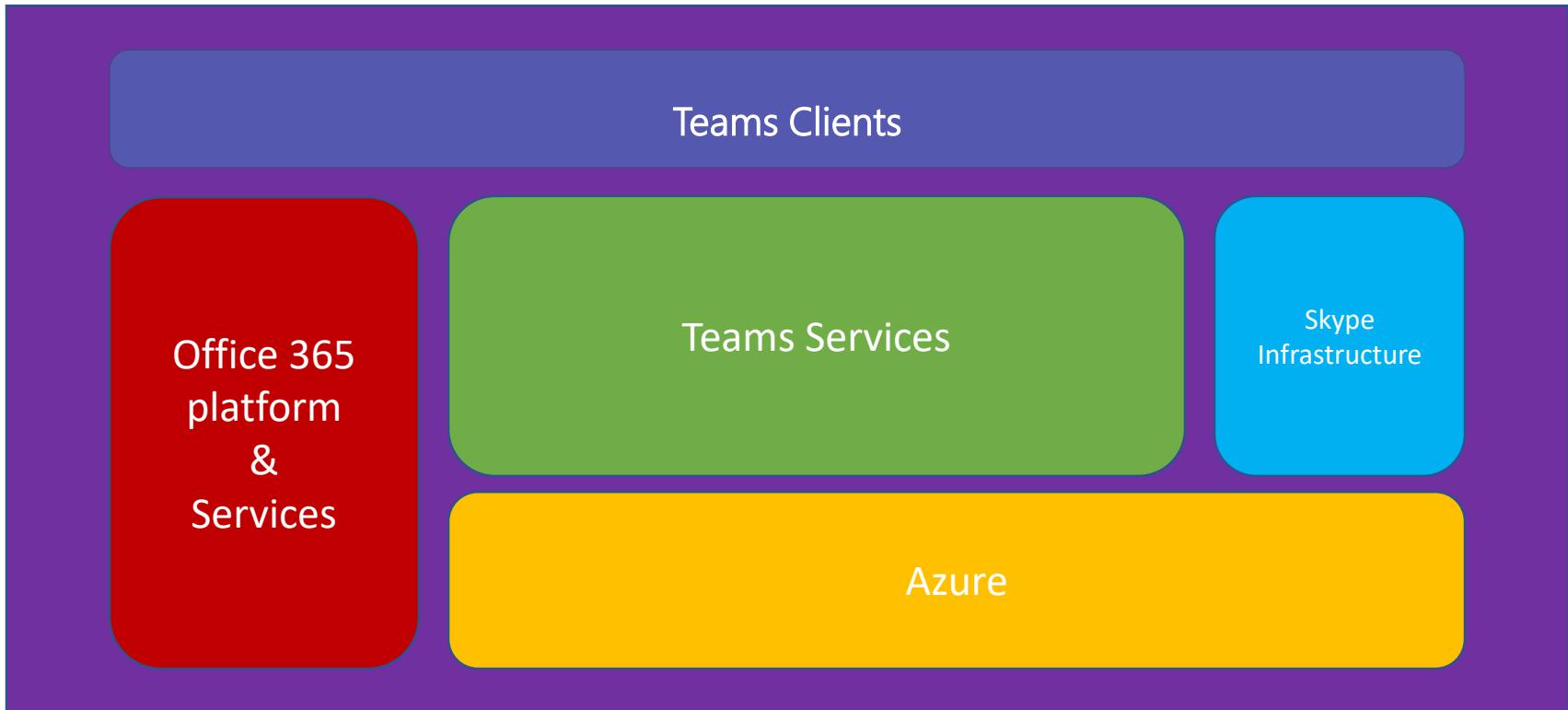
## Lesson 10

# Teams System Brief Overview

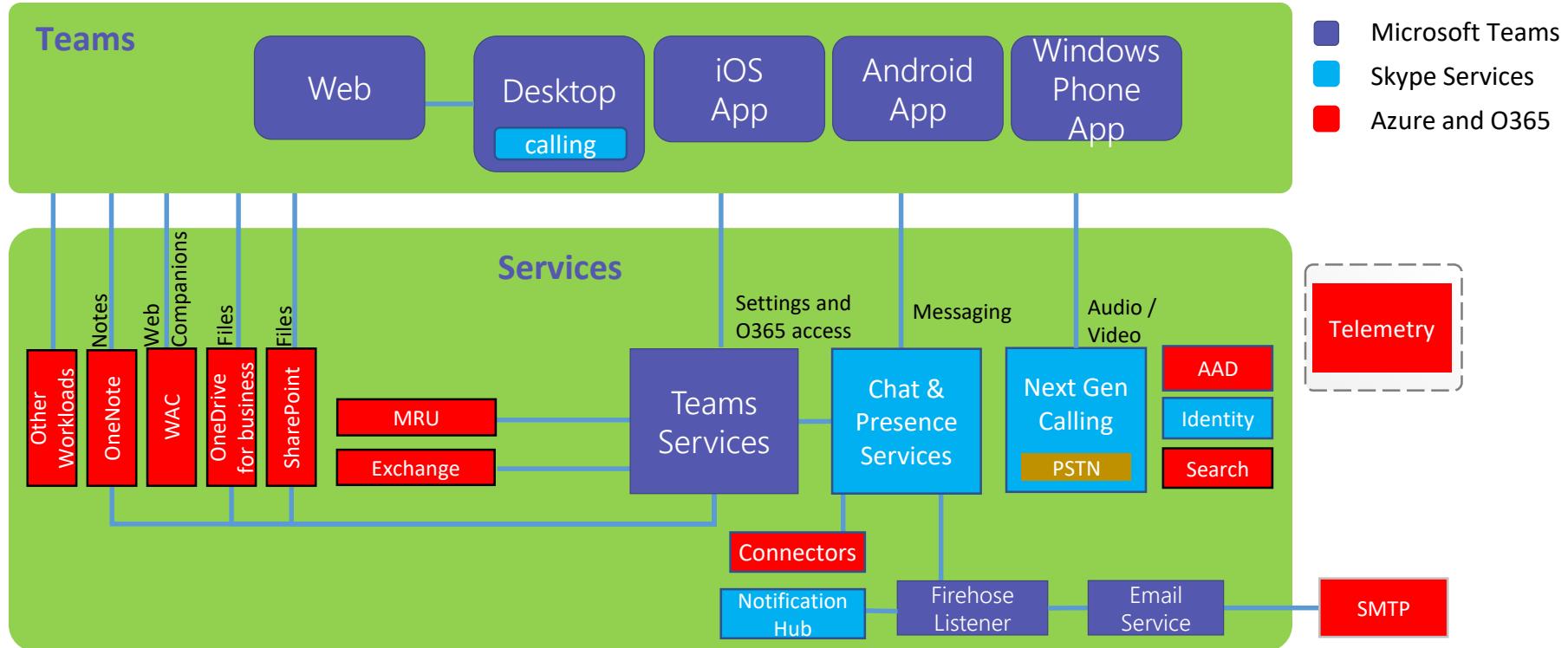


- After completing this lesson you will:
  - Understand Microsoft Phone System Direct Routing Topology
  - Identify Direct Routing Solution Components
  - Identify Direct Routing Benefits
  - Understand the SBC FQDN requirements

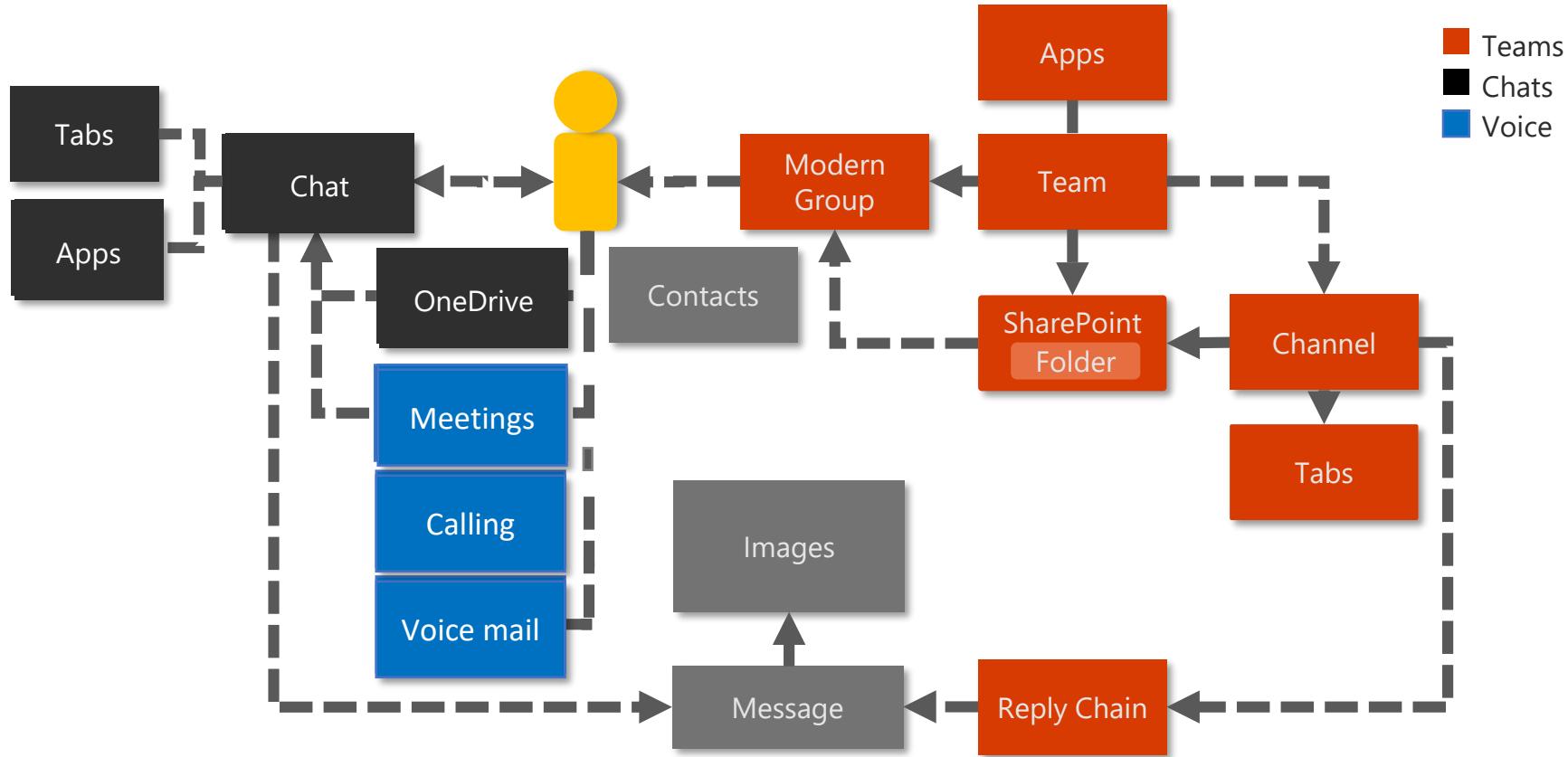
# Teams bring together Office 365 and Skype



# High Level Architecture



# Teams Logical Architecture



# Teams as your phone

Contacts, History and Voicemail

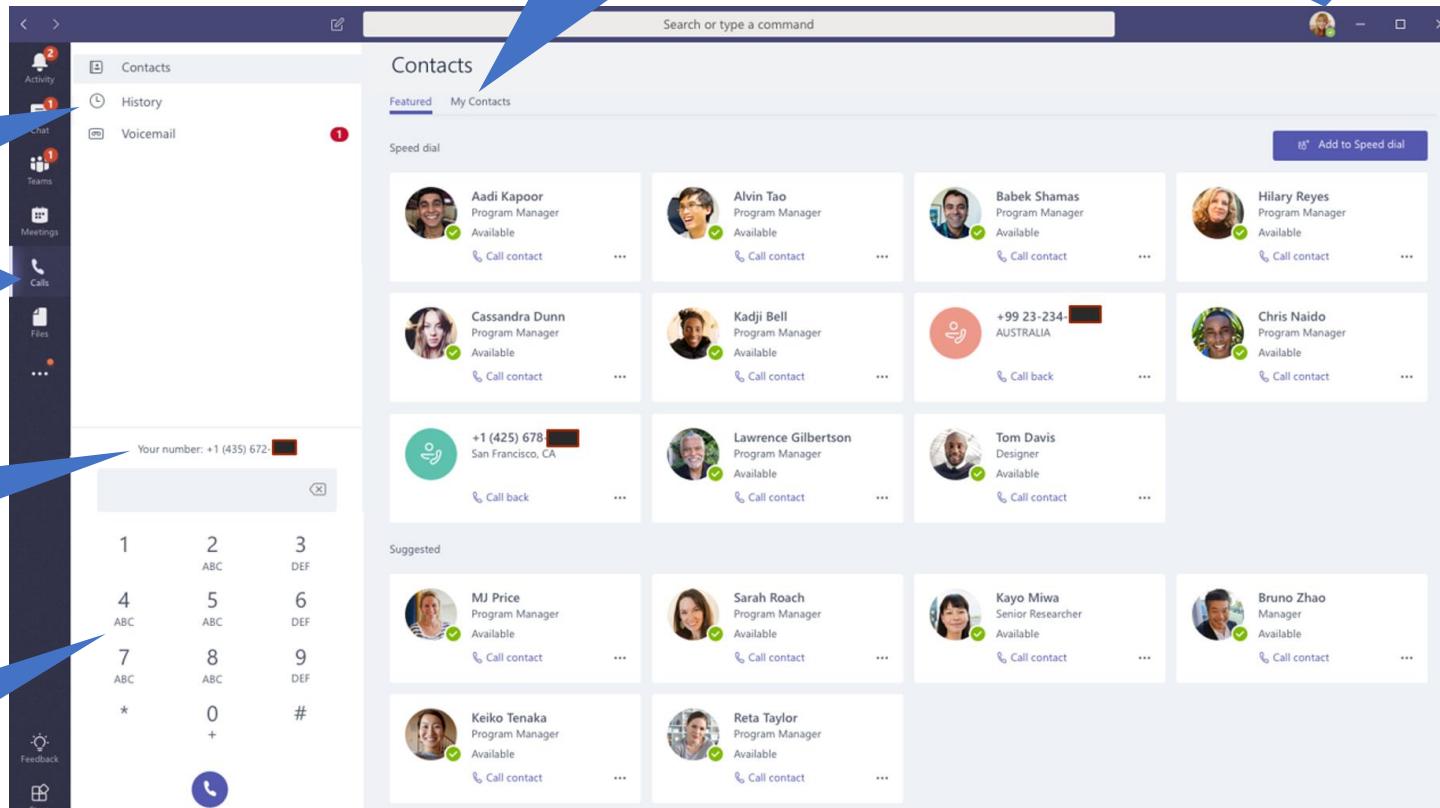
Menu in client for calling functionality

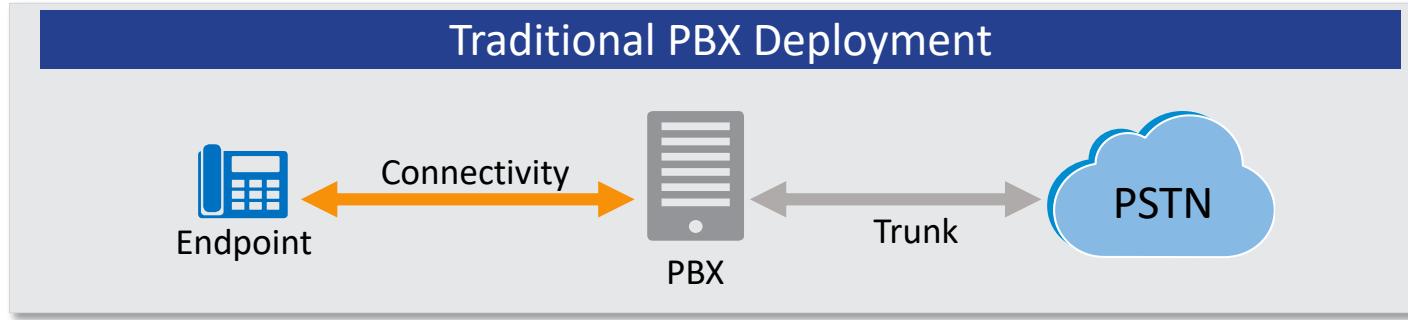
Your phone number displayed here

Dial pad to dial phone numbers

Access your contacts

Manage user settings





- **PBX is a Phone System**
  - Provide voice features to the customers
  - Connect calls between users
  - Send/receive calls to/from PSTN
- **Endpoints**
  - Users which consume PBX features
- **Trunk**
  - Connect the PBX to the PSTN network

- **Endpoints**

- Desktop clients running on PC, MAC and Web
- Mobile clients running on iOS and Android OSs
- IP Phones

- **Phone System**

- Provide PBX features for all Teams users (appropriate license is required)

- **Trunk**

- Calling Plan
- Direct Routing



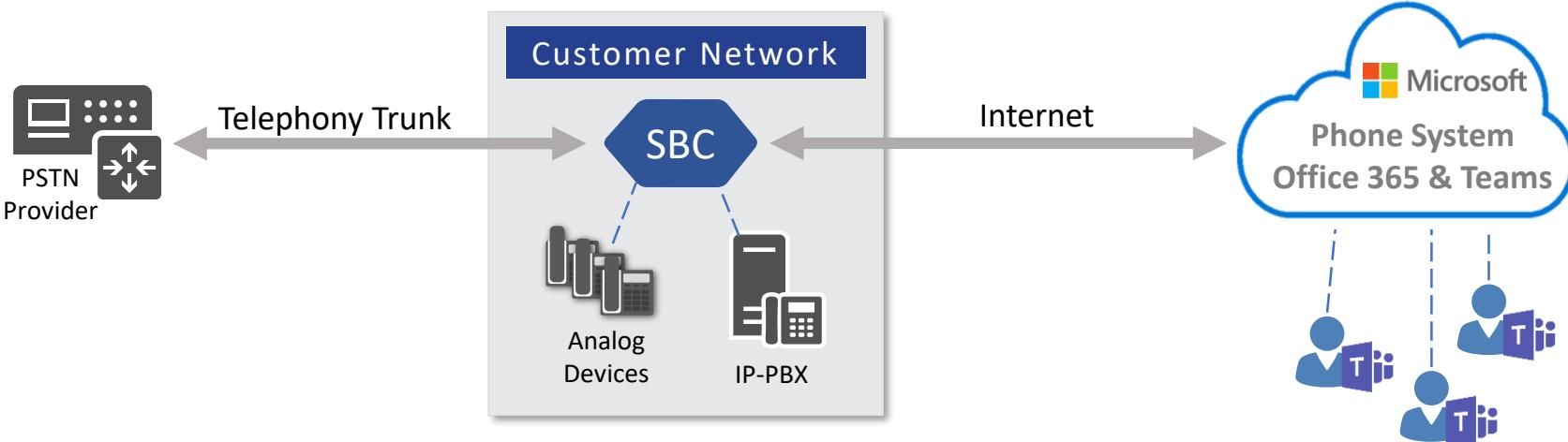
- **Calling Plan**

- Calling in Teams is powered by Phone System (formerly known as Cloud PBX)
- PSTN connectivity provided directly by Microsoft
- No on-premises equipment required
- New phone numbers from Microsoft or port existing numbers (if available)

- **Direct Routing**

- Connecting Office 365 with the customer infrastructure
- Using existing customer phone numbers
- SBC on-premises integrates with existing PSTN connectivity or/and old PBX

# Microsoft Teams Direct Routing



- Allows customers to connect their Voice Trunks directly to Office 365
- Allows customers with users in the Microsoft Cloud to continue using 3<sup>rd</sup> party systems such as PBXs, IP-PBXs and Analog Telephony Adaptors (ATA) devices helping preserve key investments



Phone System, when paired with Direct Routing, provides a full enterprise calling experience for Office 365 users in Teams

# How we connect to Office 365 over the Internet



## Corporate Network

Full control  
Full responsibility  
Higher costs for managed  
WAN connections

## Internet

Very limited control  
Can select ISP  
Usually higher BW at lower costs

Corporate Network

This is not what's happening



Internet



## Corporate Network

Full control  
Full responsibility  
Higher costs for managed  
WAN connections

## Internet

Very limited control  
Can select ISP  
Usually higher BW  
at lower costs

## MSFT Network

Zero jitter & loss  
Latency only imposed by  
distance & Speed of light  
Part of Office 365 & Azure

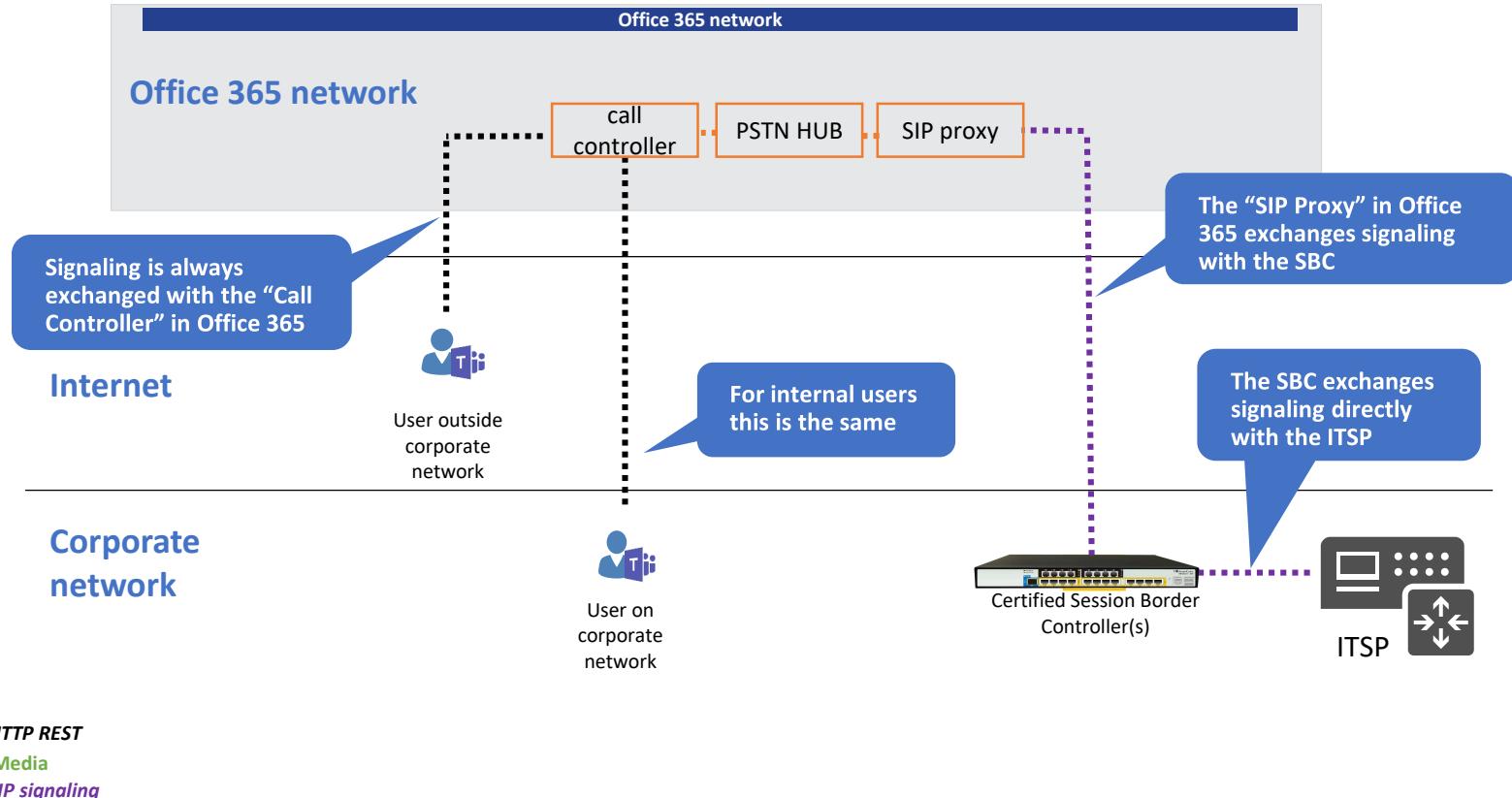
Corporate Network



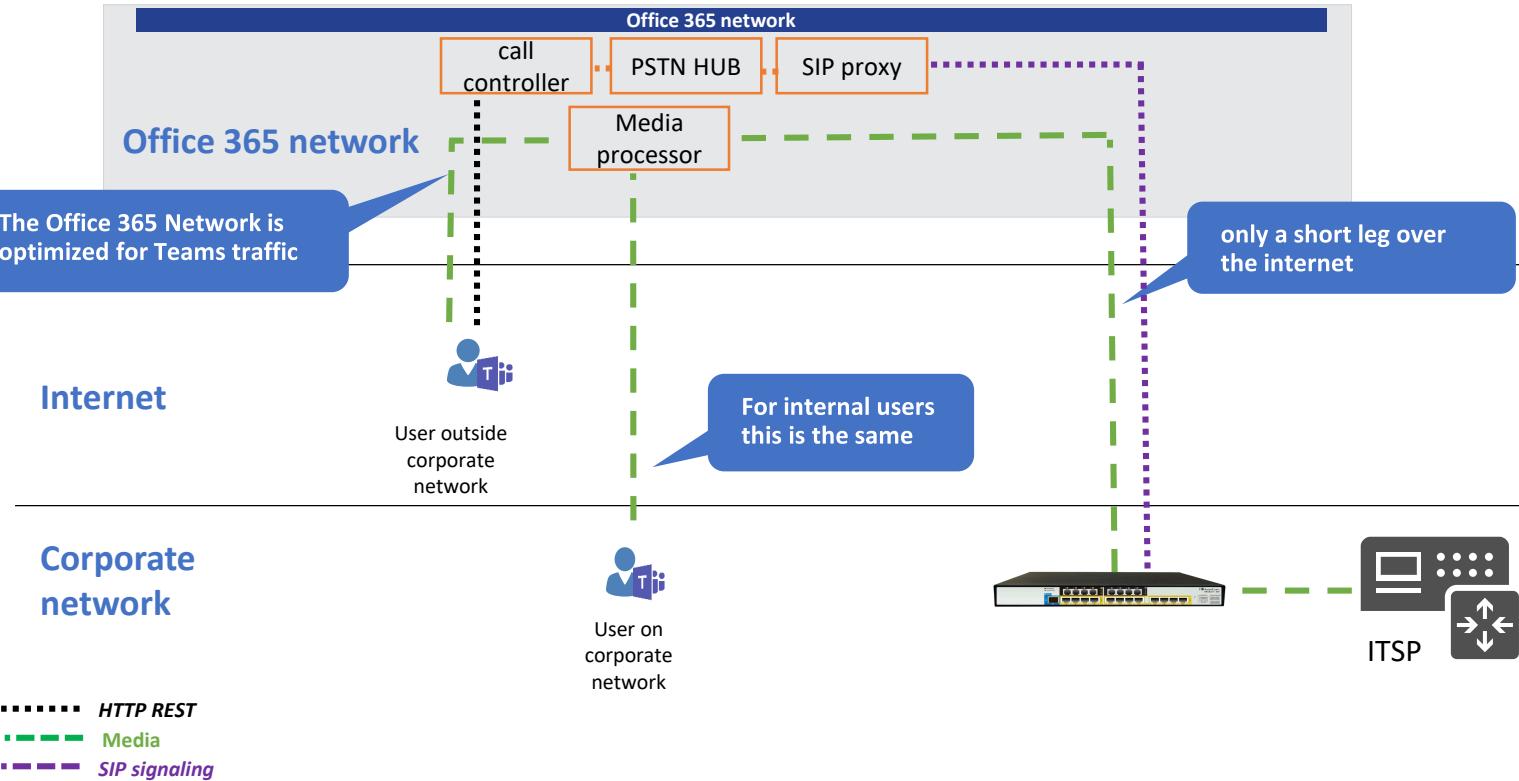
Internet

MSFT Network

# Direct Routing Signaling Path

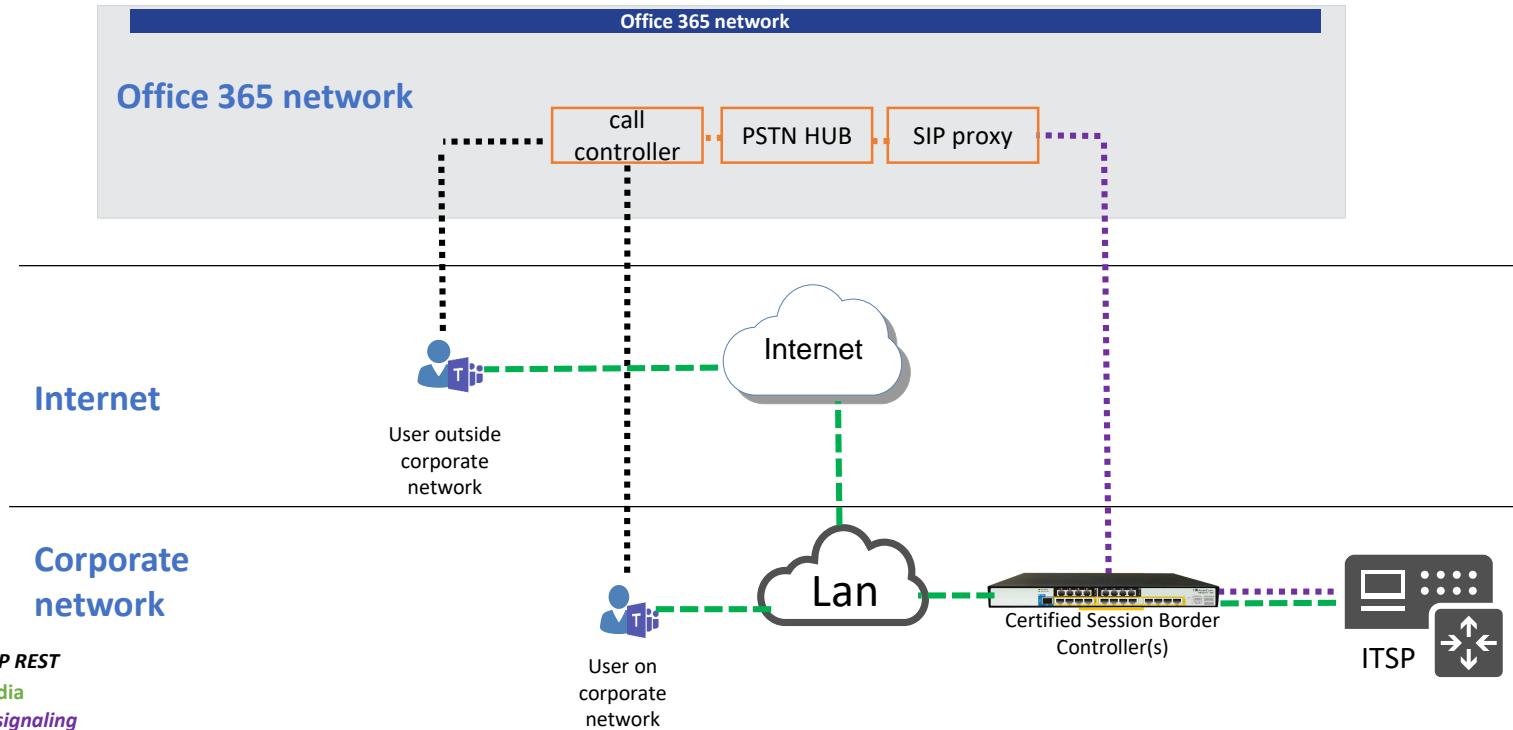


# Teams Direct Media call without Media ByPass



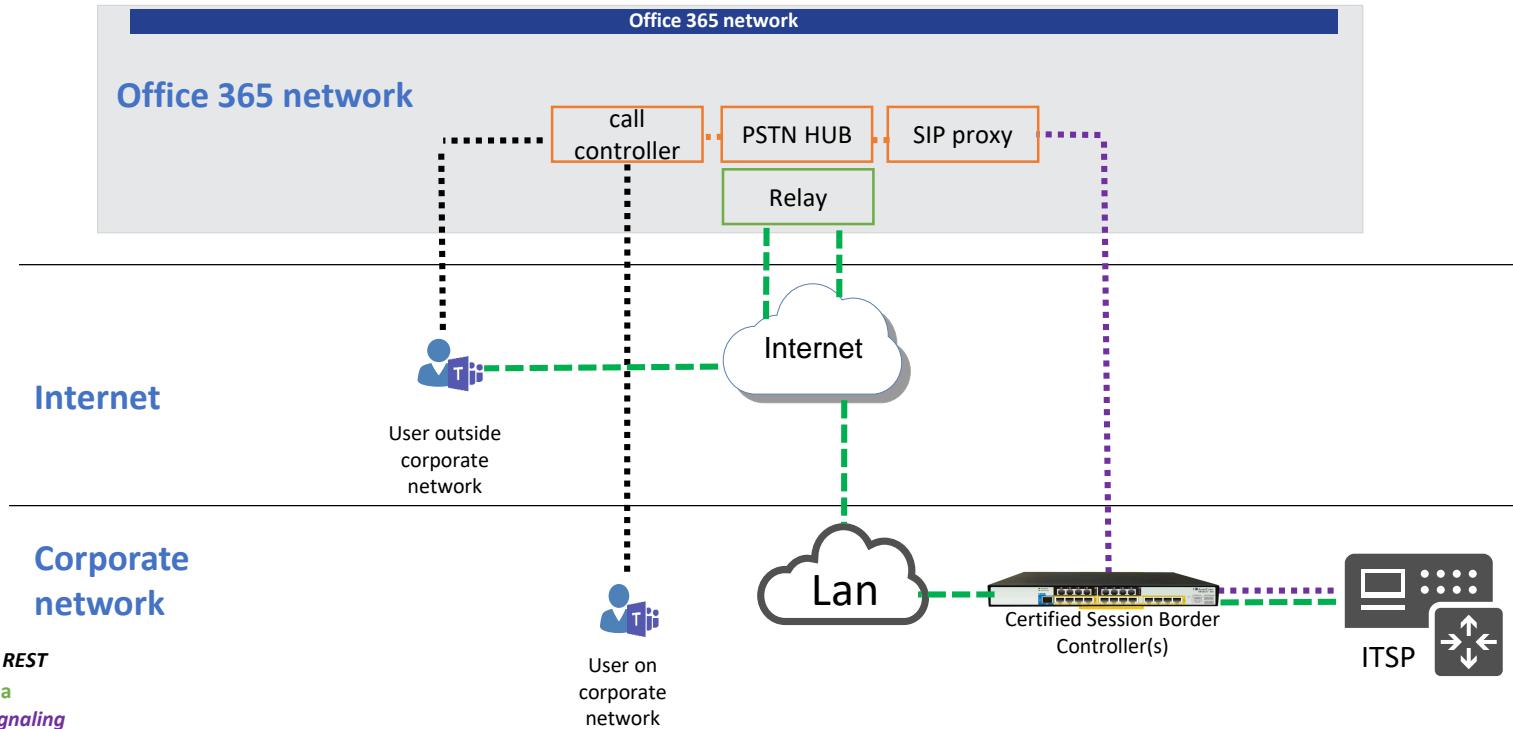
# Teams Direct Media call with Media ByPass (1)

- Client located on customer premises or Customer SBC has a public IP and media ports opened to Internet



# Teams Direct Media call with Media ByPass (2)

- Client located outside of the Customer premises



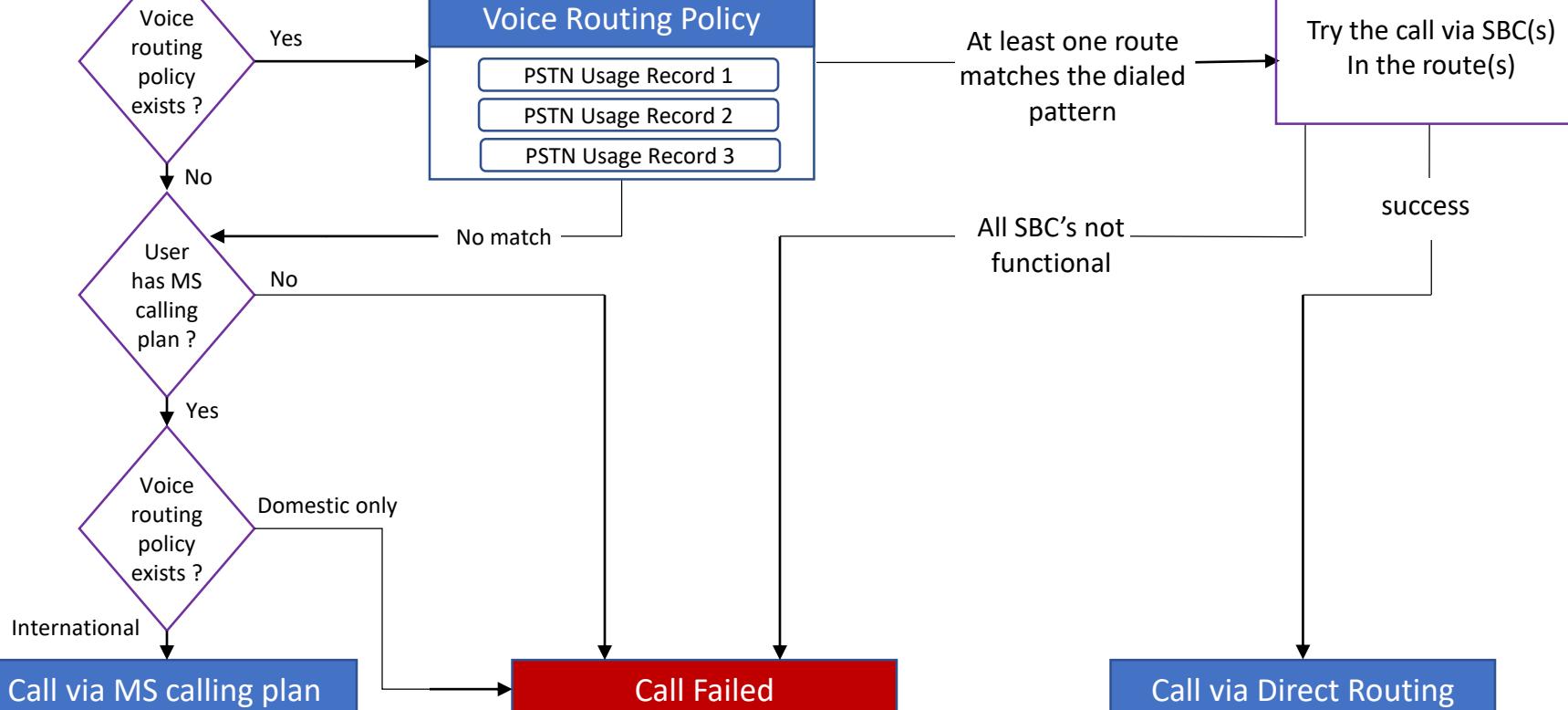
- Normalize phone numbers :
  - PSTN network might expect different phone number than user want to dial
  - Normalize all phone numbers to E.164 format
  - Example :
    - User dial 555 123 4567
    - Normalized number is +1 555 123 4567
    - Dial plan has set of rules for having numbers normalized
  - Teams has a built in rules for the most common normalization rules
  - Custom rules can be build to allow short digit calling
    - E.g. to allow to dial extensions directly

# Voice Routing Basics

User from Germany makes a call to +1 (800) 642-7676



Usage evaluated in order  
Every usage can have multiple routes



Interoperability  
with third-party  
systems

Leverage existing  
contracts with  
service providers

DID for every user

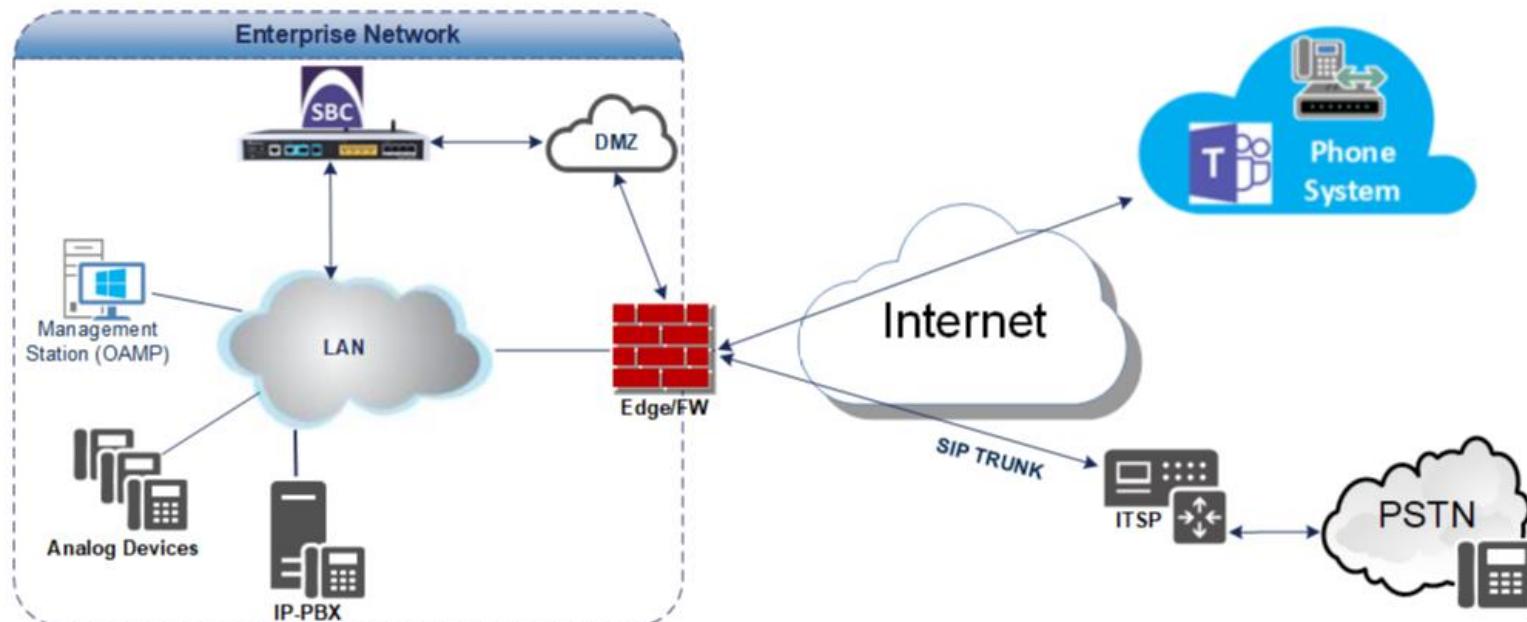
Where Calling  
Plans not available

Can be combined  
with Calling Plans

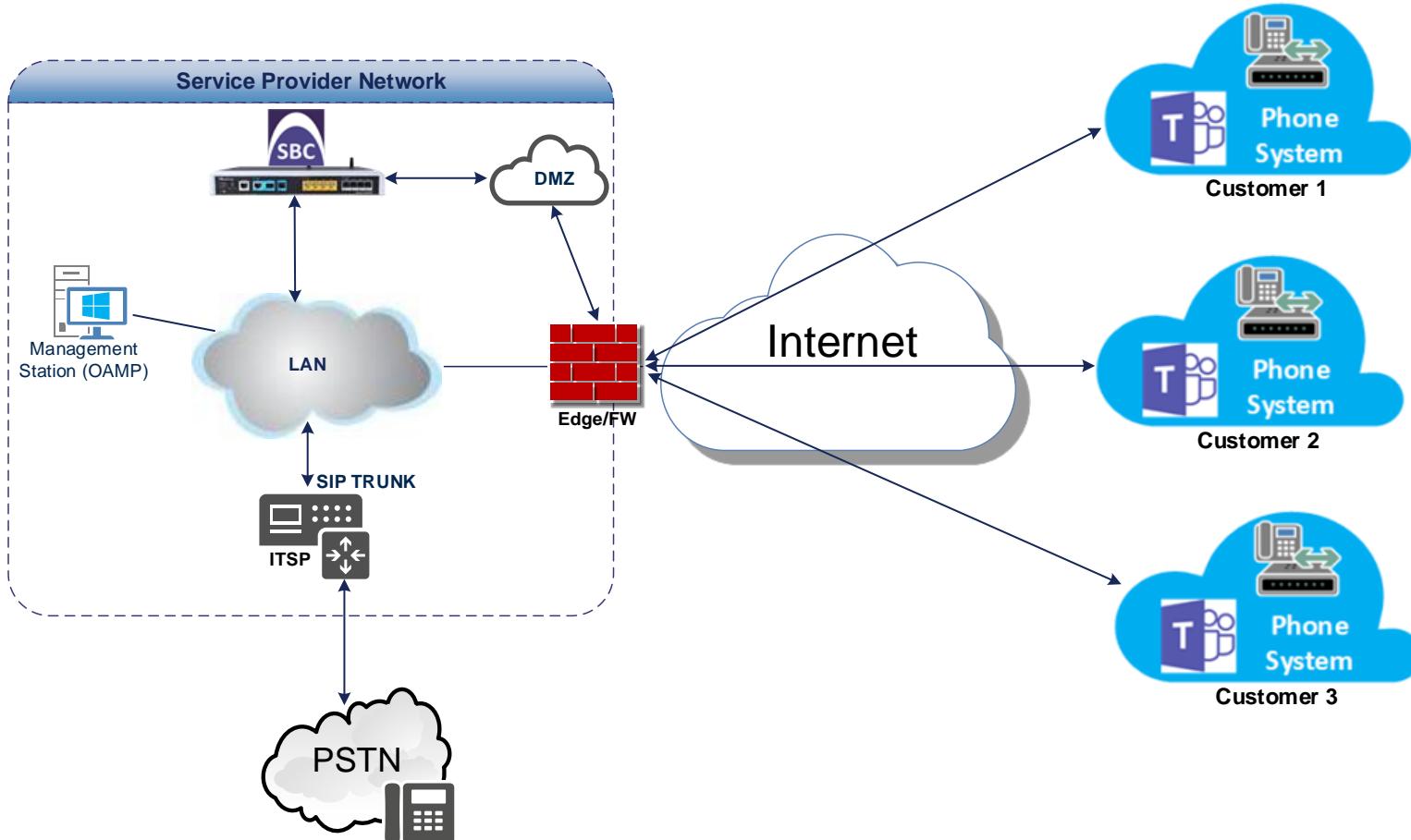
Less Hardware  
Footprint  
(compared to  
Skype for Business)

Skype for Business

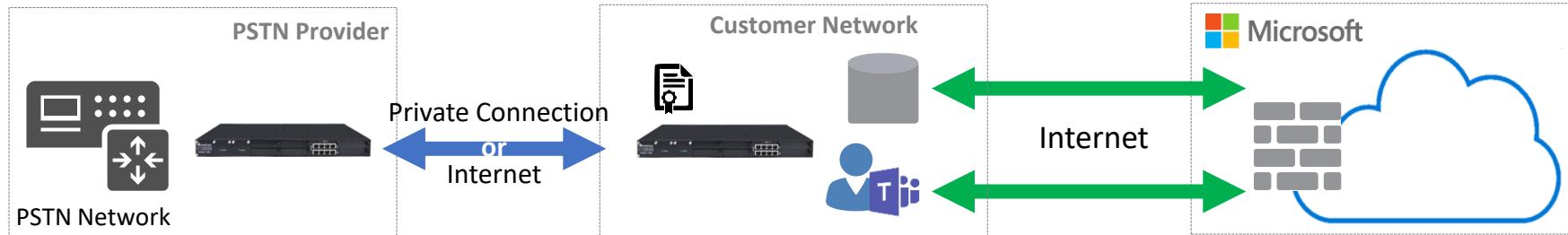
# Direct Routing Enterprise Model



# Direct Routing Hosting Model



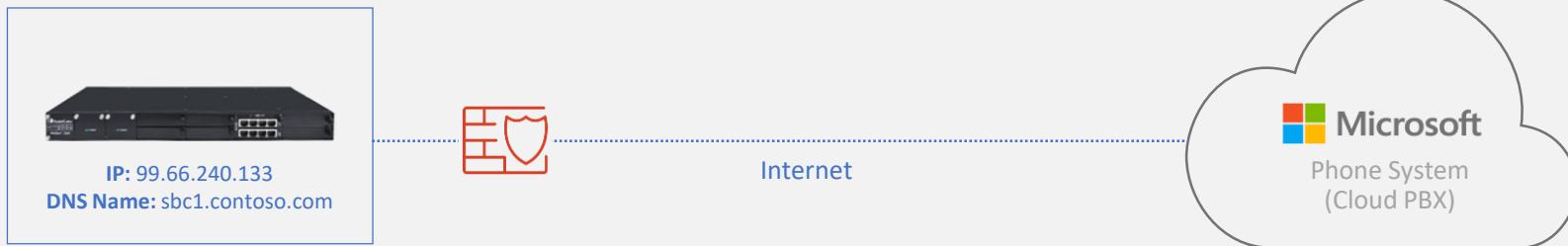
# Direct Routing Solution Components



## Requirements to each involved party:

Carrier	Customer	Microsoft
Telephony Trunk	E5 or E3 + Phone System License	Phone System
Support	Contract with provider or carrier	Teams Clients
GW application as an Option	AudioCodes SBC with Public IP, FQDN, DNS record and Public Trusted Certificate Access to the SBC from Office365 Configuration of the SBC with Office 365 and Carrier Open ports in the corporate firewall for signaling and media to/from Direct Routing	Support Configuration guidelines/documentation

# SBC FQDN Requirements



DNS name registered in  
Office 365 tenant

contoso.onmicrosoft.com

Can be used for SBC FQDN



Examples of FQDNs

Using \*.onmicrosoft.com domains is not supported for SBC names

contoso.com



**Valid names:**

- sbc1.contoso.com;
- ussbcs15.contoso.com;
- europe.contoso.com

**Non-valid name:**

- sbc1.europe.contoso.com (requires registering domain name europe.contoso.com in "Domains" first)

# Add Domain in Office 365

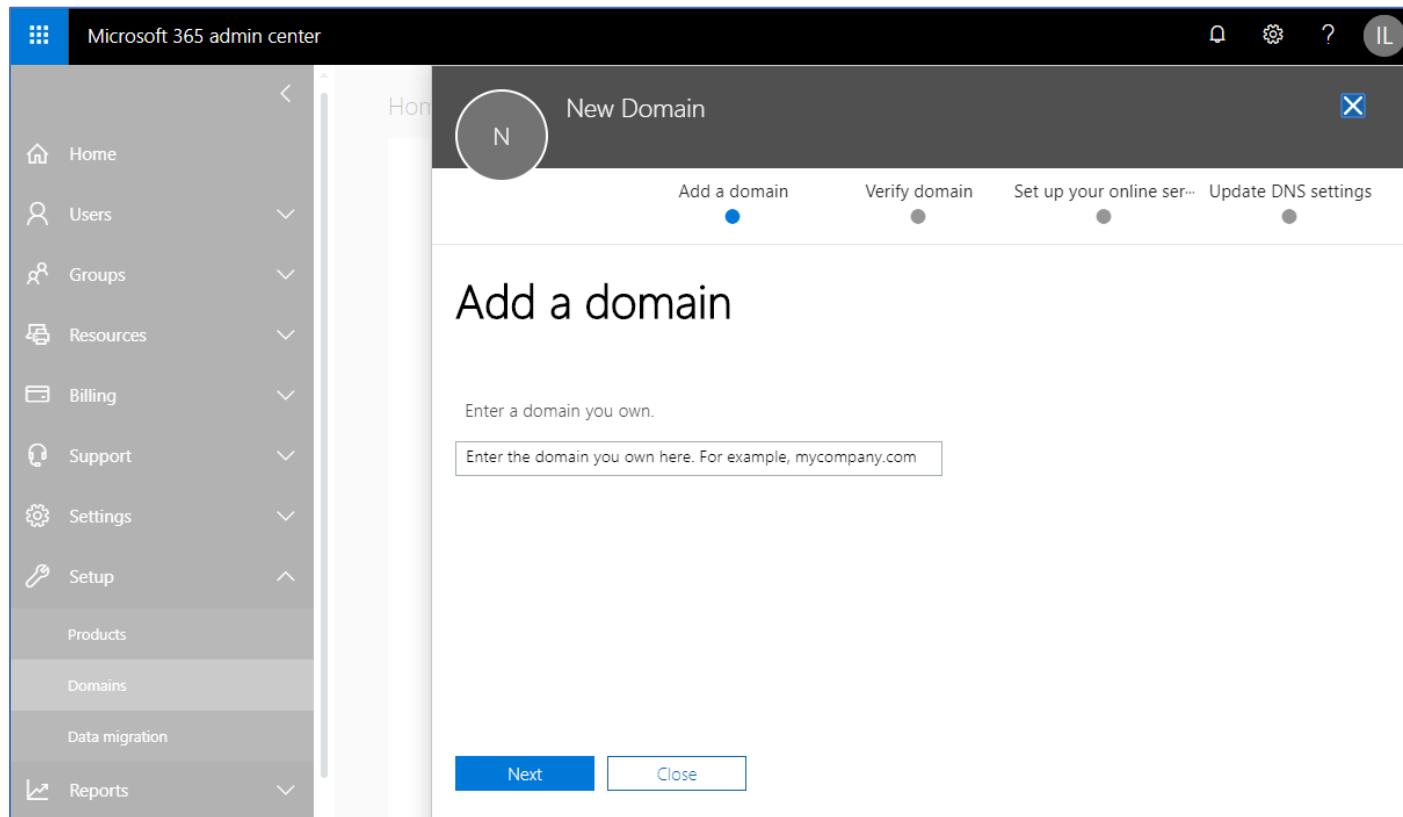
- Login to the Office 365 account as a Tenant Administrator

- Go to the



- On the left menu, click **Setup**, then **Domains**

- Go through wizard for adding new domain



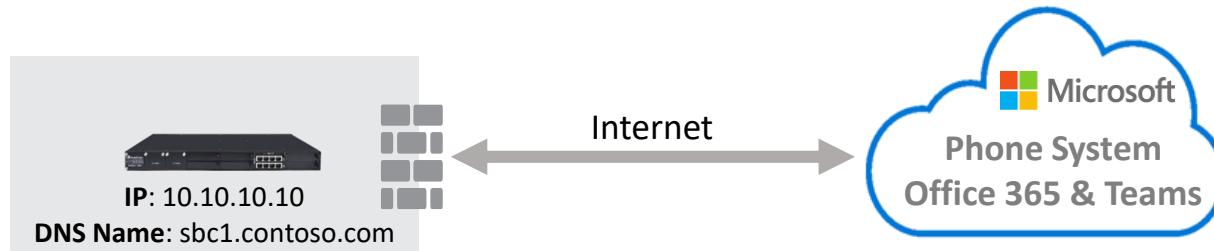
# Public Trusted Certificate for the SBC

- Microsoft strongly recommends that you request the certificate for the SBC by generating a certification signing request (CSR)
- The certificate needs to have the SBC FQDN in the subject, common name (CN), or subject alternate name (SAN) fields
- Alternatively, Direct Routing supports a wildcard in the common name or SAN, and the wildcard needs to conform to standard RFC HTTP Over TLS
  - An example would be using `*.contoso.com` in the SAN, which would match the SBC FQDN `sbc.contoso.com`, but wouldn't match with `sbc.test.contoso.com`

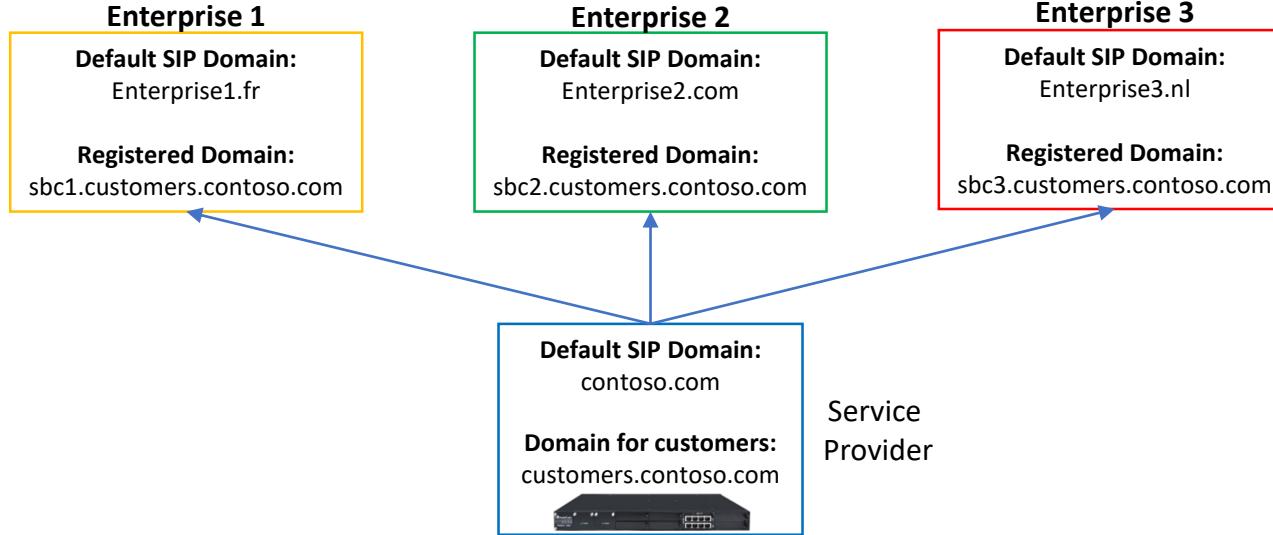
	Scenario <b>Minimize certificate cost</b>	Scenario <b>Balance the cost and security</b>	Scenario <b>Maximize security</b>
<b>Description</b>	This scenario is for companies that want to pair many SBCs or change them frequently	This scenario is good for companies that do not change the gateways frequently. In the example below, a company has four SBCs ( <code>gw1.contoso.com</code> ; <code>gw2.contoso.com</code> ; <code>gw3.contoso.com</code> ; <code>gw4.contoso.com</code> ).	In this scenario the company assigns a certificate to each gateway. There is only one certificate for every gateway.
<b>Subject name</b>	<code>gw1.contoso.com</code>	<code>gw1.contoso.com</code>	<code>gw1.contoso.com</code>
<b>SAN</b>	<code>*.contoso.com</code>	<ul style="list-style-type: none"><li>• <code>gw1.contoso.com</code></li><li>• <code>gw2.contoso.com</code></li><li>• <code>gw3.contoso.com</code></li><li>• <code>gw4.contoso.com</code></li></ul>	<code>gw1.contoso.com</code>

# SBC Domain Names in Enterprise Model

Register and activate subdomain in customer tenant	sbc1.contoso.com
Configure trunk from the Service Provider to the customer tenant	



# SBC Domain Names in Hosting Model

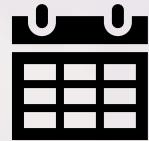


Deploy and configure SBC	
Register domain name in the Service Provider tenant	customers.contoso.com
Request wildcard certificate	*.customers.contoso.com
Register subdomain for every customer	sbc1.customers.contoso.com
Activate domain by adding at least one user with matching SIP address	dummyuser@customers.contoso.com
Use FQDN with customer subdomain for SBC	sbc1.customers.contoso.com



## Lesson 11

# SBC Direct Routing Configuration for Teams



- After completing this lesson you'll :
  - Know the relevant Parameters needed for Teams to SIP trunk configuration
  - Understand the common Microsoft PowerShell configuration commands

# Prerequisites (1)

- Before getting started make sure that the following License Keys exist:

- Teams - enables working with Microsoft Teams
- MediaEncryption, StrongEncryption and EncryptControlProtocol:** enable working with TLS and SRTP
- SBC Sessions:** enables SBC (IP-to-IP) feature

Product Key	Local License Key	Serial Number	Device Type
	49/9/68		/2
GENERAL	Mode	Serial Number	Device Type
High Availability (HA)	SIP	SBC Capacity	
DSP Channels	MGCP	SBC Sessions	Local Actual
IPMedia DSP Channels		Far End Users (FEU)	100 100
60		100	100
60		100	600
SKYPE FOR BUSINESS	VOIP SIGNALING PROTOCOLS	CODERS	
MSEFT	Voice Quality Monitoring	G.723 NETCODER AMR G.729 G.727 G.728	
TEAMS	Test Call	GSM-EFR GSM-FR EVRC QCELP ILBC EVRC-B	
	RTCP-XR	AMR-WB G.722 Enhanced G.711 MS RTA-NB	
	Media Enhancement	MS RTA-WB SILK-NB SILK-WB Speex-NB	
		Speex-WB Opus-NB Opus-WB	
TELEPHONY INTERFACES	VOIP FEATURES	IP MEDIA FEATURES	
E1 Trunks	Voice Quality Monitoring	Conference	
T1 Trunks	Test Call		
2	RTCP-XR		
2	Media Enhancement		
	SECURITY FEATURES		
	IPSec		
	Media Encryption		
	Strong Encryption		
	Encrypt Control Protocol		

- In addition you have the following :
    - Public IP address
    - FQDN name matching SIP addresses of the users
    - Public certificate, issued by one of the MS approved CA's
- 
- ❖ This configuration section will cover only the relevant parts related to Teams direct routing SIP trunk connectivity

- Create and enable new PSTN Gateway :

- *New-CsOnlinePSTNGateway -Identity tr-sbc1.audctrunk.aceducation.info -SipSignallingPort 5061 -Enabled \$True*



- Create new PSTN Usage:

- *Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="Tr-Gr1-PSTNUsage"}*



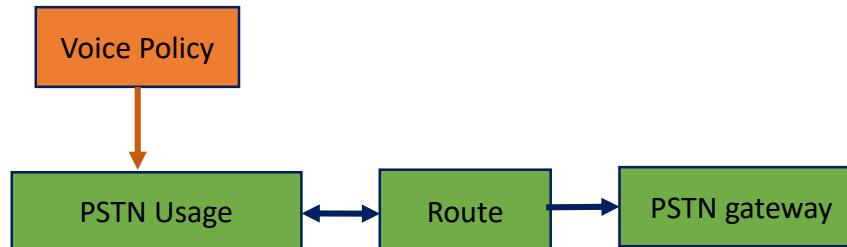
- Create new Voice Route and associated it to PSTN Gateway and PSTN Usage:

- *New-CsOnlineVoiceRoute -Identity Tr-Gr1-VoiceRoute -NumberPattern "\+5555" -OnlinePstnGatewayList tr-sbc1.audctrunk.aceducation.info -Priority 1 -OnlinePstnUsages Tr-Gr1-PSTNUsage*



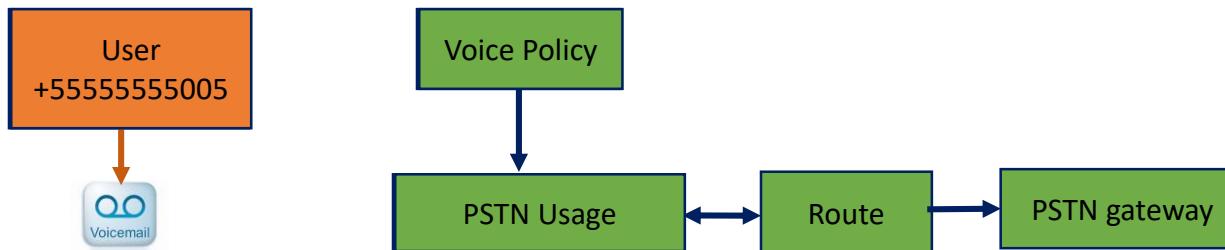
- Assign the Voice Route to PSTN Usage:

- `New-CsOnlineVoiceRoutingPolicy Tr-Gr1-VoiceRoute -OnlinePstnUsages Tr -Gr1PSTNUsage`



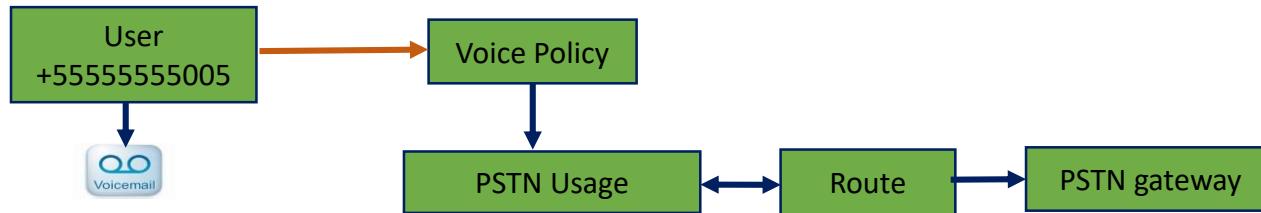
- Enabling user and assigning to it voicemail and a number:

- `Set-CsUser -Identity tr-user1@audio-codes.net -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:+11115551005`



- Assigning the user to the Voice Route:

- *Grant-CsOnlineVoiceRoutingPolicy -PolicyName "Tr-Gr1-VoiceRoute"  
-Identity tr-user1@audio-codes.net*



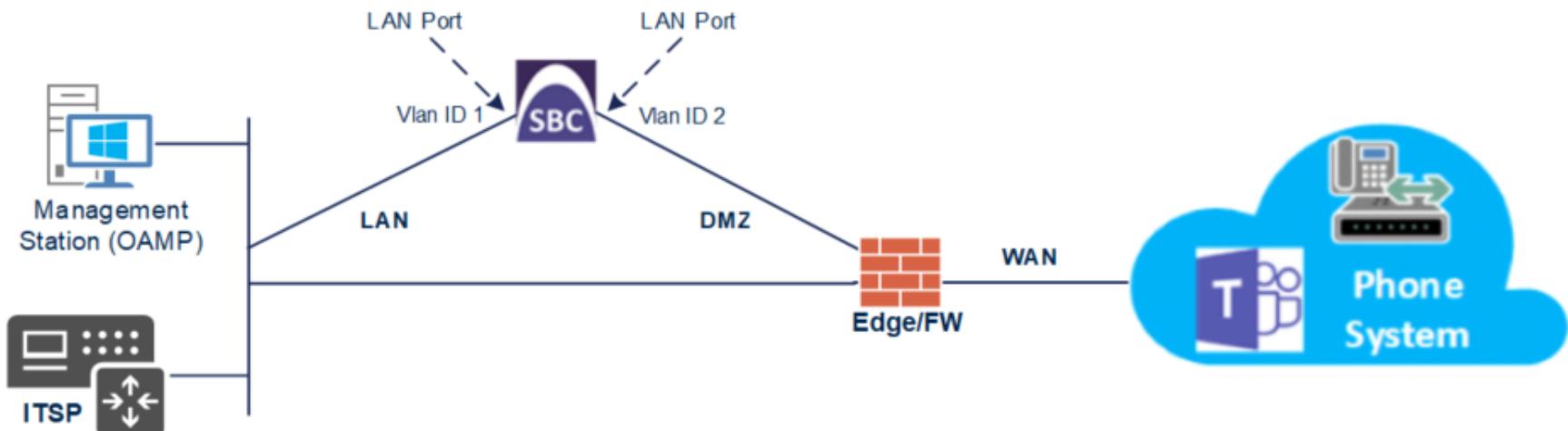
- Use the ***Get-CsOnlinePSTNGateway*** command from the management shell :

```
PS U:\> Get-CsOnlinePSTNGateway -Identity tr-sbc1.audctrunk.aceducation.info

Identity          : tr-sbc1.audctrunk.aceducation.info
Fqdn              : tr-sbc1.audctrunk.aceducation.info
SipSignallingPort : 5061
FailoverTimeSeconds : 10
ForwardCallHistory : False
ForwardPai        : False
SendSipOptions    : True
MaxConcurrentSessions :
Enabled           : True
MediaBypass       : False
GatewaySiteId     :
GatewaySiteLbrEnabled : False
FailoverResponseCodes : 408,503,504
```

# SBC Configuration

- SBC connects to the WAN through a DMZ network



# Configure VLAN's & IP Interface's

- LAN and WAN VLANs configuration

## Ethernet Devices (2)

Ethernet Devices (2)					
+ New	Edit		Page 1 of 1	Show 10 records per page	
INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING	MTU
0	1	GROUP_1	vlan 1	Untagged	1500
1	2	GROUP_2	vlan 2	Untagged	1500

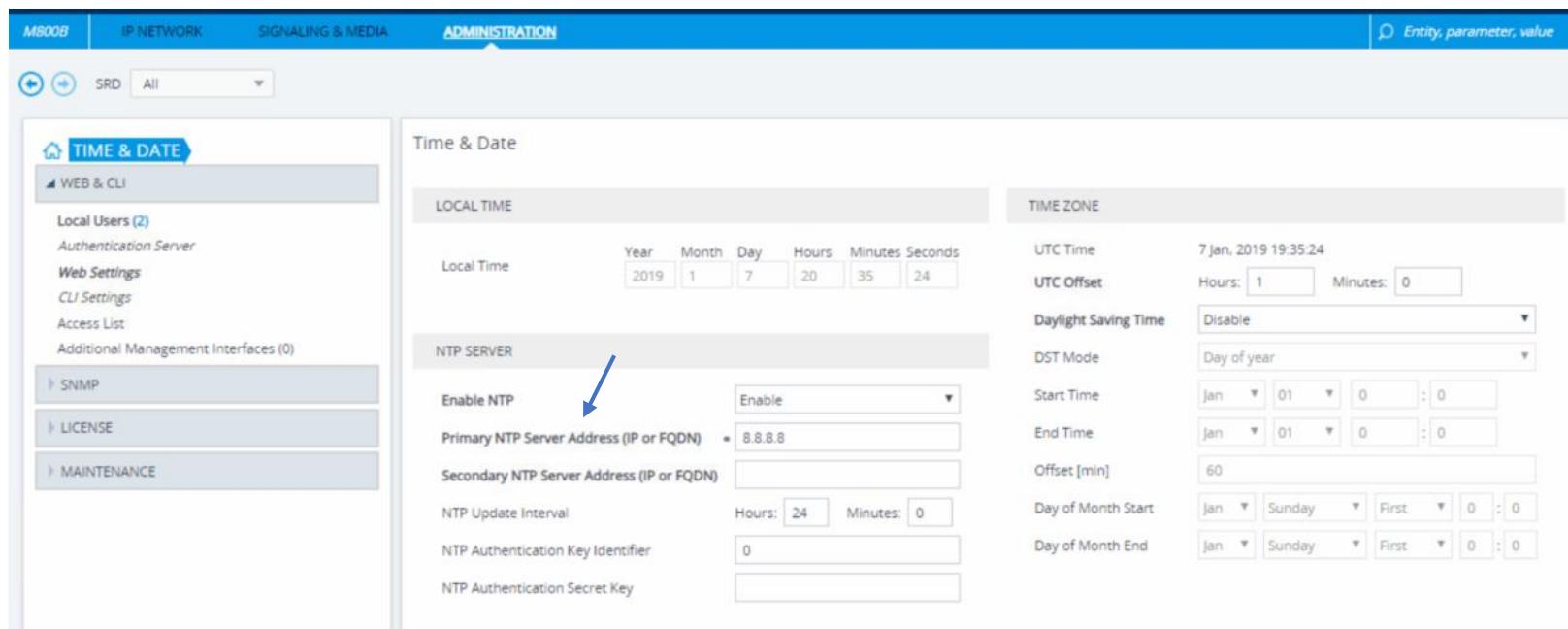
- IP Interface Table

## IP Interfaces (2)

IP Interfaces (2)									
+ New	Edit		Page 1 of 1	Show 10 records per page					
INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	Voice	OAMP + Media + C	IPv4 Manual	10.15.11.1	16	10.15.0.1	10.15.10.1	0.0.0.0	vlan 1
1	DMZ	Media + Control	IPv4 Manual	195.189.192.251	25	195.189.192.129	8.8.8.8	0.0.0.0	vlan 2

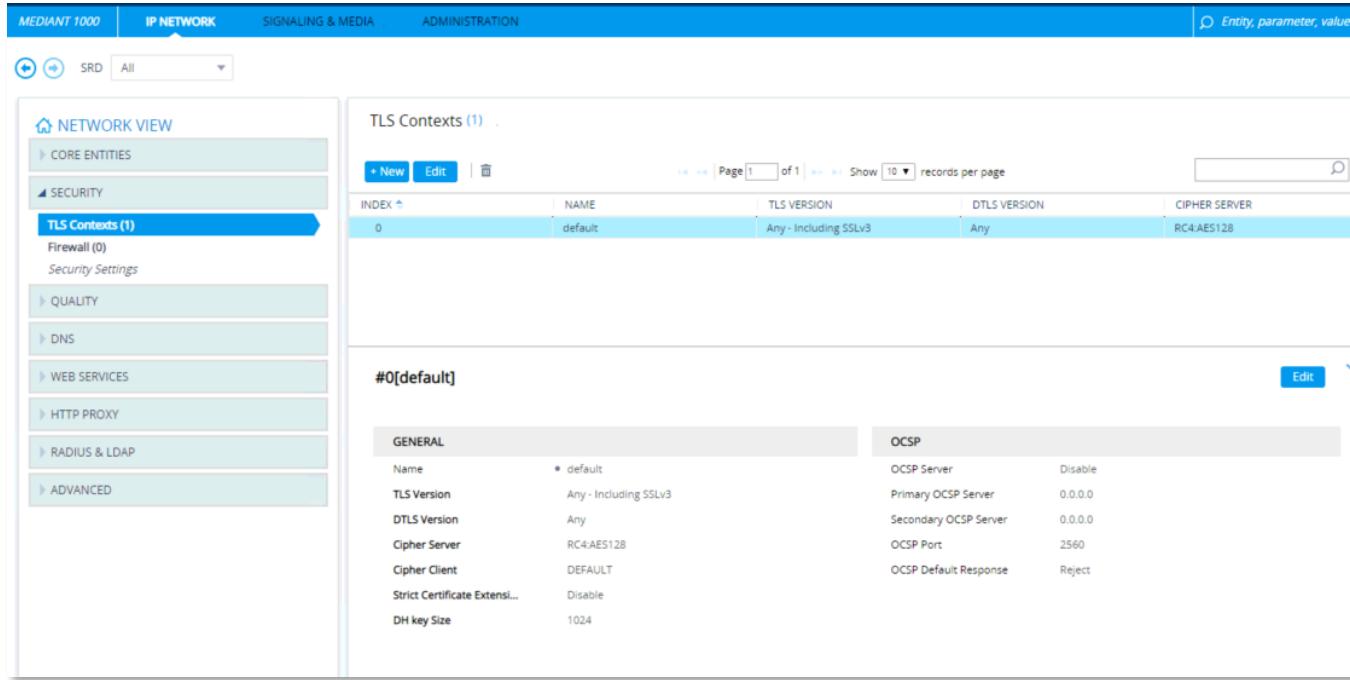
## • Network Time Protocol (NTP)

- Synchronizes the system time to a time source within the network
- Eliminating any potential issues should the local system clock 'drift' during operation
- The client requests a time update from the user-defined



The screenshot shows the 'TIME & DATE' configuration page under the 'ADMINISTRATION' tab. On the left sidebar, 'Local Users (2)' is selected. In the main panel, the 'LOCAL TIME' section shows the current date and time as 2019-01-07 20:35:24. The 'TIME ZONE' section shows UTC Time as 7 Jan, 2019 19:35:24 and UTC Offset as Hours: 1 Minutes: 0. The 'NTP SERVER' section has 'Enable NTP' set to 'Enable' and the 'Primary NTP Server Address (IP or FQDN)' field filled with '8.8.8.8'. Other fields include 'Secondary NTP Server Address (IP or FQDN)', 'NTP Update Interval' (set to 24 hours), 'NTP Authentication Key Identifier' (set to 0), and 'NTP Authentication Secret Key' (empty).

- The TLS Contexts table lets you configure up to 15 TLS certificates
- The device is shipped with a default TLS Context (ID 0 and string name "default")
- The default context can't be deleted



The screenshot shows the MEDIANET 1000 web interface with the following details:

- Top Navigation:** MEDIANET 1000, IP NETWORK, SIGNALING & MEDIA, ADMINISTRATION.
- Left Sidebar:** NETWORK VIEW, CORE ENTITIES, SECURITY (selected), TLS Contexts (1), Firewall (0), Security Settings, QUALITY, DNS, WEB SERVICES, HTTP PROXY, RADIUS & LDAP, ADVANCED.
- Table Header:** TLS Contexts (1). Buttons: New, Edit, Delete. Pagination: Page 1 of 1, Show 10 records per page.
- Table Data:**

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	default	Any - Including SSLv3	Any	RC4:AES128
- Selected Row:** #0[default]. Buttons: Edit, Delete.
- General Tab:** Name: default, TLS Version: Any - Including SSLv3, DTLS Version: Any, Cipher Server: RC4:AES128, Cipher Client: DEFAULT, Strict Certificate Extension: Disable, DH key Size: 1024.
- OCSP Tab:** OCSP Server: Disable, Primary OCSP Server: 0.0.0.0, Secondary OCSP Server: 0.0.0.0, OCSP Port: 2560, OCSP Default Response: Reject.

# Creating TLS Context

- Configuring TLS Context for Teams Direct Routing

TLS Contexts [Teams]

GENERAL		OCSP	
Index	1	OCSP Server	Disable ▾
Name	Teams	Primary OCSP Server	0.0.0.0
TLS Version	TLSv1.2 ▾	Secondary OCSP Server	0.0.0.0
DTLS Version	Any ▾	OCSP Port	2560
Cipher Server	RC4:AES128	OCSP Default Response	Reject ▾
Cipher Client	DEFAULT		
Strict Certificate Extension Validation	Disable ▾		
DH key Size	1024 ▾		

- **The Procedure :**

- Generating a Certificate Signing Request (CSR)
- Requesting Device Certificate from CA
- Obtaining Trusted Root Certificate from CA
- Deploying Device and Trusted Root Certificates on Gateway/E-SBC



# Creating CSR

CERTIFICATE SIGNING REQUEST

Common Name [CN]	<input type="text" value="SBC1.Audctrunk.aceducation.info"/>
1st Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/>
2nd Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/>
3rd Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/>
4th Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/>
5th Subject Alternative Name [SAN]	<input type="text" value="EMAIL"/>
Organizational Unit [OU] (optional)	<input type="text" value="Headquarters"/>
Company name [O] (optional)	<input type="text" value="Corporate"/>
Locality or city name [L] (optional)	<input type="text" value="Poughkeepsie"/>
State [ST] (optional)	<input type="text" value="New York"/>
Country code [C] (optional)	<input type="text" value="US"/>
Signature Algorithm	<input type="text" value="SHA-256"/>

**Create CSR**

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCAb0CAgAwggYnxKDAmBgNVBAMHd1NCQzEuQXVhK3Rydls5rLmFj2wR1Y2F8
alvJLm1uZm8xFTATB8gVBAsMDEh2VhRcdvNydgVyczESMBAGa1UECgqJQ29yG9y
YXN1RRUmEwYDVQQIDaxQb3Vnadt1ZKBzaWUkETAPBnVNBAGKCE5IdyGzB3JPMQSw
CQYDVQQGEwJVUzECAS1wQYJKoZIhvNAQE8BQADggEPADCCAQoCggEBAM/BLfyU
+buVdhS81kgZDrMyJUhQqexuxrbGh/63J0g4cYmcCjplTw2At1zbBLBvKwWfI
uakJE1doCdG2gdzd1Lx7Bv1sByjkNmHvSqjy+1t0fc2q0itnYScIdLzoNLVwx
X7+7yB61q1uPTK1nPy2r18cJHLch+e6zt1gIIVuzu+e6sz58X56LG/D9unCfmY3
Ys0q17wpklUmwu448E570215g7rovLuo7efNeosbjyAvgoRmCaosn8707wza1d
TgPMhybo+1Au8QnbeysBNnsvk0Ag11a8QjXoAeC76LA0V2zzcs8ovr1/hc0AA
Y7+sBr90J+955NC4WeAaaAMAA08CSqGS1b3DQBCwUA4A18AQm/TqqVlUj21B+
9Q1odrs5zkmof6FbxJVQotwE3ggT+p3w++STNg2k9E4V7Ydv9z59jEQpkX12E12
tueHmoKLwc/1Fc1st#1F1Q9sw2115M421lhK0itkgJttx+akU6q+J251f7tabbU
Ka1u90fJ4yqeakYee+Q8qrri2yuVrjqD31dvdOHsdDuyBFrasdFc#0df1zC6/
oYqquks1D9gvFv+1oLex/9gxFn256zoftdrv8c7qw/vkA+YqMawInsoP02X5
o+1W622YYDgJ1EPTJEvhngX2cyerYu1Arb7ctMp0uvyFPcZHjaZZj+cF3wPHQZ
BT3MVvo/
-----END CERTIFICATE REQUEST-----
```

- Uploading the Certificate Obtained from the Certification Authority

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase (optional)

Send Private Key file from your computer to the device.  
The file must be in either PEM or PFX (PKCS#12) format.

No file chosen

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send Device Certificate file from your computer to the device.  
The file must be in textual PEM format.

No file chosen  ←

- Import and verify the certificate details

TLS Context [#1] > Trusted Root Certificates

View Import Export Remove

INDEX	SUBJECT	ISSUER	EXPIRES
0	DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031
1	RapidSSL RSA CA 2018	DigiCert Global Root CA	11/06/2027

Page 1 of 1 10 ▾ View 1 - 2 of 2

**Selected Row #0**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

08:3b:e0:56:90:42:46:b1:a1:75:6a:c9:59:91:c7:4a

Signature Algorithm: sha1WithRSAEncryption

# Device Certificate Information

- Certificate details

 TLS Context [#1] > Certificate Information

**PRIVATE KEY**

Key size: 2048 bits

Status: OK

**CERTIFICATE**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:  
06:d7:22:bc:07:a6:d1:c7:81:a7:c7:b3:d9:b5:3c:ae

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018

Validity

Not Before: May 22 00:00:00 2018 GMT

Not After : May 22 12:00:00 2019 GMT

Subject: CN=\*.audctrunk.aceducation.info

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

- SRV records help with service discovery
- For example, SRV records are used in VoIP to define where a SIP service may be found
- An SRV record typically defines a symbolic name and the transport protocol used as part of the domain name
- It defines the priority, weight, port, and target for the service in the record content
- The SRV RR allows administrators to use several servers for a single domain name

# Internal SRV Table – Old Method

- The Internal SRV table resolves host names to DNS records
- Three different records can be assigned to each host name
- Each record contains

- Priority
- weight
- Port

Parameter	Value
Domain Name	teams.local (FQDN is case-sensitive; configure in line with the configuration of the Teams Proxy Set)
Transport Type	TLS
1st ENTRY	
DNS Name 1	sip.pstnhub.microsoft.com
Priority 1	1
Weight 1	1
Port 1	5061
2nd ENTRY	
DNS Name 2	sip2.pstnhub.microsoft.com
Priority 2	2
Weight 2	1
Port 2	5061
3rd ENTRY	
DNS Name 3	sip3.pstnhub.microsoft.com
Priority 3	3
Weight 3	1
Port 3	5061

# SRV Table Configuration Example – Old Method

Internal SRV (1)

INDEX	DOMAIN NAME	TRANSPORT TYPE	DNS NAME 1	DNS NAME 2	DNS NAME 3
0	teams.local	TLS	sip.pstnhub.microsoft.com	sip2.pstnhub.microsoft.com	sip3.pstnhub.microsoft.com

#0

GENERAL		2ND ENTRY	
Domain Name	* teams.local	DNS Name 2	* sip2.pstnhub.microsoft.com
Transport Type	* TLS	Priority 2	* 2
		Weight 2	* 1
		Port 2	* 5061

1ST ENTRY

DNS Name 1	* sip.pstnhub.microsoft.com
Priority 1	* 1
Weight 1	* 1
Port 1	* 5061

3RD ENTRY

DNS Name 3	* sip3.pstnhub.microsoft.com
Priority 3	* 3
Weight 3	* 1
Port 3	* 5061

# Teams Proxy Set – Old Method

Teams SBC 2    SETUP    MONITOR    TROUBLESHOOT

GROUP-2-VESBC    IP NETWORK    SIGNALING & MEDIA    ADMINISTRATION    Save    Reset    Actions ▾    Admin

Entity, parameter, value

SRD All

TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)**
- IP Groups (2)

CODERS & PROFILES

SBC

- Classification (1)
- Routing
  - Routing Policies (1)
  - IP-to-IP Routing (4)
  - Alternative Reasons Set (0)
  - IP Group Set (0)
- Manipulation
  - SBC General Settings
  - Call Admission Control Profile (0)
  - Malicious Signature (12)
  - External Media Source (0)
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- MEDIA
- INTRUSION DETECTION
- SIP RECORDING

Proxy Sets (2) .

+ New    Edit    Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ITSP	DefaultSRD (#0)	ITSP	60		Disable
1	Teams	DefaultSRD (#0)	Teams	60		Enable

#1[Teams]    DefaultSRD

Edit

GENERAL

Name: Teams

SBC IPV4 SIP Interface: Teams

TLS Context Name: ..

REduNDANCY

Redundancy Mode: Enable

Proxy Hot Swap: Enable

Proxy Load Balancing ...: Random Weights

Min. Active Servers for...: 1

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time ...: 60

Keep-Alive Failure Resp...:

Success Detection Retr...: 1

Success Detection Inte...: 10

Failure Detection Retra...: -1

ADVANCED

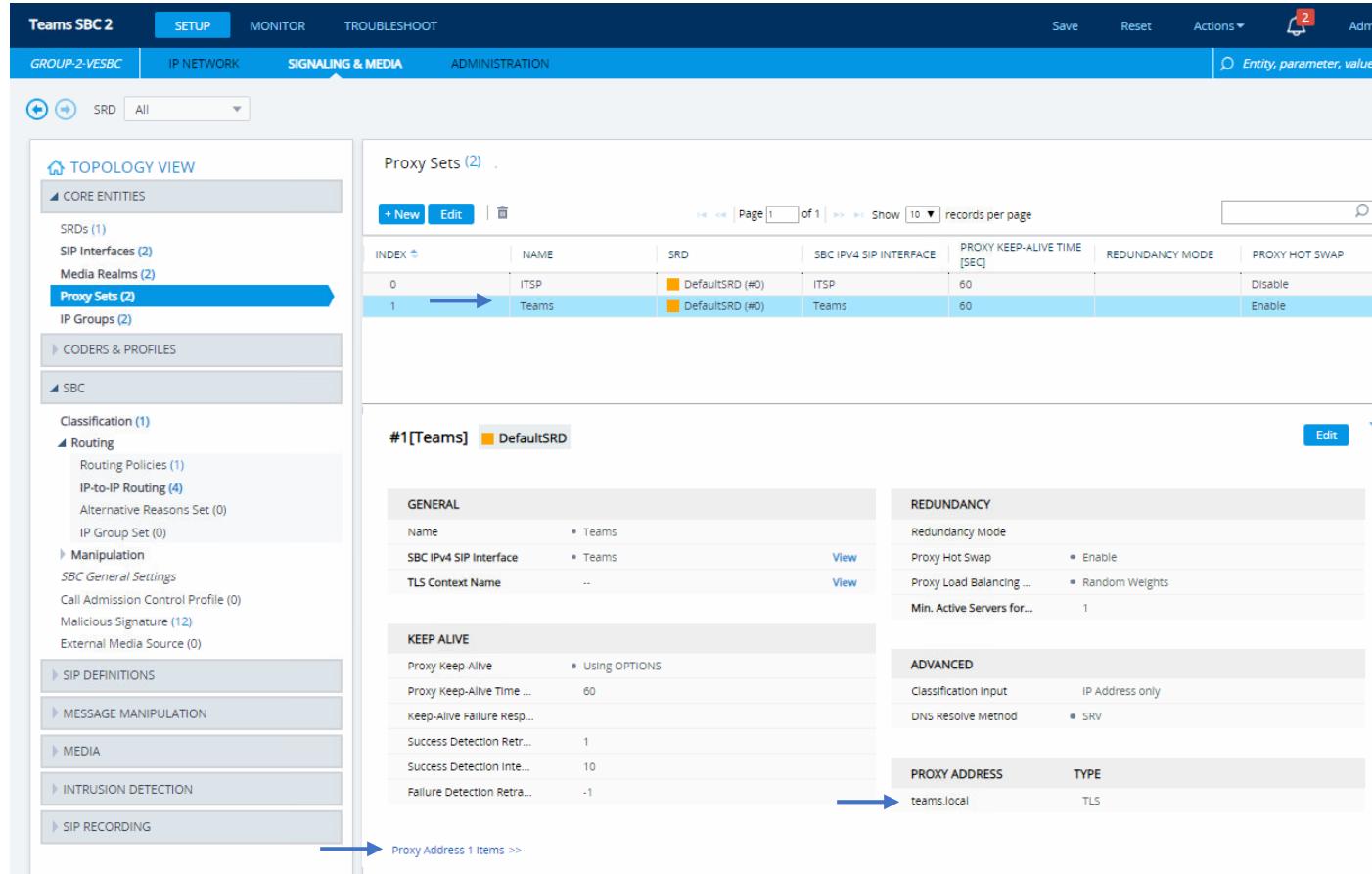
Classification Input: IP Address only

DNS Resolve Method: SRV

PROXY ADDRESS    TYPE

teams.local    TLS

Proxy Address 1 Items >>



# Teams Proxy Address Child Table – Old Method

Teams SBC 2    **SETUP**    MONITOR    TROUBLESHOOT    Save    Reset    Actions ▾    Admin ▾

GROUP-2-VESBC    IP NETWORK    SIGNALING & MEDIA    ADMINISTRATION    Entity, parameter, value

SRD    All

**TOPOLOGY VIEW**

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)**
- IP Groups (2)

CODERS & PROFILES

SBC

Classification (1)

Routing

- Routing Policies (1)
- IP-to-IP Routing (4)
- Alternative Reasons Set (0)
- IP Group Set (0)

Manipulation

SBC General Settings

Call Admission Control Profile (0)

Malicious Signature (12)

**Proxy Sets [#1] > Proxy Address (1)**

+ New    Edit   

Page 1 of 1    Show 10 records per page

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	teams.local	TLS

#0

Edit

GENERAL

Proxy Address	teams.local
Transport Type	TLS
Proxy Priority	0
Proxy Random Weight	0

# Configure Teams Servers in Teams Proxy Set - New

Teams SBC 1    SETUP    MONITOR    TROUBLESHOOT

GROUP-1-VESBC    IP NETWORK    SIGNALING & MEDIA    ADMINISTRATION

Save    Reset    Actions ▾    Admin    Entity, parameter, value

Topology View    CORE ENTITIES    SRD All

Proxy Sets (2)    IP Groups (3)

CODERS & PROFILES    SBC

Classification (1)    Routing (1)    IP-to-IP Routing (4)    Alternative Reasons Set (1)    IP Group Set (0)

Manipulation    SBC General Settings    Call Admission Control Profile (0)    Malicious Signature (12)    External Media Source (0)

SIP DEFINITIONS    MESSAGE MANIPULATION    MEDIA    INTRUSION DETECTION    SIP RECORDING

Proxy Sets (2) .

+ New    Edit    Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ITSP	DefaultSRD (#0)	ITSP	60		Disable
1	Teams	DefaultSRD (#0)	Teams	60		Enable

#1[Teams]    DefaultSRD    Edit

GENERAL

Name	* Teams
SBC IPv4 SIP Interface	* Teams
TLS Context Name	--

REDUNDANCY

Redundancy Mode	
Proxy Hot Swap	Enable
Proxy Load Balancing ...	Random Weights
Min. Active Servers for...	1

KEEP ALIVE

Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time ...	60
Keep-Alive Failure Resp...	
Success Detection Retr...	1
Success Detection Inte...	10
Failure Detection Retra...	-1

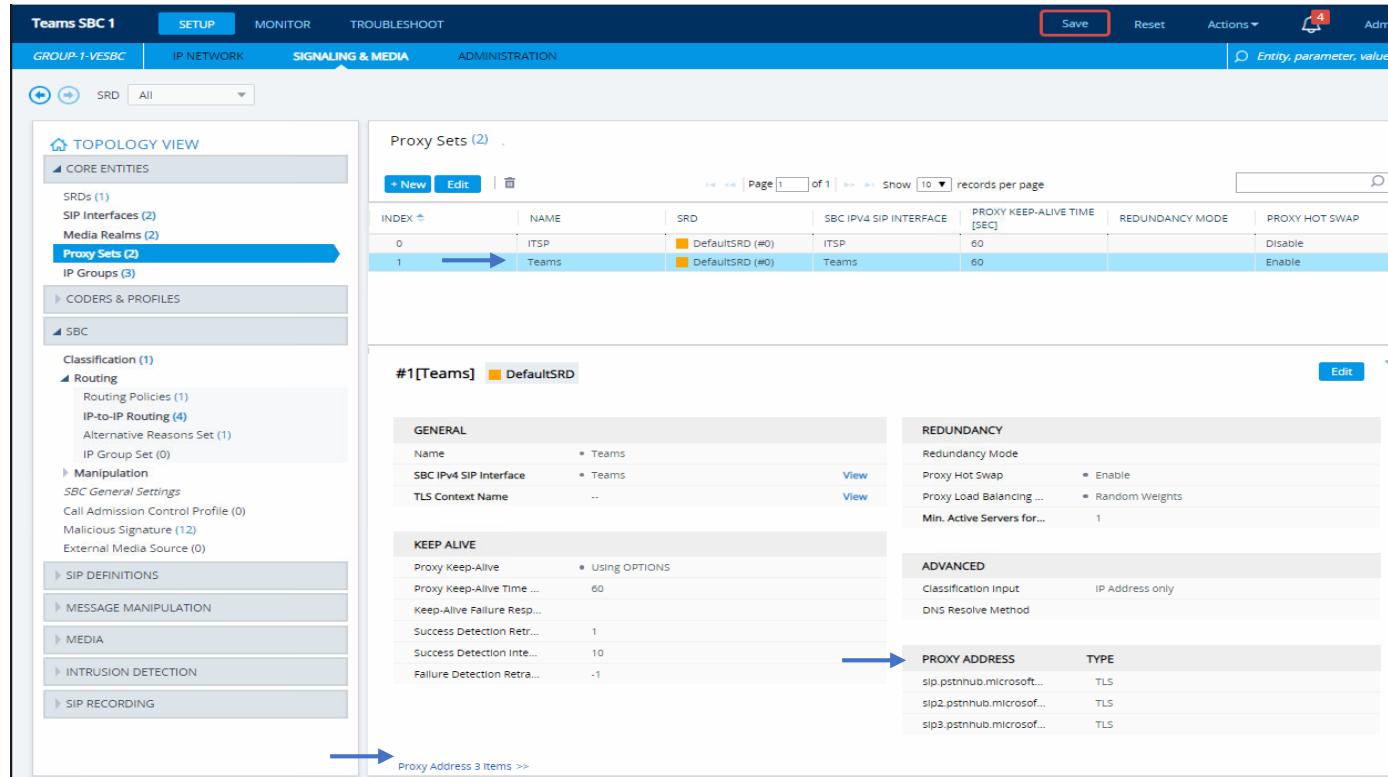
ADVANCED

Classification Input	IP Address only
DNS Resolve Method	

PROXY ADDRESS    TYPE

sip.pstnhub.microsoft...	TLS
sip2.pstnhub.microsoft...	TLS
sip3.pstnhub.microsoft...	TLS

Proxy Address 3 items >>



# Configure Teams Servers in Teams Proxy Set - New

Teams SBC 1    SETUP    MONITOR    TROUBLESHOOT    Save    Reset    Actions ▾    Admin ▾    4

GROUP-1-VESBC    IP NETWORK    SIGNALING & MEDIA    ADMINISTRATION    Entity, parameter, value

SRD All

**TOPOLOGY VIEW**

Core Entities

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)**
- IP Groups (3)

Coders & Profiles

SBC

Classification (1)

Routing

- Routing Policies (1)
- IP-to-IP Routing (4)
- Alternative Reasons Set (1)
- IP Group Set (0)

Manipulation

- SBC General Settings
- Call Admission Control Profile (0)
- Malicious Signature (12)

**Proxy Sets [#1] > Proxy Address (3)**

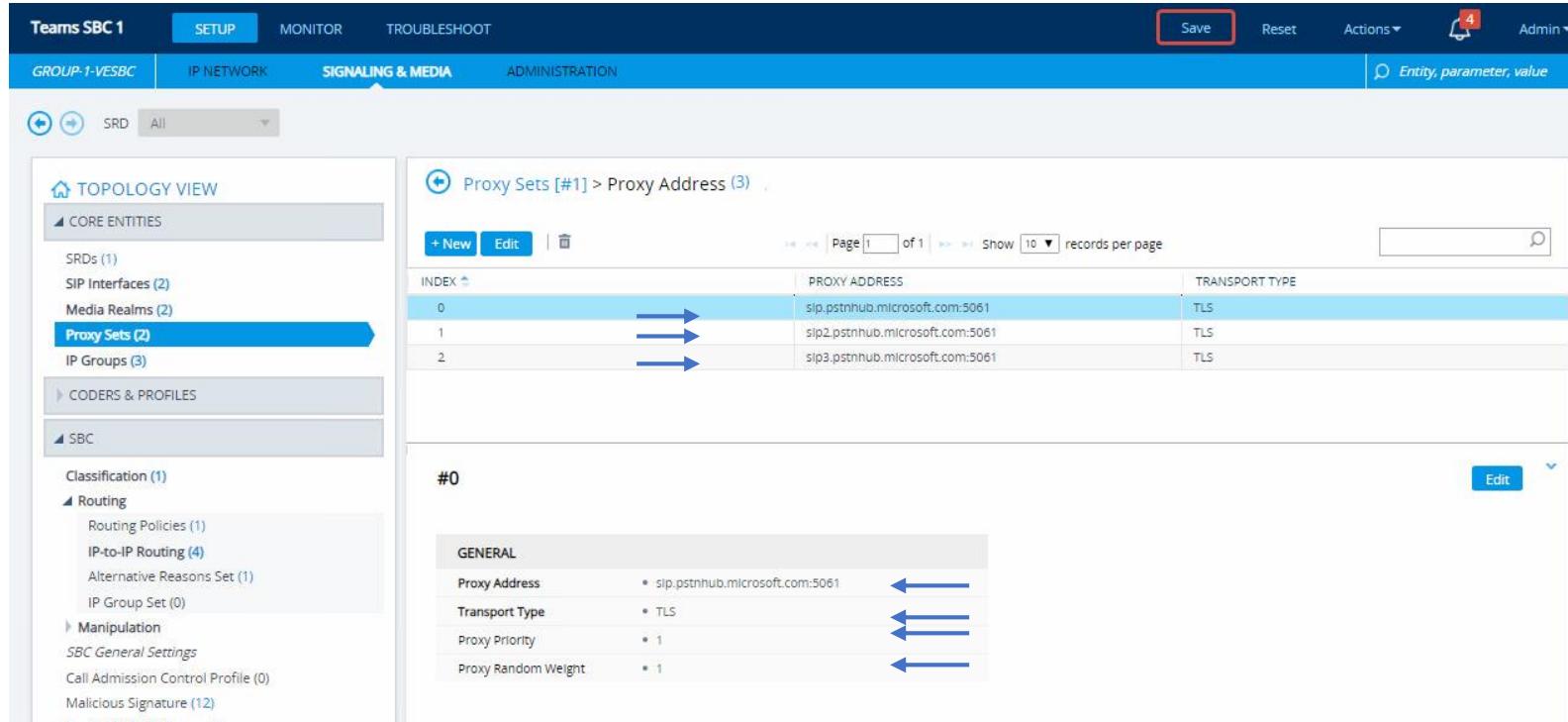
+ New    Edit    Page [ ] of [ ] Show 10 records per page

INDEX	PROXY ADDRESS	TRANSPORT TYPE
0	sip.pstnhub.microsoft.com:5061	TLS
1	sip2.pstnhub.microsoft.com:5061	TLS
2	sip3.pstnhub.microsoft.com:5061	TLS

#0

GENERAL

Proxy Address	* sip.pstnhub.microsoft.com:5061
Transport Type	* TLS
Proxy Priority	* 1
Proxy Random Weight	* 1



The diagram illustrates the configuration flow. It starts with the 'Proxy Sets (2)' entry in the 'Core Entities' section of the left sidebar. A blue arrow points from this entry to the 'Proxy Sets [#1] > Proxy Address (3)' table in the main content area. Another blue arrow points from the 'Proxy Address' row for index #0 to its detailed configuration panel below, specifically the 'Proxy Address' field.

- Microsoft Teams Direct Routing supports the SILK and OPUS coders
- The Coder Group ID for this entity will be assigned to its corresponding IP Profile

Coder Groups

Coder Group Name

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
SILK-NB	▼ 20	▼ 8	76	N/A	▼
SILK-WB	▼ 20	▼ 16	77	N/A	▼
G.711A-law	▼ 20	▼ 64	8	Disabled	▼
G.711U-law	▼ 20	▼ 64	0	Disabled	▼
G.729	▼ 20	▼ 8	18	Disabled	▼
	▼	▼	▼	▼	▼
	▼	▼	▼	▼	▼
	▼	▼	▼	▼	▼
	▼	▼	▼	▼	▼
	▼	▼	▼	▼	▼

Codec	BW/Kbps	Brief Description
G.711	64	Delivers precise speech transmission. It is one of the oldest codecs around (1972) and works best in high bandwidth. It gives a MOS of 4.2
G.729	8	Excellent bandwidth utilization. Error-tolerant.
G.722	48/56/64	Adapts to varying compressions and bandwidth is conserved with network congestion. It captures ranges of frequency twice as large as G.711, resulting in better quality and clarity, close to or even better than with PSTN
SILK	6 to 40	SILK has been developed by Skype and is now licensed out, being available as open-source freeware, which has made many other apps and services to use it. It is a base for the newest codec named Opus. WhatsApp is an example of an app using the Opus codec for voice calls.
OPUS	6 to 510	Opus can handle a wide range of audio applications, including Voice over IP, videoconferencing, in-game chat, and even remote live music performances. It can scale from low bitrate narrowband speech to very high quality stereo music

# Teams & ITSP IP Profiles

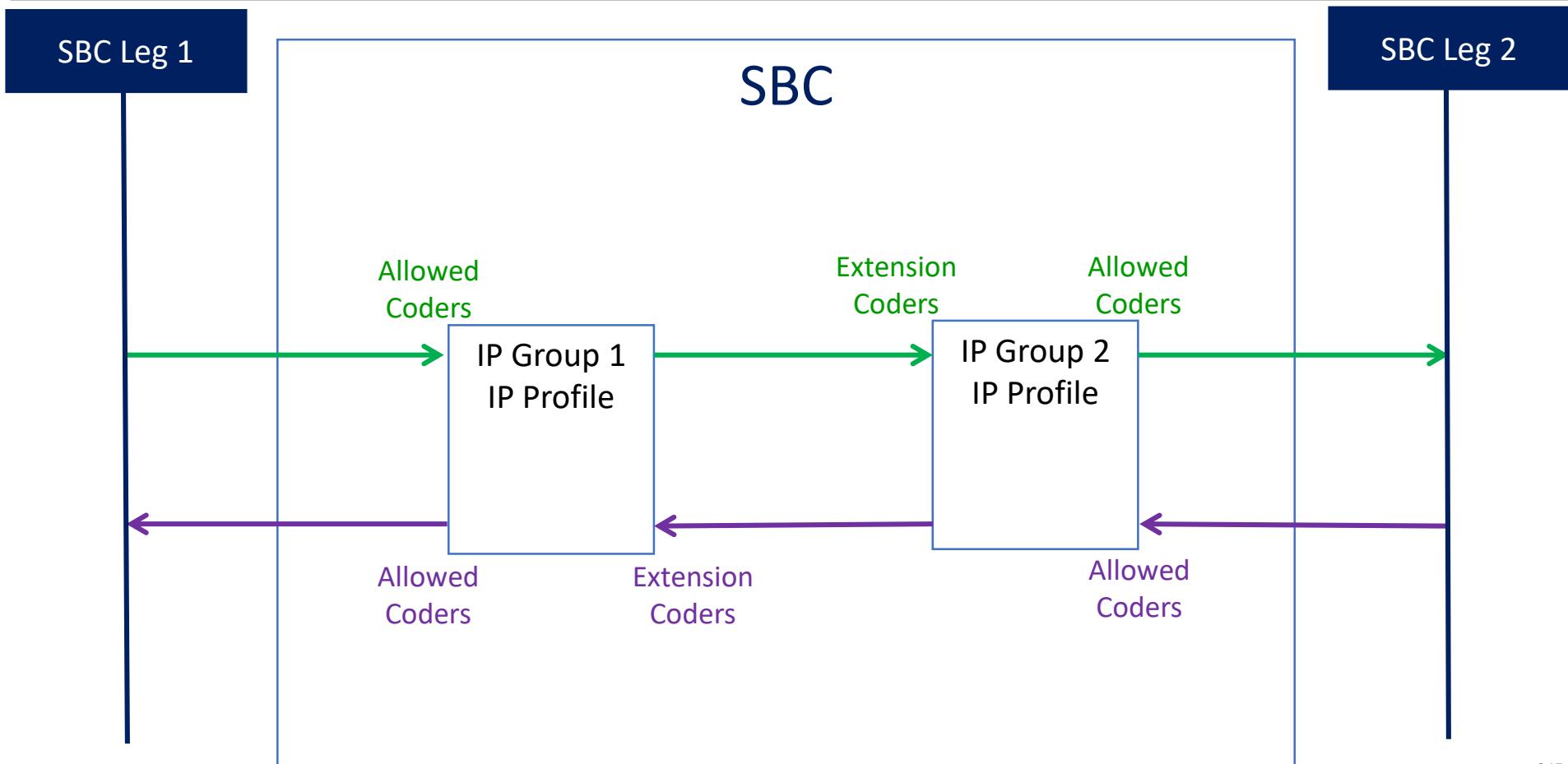
Parameter	Value
<b>Name</b>	<i>Teams (arbitrary descriptive name)</i>
<b>Media Security</b>	
SBC Media Security Mode	SRTP
<b>SBC Early Media</b>	
Remote Early Media RTP Detection Mode	By Media (required, as Microsoft Teams Direct Routing does not send RTP immediately to remote side when it sends a SIP 18x response)
<b>SBC Media</b>	
Extension Coders Group	AudioCodersGroups_1
ICE Mode	Lite (required only when Media Bypass enabled on Microsoft Teams)
<b>SBC Signaling</b>	
Remote Update Support	Not Supported
Remote re-INVITE Support	Supported Only With SDP
Remote Delayed Offer Support	Not Supported
<b>SBC Forward and Transfer</b>	
Remote REFER Mode	Handle Locally
Remote 3xx Mode	Handle Locally
<b>SBC Hold</b>	
Remote Hold Format	Inactive (some SIP Trunk may answer with a=inactive and IP=0.0.0.0 in response to the Re-Invite with Hold request from Teams. Microsoft Media Stack doesn't support this format. So, SBC will replace 0.0.0.0 with its IP address)

Parameter	Value
<b>Name</b>	<i>SIPTrunk</i>
<b>Media Security</b>	
SBC Media Security Mode	RTP
<b>SBC Media</b>	
Allowed Audio Coders	SIPTrunk Allowed Coders
Allowed Coders Mode	Preference (lists Allowed Coders first and then original coders in received SDP offer)
<b>SBC Signaling</b>	
P-Asserted-Identity Header Mode	Add (required for anonymous calls)
<b>SBC Forward and Transfer</b>	
Remote REFER Mode	Handle Locally
Remote Replaces Mode	Handle Locally
Remote 3xx Mode	Handle Locally

- **SBC Media Security Mode = SRTP**
  - Mandatory – SRTP only
- **Remote Early Media RTP Detection Mode = By Media**
  - Teams does not immediately send RTP/SRTP to the remote side if it sends a SIP 18x response
- **RFC 2833 Mode = Extend**
  - Each outgoing offer/answer includes RFC 2833 in the offered SDP
- **Remote Update Support = Not Supported**
  - UPDATE method not supported before and after the call is connected
  - Avoid SDP negotiation before the connect
- **Remote re-INVITE = Supported Only With SDP**
  - Re-INVITE is supported, but only with SDP
  - If the incoming re-INVITE arrives without SDP, the E-SBC creates an SDP and adds it to the outgoing re-INVITE
- **Remote Refer Mode = Handle Locally**
  - Skype for Business does not support receiving SIP REFER messages
  - Incoming REFER request message is handled without forwarding it to the Skype for Business
- **Remote 3xx Mode = Handle Locally**
  - Skype for Business does not support receiving SIP 3xx messages
- **Remote Delayed Offer Support = Not Supported**
  - The E-SBC does not allow INVITE requests without SDP
  - The E-SBC creates an SDP and adds it to the outgoing offer

- **Allowed coders:**
  - Determine coders to be used for a specific SBC leg
  - Excluded coders are removed from the SDP offer
- **Extension codes:**
  - Extends the Media offering's coders
  - Extended coders are added only on the outgoing leg
- **Preference mode Parameter - manipulation options:**
  - Extension coders are added at the end of the coder list (default)
  - Extension coders arranged according to order in the Allowed Coders Group table

# Coder Transcoding Flow



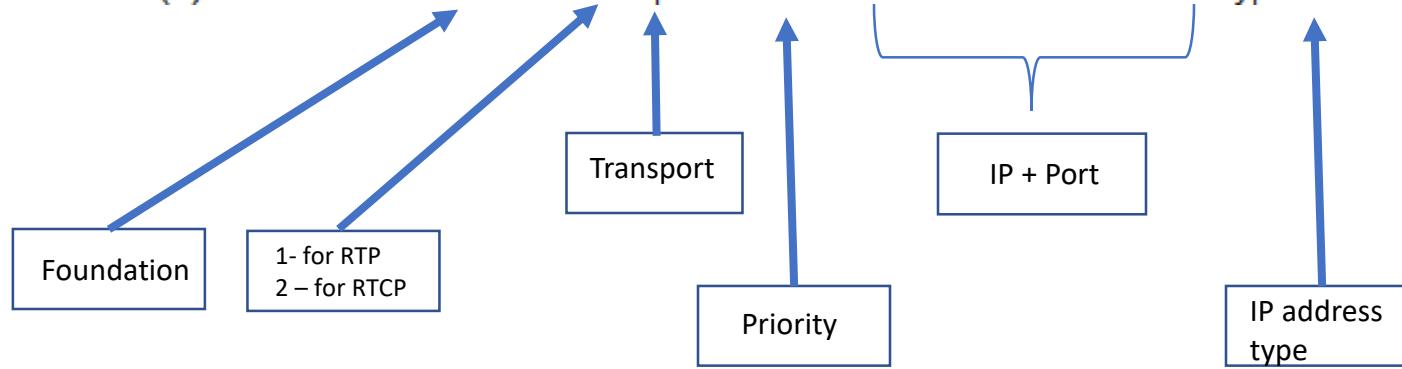
- Typically all devices located behind NAT (home network, office network etc.)
- In order for clients behind NATs and/or firewalls to send media (RTP) between one another, they need to discover each other's IP address and port as seen by the "outside" world
- If both peers are located in different private networks behind a NAT, the peers must coordinate to determine the best communication path between them
- ICE first tries to make a connection using the client's private local address
- If that fails (which it will for clients behind NATs), ICE obtains an external (public) address using a STUN server, and if that fails, traffic is routed through a TURN relay server (which has a public address)

- The SBC is located at the WAN (one leg in the WAN or DMZ) and has global address
- Hence SBC required to implement only ICE Lite
- It supports remote endpoints that initiate ICE to discover their workable public IP address with the device
- Therefore, the device supports the receipt of STUN binding requests for connectivity checks of ICE candidates and responds to them with STUN responses
- Note that in the response to the INVITE message received from the remote endpoint, the device sends only a single candidate for its own IP address
- This is the IP address that the client uses as a remote IP address

- These addresses :ports (local, STUN, TURN and any other network address) of the client are termed "candidates"
- Each client sends its candidates to the other in the SDP body of the INVITE message
- *The ICE and the Candidates list in SDP are the trigger for having the STUN messages initiated*
- Peers then perform connectivity checks per candidate of the other peer, using STUN binding requests sent on the RTP and RTCP ports
- ICE tries each candidate and selects the one that works (i.e., media can flow between the clients)

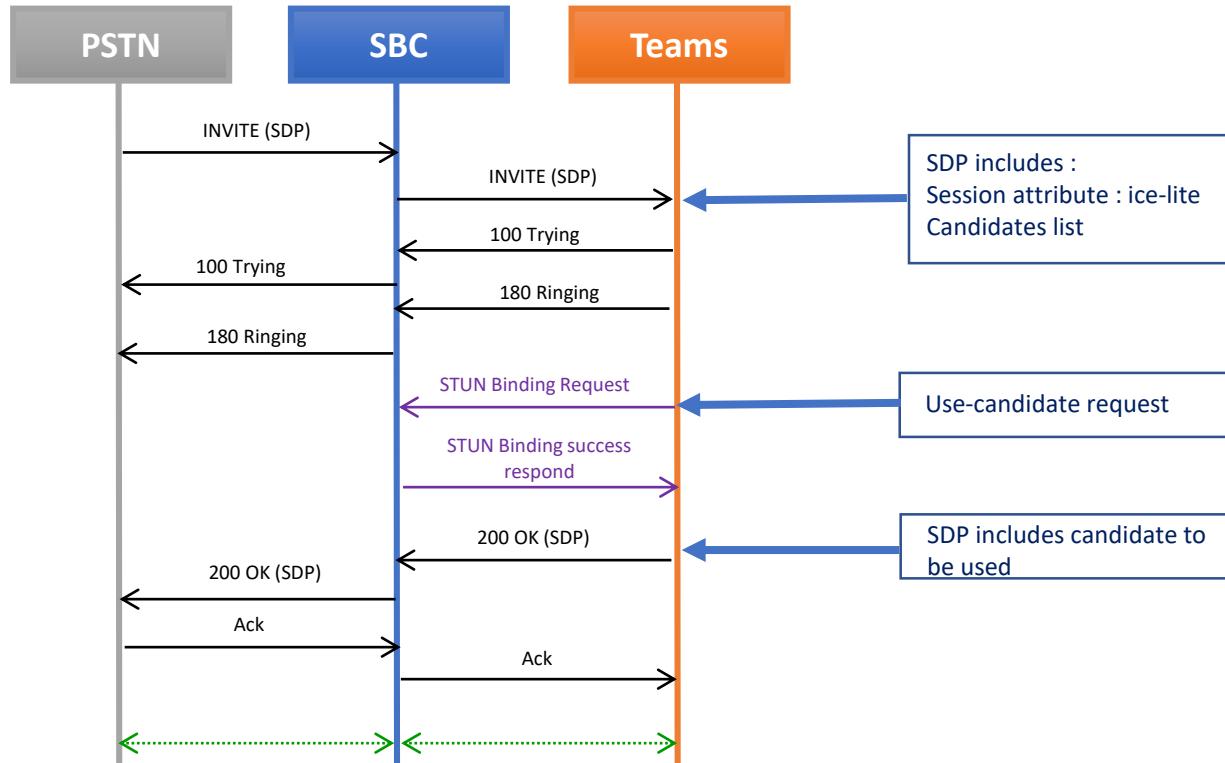
```
> Request-Line: INVITE sip:+11115551005@10.15.10.5 SIP/2.0
> Message Header
< Message Body
  < Session Description Protocol
    Session Description Protocol Version (v): 0
    < Owner/Creator, Session Id (o): 11115551201 817689922 23978012 IN IP4 195.189.192.251
      Session Name (s): Talk
    > Connection Information (c): IN IP4 195.189.192.251
    > Time Description, active time (t): 0 0
    > Session Attribute (a): rtcp-xr:rcvr-rtt=all:10000 stat-summary=loss,dup,jitt,TTL voip-metrics
      Session Attribute (a): ice-lite
    > Media Description, name and address (m): audio 7150 RTP/SAVP 8 0 101
    > Media Attribute (a): rtpmap:101 telephone-event/8000
    > Media Attribute (a): ice-ufrag:hZfvKBWClH4XH7YI
    > Media Attribute (a): ice-pwd:mVUku9Z0WPMIwlEmDM5iafCa
    > Media Attribute (a): candidate:1602914086 1 udp 2130706431 195.189.192.251 7150 typ host
    > Media Attribute (a): candidate:1602914086 2 udp 2130706430 195.189.192.251 7151 typ host
    > Media Attribute (a): crypto:1 AES_CM_128_HMAC_SHA1_80 inline:/D8HQhMiqwLwsk+AN0B6tH/fS4dJK2CW97xPwzZQ|2^31
    > Media Attribute (a): crypto:2 AES_CM_128_HMAC_SHA1_32 inline:+gM4Evw+WDxE/o0UGLSFZrf6u7ezGL25C6tqw1YZ|2^31
    > Media Attribute (a): crypto:3 AES_256_CM_HMAC_SHA1_80 inline:TVoFCvpstpH6HRHZA4EfnpqYpQ2ssrhTRLcYApir/MYo+LxqfXORFmxan/xucpq|2^31
    > Media Attribute (a): crypto:4 AES_256_CM_HMAC_SHA1_32 inline:qZVGImKG0xujpUuIQJ8vRm0zDGET3Yp9zjHmjQJq7BBF1fspuggFydZn28j5E|2^31
```

- > Media Attribute (a): candidate:1602914086 1 udp 2130706431 195.189.192.251 7150 typ host
- > Media Attribute (a): candidate:1602914086 2 udp 2130706430 195.189.192.251 7151 typ host



- A STUN (Session Traversal of User Datagram Protocol [UDP] Through Network Address Translators [NATs]) server allows NAT clients (i.e. IP Phones behind a firewall) to setup phone calls to a VoIP provider hosted outside of the local network
- The STUN server allows clients to find out their public address, the type of NAT they are behind and the Internet side port associated by the NAT with a particular local port
- This information is used to set up UDP communication between the client and the VoIP provider to establish a call

# Generic call flow from PSTN to Teams



## SBC → Teams

```
✓ Session Initiation Protocol (INVITE)
  > Request-Line: INVITE sip:+11115551005@10.15.10.5 SIP/2.0
  > Message Header
  ✓ Message Body
    ✓ Session Description Protocol
      Session Description Protocol Version (v): 0
      > Owner/Creator, Session Id (o): 11115551201 817689922 23978012 IN IP4 195.189.192.251
      Session Name (s): Talk
      > Connection Information (c): IN IP4 195.189.192.251
      > Time Description, active time (t): 0 0
      > Session Attribute (a): rtcp-xr:rcvr-rtt=all:10000 stat-summary=loss,dup,jitt,TTL voip-metrics
      Session Attribute (a): ice-lite ←
      > Media Description, name and address (m): audio 7150 RTP/SAVP 8 0 101
      > Media Attribute (a): rtpmap:101 telephone-event/8000
      > Media Attribute (a): ice-ufrag:hZfvKBWClH4XH7YI
      > Media Attribute (a): ice-pwd:mVUku9Z0WPMIwlEmDM5iafCa
      > Media Attribute (a): candidate:1602914086 1 udp 2130706431 195.189.192.251 7150 typ host ←
      > Media Attribute (a): candidate:1602914086 2 udp 2130706430 195.189.192.251 7151 typ host ←
      > Media Attribute (a): crypto:1 AES_CM_128_HMAC_SHA1_80 inline:/D8HQhMiqwLwsk+AN0B6tH/fS4dJK2CW97xPwzzQ|2^31
      > Media Attribute (a): crypto:2 AES_CM_128_HMAC_SHA1_32 inline:+gM4Evw+WDxE/o0UGLSFZrf6u7ezGL25C6tqw1YZ|2^31
      > Media Attribute (a): crypto:3 AES_256_CM_HMAC_SHA1_80 inline:TvoFCvpstph6HRHZA4EfnpqYpQ2ssrhTRLcYApI/MYo+LxqfXORFmxan/xucpq|2^31
      > Media Attribute (a): crypto:4 AES_256_CM_HMAC_SHA1_32 inline:qZVGIwMKGOxujpUuIQJ8vRm0zDGET3Yp9zjHmjQJq7BBF1fspuggFydZn28j5E|2^31
```

Teams → SBC

Session Traversal Utilities for NAT  
[Response In: 372]

Message Type: 0x0001 (Binding Request) ←

..... 0 ..... = Message Class: 0x00 Request (0)  
..00 000. 000. 0001 = Message Method: 0x0001 Binding (0x001)  
..0. ..... .... .... = Message Method Assignment: IETF Review (0x0000)

Message Length: 100  
Message Cookie: 2112a442  
Message Transaction ID: 16837ebe97ab47e0fc5fc0f2

Attributes

- USERNAME: hZfvKBWC1H4XH7YI:Xp3g
- ICE-CONTROLLING
- MS-IMPLEMENTATION-VERSION: Unknown (0x7)
- Unknown
- USE-CANDIDATE ←
- PRIORITY
- MESSAGE-INTEGRITY
- FINGERPRINT

Data (157 bytes)

Data: 095d7d88d81fab0000013400000134001402094bfc381700...  
[Length: 157]

## SBC → Teams

```
Session Traversal Utilities for NAT
[Request In: 371]
[Time: 0.000003000 seconds]
Message Type: 0x0101 (Binding Success Response) ←
.... ....1 ...0 .... = Message Class: 0x10 Success Response (2)
..00 000. 000. 0001 = Message Method: 0x0001 Binding (0x001)
..0. .... ..... .... = Message Method Assignment: IETF Review (0x0)
Message Length: 44
Message Cookie: 2112a442
Message Transaction ID: 16837ebe97ab47e0fc5fc0f2
Attributes
> XOR-MAPPED-ADDRESS: 52.114.116.53:50491 ←
> MESSAGE-INTEGRITY
> FINGERPRINT
Data (101 bytes)
Data: 095d7d88f61fac0000013400000134001502094bfc381700...
[Length: 101]
```

Teams → SBC



•	514	27.124736	52.114.75.24	195.189.192.251	SIP/SDP	229 Status: 200 OK   , DrSeq=8248, SrcID=-1
<ul style="list-style-type: none"><li>&gt; Message Header</li><li>Message Body<ul style="list-style-type: none"><li>Session Description Protocol<ul style="list-style-type: none"><li>Session Description Protocol Version (v): 0</li><li>Owner/Creator, Session Id (o): - 43994 1 IN IP4 127.0.0.1</li><li>Session Name (s): session</li><li>Connection Information (c): IN IP4 52.114.116.53</li><li>Bandwidth Information (b): CT:10000000</li><li>Time Description, active time (t): 0 0</li><li>Media Description, name and address (m): audio 50490 RTP/SAVP 8 0 101</li><li>Connection Information (c): IN IP4 52.114.116.53</li><li>Media Attribute (a): rtcp:50491</li><li>Media Attribute (a): ice-ufrag:Xp3g</li><li>Media Attribute (a): ice-pwd:G5gX2h/PQAZ2b+0j/RL3oxL7</li><li>Media Attribute (a): candidate:1 1 UDP 2130706431 52.114.116.53 50490 typ srflx raddr 10.0.0.29 rport 50490 ←</li><li>Media Attribute (a): candidate:1 2 UDP 2130705918 52.114.116.53 50491 typ srflx raddr 10.0.0.29 rport 50491</li><li>Media Attribute (a): candidate:2 1 tcp-act 2121006078 52.114.116.53 49152 typ srflx raddr 10.0.0.29 rport 49152</li><li>Media Attribute (a): candidate:2 2 tcp-act 2121006078 52.114.116.53 49152 typ srflx raddr 10.0.0.29 rport 49152</li><li>Media Attribute (a): label:main-audio</li><li>Media Attribute (a): crypto:1 AES_CM_128_HMAC_SHA1_80 inline:R2IkrwsOUCZ0GrQE+jmBuRCqP8McJqt4DIy1Ii06 2^31</li><li>Media Attribute (a): sendrecv</li><li>Media Attribute (a): rtpmap:8 PCMA/8000</li><li>Media Attribute (a): rtpmap:0 PCMU/8000</li><li>Media Attribute (a): rtpmap:101 telephone-event/8000</li></ul></li></ul></li></ul>						

- SRTP is a mandatory requirement

Media Security

GENERAL

→ Media Security      • Enable ▾

Media Security Behavior      Preferable ▾

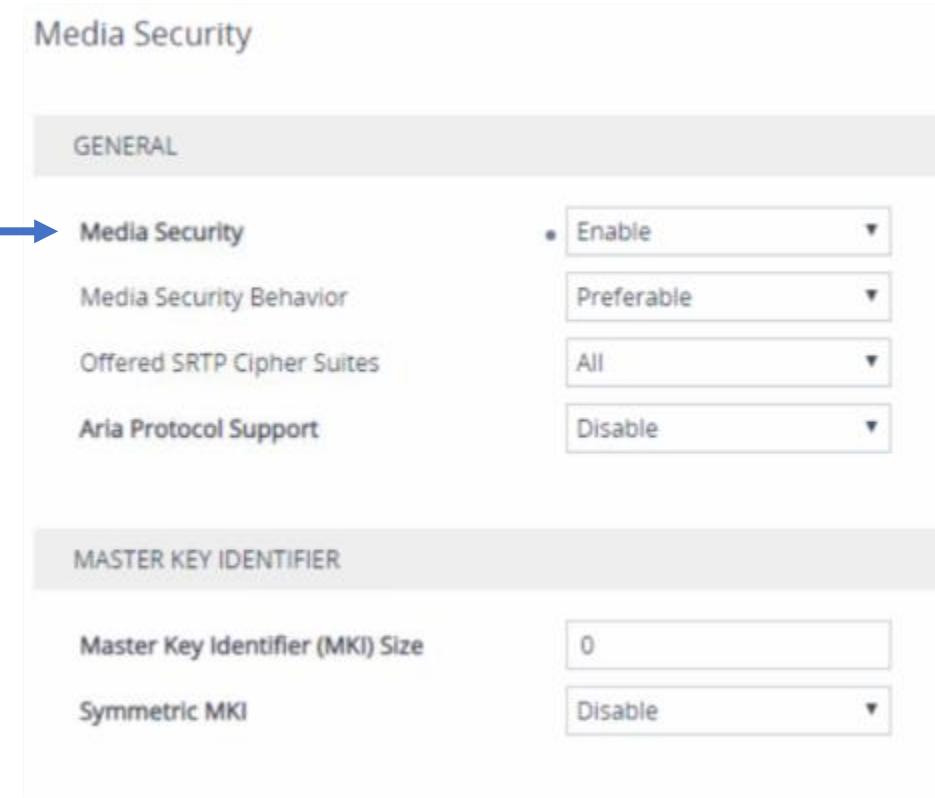
Offered SRTP Cipher Suites      All ▾

Aria Protocol Support      Disable ▾

MASTER KEY IDENTIFIER

Master Key Identifier (MKI) Size      0

Symmetric MKI      Disable ▾



# Condition Table

- Needed for having the Source classified

Message Conditions (1)

+ New	Edit		Page 1 of 1	Show 10 records per page	
INDEX	NAME		CONDITION		
0	Teams-Contact		Header.Contact.URL.Host contains 'pstnhub.microsoft.com'		

#0[Teams-Contact] Edit

**GENERAL**

Name	Teams-Contact
Condition	Header.Contact.URL.Host contains 'pstnhub.microsoft.c...

# Classification Table

- Condition to be attached

MATCH	
Index	0
Name	* Teams
Source SIP Interface	Any <a href="#">View</a>
Source IP Address	
Source Transport Type	Any
Source Port	0
Source Username Pattern	*
Source Host	*
Destination Username Pattern	*
Destination Host	* tr-sbc1.audctrunk.aceducation.info
Message Condition	#0 [Teams-Contact] <a href="#">View</a>

# IP to IP Routing table

## IP-to-IP Routing (4)

- New	Edit	Insert	Page 1 of 1	Show 10 records per page	Search						
INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Options terminal	Default_SBCRout	Route Row	Any	OPTIONS	*	*	Internal	--	--	
1	REFER Re-routing	Default_SBCRout	Route Row	Any	All	*	*	Request URI	Teams	--	
2	Teams to ITSP	Default_SBCRout	Route Row	Teams	All	*	*	IP Group	ITSP	--	
3	ITSP to Teams	Default_SBCRout	Route Row	ITSP	All	*	*	IP Group	Teams	--	

#2[Teams to ITSP] # [Default\_SBCRoutingPolicy]

Edit

GENERAL		ACTION	
Name	* Teams to ITSP	Destination Type	IP Group
Alternative Route Options	Route Row	Destination IP Group	# [ITSP] <a href="#">View</a>
		Destination SIP Interface	# [-] <a href="#">View</a>
		Destination Address	
		Destination Port	0
		Destination Transport Type	
		IP Group Set	# [-] <a href="#">View</a>
		Call Setup Rules Set ID	-1
		Group Policy	Sequential
		Cost Group	# [-] <a href="#">View</a>
		Routing Tag Name	default
		Internal Action	
MATCH			
Source IP Group	* # [Teams] <a href="#">View</a>		
Request Type	All		
Source Username Pattern	*		
Source Host	*		
Source Tag			
Destination Username Pat...	*		
Destination Host	*		
Destination Tag			
Message Condition	# [-] <a href="#">View</a>		
Call Trigger	Any		
ReRoute IP Group	* # [Any] <a href="#">View</a>		



## Hands-on Lab 3

### Teams to SIP Trunk Connection





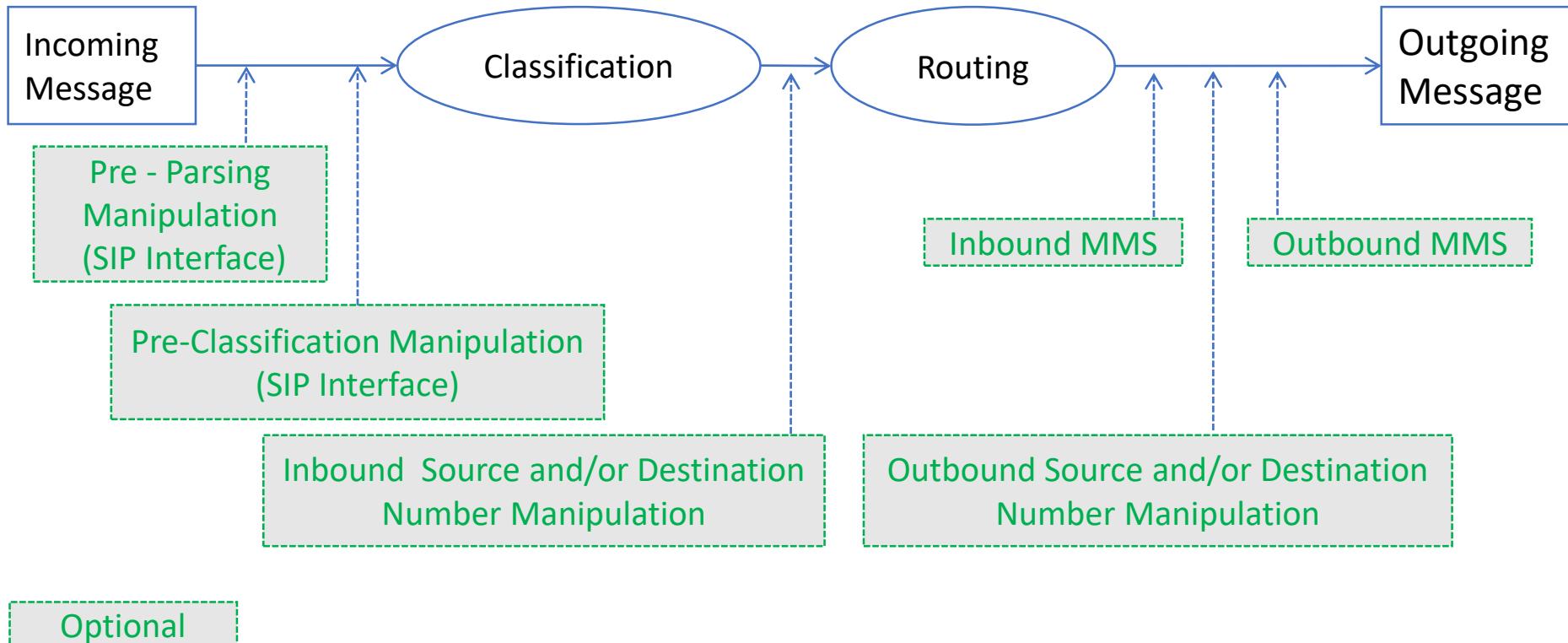
## Lesson 12

# SBC Number & Message Manipulation



- After completing this lesson, you'll:
  - Understand the reasons for Number & Message Manipulation
  - Know how to perform Number & Message Manipulation

- Manipulations include:
  - Number Manipulations (Inbound & Outbound)
  - Message Manipulations (Inbound & Outbound)



- Done according to manipulation tables, similar to what's done for routing
- Select manipulation rule in a table according to:
  - Source IP Group
  - Source and/or destination host and/or user prefixes
- Outbound manipulations are done after routing
- Outbound manipulation rule matching can be done by destination IP Group

- Configure rules to manipulate SIP URI user part (source and destination) of inbound SIP dialog requests
- Apply these to different SIP dialog message types (INVITE or REGISTER)
- Manipulation of Destination URI user part performed on these SIP headers:
  - Request URI
  - To
  - Remote-Party-ID (if it exists)
- Manipulation of Source URI user part is performed on these SIP headers:
  - From
  - P-Asserted (if it exists)
  - P-Preferred (if it exists)
  - Remote-Party-ID (if it exists)

# SBC Inbound Number Manipulations

Inbound Manipulations [convert number format]

GENERAL

Index: 0  
Name: convert number format  
Additional Manipulation: No  
Manipulation Purpose: Normal

MATCH

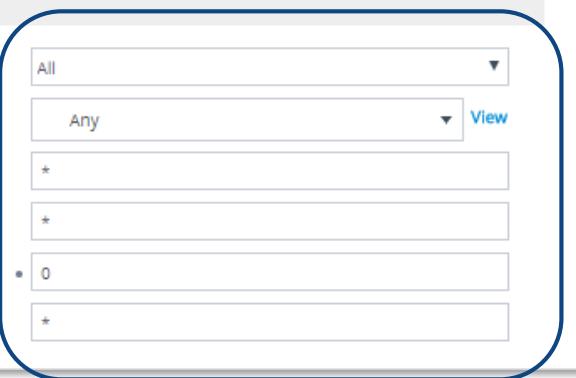
Request Type: All  
Source IP Group: Any  
Source Username Pattern: \*  
Source Host: \*  
Destination Username Pattern: 0  
Destination Host: \*

ACTION

Manipulated Item  
Remove From Left  
Remove From Right  
Leave From Right  
Prefix to Add  
Suffix to Add

Action to take area

Destination: 1  
1  
0  
255  
-9723



Matching area

Action to take area

# SBC Inbound Number Manipulations – Match Area

- **Name**
- **Additional Manipulation:** use same matching condition as row listed above
- **Manipulation Purpose:** Defines the purpose of the manipulation
- **Request Type:** SIP request type to which the rule is applied
- **Source IP Group:** the IP Group from where the incoming INVITE is received
- **Source Username Pattern**
- **Source Host**
- **Destination Username Pattern**
- **Destination Host**

Inbound Manipulations [convert number format]

GENERAL	
Index	0
Name	convert number format
Additional Manipulation	No
Manipulation Purpose	Normal

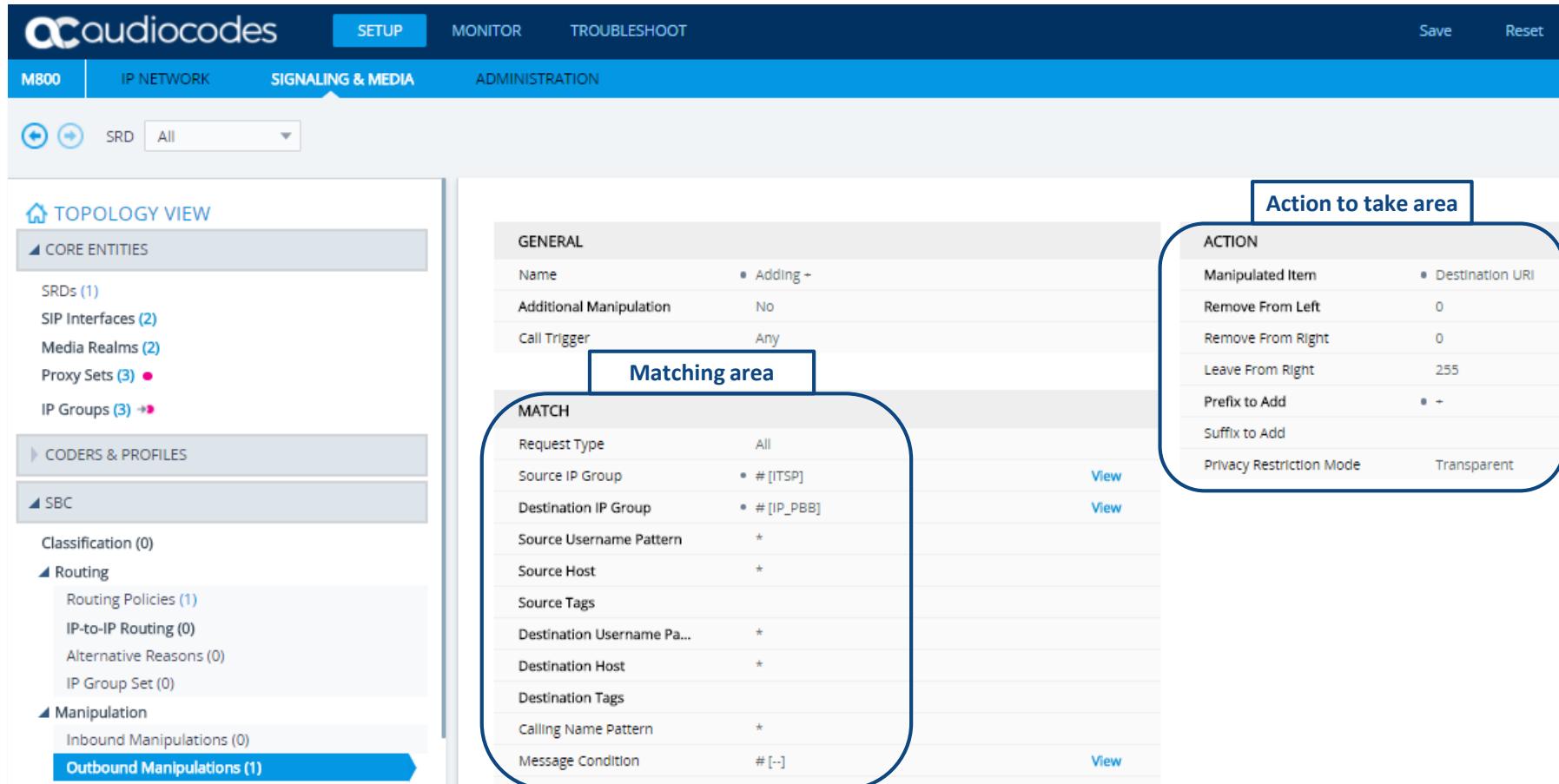
MATCH	
Request Type	All
Source IP Group	Any <a href="#">View</a>
Source Username Pattern	*
Source Host	*
Destination Username Pattern	0
Destination Host	*

- **Manipulated Item:** Determines whether the Source or Destination SIP URI user part is manipulated
- **Remove From Left**
- **Remove From Right**
- **Leave From Right:** Defines the number of characters that you want retained from the right of the user part
- **Prefix to Add**
- **Suffix to Add**

ACTION	
Manipulated Item	• Destination
Remove From Left	• 1
Remove From Right	0
Leave From Right	255
Prefix to Add	• +9723
Suffix to Add	

- Configure rules to manipulate SIP URI user part (Source and Destination) of outbound SIP dialog requests
- Rules correspond to Source IP Group and Source and Destination host and user prefixes
- Rules can be applied to user-defined SIP request type (INVITE, OPTIONS, SUBSCRIBE and/or REGISTER)
- Manipulation of Destination URI user part performed on these SIP headers:
  - Request URI
  - To
  - Remote-Party-ID (if it exists)
- Manipulation of Source URI user part is performed on these SIP headers:
  - From
  - P-Asserted (if it exists)
  - P-Preferred (if it exists)
  - Remote-Party-ID (if it exists)

# SBC Outbound Number Manipulations



The screenshot shows the audiocodes M800 web interface under the **SIGNALING & MEDIA** tab. In the left sidebar, under the **MANIPULATION** section, the **Outbound Manipulations (1)** link is highlighted.

The main configuration page displays a single manipulation rule:

- GENERAL** tab:
  - Name: Adding +
  - Additional Manipulation: No
  - Call Trigger: Any
- MATCH** tab:
  - Request Type: All
  - Source IP Group: # [ITSP] [View](#)
  - Destination IP Group: # [IP\_PBB] [View](#)
  - Source Username Pattern: \*
  - Source Host: \*
  - Source Tags
  - Destination Username Pa...: \*
  - Destination Host: \*
  - Destination Tags
  - Calling Name Pattern: \*
  - Message Condition: # [-] [View](#)
- Action to take area** (highlighted with a blue rounded rectangle):
  - ACTION**
  - Manipulated Item: Destination URL [Edit](#)
  - Remove From Left: 0
  - Remove From Right: 0
  - Leave From Right: 255
  - Prefix to Add: [+](#)
  - Suffix to Add
  - Privacy Restriction Mode: Transparent

- Same parameters as inbound, except for:

- Call Trigger
  - Reason for the re-routing of the SIP request:  
Any, 3xx, REFER, 3xx or REFER, Initial only
- Destination IP Group
  - IP Group where the INVITE is being sent
- Calling Name Pattern
  - Pattern of the calling name (Caller ID)  
Appears in the SIP From header
- Message Condition
  - Assigns a Message Condition rule as a matching characteristic
- Destination Tags
  - Assigns a prefix tag to denote destination URI user names corresponding to the tag configured in the associated Dial Plan
- Reroute IP Group
  - Defines the IP Group that initiated (sent) the SIP redirect response. The parameter functions together with the 'Call Trigger' parameter

*Outbound Manipulations*

MATCH	
Request Type	All
Source IP Group	Any
Destination IP Group	Any
Source Username Pattern	*
Source Host	*
Source Tags	
Destination Username Pattern	*
Destination Host	*
Destination Tags	
Calling Name Pattern	*
Message Condition	--
ReRoute IP Group	Any

- Same parameters as in Inbound except for:
- Privacy Restriction Mode
  - Determines user privacy handling by restricting source user identity in outgoing SIP dialogs

ACTION	
Manipulated Item	Source URI
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	
Suffix to Add	
Privacy Restriction Mode	Transparent

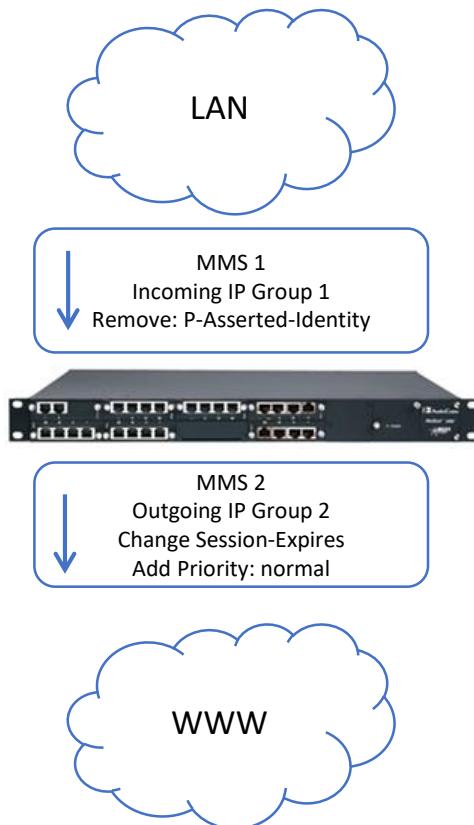
# Message Manipulation

- Key SBC requirements:
  - Each customer has distinct requirements for SBC fundamentals of Security, Interworking and Interoperability
  - Multiple devices support SIP but do not interwork because of differences in how the protocol is implemented or interpreted
  - Manipulation customizes SIP messaging on either side to what devices in that network segment expect
  - ITSPs or enterprises may have policies for which SIP messaging fields should be present before a SIP call enters their network
  - Resolves incompatibilities between SIP devices inside the enterprise network or between networks
  - Self-service programmable tool that saves the time required to develop a software ‘patch’ for each customer

- A combination of rules, specified as a set or group of actions, to be attached to an IP Group
- On the SBC application Message Manipulation rules can be applied pre- or post-classification
- Pre-classification Process:
  - On incoming SIP dialog-initiating messages (e.g., INVITE) prior to the classification process
  - The Manipulation Set ID is assigned to the SIP Interface on which the call is received
- Post-classification Process:
  - On inbound and/or outbound SIP messages after the call has been successfully classified
  - The Manipulation Set ID is assigned to the relevant IP Group in the IP Group table

- IP Group pages display 2 fields:
  - Inbound manipulation set
    - Set of rules to apply to incoming messages (from this IP Group)
  - Outbound manipulation set
    - Set of rules to apply to outgoing messages (to this IP Group)

# Message Manipulation

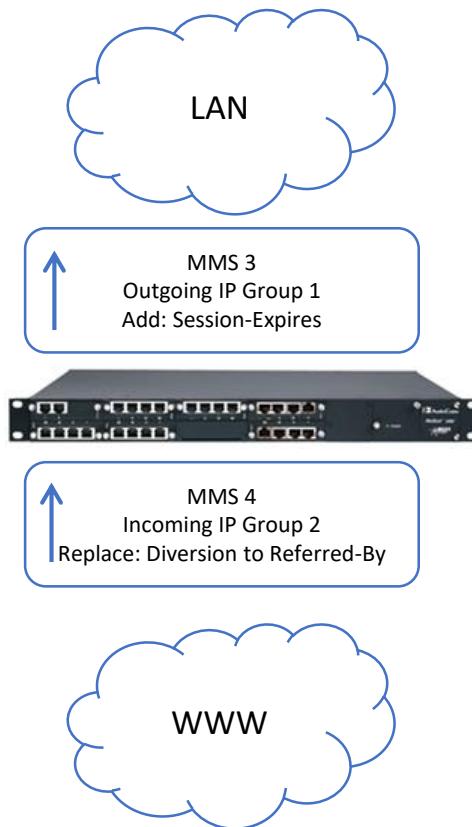


INVITE sip:5550000@10.15.5.1;user=phone  
From: <sip:4000@10.15.5.5>;tag=1c1218068773  
To: <sip:5550000@10.15.5.1;user=phone>  
**P-Asserted-Identity: <sip:4000@10.15.5.5>**  
**Session-Expires: 300**

INVITE sip:5550000@10.15.5.1;user=phone  
From: <sip:4000@10.15.5.5>;tag=1c1218068773  
To: <sip:5550000@10.15.5.1;user=phone>  
**Session-Expires: 300**

INVITE sip:5550000@ITSP.com;user=phone SIP/2.0  
From: <sip:9764000@audiocodes.com>;tag=1c456353708  
To: <sip:5550000@ITSP.com;user=phone>  
**Session-Expires: 100**  
**Priority: normal**

# Message Manipulation



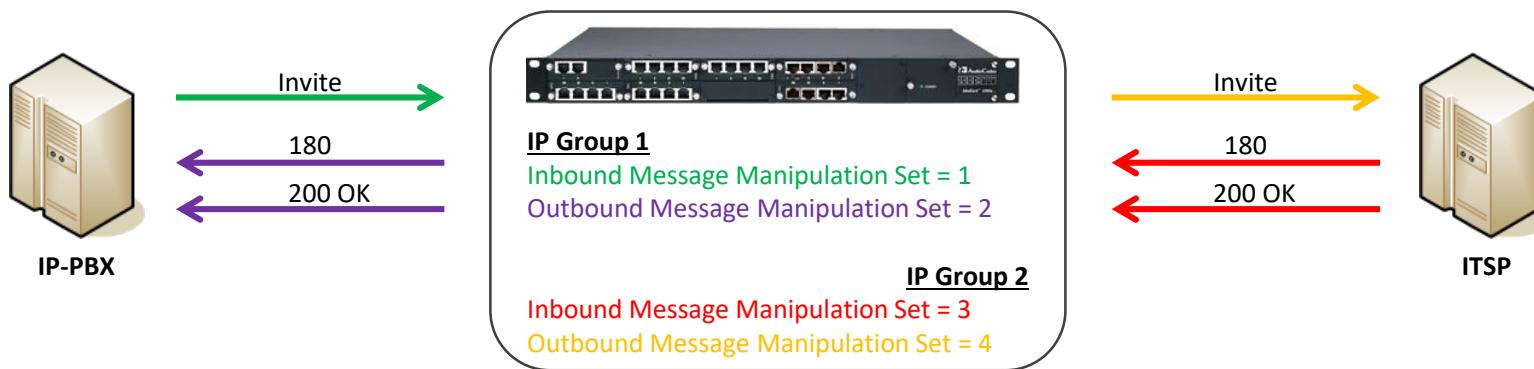
INVITE sip:4000@10.15.5.5;user=phone SIP/2.0  
From: <sip:5550000@10.15.5.1>;tag=1c1759077219  
To: <sip:4000@10.15.5.5;user=phone>  
**Referred-By: <tel:5550001>;reason=unconditional;counter=1**  
Session-Expires: 300

INVITE sip:9764000@audiocodes.com;user=phone SIP/2.0  
From: <sip:5550000@ITSP.com>;tag=1c431593140  
To: <sip:9764000@audiocodes.com;user=phone>  
**Referred-By: <tel:5550001>;reason=unconditional;counter=1**

INVITE sip:9764000@audiocodes.com;user=phone SIP/2.0  
From: <sip:5550000@10.15.7.10>;tag=1c431593140  
To: <sip:9764000@audiocodes.com;user=phone>  
**Diversion: <tel:5550001>;reason=unconditional;counter=1**

# Inbound/Outbound Manipulation

- Applied per message and not per call
- For example:
  - IP Group 1 has 2 Message Manipulation Sets, one for Outbound and one for Inbound, for the same call:
    - Incoming INVITE goes through Inbound MMS
    - 180 and 200 OK responses go through Outbound MMS
  - IP Group 2 has 2 Message Manipulation Sets, one for Outbound and one for Inbound, for the same call:
    - Outgoing INVITE goes through Outbound MMS
    - 180 and 200 OK responses go through Inbound MMS



# Message Manipulation Configuration



- Message Manipulation Table used to configure rules and relate them to a set of rules
- Rule configuration enables adding, modifying or removing most message content
- A rule can be conditionally applied
- Removing/Adding mandatory SIP Headers is not allowed
- Modifying Mandatory SIP Headers is allowed, performed only on requests to initiate new dialogs
  - Mandatory Headers include:
    - Request URI, To, From, Contact, Via, CSeq, Call-Id and Max-Forwards
  - Mandatory SDP headers include:
    - v, o, s, t ,c, m
- When multiple rules apply to the same header, the second rule applies to the first rule's result string
- Manipulating a value in the Message body automatically changes the content-length header

- Request URI
  - User and Host parts are subject to manipulations
- To
  - User and Host parts are subject to manipulations
  - TAG generated by SBC for incoming and outgoing legs; it's different in each leg
- From
  - User and Host parts are subject to manipulations
  - TAG generated by remote UA for incoming leg, generated by SBC for outgoing leg
- Contact
  - Local contact is set to be SBC address (IP, Port and Transport Type) according to SIP Interface used in each leg

- Call-ID

- Each leg has its own Call-ID without regard to peer leg
- For incoming SIP legs, it's determined by remote UA, outgoing legs' Call-IDs are generated by SBC

- CSeq

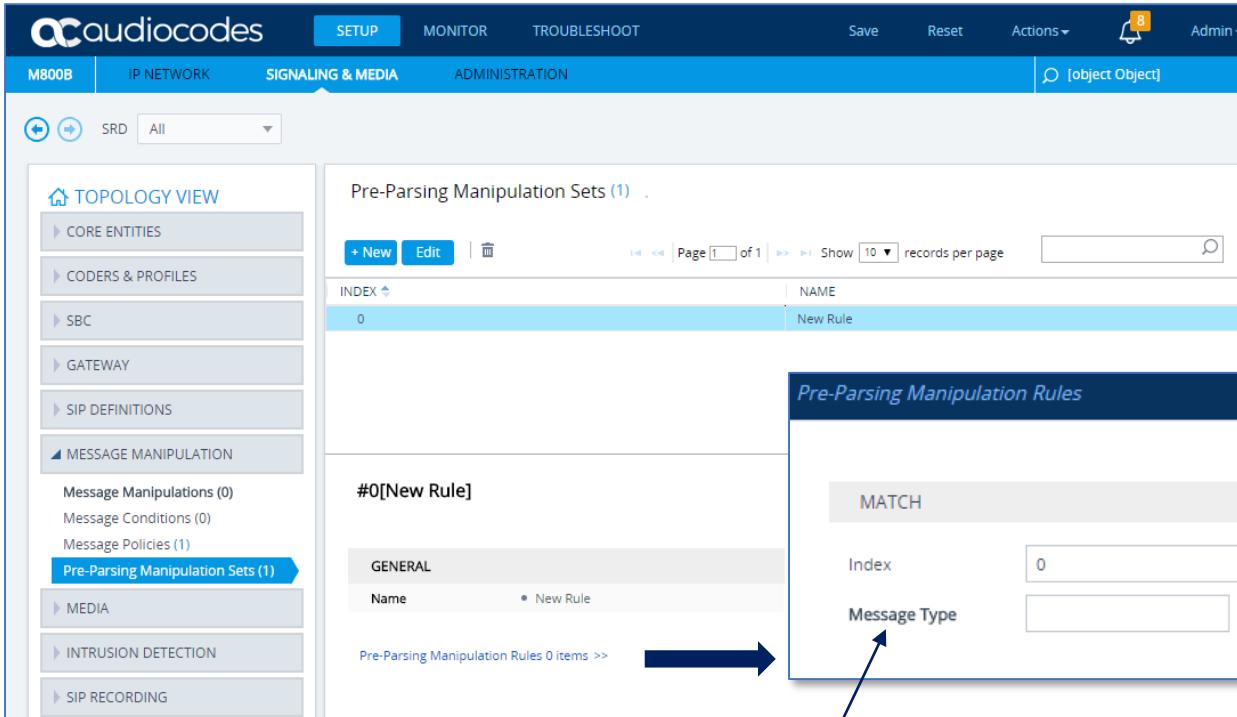
- Each leg has its own call sequence (CSEQ) numbering

- Via

- Each leg has its own VIA policy without regard to peer leg
- Outgoing transactions generate their own VIA according to the SIP Interface they use

- Messages can be manipulated in their original format (plain text) as received from the network
- Pre-Parsing Manipulation is done before Pre-Classification Manipulation and Classification
- Pre-parsing rules assigned to the SIP Interface
- Regular expression (regex) is used to search for (match) in the incoming message as well as to replace the matched pattern
- Parent – Child Table type

# Pre-Parsing Manipulation Sets



The screenshot shows the audiocodes M800B IP NETWORK configuration interface. The top navigation bar includes SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, Admin, and a notification icon with 8 alerts. The left sidebar menu under MESSAGE MANIPULATION includes CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, SIP DEFINITIONS, and MESSAGE MANIPULATION, with Pre-Parsing Manipulation Sets (1) selected. The main content area displays a table titled "Pre-Parsing Manipulation Sets (1)". The table has one row indexed at 0, named "New Rule". Below this, a modal window titled "Pre-Parsing Manipulation Rules" is open, showing fields for MATCH (Index: 0, Message Type), ACTION (Pattern, Replace-With), and Options (Any or empty, <SIP Method>, <SIP Method>.request, <SIP Method>.response.<response code>).

Defines a pattern, based on **regex**, to search for (match) in the incoming message

MATCH  
Index: 0  
Message Type

ACTION  
Pattern:  
Replace-With:

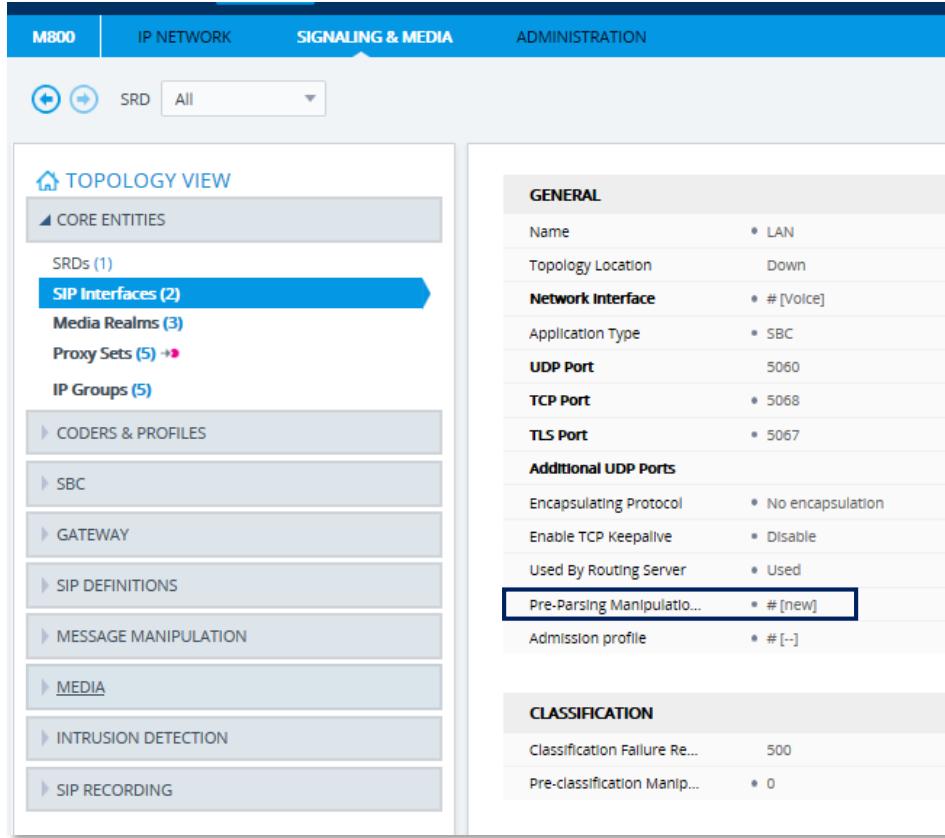
## Options:

- Any or empty
- <SIP Method>
- <SIP Method>.request
- <SIP Method>.response.<response code>

Defines a pattern, based on **regex**, to replace the matched pattern

# SIP Interface Pre-Parsing

- Assigned pre-parsing rules set to the SIP Interface



The screenshot shows the audiocodes M800 interface with the following navigation tabs: M800, IP NETWORK, SIGNALING & MEDIA (selected), and ADMINISTRATION. In the IP NETWORK section, the 'SRD' dropdown is set to 'All'. The left sidebar under 'TOPLOGY VIEW' includes sections for CORE ENTITIES (SRDs 1, SIP Interfaces 2, Media Realms 3), PROXY SETS (5), and IP GROUPS (5). The right panel displays configuration settings for a selected SIP Interface:

GENERAL	
Name	• LAN
Topology Location	Down
Network Interface	• # [Voice]
Application Type	▪ SBC
UDP Port	5060
TCP Port	• 5068
TLS Port	• 5067
Additional UDP Ports	
Encapsulating Protocol	• No encapsulation
Enable TCP Keepalive	• Disable
Used By Routing Server	• Used
Pre-Parsing Manipulatio...	• # [new] (highlighted)
Admission profile	• # [-]
CLASSIFICATION	
Classification Failure Re...	500
Pre-classification Manip...	• 0

# SIP Interface Pre-Classification

- Assigned a Message Manipulation Set ID to the SIP Interface
- Applied SIP Message Manipulation rules on incoming SIP initiating-dialog request messages received on this SIP Interface, prior to the Classification process
- By default, no Message Manipulation Set ID is defined

*SIP Interfaces [SIPInterface\_LAN]*

Application Type	<input checked="" type="radio"/> SBC
UDP Port	5060
TCP Port	5060
TLS Port	0
Additional UDP Ports	
Encapsulating Protocol	No encapsulation
Enable TCP Keepalive	Disable
Used By Routing Server	Not Used
Pre-Parsing Manipulation Set	-- <a href="#">View</a>
CAC Profile	-- <a href="#">View</a>

**CLASSIFICATION**

Classification Failure Response Type	500
Pre-classification Manipulation Set ID	-1

# Message Manipulation Table

- Post-Classification Process: message manipulation is done on inbound and/or outbound SIP messages after the call has been successfully classified

*Message Manipulations*

GENERAL		ACTION	
Index	0	Action Subject	<input type="text"/> <span>Editor</span>
Name	<input type="text"/>	Action Type	<input type="text" value="Add"/> ▼
Manipulation Set ID	0	Action Value	<input type="text"/> <span>Editor</span>
Row Role	Use Current Condition		
MATCH			
Message Type	<input type="text"/> <span>Editor</span>		
Condition	<input type="text"/> <span>Editor</span>		

# Message Manipulation – Manipulation Set ID

- Each Manipulation Set rule contains a Manipulation Set ID
- Same Manipulation Set ID can be configured for multiple rules
  - Up to 20 Manipulation sets and up to 102 rules per manipulation set (Total 1500 rules)
- Assigned to IP Group for inbound and/or outbound messages

#2[ITSP] # [DefaultSRD]

GENERAL	
Name	• ITSP
Topology Location	• Up
Type	Server
Proxy Set	• # [PROXY_ITSP] <a href="#">View</a>
IP Profile	# [-] <a href="#">View</a>
Media Realm	# [-] <a href="#">View</a>
Contact User	
SIP Group Name	
Created By Routing Se...	No
Used By Routing Server	Not Used
Proxy Set Connectivity	Not Connected
QUALITY OF EXPERIENCE	
QoE Profile	# [-]
Bandwidth Profile	# [-]
MESSAGE MANIPULATION	
Inbound Message Ma...	-1
Outbound Message ...	-1
Message Manipulatio...	
Message Manipulatio...	
SBC REGISTRATION AND AUTHENTICATION	
Max. Number of Regi...	-1

# Message Manipulation – Syntax

Screenshot of the audiocodes M800 web interface showing the 'MESSAGE MANIPULATION' section.

The top navigation bar includes: SETUP, MONITOR, TROUBLESHOOT, Save (highlighted with a red box), Reset, Actions, Admin, and a notification icon (15).

The left sidebar shows navigation categories: CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, SIP DEFINITIONS, and MESSAGE MANIPULATION (selected). Under MESSAGE MANIPULATION, there are links for Message Manipulations (1), Message Conditions (0), Message Policies (1), and Pre-Parsing Manipulation Sets (0).

The main content area displays the 'Message Manipulations (1)' table:

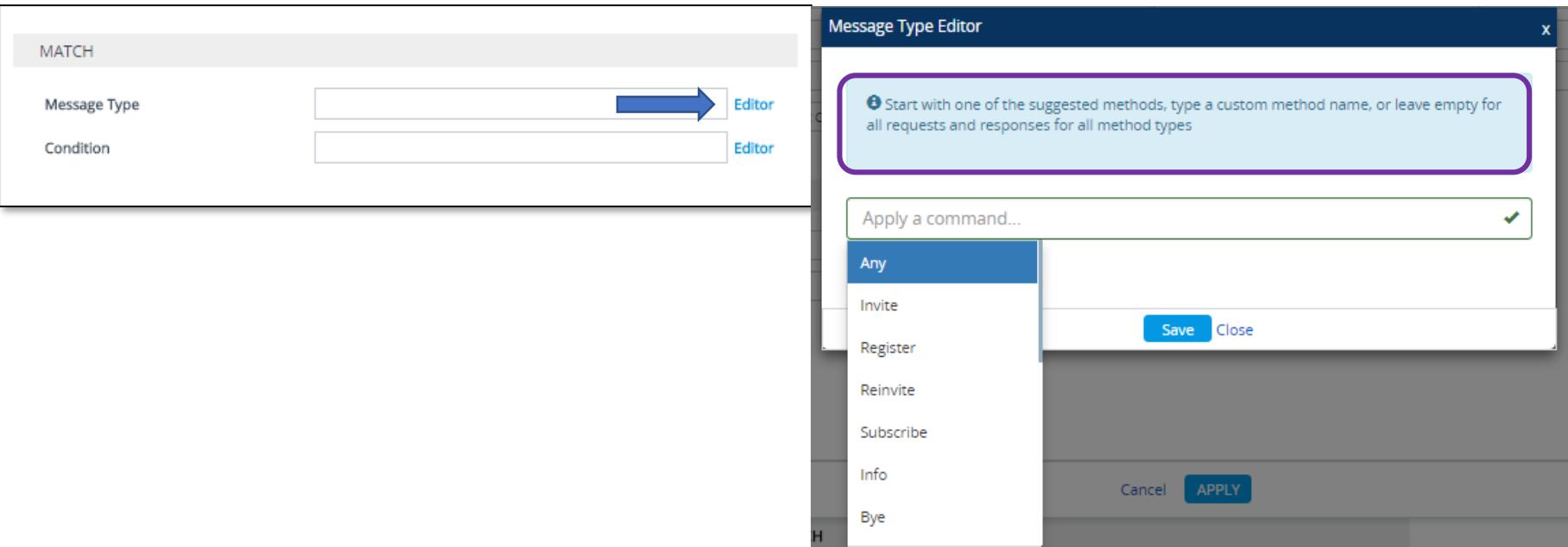
INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0		0	Invite		Header.New Header	Add	'ITSP.com'	Use Current Condition

Below the table, a row #0 is shown with an Edit button. A secondary table at the bottom defines the columns:

General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Element	Action Type	Action Value

# Auto Completion Editor

- Auto-completion for parameters whose values are configured using special syntax
- An Editor button is displayed alongside their fields, which when clicked opens a syntax editor
- As text is typed in the field the user is prompted with optional syntax

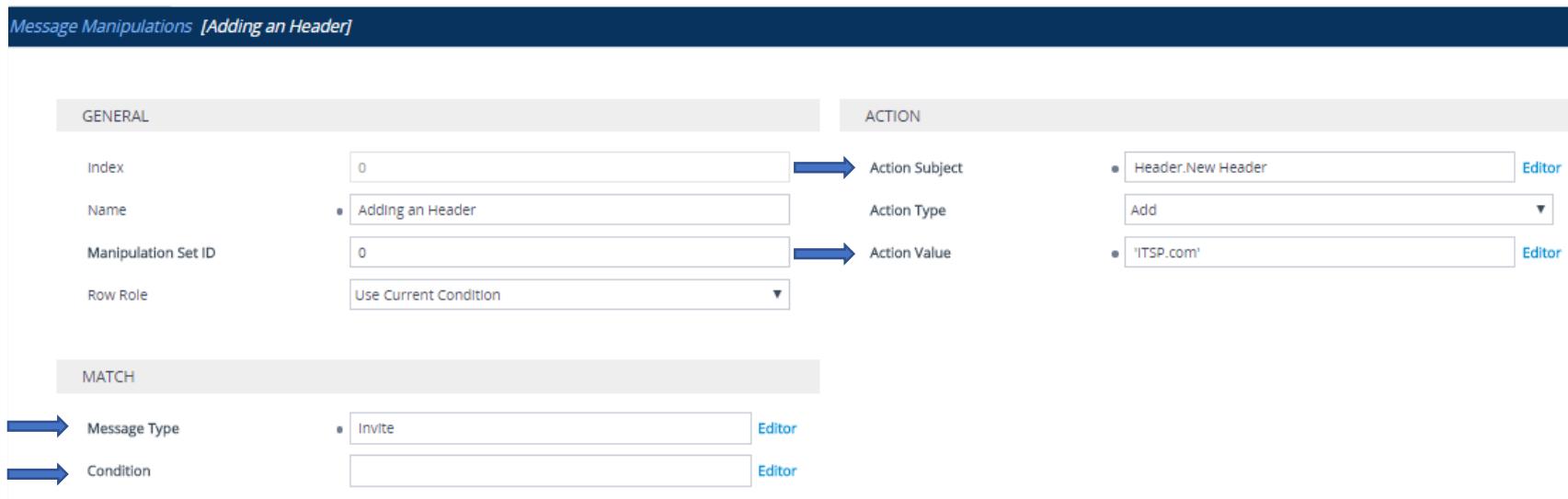


The screenshot illustrates the Auto Completion Editor interface. On the left, there is a 'MATCH' section with two input fields: 'Message Type' and 'Condition'. Each field has an 'Editor' button to its right, indicated by a blue arrow pointing to a detailed view. On the right, a modal window titled 'Message Type Editor' is open. It contains a message box stating: 'Start with one of the suggested methods, type a custom method name, or leave empty for all requests and responses for all method types'. Below this is a dropdown menu labeled 'Apply a command...' containing options: Any, Invite, Register, Reinvite, Subscribe, Info, and Bye. At the bottom of the modal are 'Save' and 'Close' buttons, and at the very bottom are 'Cancel' and 'APPLY' buttons.

- Auto Completion is supported in the following fields:

- Message Type
- Condition
- Action Subject
- Action Value

*Message Manipulations [Adding an Header]*



The screenshot shows the 'Message Manipulations [Adding an Header]' configuration screen. It is divided into three main sections: GENERAL, ACTION, and MATCH.

**GENERAL** section:

- Index: 0
- Name: Adding an Header
- Manipulation Set ID: 0
- Row Role: Use Current Condition

**ACTION** section:

- Action Subject: Header.New Header
- Action Type: Add
- Action Value: 'ITSP.com'

**MATCH** section:

- Message Type: Invite
- Condition: (empty field)

Blue arrows point from the 'Name' field in the GENERAL section to the 'Action Subject' and 'Action Value' fields in the ACTION section, and from the 'Message Type' field in the MATCH section to its respective field.

General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Subject	Action Type	Action Value

- Determines which condition to use for this table row's rule
- 2 options:
  - **Use Current Condition** = use only the condition entered in this row
  - **Use Previous Condition** = use the condition of the rule configured directly above this row (to perform the defined action)
- When multiple manipulations rules apply to the same header, the next rule applies to the result string of the previous rule

# Message Manipulation – Message Type

- The Message Type to manipulate
- Rule applied only if this is the message type
- Syntax: *method.message-role.response-code*
- Method
  - Invite, Subscribe, Refer – rule applies only to specific messages
  - Unknown – Unknown methods also allowed
  - Any (or empty) – No limitation on method type
- Message-role
  - Request – Rule applies only on requests
  - Response – Rule applies only on Response message
- Response-code
  - 3xx – Any redirection response
  - 200 – Only 200 OK response

General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Subject	Action Type	Action Value

## Examples:

- Invite
- Invite.Request
- Invite.Response.180
- Register
- Any

# Message Manipulation – Condition

- Rule-matching criteria (conditions)
- If criterion (condition) exists, rule applies
- Editor Options:
  - Header, Body, Param, Var, SrcTags, DstTags, Message
- Syntax: *<option type> <match-type> match-condition*
- Match-type
  - “==”, “!=”, “>”, “<”, “>=”, “<=”, “contains”, “!contains”, “exists”, “!exists”, “len>”, “len<”, “len==”, “regex”
- Logical-expression
  - “AND” – Logical And
  - “OR” – Logical Or

General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Subject	Action Type	Action Value

## Examples:

- header.contact contains ‘audiocodes.com’
- header.from.url.user == ‘100’ OR header.from.url.user == ‘200’ OR header.from.url.user == ‘300’
- header.from.url.user == ‘100’ AND header.to.url.user == ‘200’

# Message Manipulation – Action Element

- SIP Header on which manipulation is performed
- Message element that changes

General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Subject	Action Type	Action Value

• Syntax: ("header"/"body").message-element-name [ .header-index] [.(sub-element/sub-element-param)]

## • Editor Options:

- Header, Body, Param, Var, Message

## • Message-element-name – Name of message element

- From, To, Application/SDP

## • Header-index – Header's index in the list of headers (if several same-type headers arrive)

- 0 or none = first header
- 1 = second header
- 4 = fifth header

## • Sub-element – Header's element

- User, Host

## Examples:

- header.via.2
- header.from
- header.contact.url.user
- header.referred-by.url.host

# Message Manipulation – Action Type

- The action to be performed on the element

- Syntax:

- **Add** = adds a new header (or parameter or body) - default
- **Remove** = removes a header (or parameter or body)
- **Modify** = sets the element to the new value (replace the entire element)
- **Add Prefix** = adds the value at the beginning of the element string
- **Remove Prefix** = removes the value from the beginning of the element string
- **Add Suffix** = adds the value at the end of the element string
- **Remove Suffix** = removes the value from the end of the element string
- **Normalize** = removes unknown SIP message elements before forwarding the message

General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Subject	Action Type	Action Value

# Message Manipulation – Action Value

- Value to use in the manipulation
- Syntax: *(string/message-element/param) ("+"(string/message-element/param))*

- String
  - 'test.local', '<sip:100@1.2.10.10:5067>'
- Message-element
  - header.from.user, header.contact.url.user
- Param
  - param.ipg.src.user, param.call.dst.host
- Combination
  - param.ipg.dst.host + '.com'

General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Subject	Action Type	Action Value

## Examples:

- '3600'
- 'Bob'
- header.to.url.host
- 'Mike@'+Header.To.URL.Host.Name
- Param.IPG.Dst.User+'com'

# SIP Message Manipulation – Example Rules

**GENERAL**

Index: 0

Name: Remove History-Info.1

Manipulation Set ID: 0

Row Role: Use Current Condition

**ACTION**

Action Subject: Header.History-Info.1

Action Type: Remove

Action Value:

**MATCH**

Message Type: Invite

Condition:

**GENERAL**

Index: 1

Name: Change Privacy

Manipulation Set ID: 0

Row Role: Use Current Condition

**ACTION**

Action Subject: Header.Privacy

Action Type: Modify

Action Value: 'id'

**MATCH**

Message Type: Invite.Request

Condition: Header.Privacy contains 'None'

# SIP Message Manipulation – Example Rules

GENERAL		ACTION		
Index	1	Action Subject	• Header.Request-URI.MethodType <a href="#">Editor</a>	
Name	• Change Response	Action Type	• Modify <a href="#">▼</a>	
Manipulation Set ID	0	Action Value	• '486' <a href="#">Editor</a>	
Row Role	Use Current Condition			
MATCH		ACTION		
Message Type	Index	2	Action Subject	• Header.From.URL.User <a href="#">Editor</a>
Condition	Name	• Change From	Action Type	• Modify <a href="#">▼</a>
Manipulation Set ID	0	Action Value	• 'Mike' <a href="#">Editor</a>	
Row Role	Use Current Condition			
MATCH				
Message Type	• Any.Request <a href="#">Editor</a>			
Condition	• Header.From.URL.User != '100' <a href="#">Editor</a>			

# Example: Change Referred-By to Diversion

- ITSP expects Diversion and not Referred-By

GENERAL		ACTION	
Index	2	Action Subject	Header.Diversion <span style="float: right;">Editor</span>
Name	Referred-By to Diversion	Action Type	Add
Manipulation Set ID	0	Action Value	'<' + Header.Referred-By.URL <span style="float: right;">Editor</span>
Row Role	Use Current Condition		
MATCH			
Message Type	Any.Request	Action Subject	Header.Referred-By <span style="float: right;">Editor</span>
Condition	Header.Referred-By exists	Action Type	Remove
		Action Value	<span style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px;"></span> <span style="float: right;">Editor</span>
GENERAL			
Index	3	Action Subject	Header.Referred-By <span style="float: right;">Editor</span>
Name	Referred-By to Diversion	Action Type	Remove
Manipulation Set ID	0	Action Value	<span style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px;"></span> <span style="float: right;">Editor</span>
Row Role	Use Previous Condition		
MATCH			
Message Type	<span style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px;"></span> <span style="float: right;">Editor</span>		
Condition	<span style="border: 1px solid #ccc; padding: 2px; width: 150px; height: 20px;"></span> <span style="float: right;">Editor</span>		

# Examples based on the Message Body (1)

- If the address in the SDP is 10.15.11.1, the SBC adds a new SIP header, "IPSource" whose value is set to the type of the source IP Group

GENERAL		ACTION	
Index	4	Action Subject	• Header.IPSource <a href="#">Editor</a>
Name	• New SIP Header	Action Type	Add <a href="#">▼</a>
Manipulation Set ID	• 1	Action Value	• Param.IPG.Src.Type <a href="#">Editor</a>
Row Role	Use Current Condition <a href="#">▼</a>		
MATCH			
Message Type	• Invite <a href="#">Editor</a>		
Condition	• Param.Message.SDP.Address == '10.15.11.1' <a href="#">Editor</a>		

# Examples based on the Message Body (2)

- If 200 OK response on ReInvite received with 0.0.0.0 in SDP address and it should be changed to SBC address from the origin ('o=') SDP

GENERAL		ACTION	
Index	3	Action Subject	• Param.Message.SDP.Address <span style="float: right;">Editor</span>
Name	• 0.0.0.0 to Orig Address	Action Type	• Modify <span style="float: right;">▼</span>
Manipulation Set ID	• 5	Action Value	• Param.Message.SDP.OriginAddress <span style="float: right;">Editor</span>
Row Role	Use Current Condition <span style="float: right;">▼</span>		
MATCH			
Message Type	• Reinvite.Response.2xx <span style="float: right;">Editor</span>		
Condition	• Param.Message.SDP.Address == '0.0.0.0' <span style="float: right;">Editor</span>		

# Examples based on the Message Body (3)

- If the RTP mode is inactive, add a new parameter, "origin" to the From header. The value of the parameter is set to the 'o=' address in the SDP

GENERAL		ACTION	
Index	5	Action Subject	• Header.From.Param.Origin <span style="float: right;">Editor</span>
Name	• Add Orig Parameter	Action Type	• Add <span style="float: right;">▼</span>
Manipulation Set ID	• 6	Action Value	• Param.Message.SDP.OriginAddress <span style="float: right;">Editor</span>
Row Role	Use Current Condition <span style="float: right;">▼</span>		
MATCH			
Message Type	• Any <span style="float: right;">Editor</span>		
Condition	• Param.Message.SDP.RTPMode == 'inactive' <span style="float: right;">Editor</span>		

- Feature that can be enabled per manipulation rule when Action Type is set to "Normalize"
- Removes unknown or non-standard SIP message elements before forwarding the message
- These elements can include SIP headers, SIP header parameters, and SDP body fields
- The device normalizes the following SIP elements:
  - URLs:
    - User part is normalized
  - Headers:
    - Unknown header parameters are removed
    - URLs are normalized
  - SDP Body:
    - Removes unnecessary SDP fields (except m=, v=, o=, s=, c=, t=, and r=)
    - Removes unknown media with all its attributes

# SIP Message Normalization – Examples

General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Subject	Action Type	Action Value
Example 1	1	Use Current Condition	invite		header.to	Normalize	
Example 2	4	Use Current Condition	invite		message	Normalize	

- Example 1:

- To header before normalization:
  - To: <sip:1-800-300-500;phone-context=1@10.33.2.17;user=phone;UnknownUrlParam>
- To header after normalization:
  - To: <sip:1800300500@10.33.2.17;user=phone>

- Example 2:

- All the headers to be normalized

# SIP Message Normalization – Body Example



General			Match		Action		
Name	Manipulation Set ID	Row Role	Message Type	Condition	Action Element	Action Type	Action Value
Example 3	4	Use Current Condition	invite		body.sdp	Normalize	

## SDP before normalization

v=0  
o=SMG 791285 795617 IN IP4 10.33.2.17  
s=Phone-Call  
**i=A Seminar on the session description protocol**  
**u=http://www.example.com/seminars/sdp.pdf**  
**e=j.doe@example.com (Jane Doe)**  
c=IN IP4 10.33.2.26  
t=0 0  
**m=unknown 6000 RTP/AVP 8**  
**a=unknown**  
**a=sendrecv**  
**a=ptime:20**  
m=audio 6000 RTP/AVP 8  
a=rtpmap:8 pcma/8000  
a=sendrecv  
**a=unknown**  
a=ptime:20

## SDP after normalization

v=0  
o=SMG 791285 795617 IN IP4 10.33.2.17  
s=Phone-Call  
c=IN IP4 10.33.2.26  
t=0 0  
m=audio 6000 RTP/AVP 8  
a=rtpmap:8 pcma/8000  
a=sendrecv  
a=ptime:20

# Message and Number Manipulation – Example



```
INVITE sip:5550000@10.15.5.1;user=phone SIP/2.0
Via: SIP/2.0/TCP 10.15.5.5:5050;branch=z9hG4ac8071985;alias
Max-Forwards: 70
From: <sip:4000@10.15.5.5>;tag=1c1218068773
To: <sip:5550000@10.15.5.1;user=phone>
Call-ID: 121806822010120101484@10.15.5.5
CSeq: 1 INVITE
Contact: <sip:4000@10.15.5.5:5050;transport=tcp>
Privacy: none
P-Asserted-Identity: <sip:4000@10.15.5.5>
```

```
INVITE sip:5550000@ITSP.com;user=phone SIP/2.0
Via: SIP/2.0/UDP 200.100.10.2;branch=z9hG4ac463637
Max-Forwards: 10
From: <sip:9764000@audiocodes.com>;tag=1c456353708
To: <sip:5550000@ITSP.com;user=phone>
Call-ID: 4563049822722010203627@200.100.10.2
CSeq: 1 INVITE
Contact: <sip:4000@200.100.10.2:5060>
Privacy: session
P-Asserted-Identity: <sip:9764000@audiocodes.com>
Priority: emergency
```

**Number Manipulation can be done in the:**

- A. Inbound leg before Routing only
- B. Outbound leg after Routing only
- C. Inbound and outbound legs
- D. None of the above



**Which one is false:**

- A. Outbound number manipulation rule matching can be done by destination IP Group
- B. Inbound number manipulation rule matching can be done by destination IP Group
- C. Outbound number manipulation rule matching can be done by source IP Group
- D. Inbound number manipulation rule matching can be done by destination host

By using Message Manipulation we can:

- A. Use it as a trigger for an alternative routing
- B. Overcome Interworking and Interoperability issues
- C. Increase the bandwidth used by the UA's
- D. All of the above

By using the IP-to-IP manipulation tables we can manipulate the:

- A. Source Number
- B. Destination number
- C. SIP message
- D. Source number and Destination number





Hands-on Lab 4

SIP Header Manipulation





## Lesson 12

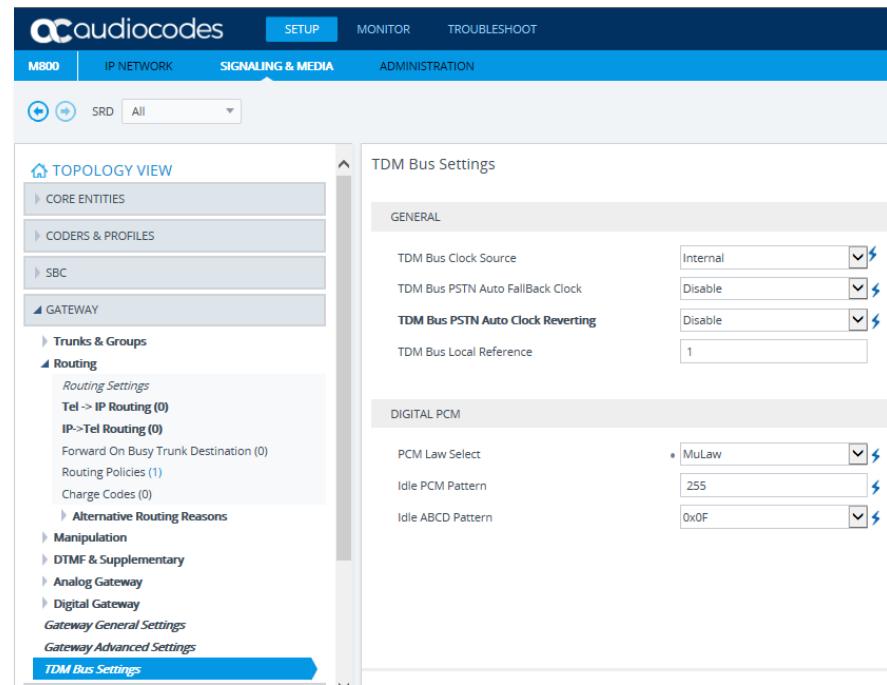
# Digital Gateways Basic Configuration



- After completing this lesson you will:
  - Know how to configure the basic gateway parameters

# Configuring TDM Bus

- **TDM Bus Clock Source (Network/Internal)**
  - Clock source on which the gateway synchronizes
- **TDM Bus PSTN Auto FallBack Clock (relevant if TDMBusClockSource = Network)**
  - Disable = Recovers the clock from the E1/T1 line defined by parameter 'TDM Bus Local Reference'
  - Enable = Recovers the clock from any connected synchronized slave E1/T1 line
- **TDM Bus Local Reference**
  - Determines the Trunk ID used to synchronize the gateway's clock when using external clock
- **PCM Law Select (A-law/μ-law)**
  - Usually A-Law for E1 and μ-Law for T1



- **Protocol Type**

- Sets the PSTN protocol to be used for this trunk
  - If 'Protocol Type' of all PRI trunks displays 'None', select the protocol type (E1/T1) for a single trunk and reset the gateway
  - Only after the reset you will be able to continue configuring the trunks

- **Clock Master**

- Determines Tx clock source of E1/T1 line
- Recovered (0) = Generate clock according to Rx of E1/T1 line
- Generated (1) = Generate clock according to internal TDM bus

- **ISDN Termination Side**

- User side = ISDN User Termination Side (TE)
- Network side = ISDN Network Termination Side (NT)
- Select 'User side' when the PSTN or PBX side is configured as 'Network side' and vice-versa

# Configuring Key Trunk Parameters

audiocodes

SETUP MONITOR TROUBLESHOOT

Saved Entity, parameter, value Admin

MEDIANT 1000 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

TOPOLOGY VIEW CORE ENTITIES

- SRDs (1)
- SIP Interfaces (1)
- Media Realms (1)
- Proxy Sets (1)
- IP Groups (1)

CODERS & PROFILES

SBC

GATEWAY

Trunks & Groups

- Trunks
- Trunk Groups
- Trunk Group Settings (1)
- CAS State Machines

Routing

- Routing Settings
- Tel -> IP Routing (0)
- IP -> Tel Routing (0)
- Forward On Busy Trunk Destination (0)
- Routing Policies (1)
- Charge Codes (0)
- Alternative Routing Reasons

Manipulation

DTMF & Supplementary

Analog Gateway

Digital Gateway

Gateway General Settings

Trunk Settings

GENERAL

- Module ID: 1
- Trunk ID: 1
- Trunk Configuration State: Active
- Protocol Type: E1 EURO ISDN

ADVANCED SETTINGS

- PSTN Alert Timeout: -1
- Transfer Mode: Disable
- Local ISDN Ringback Tone Source: PBX
- Set PI in Rx Disconnect Message: Not Configured
- ISDN Transfer Capabilities: Not Configured
- Progress Indicator to ISDN: Not Configured
- Select Receiving of Overlap Dialing: None
- B-channel Negotiation: Not Configured
- Out-Of-Service Behavior: Not Configured
- Remove Calling Name: Use Global Parameter
- Play Ringback Tone to Trunk: Not Configured
- Call Rerouting Mode: None
- ISDN Duplicate Q931 BuffMode: 0
- Trunk Name:

TRUNK CONFIGURATION

- Clock Master: Recovered
- Auto Clock Trunk Priority: 0
- Line Code: HDB3
- Line Build Out Loss: 0 dB
- Trace Level: No Trace
- Line Build Out Overwrite: OFF
- Framing Method: E1 FRAMING MFF CRC4 EXT

ISDN CONFIGURATION

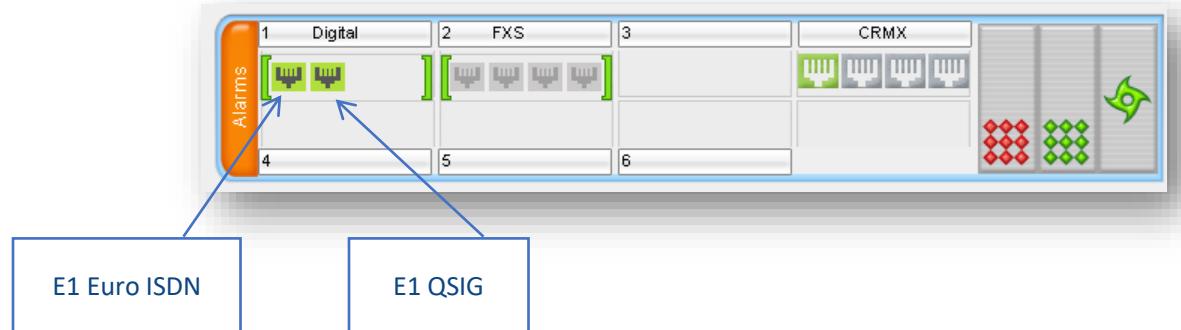
- ISDN Termination Side: User side
- Q931 Layer Response Behavior: 0x01

Buttons: Submit, Stop Trunk, Deactivate Trunk, Create Loopback

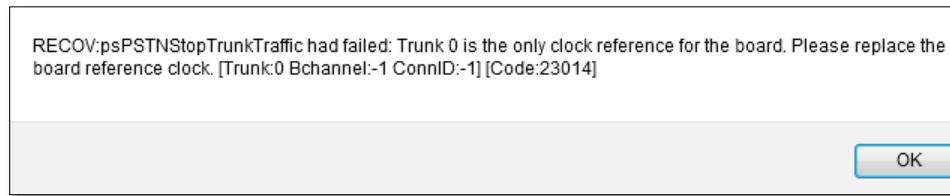
Activate Windows  
Go to PC settings to activate Windows.

# Digital Trunk Points of Information

- All Trunk spans must be of the same Line Type (all E1 or all T1)
- Different flavors of same Line Type (E1/T1) can be configured on available Trunks (e.g., E1 Euro ISDN and E1 QSIG)
- Trunks are referenced in ini file and Syslog messages as '0-7' regardless of whether physical Trunks are numbered '1-8'



- Why do I receive this message when I try to stop a trunk?

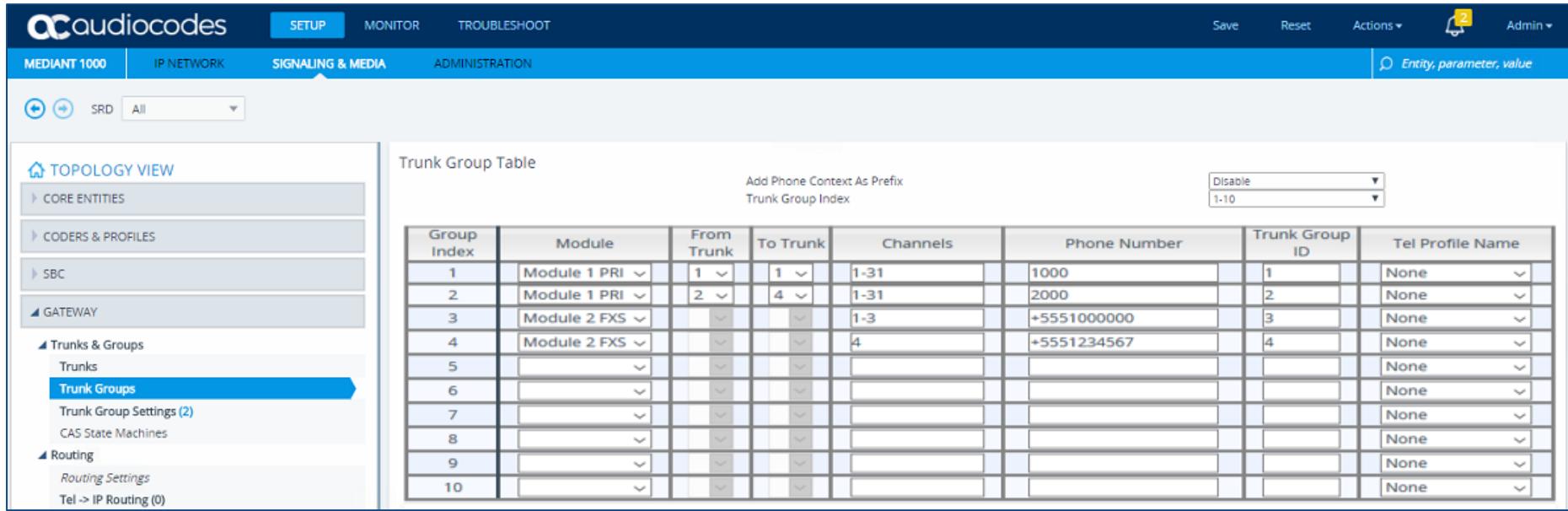


- The trunk can't be stopped because it provides the gateway's clock (assuming the gateway is synchronized with the E1/T1 clock)
- Assign a different E1/T1 trunk to provide the gateway's clock or enable 'TDM Bus PSTN Auto Clock' in the 'TDM Bus Settings' screen

- Why do I have poor voice quality on all calls?
  - Probably because the value you configured for the PCM Law Select parameter for the Mediant is incorrect
  - It must be identical to the value configured for the PCM Law Select parameter for the PBX/PSTN
  - A-law is usually used for E1 spans and  $\mu$ -law for T1 spans

# Trunk Group Table – E1/T1 and/or FXS

- Used to assign Trunk Groups, Profiles and logical telephone numbers to the gateway's channels
- Trunks or B-Channels that are not defined are disabled



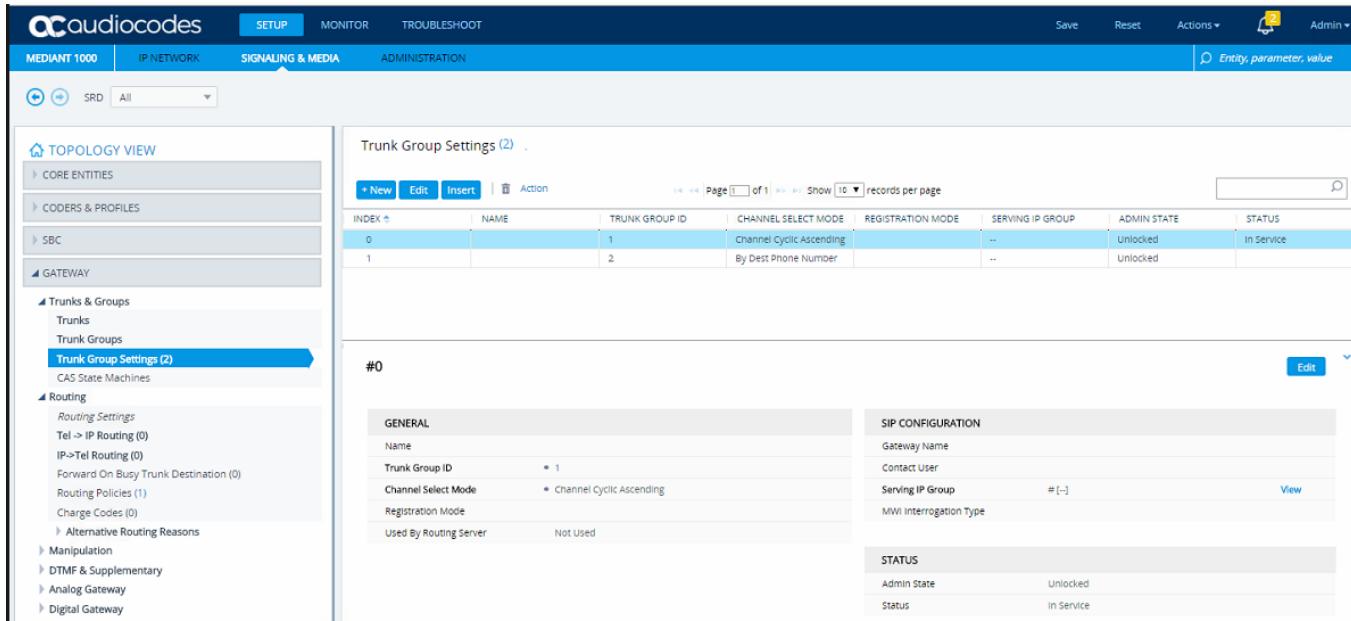
The screenshot shows the audiocodes MEDIAN1000 web interface with the following details:

- Top Navigation:** audiocodes, SETUP (selected), MONITOR, TROUBLESHOOT, Save, Reset, Actions ▾, Admin ▾.
- Left Sidebar:** TOPOLOGY VIEW, CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, Trunks & Groups (selected), Trunks (selected), Trunk Groups (selected), Trunk Group Settings (2), CAS State Machines, Routing, Routing Settings, Tel -> IP Routing (0).
- Central Content:** Trunk Group Table. The table has the following columns:

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-31	1000	1	None
2	Module 1 PRI	2	4	1-31	2000	2	None
3	Module 2 FXS			1-3	+5551000000	3	None
4	Module 2 FXS			4	+5551234567	4	None
5							None
6							None
7							None
8							None
9							None
10							None
- Buttons and Inputs:** Add Phone Context As Prefix, Trunk Group Index (dropdowns for Disable and 1-10), Entity, parameter, value search bar.

# Trunk Group Settings

- Determines the method by which new calls are assigned to channels within each Trunk Group ID
- If such a rule doesn't exist (for a specific Trunk Group), the global rule defined by the Gateway General Settings' Channel Select Mode parameter applies



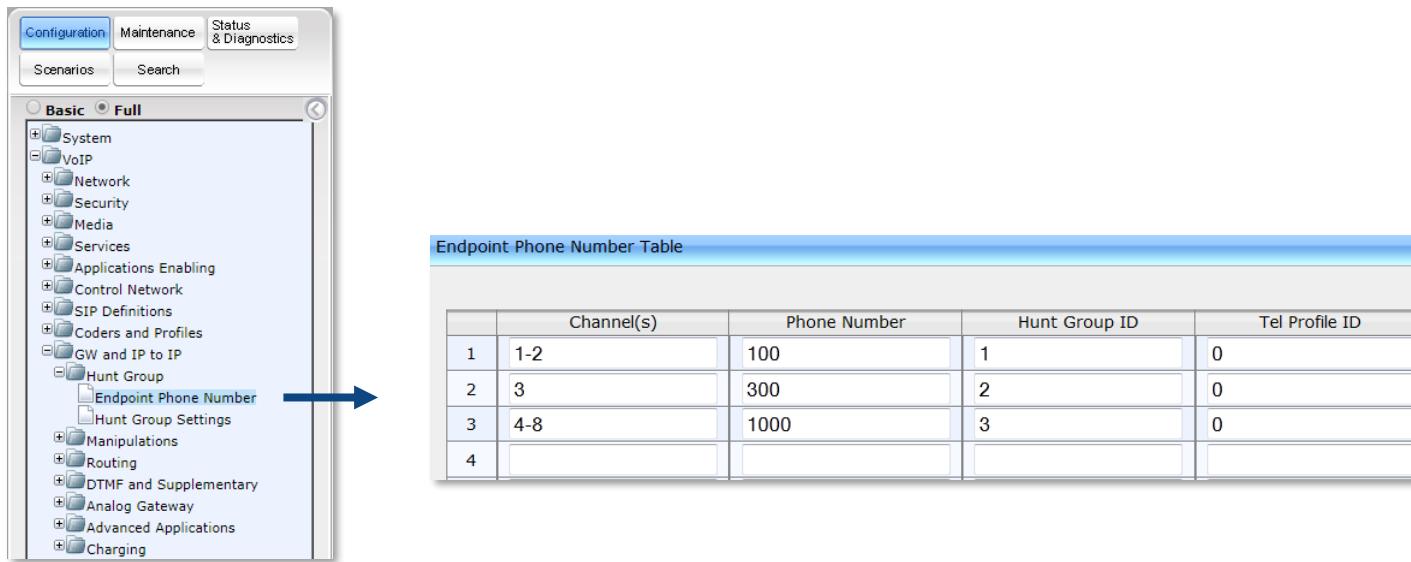
The screenshot shows the audiocodes MEDIANET 1000 web interface. The top navigation bar includes tabs for SETUP (selected), MONITOR, TROUBLESHOOT, and ADMINISTRATION. The left sidebar contains a tree view of system entities: CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, Trunks & Groups (selected), Trunks, Trunk Groups, Trunk Group Settings (2) (selected), CAS State Machines, Routing, Manipulation, DTMF & Supplementary, Analog Gateway, and Digital Gateway. The main content area displays the 'Trunk Group Settings (2)' page. It features a table with columns: INDEX, NAME, TRUNK GROUP ID, CHANNEL SELECT MODE, REGISTRATION MODE, SERVING IP GROUP, ADMIN STATE, and STATUS. Two entries are listed: Index 0 (Name: 1, Trunk Group ID: 1, Channel Select Mode: Channel Cyclic Ascending, Registration Mode: --, Serving IP Group: --, Admin State: Unlocked, Status: In Service) and Index 1 (Name: 2, Trunk Group ID: 2, Channel Select Mode: By Dest Phone Number, Registration Mode: --, Serving IP Group: --, Admin State: Unlocked, Status: In Service). Below the table, there is a detailed configuration panel for entry #0, divided into GENERAL, SIP CONFIGURATION, and STATUS sections.

INDEX	NAME	TRUNK GROUP ID	CHANNEL SELECT MODE	REGISTRATION MODE	SERVING IP GROUP	ADMIN STATE	STATUS
0	1	1	Channel Cyclic Ascending	--	--	Unlocked	In Service
1	2	2	By Dest Phone Number	--	--	Unlocked	In Service

#0

<b>GENERAL</b>	<b>SIP CONFIGURATION</b>
Name	Gateway Name
Trunk Group ID	1
Channel Select Mode	Channel Cyclic Ascending
Registration Mode	
Used By Routing Server	Not Used
<b>STATUS</b>	
Admin State	Unlocked
Status	In Service

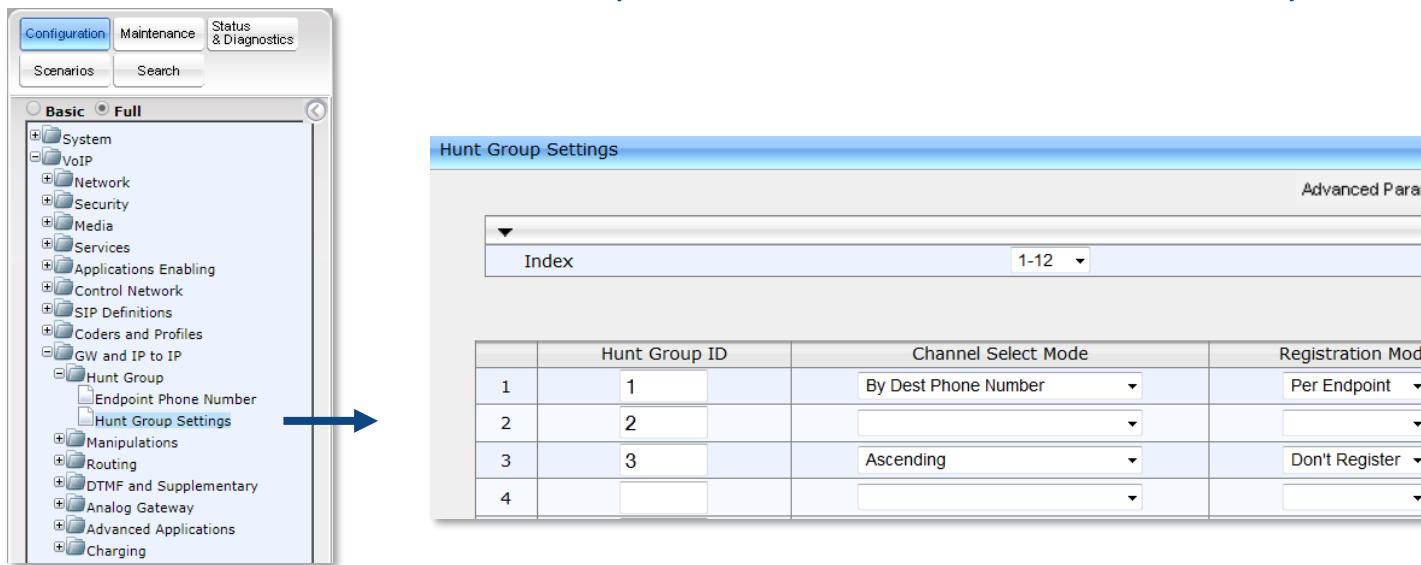
- For analog MP gateways running firmware version 6.6
  - Allows activation of the Analog Gateway ports (Channels)
  - The number of endpoints depends on the MP model
  - Allows entry of the channels in groups (n-m) or a separate channel number for each line
  - The Phone Number value can include up to 50 characters



The image shows a screenshot of the audiocodes configuration software interface. At the top, there are tabs for Configuration, Maintenance, Status & Diagnostics, Scenarios, and Search. Below the tabs is a navigation pane with a tree view of system categories: System, VoIP, Network, Security, Media, Services, Applications Enabling, Control Network, SIP Definitions, Coders and Profiles, GW and IP to IP, Hunt Group, Endpoint Phone Number, Hunt Group Settings, Manipulations, Routing, DTMF and Supplementary, Analog Gateway, Advanced Applications, and Charging. A blue arrow points from the 'Endpoint Phone Number' node in the tree to a table window titled 'Endpoint Phone Number Table'. The table has columns for Channel(s), Phone Number, Hunt Group ID, and Tel Profile ID. It contains four entries:

	Channel(s)	Phone Number	Hunt Group ID	Tel Profile ID
1	1-2	100	1	0
2	3	300	2	0
3	4-8	1000	3	0
4				

- Allows to configure settings of up to 24 Hunt Groups
- Allows you to select the method for which IP-to-Tel calls are assigned to channels within each Hunt Group
- If no method is selected for a specific Hunt Group, the setting of the global parameter, Channel Select Mode (SIP General Parameters screen) takes effect

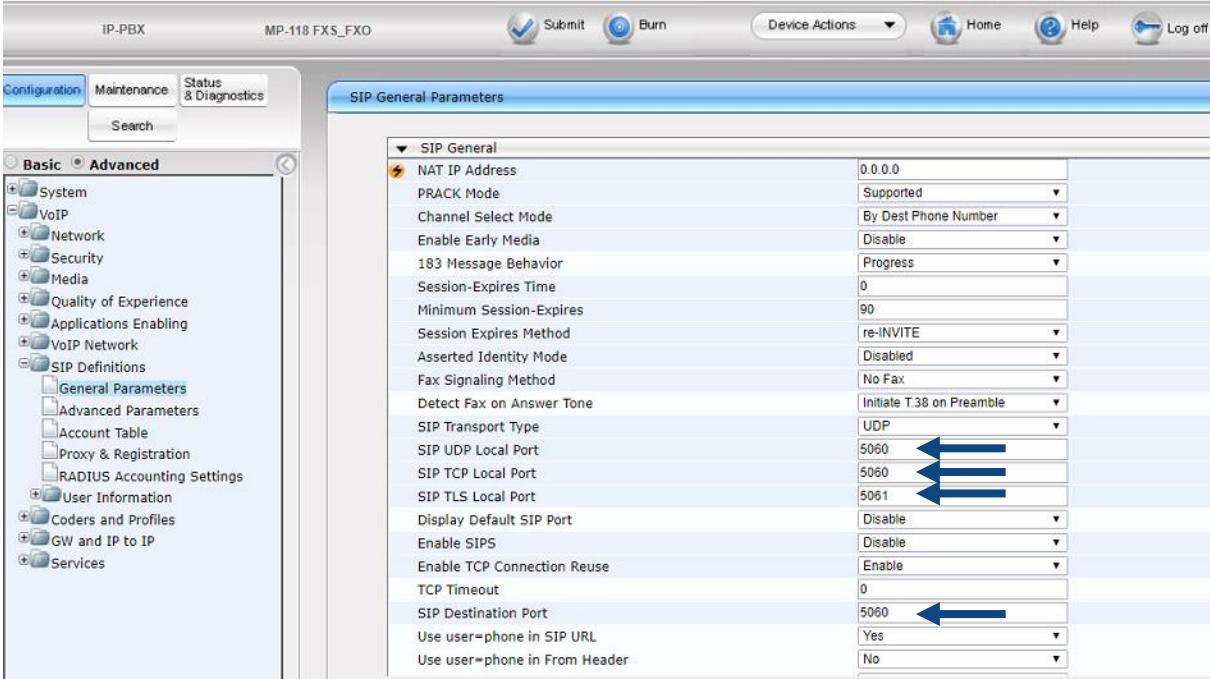


The screenshot shows the audiocodes configuration interface. The top navigation bar includes tabs for Configuration, Maintenance, Status & Diagnostics, Scenarios, and Search. A sidebar on the left is titled 'Basic' and lists various system components: System, VoIP, Network, Security, Media, Services, Applications Enabling, Control Network, SIP Definitions, Coders and Profiles, GW and IP to IP, Hunt Group, Manipulations, Routing, DTMF and Supplementary, Analog Gateway, Advanced Applications, and Charging. An arrow points from the 'Hunt Group' entry in the sidebar to the 'Hunt Group Settings' section of the main content area. The main content area is titled 'Hunt Group Settings' and contains a table with four rows, each representing a Hunt Group ID (1, 2, 3, 4). The columns are: Hunt Group ID, Channel Select Mode, and Registration Mode. Row 1: Hunt Group ID 1, Channel Select Mode 'By Dest Phone Number', Registration Mode 'Per Endpoint'. Row 2: Hunt Group ID 2, Channel Select Mode dropdown, Registration Mode dropdown. Row 3: Hunt Group ID 3, Channel Select Mode 'Ascending', Registration Mode 'Don't Register'. Row 4: Hunt Group ID 4, Channel Select Mode dropdown, Registration Mode dropdown.

	Hunt Group ID	Channel Select Mode	Registration Mode
1	1	By Dest Phone Number	Per Endpoint
2	2		
3	3	Ascending	Don't Register
4			

# General Parameters (MP Analog Gateways)

- SIP Transport Type: The default transport layer for SIP calls (UDP, TCP or TLS)
- SIP Local Port: The local listening port for SIP messages (listen port)
- SIP Destination Port: SIP port for outgoing initial SIP requests (sending port)

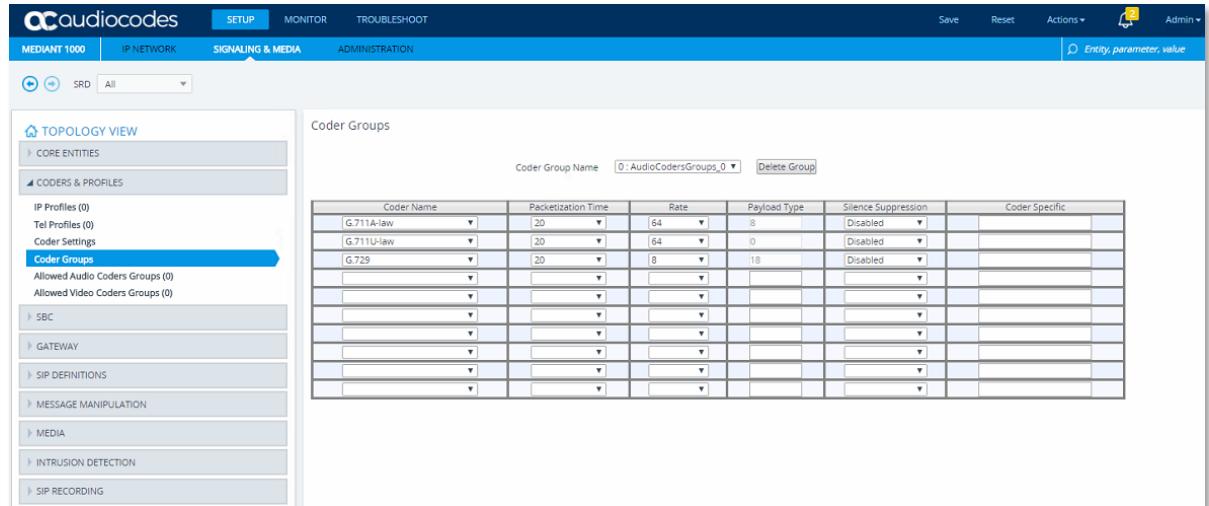


SIP General Parameters

Parameter	Value	Link
NAT IP Address	0.0.0.0	
PRACK Mode	Supported	
Channel Select Mode	By Dest Phone Number	
Enable Early Media	Disable	
183 Message Behavior	Progress	
Session-Expires Time	0	
Minimum Session-Expires	90	
Session Expires Method	re-INVITE	
Asserted Identity Mode	Disabled	
Fax Signaling Method	No Fax	
Detect Fax on Answer Tone	Initiate T.38 on Preamble	
SIP Transport Type	UDP	
SIP UDP Local Port	5060	↔
SIP TCP Local Port	5060	↔
SIP TLS Local Port	5061	↔
Display Default SIP Port	Disable	
Enable SIPS	Disable	
Enable TCP Connection Reuse	Enable	
TCP Timeout	0	
SIP Destination Port	5060	↔
Use user=phone in SIP URL	Yes	
Use user=phone in From Header	No	

# Coder Group Table

- Allows you to configure coders for the Gateway
  - The first coder in the list has the highest priority
  - A coder can appear only once in the table
- The Packetization Time determines how many coder payloads are combined into a single RTP packet
  - The Gateway always uses the packetization time requested by the remote side for sending RTP packets
- Enable/Disable the Silence Suppression option per coder



The screenshot shows the audiocodes MEDIAN 1000 web interface with the following details:

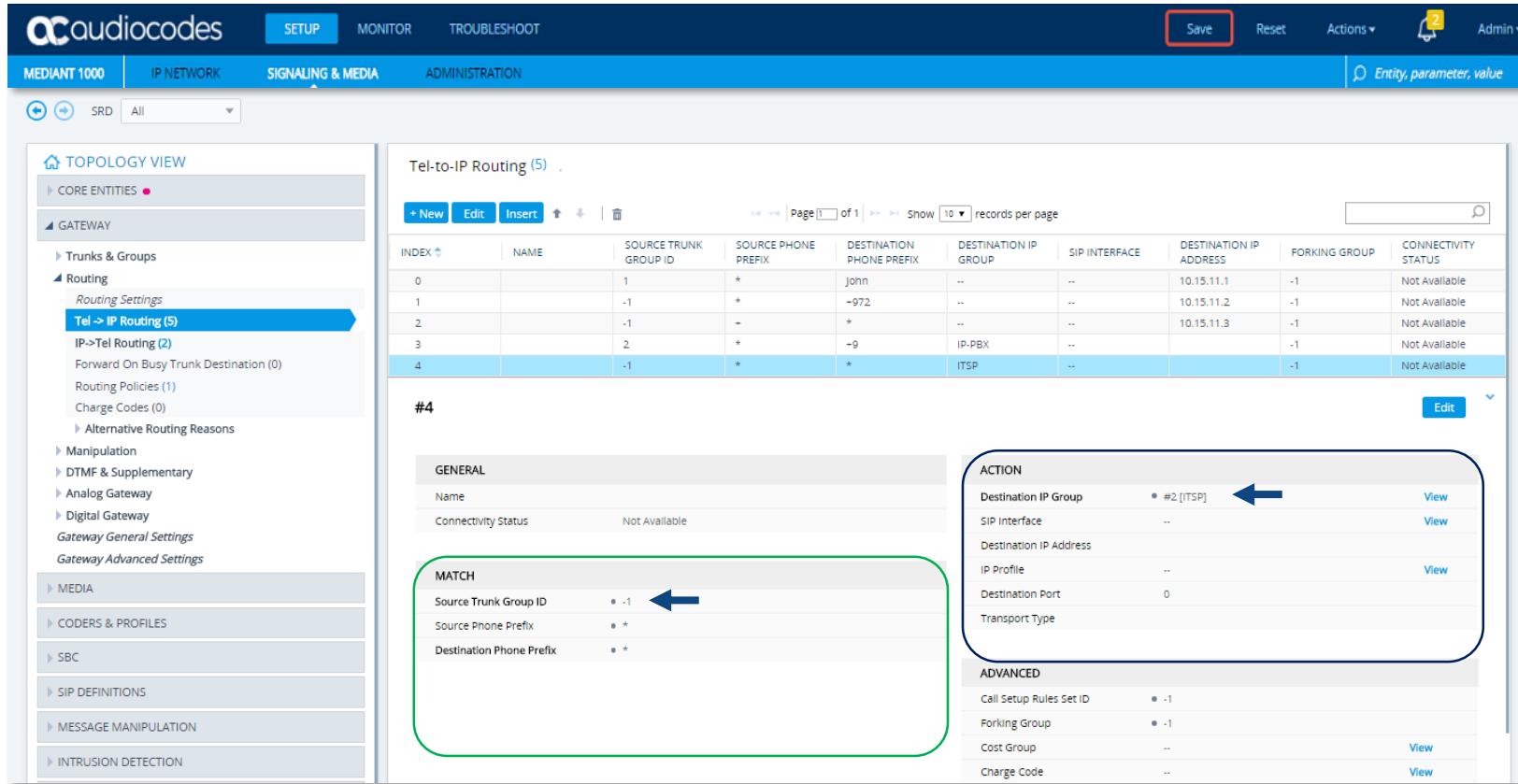
- Top Navigation:** SETUP, MONITOR, TROUBLESHOOT, ADMINISTRATION.
- Left Sidebar (Topology View):** CORE ENTITIES, CODERS & PROFILES (selected), IP Profiles (0), Tel Profiles (0), Coder Settings, Coder Groups (selected), Allowed Audio Coders Groups (0), Allowed Video Coders Groups (0), SBC, GATEWAY, SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, INTRUSION DETECTION, SIP RECORDING.
- Right Content Area:** Coder Groups table.
- Coder Groups Table Headers:** Coder Name, Packetization Time, Rate, Payload Type, Silence Suppression, Coder Specific.
- Coder Groups Table Data:** The table lists several coders with their settings:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711A-law	20	64	8	Disabled	
G.711U-law	20	64	0	Disabled	
G.729	20	8	16	Disabled	
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]
[empty]	[empty]	[empty]	[empty]	[empty]	[empty]

- 2 routing tables for incoming and outgoing calls:
  - Outbound IP Routing Table
    - Tel-to-IP/outbound IP call routing rules
    - The gateway uses these rules to route calls from Tel to IP
  - Inbound IP Routing Table
    - IP-to-Tel/inbound call routing rules
    - The gateway uses these rules to route calls from IP to Tel
- Routing can be performed before or after manipulation rules are applied

# Outbound IP Routing Table (Tel2IP)

- Used to route outgoing calls from Tel to IP



TOPOLOGY VIEW

CORE ENTITIES

GATEWAY

Trunks & Groups

Routing

Routing Settings

Tel->IP Routing (5) **#4**

IP->Tel Routing (2)

Forward On Busy Trunk Destination (0)

Routing Policies (1)

Charge Codes (0)

Alternative Routing Reasons

Manipulation

DTMF & Supplementary

Analog Gateway

Digital Gateway

Gateway General Settings

Gateway Advanced Settings

MEDIA

CODERS & PROFILES

SBC

SIP DEFINITIONS

MESSAGE MANIPULATION

INTRUSION DETECTION

SETUP MONITOR TROUBLESHOOT

Save Reset Actions ▾ Admin ▾

Entity, parameter, value

Tel-to-IP Routing (5) .

INDEX	NAME	SOURCE TRUNK GROUP ID	SOURCE PHONE PREFIX	DESTINATION PHONE PREFIX	DESTINATION IP GROUP	SIP INTERFACE	DESTINATION IP ADDRESS	FORKING GROUP	CONNECTIVITY STATUS
0		1	*	john	--	--	10.15.11.1	-1	Not Available
1		-1	*	+972	--	--	10.15.11.2	-1	Not Available
2		-1	-	*	--	--	10.15.11.3	-1	Not Available
3		2	*	-9	IP-PBX	--	--	-1	Not Available
4		-1	*	*	ITSP	--	--	-1	Not Available

#4

GENERAL

Name: Tel->IP Routing (5)

Connectivity Status: Not Available

MATCH

Source Trunk Group ID: -1

Source Phone Prefix: \*

Destination Phone Prefix: -9

ACTION

Destination IP Group: #2 [ITSP] **#4**

SIP Interface: --

Destination IP Address: --

IP Profile: --

Destination Port: 0

Transport Type: --

ADVANCED

Call Setup Rules Set ID: -1

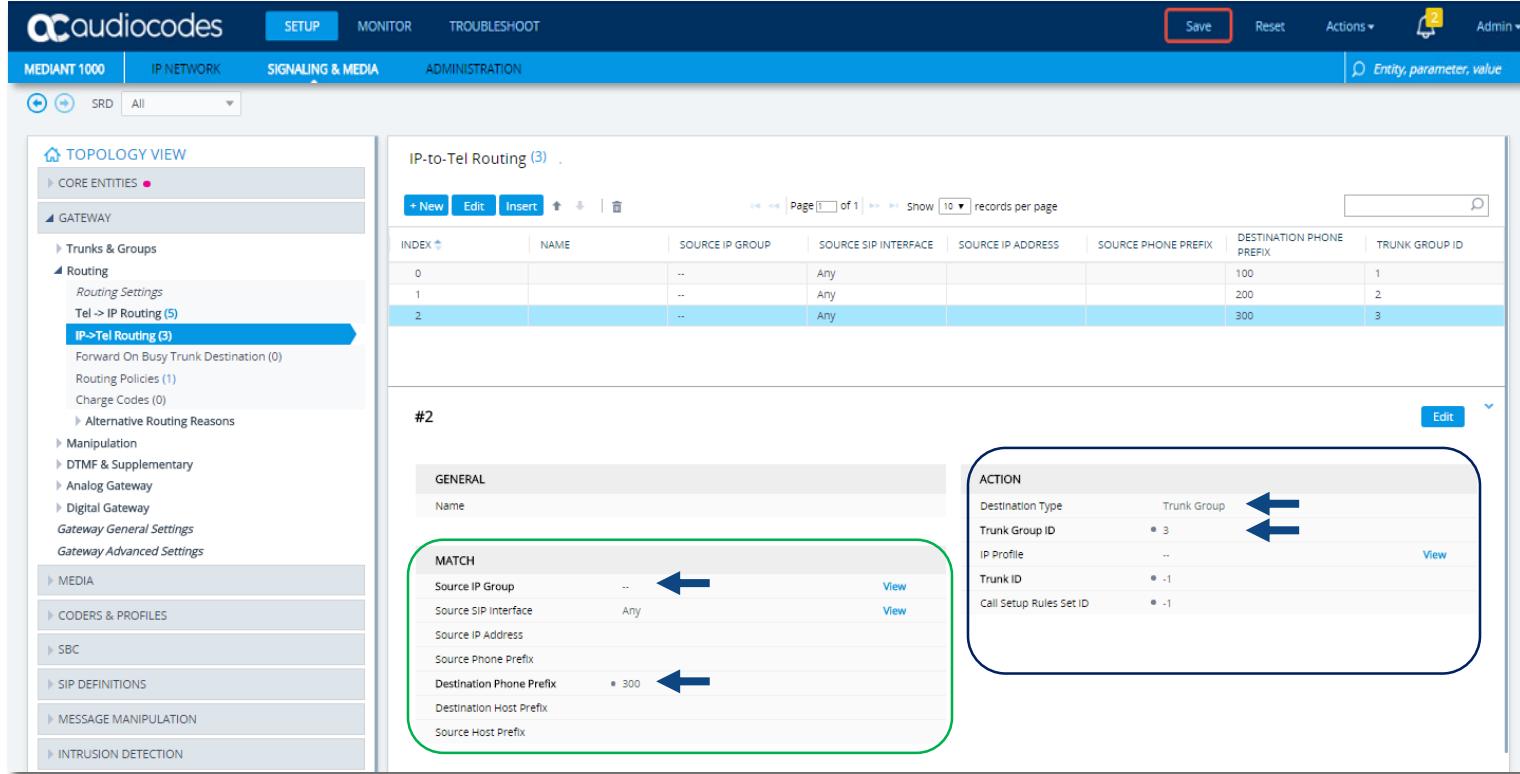
Forking Group: -1

Cost Group: --

Charge Code: --

# IP to Trunk Group Routing (IP2Tel)

- Used to route incoming IP calls to trunk groups
- Route the call to Trunk Group ID



The screenshot shows the audiocodes MEDIANT 1000 web interface. The top navigation bar includes tabs for SETUP, MONITOR, TROUBLESHOOT, and ADMINISTRATION. The main content area is titled "IP-to-Tel Routing (3)". The table displays three entries:

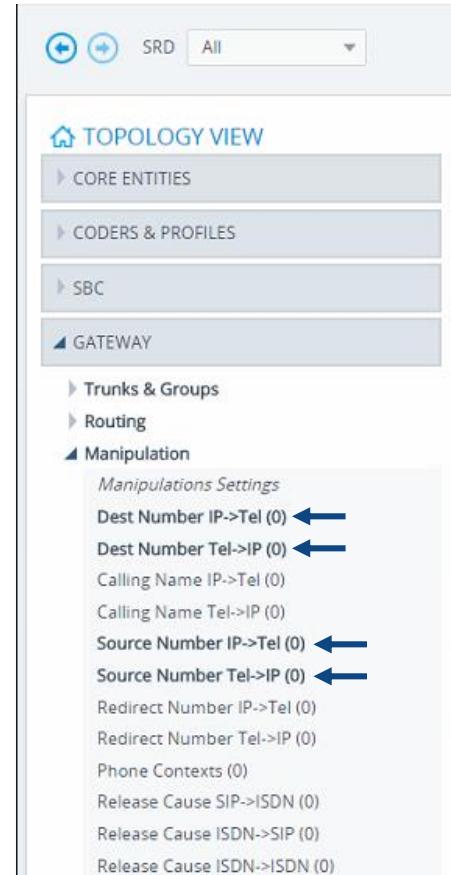
INDEX #	NAME	SOURCE IP GROUP	SOURCE SIP INTERFACE	SOURCE IP ADDRESS	SOURCE PHONE PREFIX	DESTINATION PHONE PREFIX	TRUNK GROUP ID
0		--	Any			100	1
1		--	Any			200	2
2		--	Any			300	3

The left sidebar contains a "TOPOLOGY VIEW" section with "CORE ENTITIES" and a detailed "GATEWAY" section. Under "GATEWAY", "Routing" is expanded, showing "IP->Tel Routing (3)" which is highlighted with a blue arrow. Other sections include "Manipulation", "DTMF & Supplementary", "Analog Gateway", "Digital Gateway", "Gateway General Settings", and "Gateway Advanced Settings".

The right side shows the configuration details for the selected entry (Index #2). It is divided into "GENERAL" and "ACTION" sections. The "GENERAL" section includes fields for "Name" and "MATCH" criteria. The "MATCH" criteria are circled in green and have blue arrows pointing to them. The "ACTION" section includes fields for "Destination Type", "Trunk Group ID", "IP Profile", "Trunk ID", and "Call Setup Rules Set ID". A blue double-headed arrow points between the "Trunk Group ID" field and the "ACTION" section.

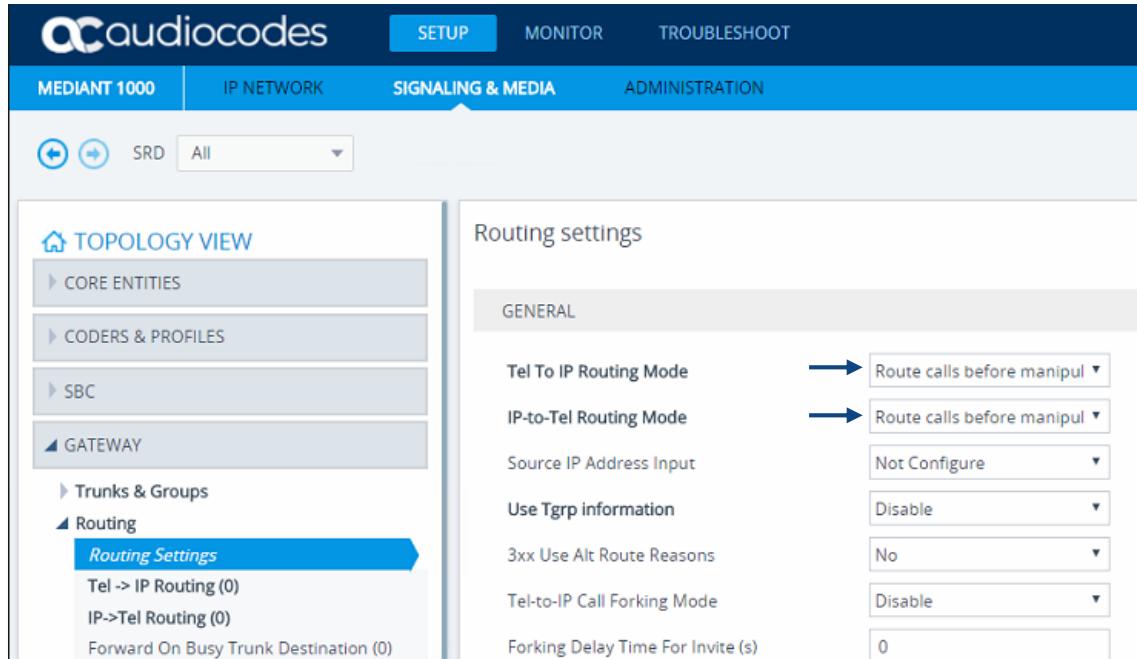
# Number Manipulation

- Number Manipulation tables for incoming and outgoing calls are provided
- Used to modify Destination and Source telephone numbers so that calls can be routed correctly
- Manipulation can occur before or after a routing decision is made
- Using Manipulation Tables you can:
- Allow/Restrict Caller ID information (Source Number for Tel-to-IP Calls)
- Assign NPI/TON to IP-to-Tel calls
- Optionally run a second (additional) ‘round’ of number manipulations for IP-to-Tel calls on an already manipulated number



# Routing Mode Parameters

- The Tel to IP Routing Mode and IP to Tel Routing Mode parameters determine the order between routing calls to Trunk Groups and manipulation of the number
- Route calls before manipulation (default)
- Route calls after manipulation



The screenshot shows the audiocodes MEDIANT 1000 web interface. The top navigation bar includes the audiocodes logo, SETUP (which is highlighted in blue), MONITOR, and TROUBLESHOOT. Below the navigation is a blue header bar with tabs: MEDIANT 1000, IP NETWORK, SIGNALING & MEDIA (which is also highlighted in blue), and ADMINISTRATION.

The main content area has two main sections:

- TOPOLOGY VIEW**: A sidebar with expandable categories: CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, TRUNKS & GROUPS, and ROUTING. The ROUTING section is expanded, and its sub-section **Routing Settings** is also expanded, indicated by a blue arrow pointing to it.
- ROUTING SETTINGS**: This section contains various configuration options:
  - GENERAL** tab
  - Tel To IP Routing Mode**: Set to "Route calls before manipul".
  - IP-to-Tel Routing Mode**: Set to "Route calls before manipul".
  - Source IP Address Input**: Set to "Not Configure".
  - Use Trgrp information**: Set to "Disable".
  - 3xx Use Alt Route Reasons**: Set to "No".
  - Tel-to-IP Call Forking Mode**: Set to "Disable".
  - Forking Delay Time For Invite (s)**: Set to "0".

A digital gateway converts in real time:

- A. Loop start signaling to RTP and variable electric currents to PCM
- B. ISDN to SIP and PCM to RTP
- C. Loop start signaling to SIP and variable electric currents to RTP
- D. All of the above

When I try to stop a trunk I receive an error message - what can I do:

- A. Only resetting the gateway can solve this problem
- B. Assign a different trunk to provide the gateway's clock
- C. Wait for all calls on the trunk to be finished
- D. Stop the trunk via the AdminPage



Which of the following is correct for a Digital Gateway?

- A. All trunk spans must be of the same Line Type (all E1 or all T1)
- B. All trunk spans must be configured with the same protocol
- C. ISDN Network termination should be the same in both sides
- D. All answers are correct

Tel to IP calls are OK but IP to Tel calls fail - a possible reason for that can be:

- A. Miss-configuration of the Proxy server
- B. Coder mismatch
- C. Glare symptoms
- D. Trunk groups are defined but no IP to Tel rules are defined





Lesson 14

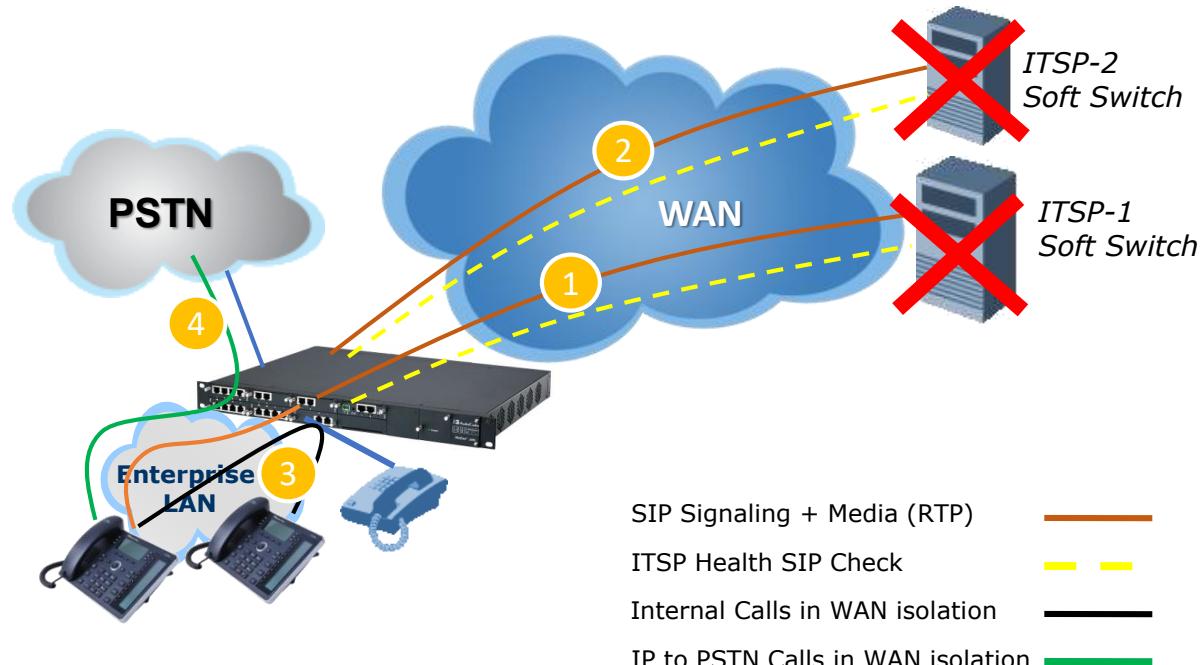
SBC Survivability



- After completing this lesson you'll:
  - Understand the survivability concept
  - Configure the SBC for survivability support
  - Configure the SBC for PSTN Fallback

- 3 survivability features:
  - Routing calls to alternative routes such as:
    - ITSP
    - IP-PBX
  - Routing calls between user agents in the local network using a dynamic DB (built according to registrations of SIP user agents)
  - Fallback to the PSTN based on E1/T1 connection (Hybrid devices)

## Continuous VoIP service for enterprise users on WAN isolation



- Based on the IP-to-IP Routing Table
- Alternative Route Options:
  - Route Row (default):
    - The first route – main routing rule. SBC first attempts to route the call to it
  - Alt Route Ignore Inputs:
    - If the call cannot be routed to the Route Row, the call is routed to this alternative route
    - This route will apply regardless of incoming SIP dialog's input characteristics
  - Alt Route Consider Inputs:
    - If the call cannot be routed to the Route Row, the call is routed to this alternative route
    - Apply only if the incoming SIP dialog matches this routing rule's input characteristics
  - Group Member Ignore Inputs:
    - This routing rule is a member of the Forking routing rule
    - The incoming call is also forked to the destination of this routing rule
    - The matching input characteristics of the routing rule are ignored
  - Group Member Consider Inputs:
    - This routing rule is a member of the Forking routing rule
    - The incoming call is also forked to the destination of this routing rule only if the incoming call matches this rule's input characteristics

# Survivability Methodology

IP-to-IP Routing (4) .

+ New Edit Insert ⌂ ⌄ Page [ ] of 1 >> >> Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	IP-PBX -> ITSP 1	Default_SBCRout	Route Row	IP-PBX	All	*	*	IP Group	ITSP 1	..	
1	IP-PBX -> ITSP 2	Default_SBCRout	Alternative Route	IP-PBX	All	*	*	IP Group	ITSP 2	..	
2	ITSP 1 -> IP-PBX	Default_SBCRout	Route Row	ITSP 1	All	*	*	IP Group	IP-PBX	..	
3	ITSP 2 -> IP-PBX	Default_SBCRout	Route Row	ITSP 2	All	*	*	IP Group	IP-PBX	..	

#1[IP-PBX -> ITSP 2] #0 [Default\_SBCRoutingPolicy]

Edit

**GENERAL**

Name	IP-PBX -> ITSP 2
Alternative Route Options	Alternative Route Ignore Inputs

**MATCH**

Source IP Group	#1 [IP-PBX]
Request Type	All
Source Username Prefix	*
Source Host	*
Source Tag	
Destination Username Pre...	*
Destination Host	*

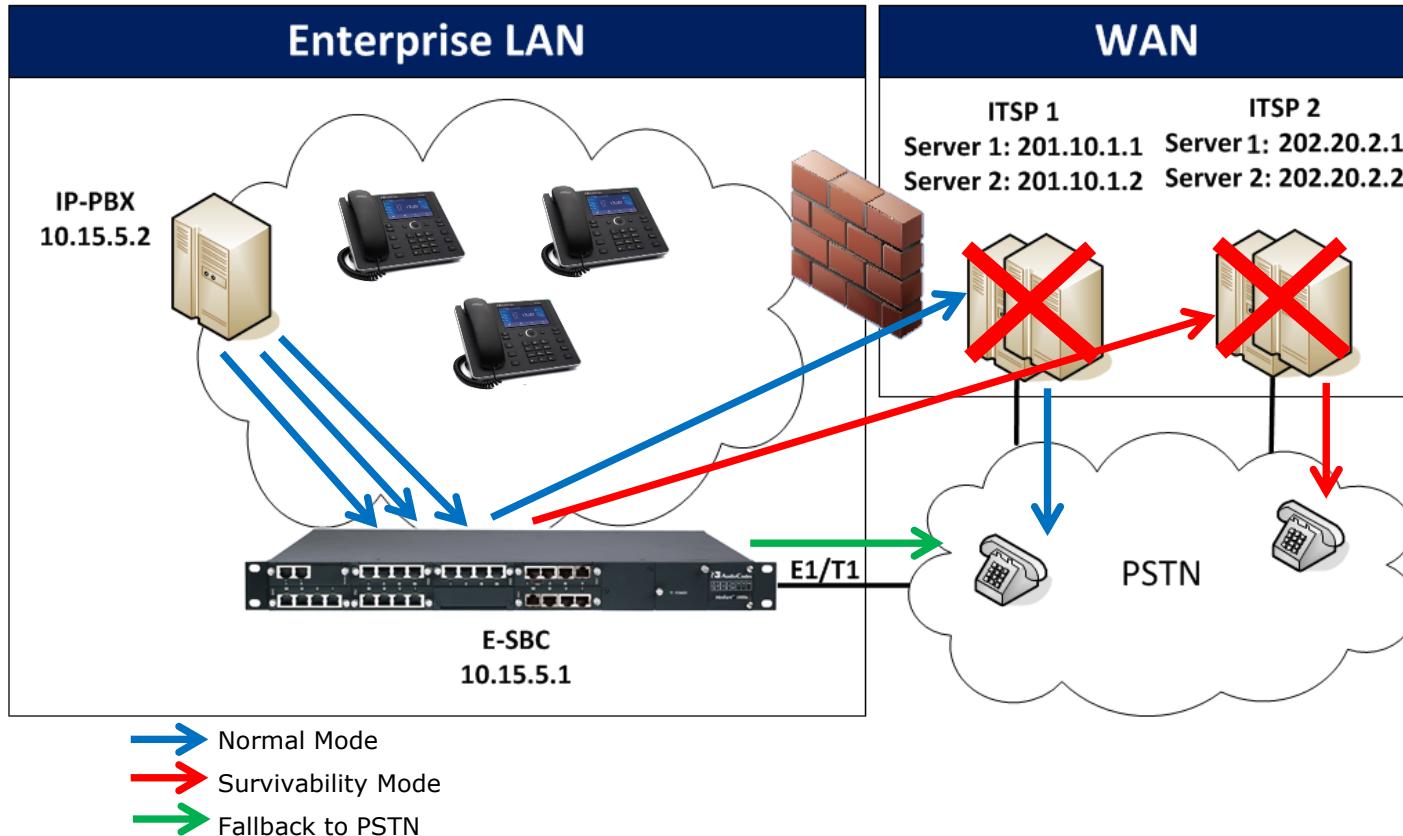
**ACTION**

Destination Type	IP Group
Destination IP Group	#3 [ITSP 2]
Destination SIP Interface	..
Destination Address	
Destination Port	0
Destination Transport Type	
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	..

The alternative routing entry must be defined in the next consecutive table entry index

439

# SBC Survivability for IP-PBX Users



# Define Media Realms

audiocodes

SETUP MONITOR TROUBLESHOOT Save Reset Actions 11 Admin

M800 IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SRD All

### TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (1)
- Media Realms (2)**
- Proxy Sets (1)
- IP Groups (1)

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

### Media Realms (2) .

+ New Edit | 1 of 1 | Show 10 records per page

INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MR-PBX	O+M+C	6000	50	6499	No
1	MR-ITSP	O+M+C	7000	50	7499	No

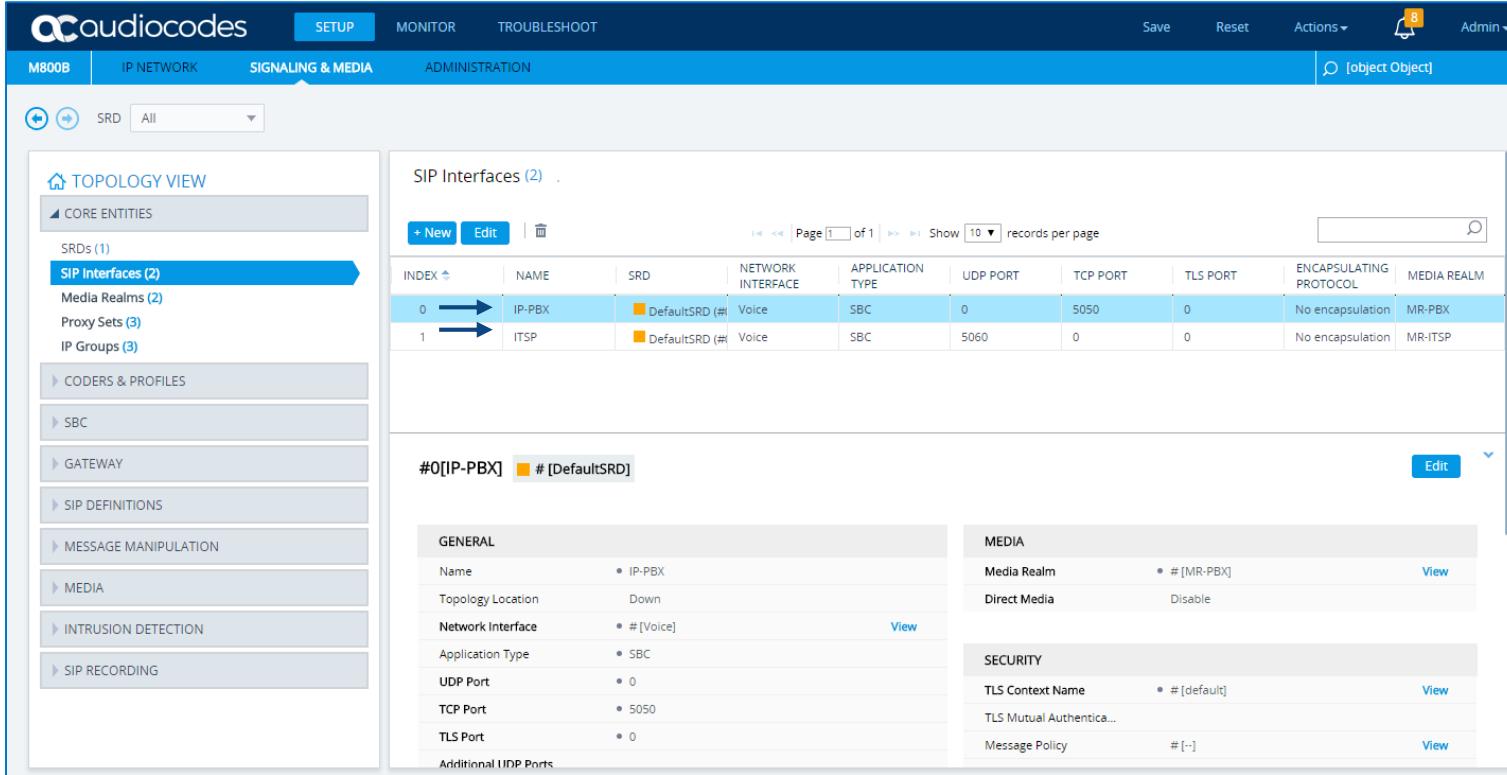
#### #1[MR-ITSP]

Edit

GENERAL		QUALITY OF EXPERIENCE	
Name	MR-ITSP	QoE Profile	# [-] <a href="#">View</a>
Topology Location	Up	Bandwidth Profile	# [-] <a href="#">View</a>
IPv4 Interface Name	# [O+M+C]	View	
Port Range Start	7000		
Number Of Media Ses...	50		
Port Range End	7499		

# Define SIP Interfaces

- SIP Interface IP-PBX: SIP port (5050) for IP-PBX, SBC application, assigned to MR-PBX
- SIP Interface ITSPs: SIP port (5060) for ITSPs, SBC application, assigned to MR-ITSP



The screenshot shows the audiocodes M800B web interface under the **SETUP** tab. The left sidebar navigation includes **TOPLOGY VIEW**, **CORE ENTITIES** (SRDs 1, SIP Interfaces 2), **CODERS & PROFILES**, **SBC**, **GATEWAY**, **SIP DEFINITIONS**, **MESSAGE MANIPULATION**, **MEDIA**, **INTRUSION DETECTION**, and **SIP RECORDING**. The main content area is titled **SIP Interfaces (2)**. It displays a table with two entries:

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATING PROTOCOL	MEDIA REALM
0	IP-PBX	DefaultSRD (#)	Voice	SBC	0	5050	0	No encapsulation	MR-PBX
1	ITSP	DefaultSRD (#)	Voice	SBC	5060	0	0	No encapsulation	MR-ITSP

Below the table, there is a summary row: **#0[IP-PBX] # [DefaultSRD]**. The detailed configuration for the IP-PBX entry is shown in three tabs: **GENERAL**, **MEDIA**, and **SECURITY**.

**GENERAL** tab details:

- Name: IP-PBX
- Topology Location: Down
- Network Interface: # [Voice]
- Application Type: SBC
- UDP Port: 0
- TCP Port: 5050
- TLS Port: 0
- Additional UDP Ports: [..]

**MEDIA** tab details:

- Media Realm: # [MR-PBX]
- Direct Media: Disable

**SECURITY** tab details:

- TLS Context Name: # [default]
- TLS Mutual Authentica...
- Message Policy: # [-]

# Define Proxy Set – IP-PBX



SERIALIZED

TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)**
- IP Groups (1)

CODERS & PROFILES

SBC •

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

SRD All

Proxy Sets (2)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	GATEWAY IPv4 SIP INTERFACE	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	--	IP-PBX	60		Disable
1	IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Disable

#1[IP-PBX] # [DefaultSRD] Edit

GENERAL

Name	IP-PBX
Gateway IPv4 SIP Interface	# [-]
SBC IPv4 SIP Interface	# [IP-PBX]
TLS Context Name	# [-]

REduNDANCY

Redundancy Mode	
Proxy Hot Swap	Disable
Proxy Load Balancing Meth...	Disable
Min. Active Servers for Loa...	1

KEEP ALIVE

Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Keep-Alive Failure Responses	
Success Detection Retries	1
Success Detection Interval	10
Failure Detection Retransmi...	-1

ADVANCED

Classification Input	IP Address only
DNS Resolve Method	

PROXY ADDRESS

10.15.11.2:5050	TCP
-----------------	-----

Save Reset Actions ▾ Admin ▾

object Object

# Define Proxy Set – ITSP 1



SERIALIZED

TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (3)**
- IP Groups (1)

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

SETUP MONITOR TROUBLESHOOT

SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions Admin

SRD All

### Proxy Sets (3) .

+ New Edit | # [ITSP 1] # [DefaultSRD]

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	GATEWAY IPv4 SIP INTERFACE	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	--	IP-PBX	60		Disable
1	IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Disable
2	ITSP 1	DefaultSRD (#0)	--	ITSP	60		Enable

**#2[ITSP 1] # [DefaultSRD]**

**GENERAL**

Name	ITSP 1	<span style="color: blue;">←</span>
Gateway IPv4 SIP Interface	# [-]	<span style="color: blue;">←</span>
SBC IPv4 SIP Interface	# [ITSP]	<span style="color: blue;">←</span>
TLS Context Name	# [-]	<span style="color: blue;">←</span>

**REDUNDANCY**

Redundancy Mode		
Proxy Hot Swap	• Enable	<span style="color: blue;">←</span>
Proxy Load Balancing Meth...	• Round Robin	<span style="color: blue;">←</span>
Min. Active Servers for Lo...	1	

**KEEP ALIVE**

Proxy Keep-Alive	• Using OPTIONS	<span style="color: blue;">←</span>
Proxy Keep-Alive Time [sec]	60	<span style="color: blue;">←</span>
Keep-Alive Failure Responses		
Success Detection Retries	1	
Success Detection Interval	10	
Failure Detection Retransm...	-1	

**ADVANCED**

Classification Input	IP Address only
DNS Resolve Method	

**PROXY ADDRESS**

201.10.1.1:5060	UDP	<span style="color: blue;">←</span>
201.10.1.2:5060	UDP	<span style="color: blue;">←</span>

444

# Define Proxy Set – ITSP 2



SERIALIZED BY: [object Object]

6 Admin ▾

Save Reset Actions ▾

TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (4)**
- IP Groups (1)

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

TOPIC

SETUP MONITOR TROUBLESHOOT

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

SRD All

Proxy Sets (4) .

+ New Edit | Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	GATEWAY IPv4 SIP INTERFACE	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0)	--	IP-PBX	60		Disable
1	IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Disable
2	ITSP 1	DefaultSRD (#0)	--	ITSP	60		Enable
3	ITSP 2	DefaultSRD (#0)	--	ITSP	60		Enable

#3[ITSP 2] # [DefaultSRD] Edit

GENERAL

Name	ITSP 2	View
Gateway IPv4 SIP Interface	# [-]	View
SBC IPv4 SIP Interface	# [ITSP]	View
TLS Context Name	# [-]	View

REduNDANCY

Redundancy Mode	Enable
Proxy Hot Swap	Round Robin
Proxy Load Balancing Meth...	
Min. Active Servers for Lo...	1

KEEP ALIVE

Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Keep-Alive Failure Responses	
Success Detection Retries	1
Success Detection Interval	10
Failure Detection Retransm...	-1

ADVANCED

Classification Input	IP Address only
DNS Resolve Method	

PROXY ADDRESS TYPE

202.20.2.1:5060	UDP
202.20.2.2:5060	UDP

445

# Define IP Group – IP-PBX



audiocodes

SETUP MONITOR TROUBLESHOOT

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions ▾ Admin ▾

SRD All

### TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (4)
- IP Groups (2)**

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

### IP Groups (2)

+ New Edit | Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPG	DefaultSRD (#)	Server	Not Configured	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	DefaultSRD (#)	Server	Not Configured	IP-PBX	--	MR-PBX		Enable	-1	-1

#1[IP-PBX] # [DefaultSRD]

Edit

**GENERAL**

Name	IP-PBX	←
Topology Location	Down	
Type	Server	←
Proxy Set	# [IP-PBX]	←
IP Profile	# [-]	View
Media Realm	# [MR-PBX]	View
Contact User		
SIP Group Name		
Created By Routing Server	No	
Used By Routing Server	Not Used	
Proxy Set Connectivity	Not Connected	

**QUALITY OF EXPERIENCE**

QoE Profile	# [-]	View
Bandwidth Profile	# [-]	View

**MESSAGE MANIPULATION**

Inbound Message Manipula...	-1
Outbound Message Manipl...	-1
Message Manipulation Use...	
Message Manipulation Use...	

**SBC REGISTRATION AND AUTHENTICATION**

Max. Number of Registered...	-1
------------------------------	----

# Define IP Group – ITSP 1



audiocodes

SETUP MONITOR TROUBLESHOOT

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions Admin ▾

SRD All

TOPLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (4)
- IP Groups (3)**

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

IP Groups (3)

+ New Edit | # [ITSP 1]

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_JPG	DefaultSRD (#)	Server	Not Configured	ProxySet_0	..	..	..	Disable	-1	-1
1	IP-PBX	DefaultSRD (#)	Server	Not Configured	IP-PBX	..	MR-PBX	..	Enable	-1	-1
2	ITSP 1	DefaultSRD (#)	Server	Not Configured	ITSP 1	..	MR-ITSP	..	Enable	-1	-1

#2[ITSP 1] # [DefaultSRD]

Edit

GENERAL

Name	ITSP 1	←
Topology Location	Up	←
Type	Server	←
Proxy Set	# [ITSP 1]	←
IP Profile	# [-]	View
Media Realm	# [MR-ITSP]	View
Contact User		
SIP Group Name		
Created By Routing Server	No	
Used By Routing Server	Not Used	
Proxy Set Connectivity	Not Connected	

QUALITY OF EXPERIENCE

QoE Profile	# [-]	View
Bandwidth Profile	# [-]	View

MESSAGE MANIPULATION

Inbound Message Manipula...	-1
Outbound Message Manipl...	-1
Message Manipulation Use...	
Message Manipulation Use...	

SBC REGISTRATION AND AUTHENTICATION

Max. Number of Registered...	-1
------------------------------	----

447

# Define IP Group – ITSP 2



SERIAL NUMBER: M800B | IP NETWORK | SIGNALING & MEDIA | ADMINISTRATION | Save | Reset | Actions | Admin

SRD All

### TOPOLOGY VIEW

CORE ENTITIES

- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (4)
- IP Groups (4)**

CODERS & PROFILES

SBC

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

### IP Groups (4)

+ New | Edit | Delete | Page 1 of 1 | Show 10 records per page | Search

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	Default_IPG	DefaultSRD #	Server	Not Configured	ProxySet_0	..	..	..	Disable	-1	-1
1	IP-PBX	DefaultSRD #	Server	Not Configured	IP-PBX	..	MR-PBX	..	Enable	-1	-1
2	ITSP 1	DefaultSRD #	Server	Not Configured	ITSP 1	..	MR-ITSP	..	Enable	-1	-1
3	ITSP 2	DefaultSRD #	Server	Not Configured	ITSP 2	..	MR-ITSP	..	Enable	-1	-1

#3[ITSP 2] [DefaultSRD]

Edit

**GENERAL**

Name	ITSP 2	←
Topology Location	Up	←
Type	Server	←
Proxy Set	# [ITSP 2]	←
IP Profile	# [-]	View
Media Realm	# [MR-ITSP]	View
Contact User		
SIP Group Name		
Created By Routing Server	No	
Used By Routing Server	Not Used	
Proxy Set Connectivity	Not Connected	

**QUALITY OF EXPERIENCE**

QoE Profile	# [-]	View
Bandwidth Profile	# [-]	View

**MESSAGE MANIPULATION**

Inbound Message Manipula...	-1
Outbound Message Manipl...	-1
Message Manipulation Use...	
Message Manipulation Use...	

**SBC REGISTRATION AND AUTHENTICATION**

Max. Number of Registered...	-1
------------------------------	----

# IP to IP Routing Table – IP-PBX to ITSP 1 (Primary Route)



SERIAL NUMBER: M800B

IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions ▾ Admin ▾

SRD All

TOPOLOGY VIEW

CORE ENTITIES

CODERS & PROFILES

SBC

Classification (0)

Routing Policies (1)

IP-to-IP Routing (2)

- Alternative Reasons (0)
- IP Group Set (0)

Manipulation

- SBC General Settings
- Call Admission Control Profile (0)
- Malicious Signature (12)
- External Media Source (0)

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

IP-to-IP Routing (2)

+ New Edit Insert Page 1 of 1 Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	OPTIONS terminal	Default_SBCRouter	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	IP-PBX to ITSP 1	Default_SBCRouter	Route Row	IP-PBX	All	*	*	IP Group	ITSP 1	--	

#1[IP-PBX to ITSP 1] # [Default\_SBCRoutingPolicy]

Edit

GENERAL

Name	IP-PBX to ITSP 1	←
Alternative Route Options	Route Row	←

ACTION

Destination Type	IP Group	←
Destination IP Group	# [ITSP 1]	←
Destination SIP Interface	# [-]	View
Destination Address		
Destination Port	0	
Destination Transport Type		
IP Group Set	# [-]	View
Call Setup Rules Set ID	-1	
Group Policy	Sequential	
Cost Group	# [-]	View
Routing Tag Name	default	
Internal Action		

Match

Source IP Group	# [IP-PBX]	←
Request Type	All	
Source Username Pattern	*	
Source Host	*	
Source Tag		
Destination Username Pattern	*	
Destination Host	*	
Destination Tag		

View

# IP to IP Routing Table – IP-PBX to ITSP 2 (Alternative Route)



**TOPOLOGY VIEW**

- CORE ENTITIES
- CODERS & PROFILES
- SBC**
  - Classification (0)
  - Routing**
    - Routing Policies (1)
      - IP-to-IP Routing (3)**
        - Alternative Reasons (0)
        - IP Group Set (0)
- GATEWAY
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- MEDIA
- INTRUSION DETECTION
- SIP RECORDING

**SETUP** MONITOR TROUBLESHOOT ADMINISTRATION

Save Reset Actions 10 Admin ▾

SRD All

**IP-to-IP Routing (3) .**

+ New	Edit	Insert	Page 1 of 1	Show 10 records per page							
INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	OPTIONS terminal	Default_SBCRoute	Route Row	Any	OPTIONS	*	*	Dest Address	..	..	internal
1	IP-PBX to ITSP 1	Default_SBCRoute	Route Row	IP-PBX	All	*	*	IP Group	ITSP 1	..	
2	IP-PBX to ITSP 2	Default_SBCRoute	Alternative Route	IP-PBX	All	*	*	IP Group	ITSP 2	..	

#2[IP-PBX to ITSP 2] # [Default\_SBCRoutingPolicy]

**GENERAL**

Name	• IP-PBX to ITSP 2	←
Alternative Route Options	• Alternative Route Ignore Inputs	←

**MATCH**

Source IP Group	• # [IP-PBX]	←	View
Request Type	All		
Source Username Pattern	*		
Source Host	*		
Source Tag			
Destination Username Pattern	*		
Destination Host	*		
Destination Tag			

**ACTION**

Destination Type	IP Group	←	
Destination IP Group	• # [ITSP 2]	←	View
Destination SIP Interface	# [-]		View
Destination Address			
Destination Port	0		
Destination Transport Type			
IP Group Set	# [-]		View
Call Setup Rules Set ID	-1		
Group Policy	Sequential		
Cost Group	# [-]		View
Routing Tag Name	default		
Internal Action			

# IP to IP Routing Table – ITSP 1 to IP-PBX



audiocodes

SETUP MONITOR TROUBLESHOOT

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions 10 Admin

SRD All

TOPOLOGY VIEW

CORE ENTITIES

CODERS & PROFILES

SBC

Classification (0)

Routing

Routing Policies (1)

IP-to-IP Routing (4)

Alternative Reasons (0)

IP Group Set (0)

Manipulation

SBC General Settings

Call Admission Control Profile (0)

Malicious Signature (12)

External Media Source (0)

GATEWAY

SIP DEFINITIONS

MESSAGE MANIPULATION

MEDIA

INTRUSION DETECTION

SIP RECORDING

IP-to-IP Routing (4)

+ New Edit Insert Page 1 of 1 Show 10 records per page

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	OPTIONS terminal	Default_SBCRoute	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	IP-PBX to ITSP 1	Default_SBCRoute	Route Row	IP-PBX	All	*	*	IP Group	ITSP 1	--	
2	IP-PBX to ITSP 2	Default_SBCRoute	Alternative Route	IP-PBX	All	*	*	IP Group	ITSP 2	--	
3	ITSP 1 to IP-PBX	Default_SBCRoute	Route Row	ITSP 1	All	*	*	IP Group	IP-PBX	--	

#3[ITSP 1 to IP-PBX] # [Default\_SBCRoutingPolicy]

Edit

GENERAL

Name: ITSP 1 to IP-PBX

Alternative Route Options: Route Row

ACTION

Destination Type: IP Group

Destination IP Group: # [IP-PBX]

Match

Source IP Group: # [ITSP 1]

Request Type: All

Source Username Pattern: \*

Source Host: \*

Source Tag: \*

Destination Username Pattern: \*

Destination Host: \*

Destination Tag: \*

ACTION

Destination Type: IP Group

Destination IP Group: # [IP-PBX]

Destination SIP Interface: # [-]

Destination Address:

Destination Port: 0

Destination Transport Type:

IP Group Set: # [-]

Call Setup Rules Set ID: -1

Group Policy: Sequential

Cost Group: # [-]

Routing Tag Name: default

Internal Action:

# IP to IP Routing Table – ITSP 2 to IP-PBX



**TOPOLOGY VIEW**

- CORE ENTITIES
- CODERS & PROFILES
- SBC**
  - Classification (0)
  - Routing**
    - Routing Policies (1)
    - IP-to-IP Routing (5)** # [ITSP 2 to IP-PBX] # [Default\_SBCRoutingPolicy]
    - Alternative Reasons (0)
    - IP Group Set (0)
  - Manipulation
  - SBC General Settings
  - Call Admission Control Profile (0)
  - Malicious Signature (12)
  - External Media Source (0)
- GATEWAY
- SIP DEFINITIONS
- MESSAGE MANIPULATION
- MEDIA
- INTRUSION DETECTION
- SIP RECORDING

**IP-to-IP Routing (5)**

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	OPTIONS terminal	Default_SBCRoute	Route Row	Any	OPTIONS	*	*	Dest Address	..	..	internal
1	IP-PBX to ITSP 1	Default_SBCRoute	Route Row	IP-PBX	All	*	*	IP Group	ITSP 1	..	
2	IP-PBX to ITSP 2	Default_SBCRoute	Alternative Route	IP-PBX	All	*	*	IP Group	ITSP 2	..	
3	ITSP 1 to IP-PBX	Default_SBCRoute	Route Row	ITSP 1	All	*	*	IP Group	IP-PBX	..	
4	ITSP 2 to IP-PBX	Default_SBCRoute	Route Row	ITSP 2	All	*	*	IP Group	IP-PBX	..	

**GENERAL**

Name	• ITSP 2 to IP-PBX	←
Alternative Route Options	Route Row	←

**MATCH**

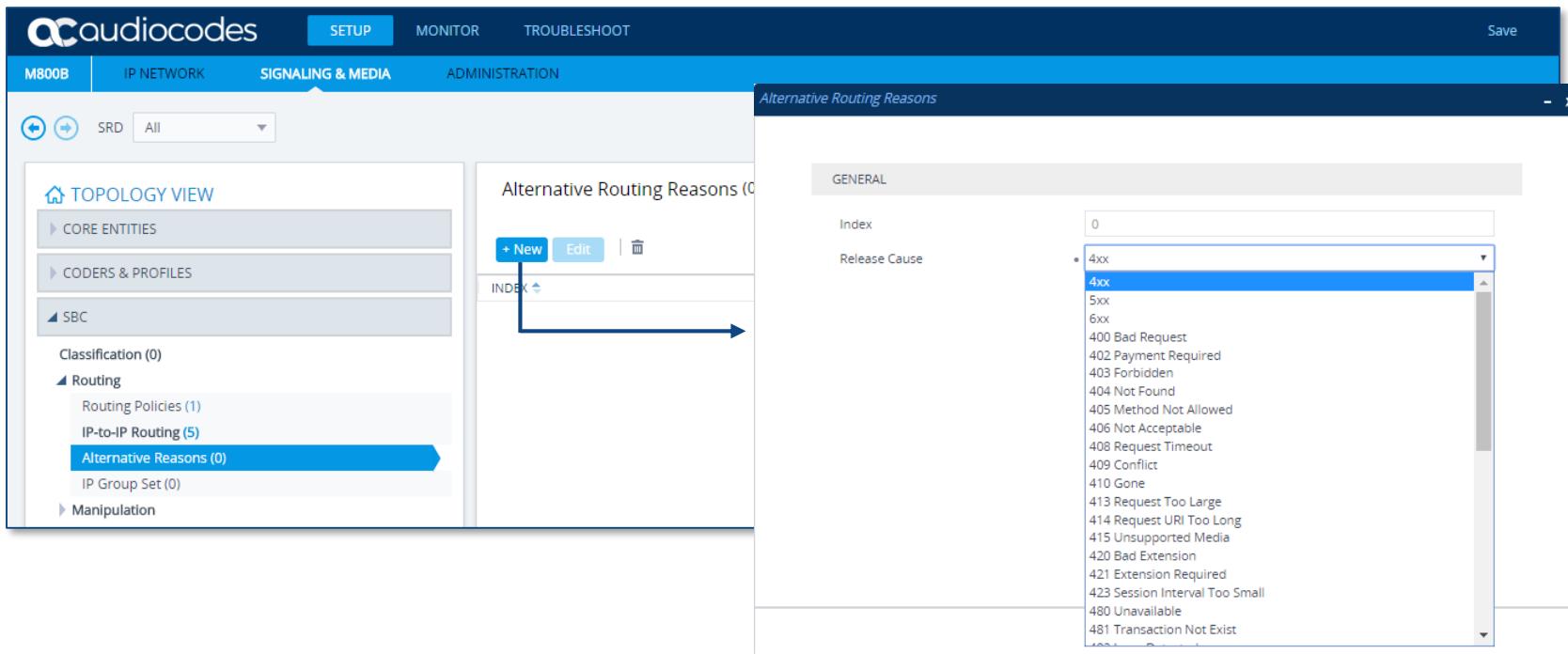
Source IP Group	• # [ITSP 2]	←	View
Request Type	All		
Source Username Pattern	*		
Source Host	*		
Source Tag			
Destination Username Pattern	*		
Destination Host	*		
Destination Tag			
Message Condition	# f..1		View

**ACTION**

Destination Type	IP Group	←	
Destination IP Group	• # [IP-PBX]	←	View
Destination SIP Interface	# [-]		View
Destination Address			
Destination Port	0		
Destination Transport Type			
IP Group Set	# [-]		View
Call Setup Rules Set ID	-1		
Group Policy	Sequential		
Cost Group	# [-]		View
Routing Tag Name	default		
Internal Action			

# Define Alternative Routing Reasons

- Enables defining up to 20 different call release reasons for call releases
- If no response, or ICMP or SIP 408 response is received, the SBC attempts to use the alternative route even if no entries are configured in the 'Alternative Routing Reasons'



The screenshot shows the audiocodes M800B web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. Below it, the main menu has tabs for 'M800B', 'IP NETWORK', 'SIGNALING & MEDIA', and 'ADMINISTRATION'. The 'SIGNALING & MEDIA' tab is selected. On the left, a sidebar under 'TOPLOGY VIEW' shows 'CORE ENTITIES', 'CODERS & PROFILES', and 'SBC'. Under 'SBC', 'Classification (0)', 'Routing' (which is expanded), 'Routing Policies (1)', 'IP-to-IP Routing (5)', and 'Alternative Reasons (0)' are listed. 'Alternative Reasons (0)' is highlighted with a blue arrow. The main content area displays the 'Alternative Routing Reasons' configuration window. This window has a 'GENERAL' tab and a 'Release Cause' dropdown menu. The dropdown menu lists various HTTP and SIP status codes categorized by index: 0, 4xx (selected), 5xx, 6xx, 400 Bad Request, 402 Payment Required, 403 Forbidden, 404 Not Found, 405 Method Not Allowed, 406 Not Acceptable, 408 Request Timeout, 409 Conflict, 410 Gone, 413 Request Too Large, 414 Request URI Too Long, 415 Unsupported Media, 420 Bad Extension, 421 Extension Required, 423 Session Interval Too Small, 480 Unavailable, and 481 Transaction Not Exist.

Index	Release Cause
0	4xx
	5xx
	6xx
	400 Bad Request
	402 Payment Required
	403 Forbidden
	404 Not Found
	405 Method Not Allowed
	406 Not Acceptable
	408 Request Timeout
	409 Conflict
	410 Gone
	413 Request Too Large
	414 Request URI Too Long
	415 Unsupported Media
	420 Bad Extension
	421 Extension Required
	423 Session Interval Too Small
	480 Unavailable
	481 Transaction Not Exist

- As was seen before, for the Gateway configure the following:
  - On the TDM tab
    - The TDM Bus Clock Source (Network/Internal)
    - The TDM Bus PSTN Auto FallBack Clock (relevant if TDMBusClockSource = Network)
    - The TDM Bus Local Reference
    - The PCM Law Select (A-law/ $\mu$ -law)
  - On the PSTN tab
    - The Protocol Type (E1 Euro ISDN, others)
    - The Clock Master of E1/T1 line (Recovered/Generated)
    - The ISDN Termination Side (User/Network side)

# Configure the TDM Bus for the Gateway



SERIAL NUMBER: M800

SETUP MONITOR TROUBLESHOOT

Save Reset Actions Entity, parameter, value Admin

CODERS & PROFILES

SBC

GATEWAY

- Trunks & Groups
- Routing
  - Routing Settings (0)
  - Tel->IP Routing (0)
  - IP->Tel Routing (0)
  - Forward On Busy Trunk Destination (0)
  - Routing Policies (1)
  - Charge Codes (0)
  - Alternative Routing Reasons
- Manipulation
- DTMF & Supplementary
- Analog Gateway
- Digital Gateway
- Gateway General Settings
- Gateway Advanced Settings

TDM Bus Settings

**TDM Bus Settings**

**GENERAL**

TDM Bus Clock Source	internal	⚡
TDM Bus PSTN Auto FallBack Clock	Disable	⚡
TDM Bus PSTN Auto Clock Reverting	Disable	⚡
TDM Bus Local Reference	1	⚡

**DIGITAL PCM**

PCM Law Select	MuLaw	⚡
Idle PCM Pattern	255	⚡
Idle ABCD Pattern	0x0F	⚡

SRD All

# Configure the Digital Trunk

audiocodes

SETUP MONITOR TROUBLESHOOT

M800 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions Entity, parameter, value Admin

SRD All

**TOPOLOGY VIEW**

- CORE ENTITIES
- CODERS & PROFILES
- SBC
- GATEWAY
  - Trunks & Groups
    - Trunks
      - Trunk Groups
      - Trunk Group Settings (1)
      - CAS State Machines
    - Routing
      - Routing Settings
        - Tel -> IP Routing (0)
        - IP->Tel Routing (0)
        - Forward On Busy Trunk Destination (0)
      - Routing Policies (1)
      - Charge Codes (0)
      - Alternative Routing Reasons
    - Manipulation
    - DTMF & Supplementary
    - Analog Gateway
    - Digital Gateway
      - Gateway General Settings
      - Gateway Advanced Settings
      - TDM Bus Settings
    - SIP DEFINITIONS

### Trunk Settings

GENERAL

Module ID	1
Trunk ID	1
Trunk Configuration State	Active
Protocol Type	E1 EURO ISDN

TRUNK CONFIGURATION

Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	HDB3
Line Build Out Loss	0 dB
Trace Level	No Trace
Line Build Out Overwrite	OFF
Framing Method	E1 FRAMING MFF CRC4 EXT

ISDN CONFIGURATION

ISDN Termination Side	User side
-----------------------	-----------

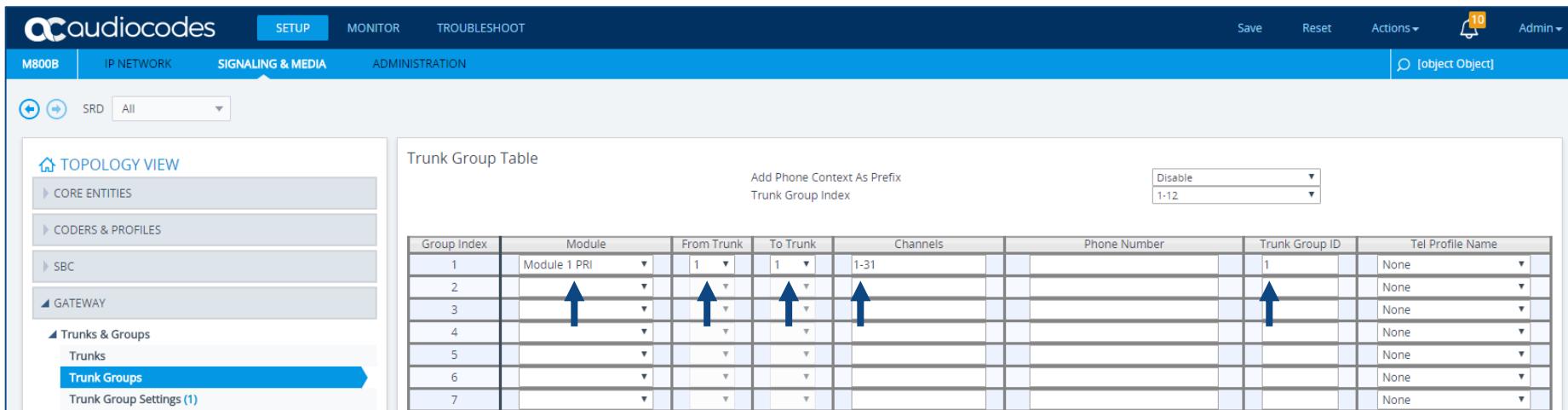
ADVANCED SETTINGS

PSTN Alert Timeout	-1
Transfer Mode	Disable
Local ISDN Ringback Tone Source	PBX
Set PI In Rx Disconnect Message	Not Configured
ISDN Transfer Capabilities	Not Configured
Progress Indicator to ISDN	Not Configured
Select Receiving of Overlap Dialing	None
B-channel Negotiation	Not Configured
Out-Of-Service Behavior	Not Configured
Remove Calling Name	Use Global Parameter
Play Ringback Tone to Trunk	Not Configured
Call Rerouting Mode	None
ISDN Duplicate Q931 BuffMode	0
Trunk Name	

Submit Stop Trunk Deactivate Trunk Create Loopback

# Configure the Trunk Group – E1/T1

- Used to assign Trunk Groups, Profiles and logical telephone numbers to the gateway's channels



audiocodes

SETUP MONITOR TROUBLESHOOT

M800B IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions ▾

Object Object

TOP TOPOLOGY VIEW

CORE ENTITIES

CODERS & PROFILES

SBC

GATEWAY

Trunks & Groups

Trunks

Trunk Groups

Trunk Group Settings (1)

Trunk Group Table

Add Phone Context As Prefix

Trunk Group Index

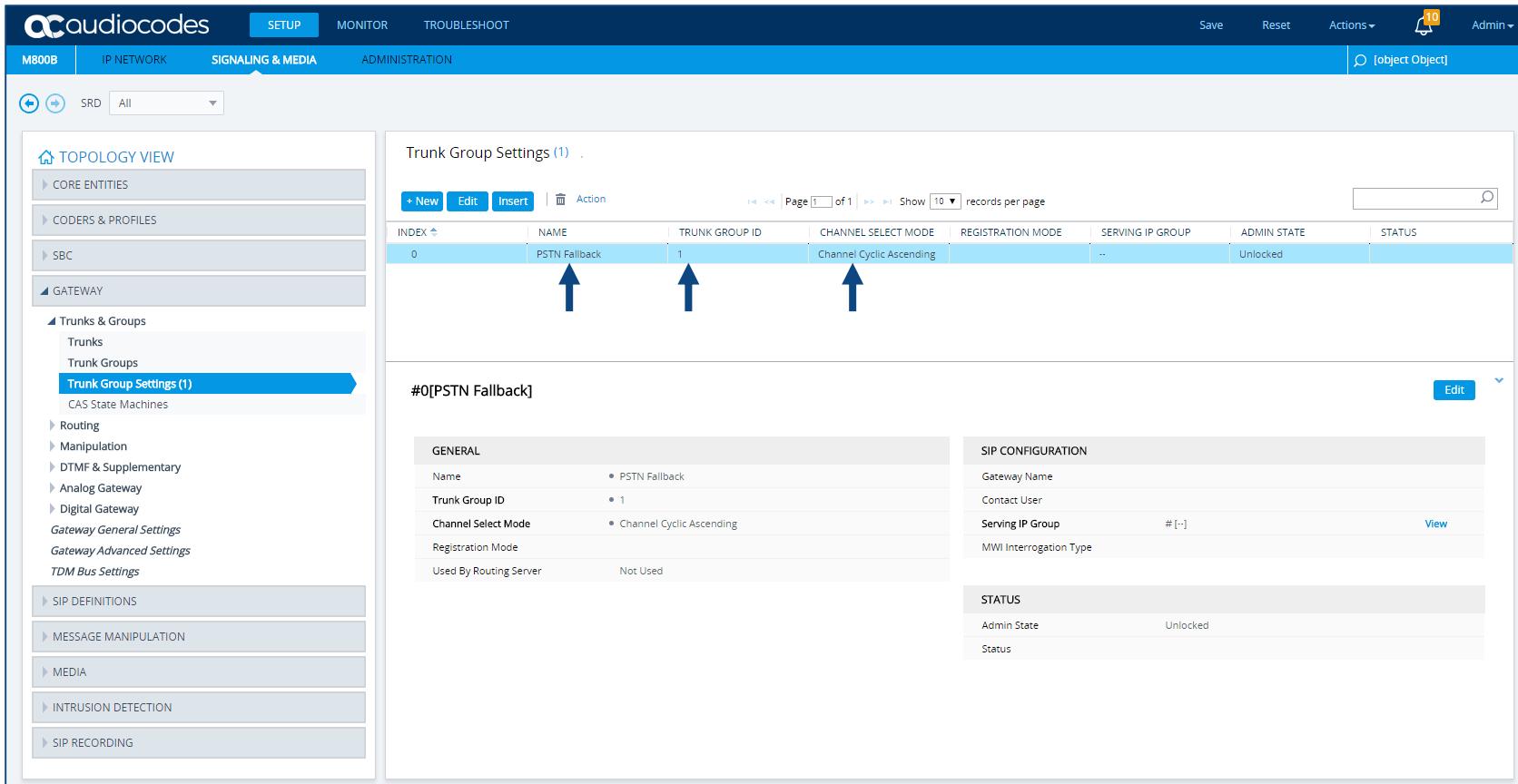
Disable

1-12

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-31		1	None
2							None
3							None
4							None
5							None
6							None
7							None

# Configure the Trunk Group Settings

- Determines the method by which new calls are assigned to channels within each Trunk Group



The screenshot shows the audiocodes M800B IP NETWORK configuration interface. The left sidebar navigation includes sections like CORE ENTITIES, CODERS & PROFILES, SBC, GATEWAY, Trunks & Groups (with Trunk Group Settings selected), SIP DEFINITIONS, MESSAGE MANIPULATION, MEDIA, INTRUSION DETECTION, and SIP RECORDING. The main content area displays 'Trunk Group Settings (1)'. A table lists one entry: #0[PSTN Fallback] with Name 'PSTN Fallback', Trunk Group ID '1', Channel Select Mode 'Channel Cyclic Ascending', and Admin State 'Unlocked'. Below the table, detailed settings for '#0[PSTN Fallback]' are shown under GENERAL, SIP CONFIGURATION, and STATUS tabs.

INDEX	NAME	TRUNK GROUP ID	CHANNEL SELECT MODE	REGISTRATION MODE	SERVING IP GROUP	ADMIN STATE	STATUS
0	PSTN Fallback	1	Channel Cyclic Ascending	--	--	Unlocked	--

**GENERAL**

Name	PSTN Fallback
Trunk Group ID	1
Channel Select Mode	Channel Cyclic Ascending
Registration Mode	
Used By Routing Server	Not Used

**SIP CONFIGURATION**

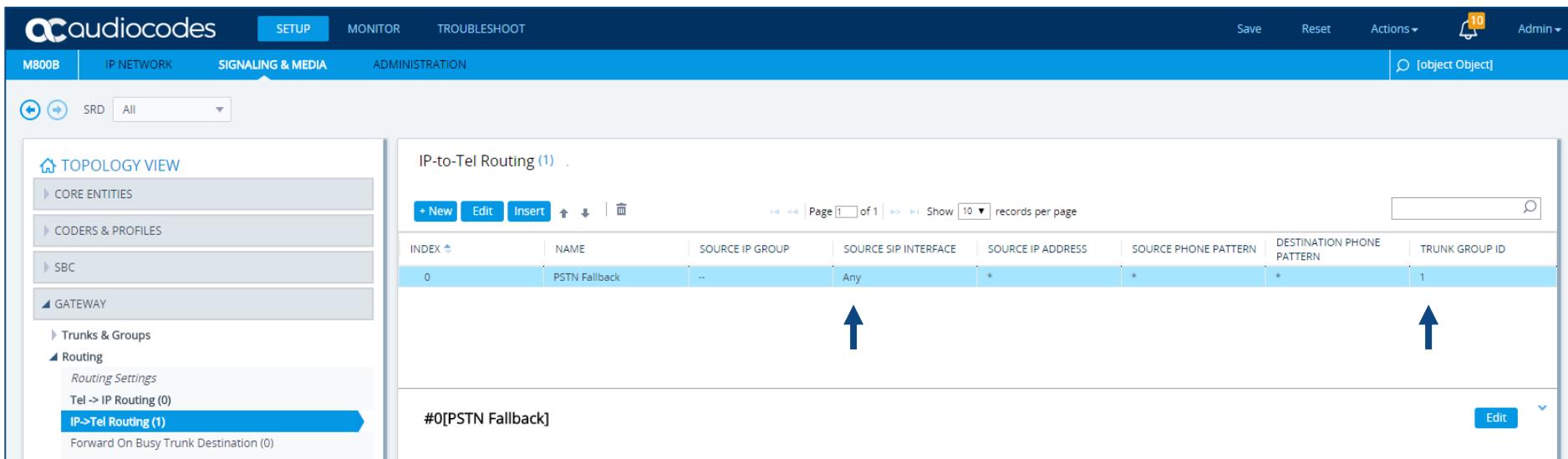
Gateway Name	
Contact User	
Serving IP Group	# [..]
MWI Interrogation Type	

**STATUS**

Admin State	Unlocked
Status	

# IP to Trunk Group Routing (IP2Tel)

- Used to route incoming IP calls to trunk groups
- Route the call to Trunk Group ID



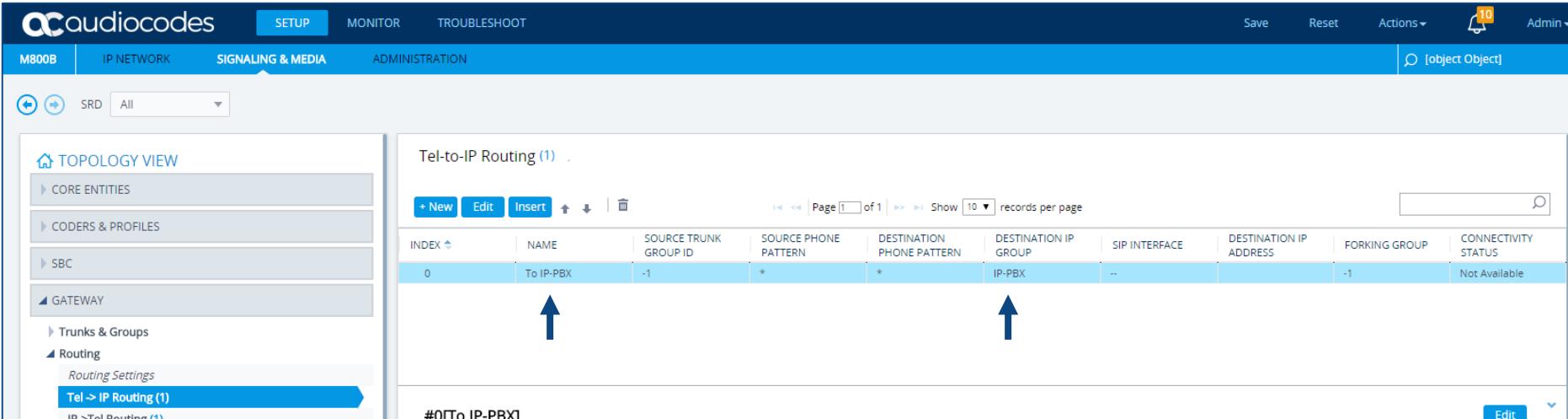
The screenshot shows the audiocodes M800B web interface under the 'SETUP' tab. In the left sidebar, under 'GATEWAY > Routing > IP->Tel Routing (1)', the 'IP->Tel Routing (1)' link is highlighted. The main panel displays the 'IP-to-Tel Routing' configuration with one entry:

INDEX	NAME	SOURCE IP GROUP	SOURCE SIP INTERFACE	SOURCE IP ADDRESS	SOURCE PHONE PATTERN	DESTINATION PHONE PATTERN	TRUNK GROUP ID
0	PSTN Fallback	..	Any	*	*	*	1

At the bottom of the table, the pattern '#0[PSTN Fallback]' is shown, followed by an 'Edit' button.

# Tel to IP Routing (Tel2IP)

- Used to route outgoing IP calls
- Route the calls to the IP-PBX IP Group

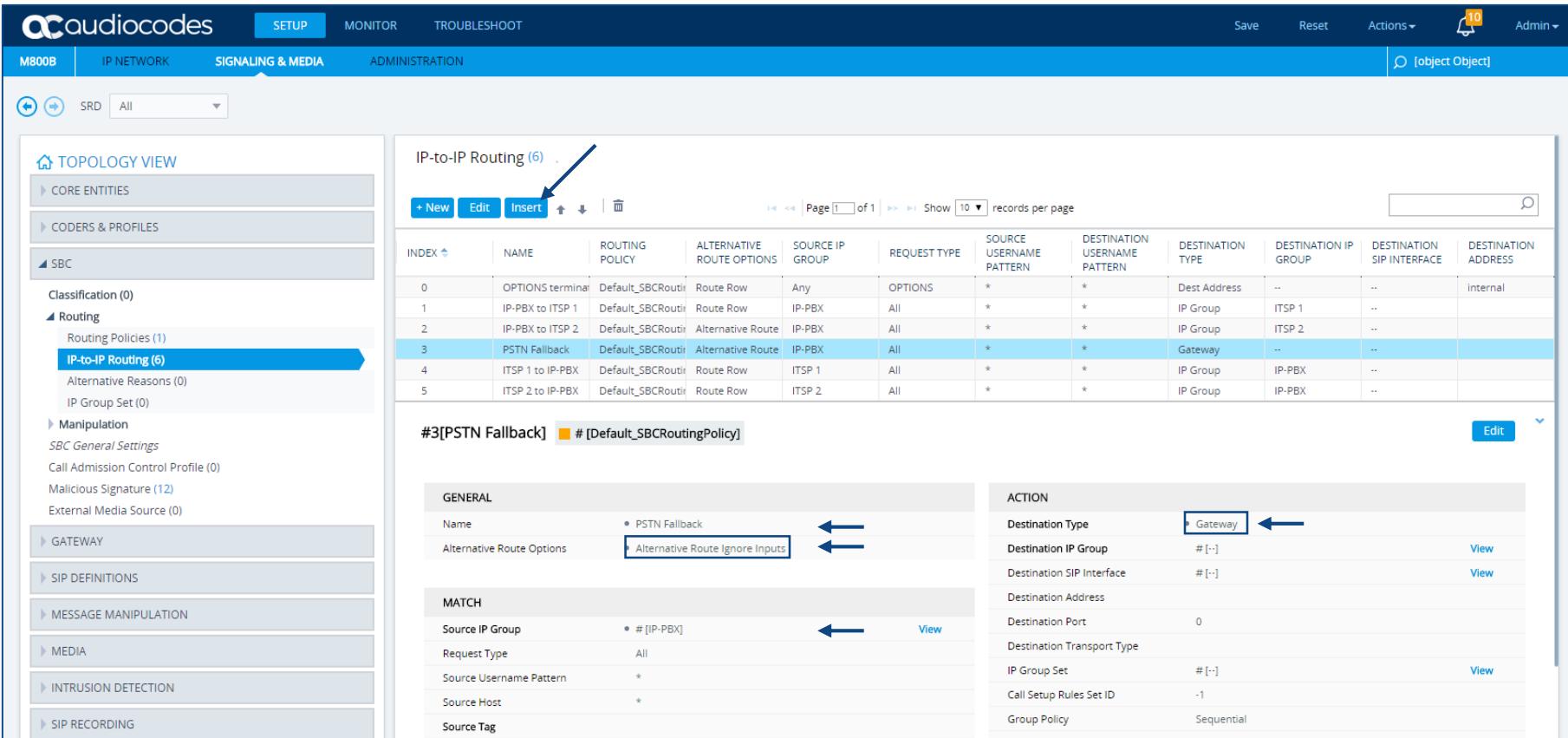


The screenshot shows the audiocodes M800B web interface under the 'SETUP' tab. In the left sidebar, under 'GATEWAY', 'Trunks & Groups' is expanded, and 'Tel->IP Routing (1)' is selected. The main panel displays a table titled 'Tel-to-IP Routing (1)'. The table has columns: INDEX, NAME, SOURCE TRUNK GROUP ID, SOURCE PHONE PATTERN, DESTINATION PHONE PATTERN, DESTINATION IP GROUP, SIP INTERFACE, DESTINATION IP ADDRESS, FORKING GROUP, and CONNECTIVITY STATUS. One row is present: INDEX 0, NAME 'To IP-PBX', SOURCE TRUNK GROUP ID -1, SOURCE PHONE PATTERN \*, DESTINATION PHONE PATTERN \*, DESTINATION IP GROUP IP-PBX, SIP INTERFACE --, DESTINATION IP ADDRESS --, FORKING GROUP -1, and CONNECTIVITY STATUS Not Available.

INDEX	NAME	SOURCE TRUNK GROUP ID	SOURCE PHONE PATTERN	DESTINATION PHONE PATTERN	DESTINATION IP GROUP	SIP INTERFACE	DESTINATION IP ADDRESS	FORKING GROUP	CONNECTIVITY STATUS
0	To IP-PBX	-1	*	*	IP-PBX	--	--	-1	Not Available

# Define IP to IP Routing Table

- Add the Gateway entry to SBC IP-to-IP Routing Table:



The screenshot shows the audiocodes M800B web interface with the following navigation path selected: **TOPLOGY VIEW** > **SBC** > **IP-to-IP Routing (6)**.

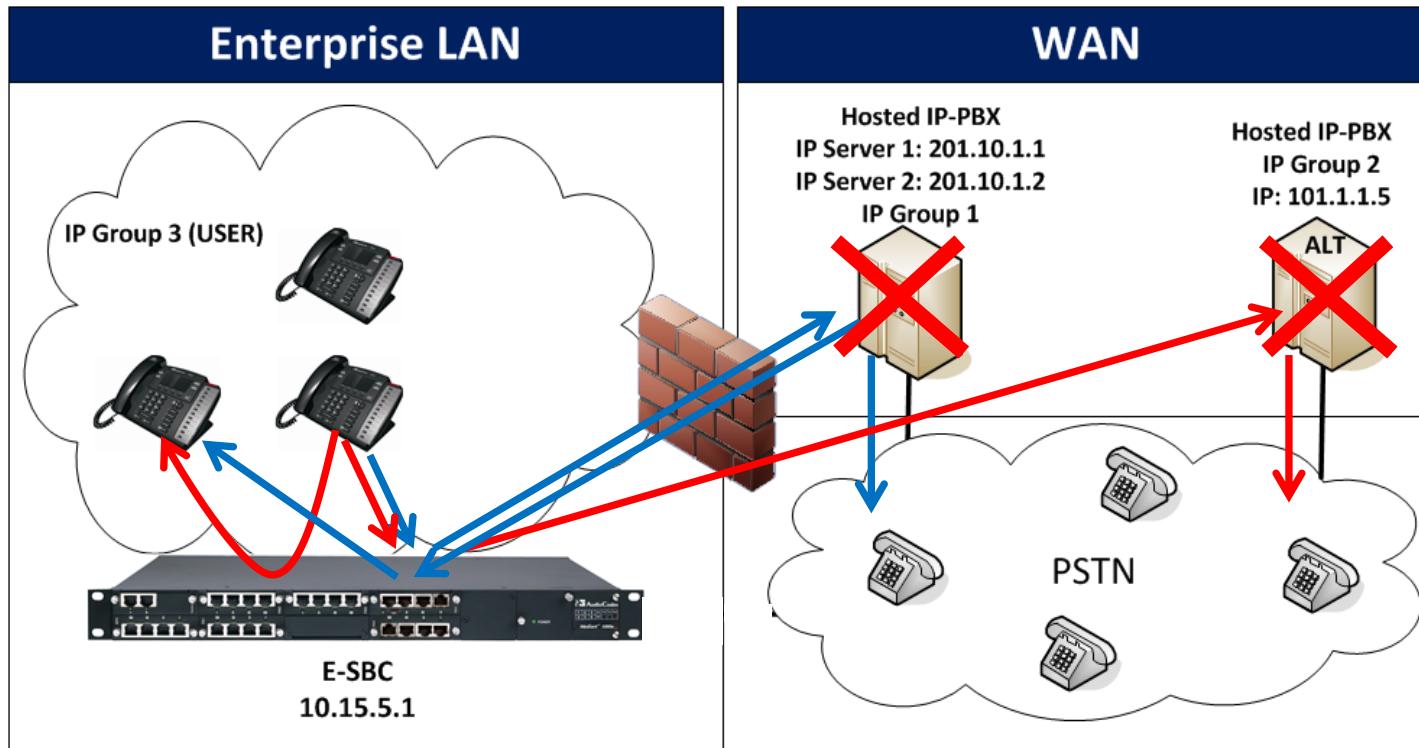
The main table displays 6 entries:

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PATTERN	DESTINATION USERNAME PATTERN	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	OPTIONS terminal	Default_SBCRoute	Route Row	Any	OPTIONS	*	*	Dest Address	..	..	internal
1	IP-PBX to ITSP 1	Default_SBCRoute	Route Row	IP-PBX	All	*	*	IP Group	ITSP 1	..	
2	IP-PBX to ITSP 2	Default_SBCRoute	Alternative Route	IP-PBX	All	*	*	IP Group	ITSP 2	..	
3	PSTN Fallback	Default_SBCRoute	Alternative Route	IP-PBX	All	*	*	Gateway	..	..	
4	ITSP 1 to IP-PBX	Default_SBCRoute	Route Row	ITSP 1	All	*	*	IP Group	IP-PBX	..	
5	ITSP 2 to IP-PBX	Default_SBCRoute	Route Row	ITSP 2	All	*	*	IP Group	IP-PBX	..	

Detailed view for entry #3 [PSTN Fallback]:

GENERAL		ACTION	
Name	PSTN Fallback	Destination Type	Gateway
Alternative Route Options	Alternative Route Ignore Inputs	Destination IP Group	# [-]
		Destination SIP Interface	# [-]
		Destination Address	
		Destination Port	0
		Destination Transport Type	
		IP Group Set	# [-]
		Call Setup Rules Set ID	-1
		Group Policy	Sequential

# SBC Survivability for LAN Users



→ Normal Mode  
→ Survivability Mode

# Define Proxy Set – Hosted IP-PBX

TOPOLOGY VIEW

CORE ENTITIES

- Applications Enabling
- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)**
- IP Groups (4)

GATEWAY

MEDIA

CODERS & PROFILES

SBC

SIP DEFINITIONS

MESSAGE MANIPULATION

INTRUSION DETECTION

SIP RECORDING

SETUP MONITOR TROUBLESHOOT

N800 IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions ▾ Entity, parameter, value

SRD All

Proxy Sets (2) .

+ New Edit |  

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	GATEWAY IPv4 SIP INTERFACE	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
1	Hosted IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Enable
2	Alternative Hosted IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Disable

#1[Hosted IP-PBX] #0 [DefaultSRD]

Edit

GENERAL

Name: Hosted IP-PBX

Gateway IPv4 SIP Interface: --

SBC IPv4 SIP Interface: #0 [IP-PBX]

Gateway IPv6 SIP Interface: --

SBC IPv6 SIP Interface: --

TLS Context Name: --

REduNDANCY

Redundancy Mode:

- Proxy Hot Swap:  Enable
- Proxy Load Balancing Met.:  Round Robin

Min. Active Servers for Lo...: 1

ADVANCED

Classification Input: IP Address only

DNS Resolve Method:

KEEP ALIVE

Proxy Keep-Alive: Using OPTIONS

Proxy Keep-Alive Time [sec]: 60

Keep-Alive Failure Respons...

PROXY ADDRESS TYPE

201.10.1.1:5060 UDP

201.10.1.2:5060 UDP

# Define Proxy Set – Alternative Hosted IP-PBX



SERIAL NUMBER: N800 | IP NETWORK | SIGNALING & MEDIA | ADMINISTRATION

Save | Reset | Actions ▾ | Admin ▾

Entity, parameter, value

SRD All

### TOPOLOGY VIEW

CORE ENTITIES

- Applications Enabling
- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)**
- IP Groups (4)

GATEWAY

MEDIA

CODERS & PROFILES

SBC

SIP DEFINITIONS

MESSAGE MANIPULATION

INTRUSION DETECTION

SIP RECORDING

### Proxy Sets (2)

INDEX	NAME	SRD	GATEWAY IPv4 SIP INTERFACE	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
1	Hosted IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Enable
2	Alternative Hosted IP-PBX	DefaultSRD (#0)	--	IP-PBX	60		Disable

#2[Alternative Hosted IP-PBX] #0[DefaultSRD]

**GENERAL**

Name	Alternative Hosted IP-PBX
Gateway IPv4 SIP Interface	--
SBC IPv4 SIP Interface	#0 [IP-PBX]
Gateway IPv6 SIP Interface	--
SBC IPv6 SIP Interface	--
TLS Context Name	--

**REDUNDANCY**

Redundancy Mode	Proxy Hot Swap	Disable
Proxy Load Balancing Met...	Min. Active Servers for Lo...	1

**ADVANCED**

Classification Input	IP Address only
DNS Resolve Method	

**KEEP ALIVE**

Proxy Keep-Alive	Disable
Proxy Keep-Alive Time [sec]	60

Keep-Alive Failure Respons...

**PROXY ADDRESS**

101.1.1.5:5060	UDP
----------------	-----

101.1.1.5:5060 UDP ←

Index: 2 | Name: Alternative Hosted IP-PBX | SRD: DefaultSRD (#0) | Gateway IPv4 SIP Interface: -- | SBC IPv4 SIP Interface: #0 [IP-PBX] | Proxy Keep-Alive Time [sec]: 60 | Redundancy Mode: Proxy Hot Swap | Min. Active Servers for Load Balancing: 1 | Classification Input: IP Address only | DNS Resolve Method: | Keep-Alive Failure Response: | Proxy Address: 101.1.1.5:5060 UDP

# Define IP Group – Hosted IP-PBX

SERVICES    SETUP    MONITOR    TROUBLESHOOT

M800 | IP NETWORK | SIGNALING & MEDIA | ADMINISTRATION

Save    Reset    Actions ▾    Admin ▾

Entity, parameter, value

SRD All

### TOPOLOGY VIEW

CORE ENTITIES

- Applications Enabling
- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)
- IP Groups (3)**

GATEWAY

MEDIA

CODERS & PROFILES

SBC

SIP DEFINITIONS

MESSAGE MANIPULATION

INTRUSION DETECTION

SIP RECORDING

### IP Groups (3) .

+ New | Edit | 

Page 1 of 1 | Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
1	Hosted IP-PBX	#0 [DefaultSRD]	Server	Not Configured	Hosted IP-PBX	--	ITSP-MR		Enable	-1	-1
2	Alternative Hoste	#0 [DefaultSRD]	Server	Not Configured	Alternative Hoste	--	ITSP-MR		Enable	-1	-1
3	LAN Users	#0 [DefaultSRD]	User	Not Configured	--	--	IP-PBX-MR		Enable	-1	-1

#1[Hosted IP-PBX] #0 [DefaultSRD] Edit

**GENERAL**

Name	Hosted IP-PBX
Topology Location	Down
Type	Server
Proxy Set	#1 [Hosted IP-PBX] <span style="float: right;">View</span>
IP Profile	-- <span style="float: right;">View</span>
Media Realm	#1 [ITSP-MR] <span style="float: right;">View</span>
Contact User	
SIP Group Name	
Created By Routing Server	No
Used By Routing Server	Not Used
Proxy Set Connectivity	Not Connected

**QUALITY OF EXPERIENCE**

QoE Profile	--	<span style="float: right;">View</span>
Bandwidth Profile	--	<span style="float: right;">View</span>

**MESSAGE MANIPULATION**

Inbound Message Mani...	-1
Outbound Message Mani...	-1
Message Manipulation Us...	
Message Manipulation Us...	

**SBC REGISTRATION AND AUTHENTICATION**



# Define IP Group – Alternative Hosted IP-PBX

IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions □ Admin □ Entity, parameter, value

SRD All

TOPOLOGY VIEW

CORE ENTITIES

- Applications Enabling
- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)
- IP Groups (3)**

GATEWAY

MEDIA

CODERS & PROFILES

SBC

SIP DEFINITIONS

MESSAGE MANIPULATION

INTRUSION DETECTION

SIP RECORDING

IP Groups (3)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
1	Hosted IP-PBX	DefaultSRD (	Server	Not Configured	Hosted IP-PBX	--	ITSP-MR		Enable	-1	-1
2	Alternative Hoste	DefaultSRD (	Server	Not Configured	Alternative Hoste	--	ITSP-MR		Enable	-1	-1
3	LAN Users	DefaultSRD (	User	Not Configured	--	--	IP-PBX-MR		Enable	-1	-1

#2[Alternative Hosted IP-PBX] #0 [DefaultSRD]

Edit

GENERAL

- Name: Alternative Hosted IP-PBX
- Topology Location: Down
- Type: Server
- Proxy Set: #2 [Alternative Hosted IP-PBX]
- IP Profile: --
- Media Realm: #1 [ITSP-MR]
- Contact User:
- SIP Group Name:
- Created By Routing Server: No
- Used By Routing Server: Not Used
- Proxy Set Connectivity: NA

View View View

QUALITY OF EXPERIENCE

- QoE Profile: --
- Bandwidth Profile: --

View View

MESSAGE MANIPULATION

- Inbound Message Manipu...: -1
- Outbound Message Mani...: -1
- Message Manipulation Us...
- Message Manipulation Us...

SBC REGISTRATION AND AUTHENTICATION

# Define IP Group – LAN Users

IP NETWORK SIGNALING & MEDIA ADMINISTRATION

Save Reset Actions □ Admin □ Entity, parameter, value

SRD All

TOPOLOGY VIEW

CORE ENTITIES

- Applications Enabling
- SRDs (1)
- SIP Interfaces (2)
- Media Realms (2)
- Proxy Sets (2)
- IP Groups (3)**

GATEWAY

MEDIA

CODERS & PROFILES

SBC

SIP DEFINITIONS

MESSAGE MANIPULATION

INTRUSION DETECTION

SIP RECORDING

IP Groups (3)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
1	Hosted IP-PBX	DefaultSRD (0)	Server	Not Configured	Hosted IP-PBX	--	ITSP-MR		Enable	-1	-1
2	Alternative Hoste	DefaultSRD (0)	Server	Not Configured	Alternative Hoste	--	ITSP-MR		Enable	-1	-1
3	LAN Users	DefaultSRD (0)	User	Not Configured	--	--	IP-PBX-MR		Enable	-1	-1

#3[LAN Users] #0 [DefaultSRD]

Edit

GENERAL

Name: LAN Users

Topology Location: Down

Type: User

Proxy Set: --

IP Profile: --

Media Realm: #0 [IP-PBX-MR]

Contact User

SIP Group Name

Created By Routing Server: No

Used By Routing Server: Not Used

Proxy Set Connectivity: NA

QUALITY OF EXPERIENCE

QoE Profile: --

Bandwidth Profile: --

MESSAGE MANIPULATION

Inbound Message Manipulation: -1

Outbound Message Manipulation: -1

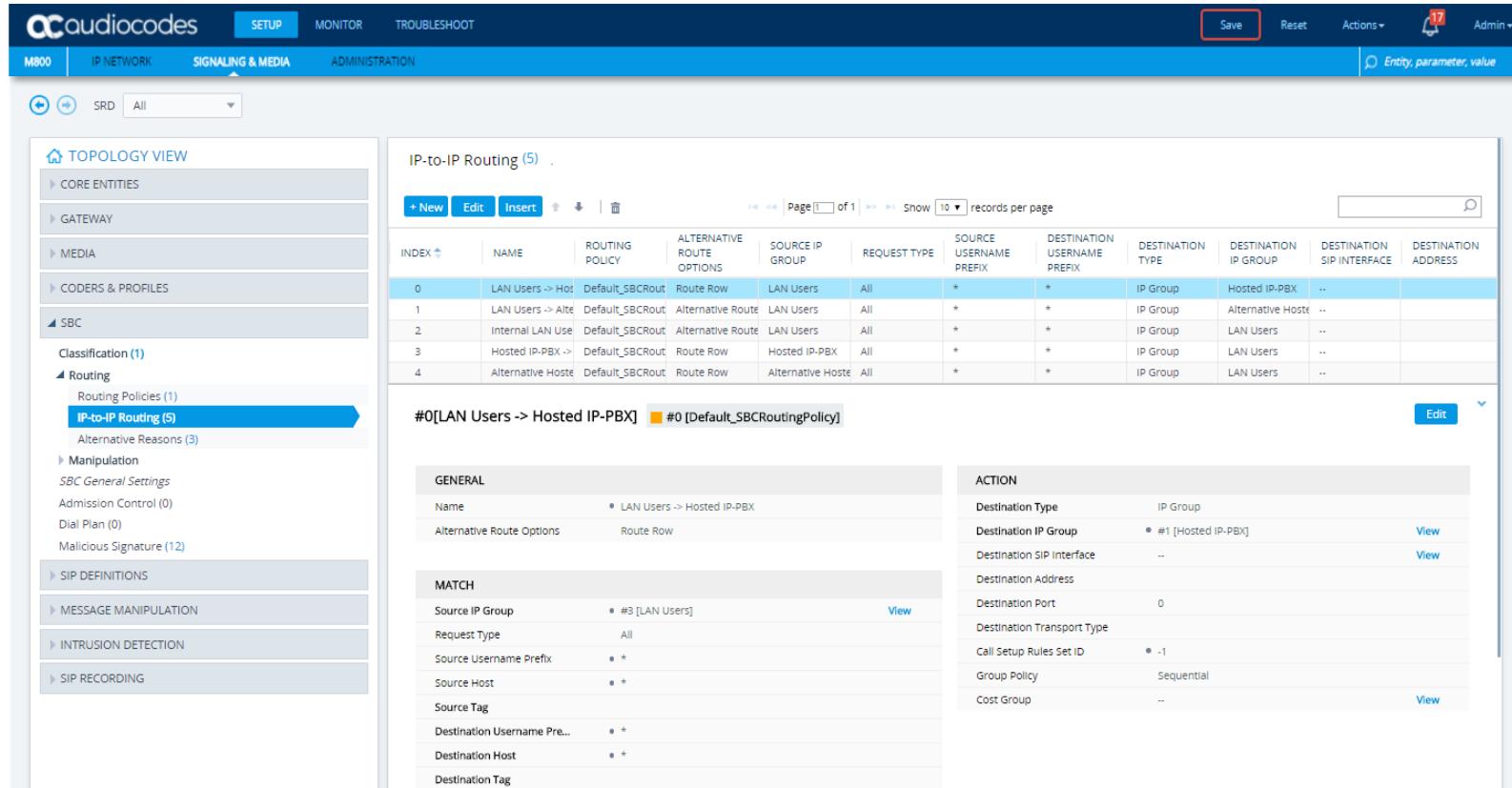
Message Manipulation Usage

Message Manipulation Usage

SBC REGISTRATION AND AUTHENTICATION

# Define IP to IP Routing Table

- Route between LAN Users IP Group and Hosted IP-PBX IP Group



The screenshot shows the audiocodes M800 web interface under the 'SIGNALING & MEDIA' tab. On the left, the 'TOPOLOGY VIEW' sidebar lists various entities like CORE ENTITIES, GATEWAY, MEDIA, CODERS & PROFILES, and SBC. Under SBC, 'IP-to-IP Routing (5)' is selected, highlighted with a blue arrow. The main content area displays the 'IP-to-IP Routing (5)' table with the following data:

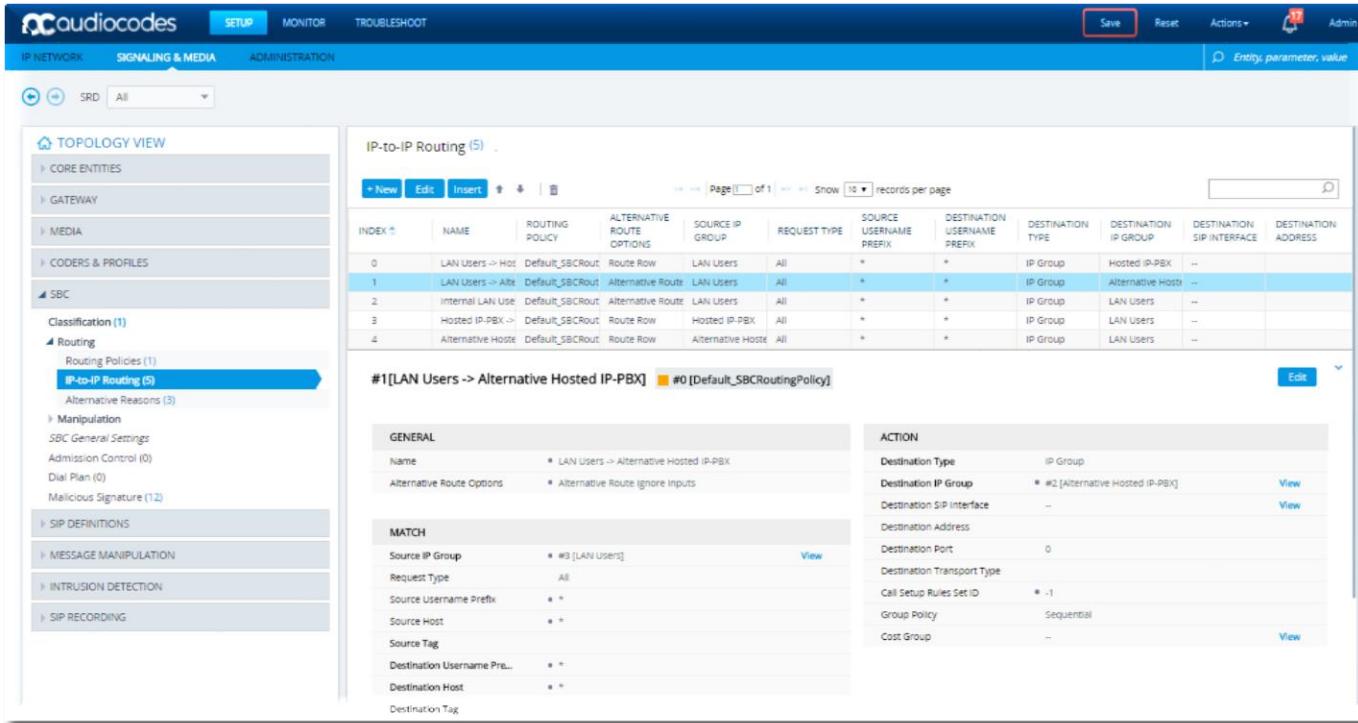
INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	LAN Users -> Hosted IP-PBX	Default_SBCRoute	Route Row	LAN Users	All	*	*	IP Group	Hosted IP-PBX	..	
1	LAN Users -> Alternative Host	Default_SBCRoute	Alternative Route	LAN Users	All	*	*	IP Group	Alternative Host	..	
2	Internal LAN Use	Default_SBCRoute	Alternative Route	LAN Users	All	*	*	IP Group	LAN Users	..	
3	Hosted IP-PBX ->	Default_SBCRoute	Route Row	Hosted IP-PBX	All	*	*	IP Group	LAN Users	..	
4	Alternative Host	Default_SBCRoute	Route Row	Alternative Host	All	*	*	IP Group	LAN Users	..	

Below the table, two specific entries are highlighted with yellow boxes: #0[LAN Users -> Hosted IP-PBX] and #0[Default\_SBCRoutingPolicy]. The detailed configuration for the first entry is shown in the bottom right panel:

GENERAL	
Name	#0[LAN Users -> Hosted IP-PBX]
Alternative Route Options	Route Row
MATCH	
Source IP Group	#3 [LAN Users]
Request Type	All
Source Username Prefix	*
Source Host	*
Source Tag	
Destination Username Prefix	*
Destination Host	*
Destination Tag	
ACTION	
Destination Type	IP Group
Destination IP Group	#1 [Hosted IP-PBX]
Destination SIP Interface	..
Destination Address	
Destination Port	0
Destination Transport Type	
Call Setup Rules Set ID	-1
Group Policy	Sequential
Cost Group	..

# Define IP to IP Routing Table

- If connection to Hosted IP-PBX fails, all calls will be routed to the Alt Hosted IP-PBX IP Group



The screenshot shows the audiocodes web interface for managing IP-to-IP Routing. The left sidebar navigation includes sections like TOPOLOGY VIEW, CORE ENTITIES, GATEWAY, MEDIA, CODERS & PROFILES, Classification (1), and Routing Policies (1). The IP-to-IP Routing (5) section is currently selected. The main content area displays a table of routing rules:

INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	LAN Users -> Hosted IP-PBX	Default_SBCRoute	Route Row	LAN Users	All	*	*	IP Group	Hosted IP-PBX	--	
1	LAN Users -> Alternative Hosted IP-PBX	Default_SBCRoute	Alternative Route	LAN Users	All	*	*	IP Group	Alternative Hosts	--	
2	Internal LAN User -> Hosted IP-PBX	Default_SBCRoute	Alternative Route	LAN Users	All	*	*	IP Group	LAN Users	--	
3	Hosted IP-PBX -> LAN User	Default_SBCRoute	Route Row	Hosted IP-PBX	All	*	*	IP Group	LAN Users	--	
4	Alternative Hosted IP-PBX -> LAN User	Default_SBCRoute	Route Row	All	*	*	*	IP Group	LAN Users	--	

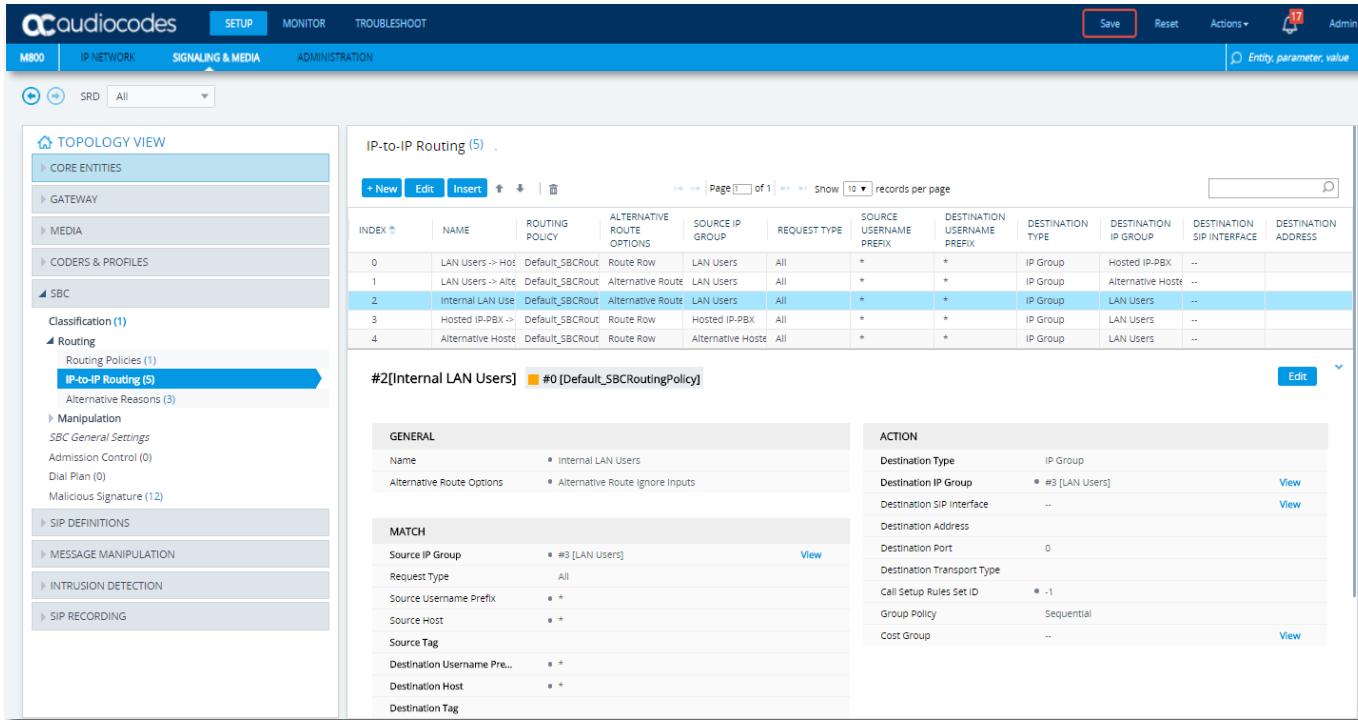
Below the table, a detailed view of rule #1 is shown:

GENERAL		ACTION	
Name	#1 [LAN Users -> Alternative Hosted IP-PBX]	Destination Type	IP Group
Alternative Route Options	#1 Alternative Route (Ignore Inputs)	Destination IP Group	#2 [Alternative Hosted IP-PBX]
		Destination SIP Interface	--
		Destination Address	
		Destination Port	0
		Destination Transport Type	
		Call Setup Rules Set ID	#1
		Group Policy	Sequential
		Cost Group	--

The bottom of the interface shows the standard Save, Reset, Actions, Admin, and Entity parameter, value buttons.

# Define IP to IP Routing Table

- If connection to Alternative Hosted IP-PBX fails too, all calls will be routed back to the LAN Users IP Group



The screenshot shows the audiocodes M800 web interface with the following details:

**Top Navigation:** SETUP (selected), MONITOR, TROUBLESHOOT, Save, Reset, Actions, Admin.

**Middle Navigation:** M800, IP NETWORK, SIGNALING & MEDIA, ADMINISTRATION, Entity, parameter, value.

**Left Sidebar:** TOPOLOGY VIEW, CORE ENTITIES, GATEWAY, MEDIA, CODERS & PROFILES, SBC, Classification (1), Routing (1), Routing Policies (1), IP-to-IP Routing (5) (selected), Alternative Reasons (3), Manipulation, SBC General Settings, Admission Control (0), Dial Plan (0), Malicious Signature (12), SIP DEFINITIONS, MESSAGE MANIPULATION, INTRUSION DETECTION, SIP RECORDING.

**Main Content:** IP-to-IP Routing (5) table.

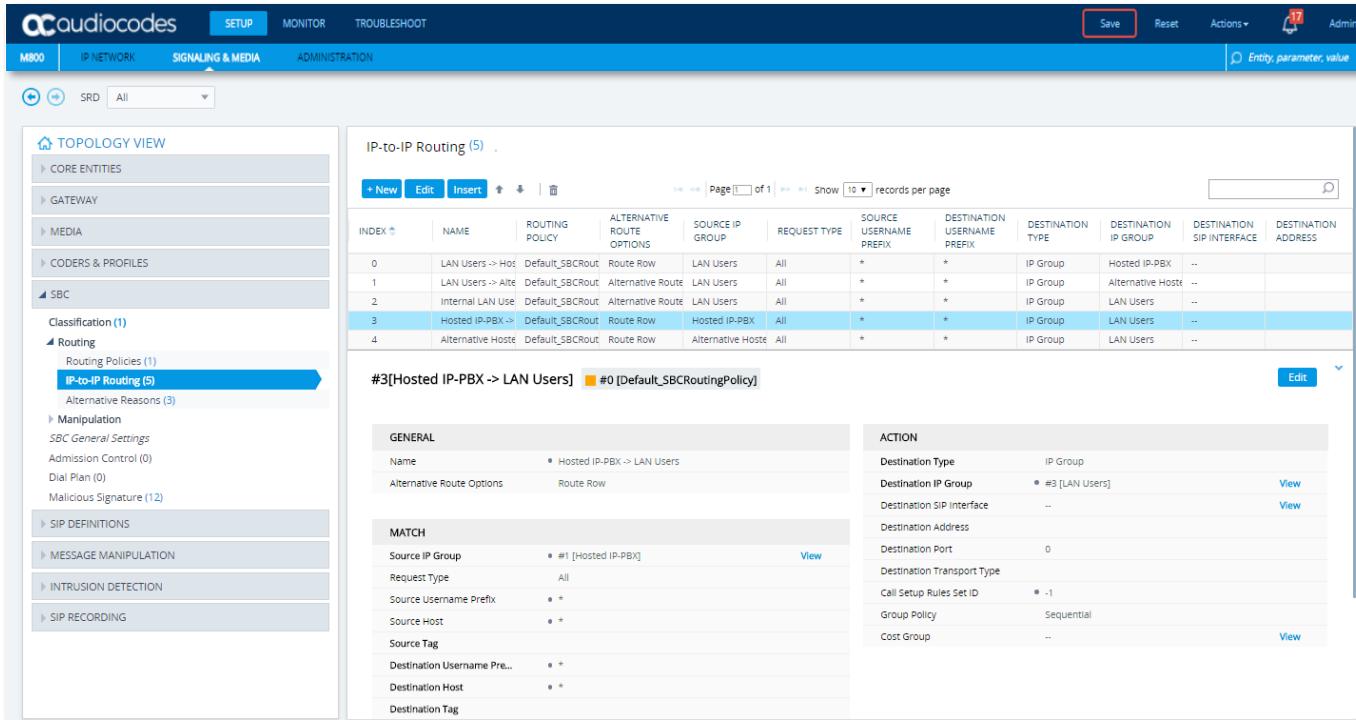
INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	LAN Users -> Hosted IP-PBX	Default_SBCRout	Route Row	LAN Users	All	*	*	IP Group	Hosted IP-PBX	--	
1	LAN Users -> Alternative Hosted IP-PBX	Default_SBCRout	Alternative Route	LAN Users	All	*	*	IP Group	Alternative Hosted IP-PBX	--	
2	Internal LAN Users	Default_SBCRout	Alternative Route	LAN Users	All	*	*	IP Group	LAN Users	--	
3	Hosted IP-PBX ->	Default_SBCRout	Route Row	Hosted IP-PBX	All	*	*	IP Group	LAN Users	--	
4	Alternative Hosted IP-PBX	Default_SBCRout	Route Row	Alternative Hosted IP-PBX	All	*	*	IP Group	LAN Users	--	

**Bottom Right Detail:** #2[Internal LAN Users] #0[Default\_SBCRoutingPolicy]

GENERAL		ACTION	
Name	Internal LAN Users	Destination Type	IP Group
Alternative Route Options	* Alternative Route (Ignore Inputs)	Destination IP Group	#3 [LAN Users] <a href="#">View</a>
		Destination SIP Interface	-- <a href="#">View</a>
		Destination Address	
		Destination Port	0
		Destination Transport Type	
		Call Setup Rules Set ID	* -1
		Group Policy	Sequential
		Cost Group	-- <a href="#">View</a>

# Define IP to IP Routing Table

- Route between Hosted IP-PBX IP Group and LAN Users IP Group



The screenshot shows the audiocodes M800 web interface under the 'SETUP' tab. The left sidebar navigation includes 'TOPLOGY VIEW', 'CORE ENTITIES', 'GATEWAY', 'MEDIA', 'CODERS & PROFILES', 'SBC', 'Classification (1)', and 'Routing'. Under 'Routing', 'Routing Policies (1)' is selected, and 'IP-to-IP Routing (5)' is highlighted. The main content area displays the 'IP-to-IP Routing (5)' table with the following data:

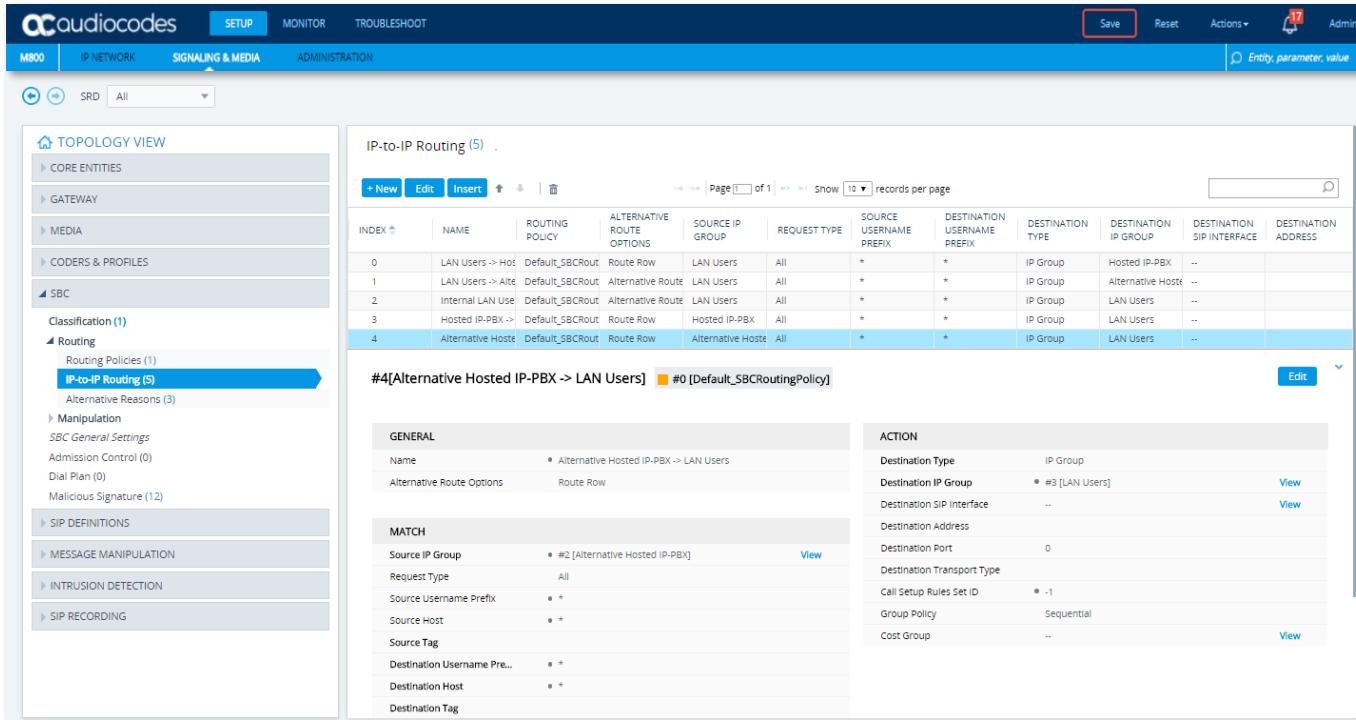
INDEX #	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	LAN Users -> Hosted IP-PBX	Default_SBCRoute	Route Row	LAN Users	All	*	*	IP Group	Hosted IP-PBX	--	
1	LAN Users -> Alternative Host	Default_SBCRoute	Alternative Route	LAN Users	All	*	*	IP Group	Alternative Host	--	
2	Internal LAN Use	Default_SBCRoute	Alternative Route	LAN Users	All	*	*	IP Group	LAN Users	--	
3	Hosted IP-PBX -> LAN Users	Default_SBCRoute	Route Row	Hosted IP-PBX	All	*	*	IP Group	LAN Users	--	
4	Alternative Host	Default_SBCRoute	Route Row	Alternative Host	All	*	*	IP Group	LAN Users	--	

Below the table, a modal window titled '#3[Hosted IP-PBX -> LAN Users] #0[Default\_SBCRoutingPolicy]' shows the detailed configuration for the third row:

GENERAL		ACTION	
Name	Hosted IP-PBX -> LAN Users	Destination Type	IP Group
Alternative Route Options	Route Row	Destination IP Group	#0 [LAN Users]
		Destination SIP Interface	--
		Destination Address	
		Destination Port	0
		Destination Transport Type	
		Call Setup Rules Set ID	* -1
		Group Policy	sequential
		Cost Group	--

# Define IP to IP Routing Table

- Route between Alternative Hosted IP-PBX IP Group and LAN Users IP Group



The screenshot shows the audiocodes M800 web interface under the 'SETUP' tab. The left sidebar navigation includes 'TOPLOGY VIEW', 'ROUTING Policies (1)', and 'IP-to-IP Routing (5)'. The main content area displays the 'IP-to-IP Routing (5)' table with the following data:

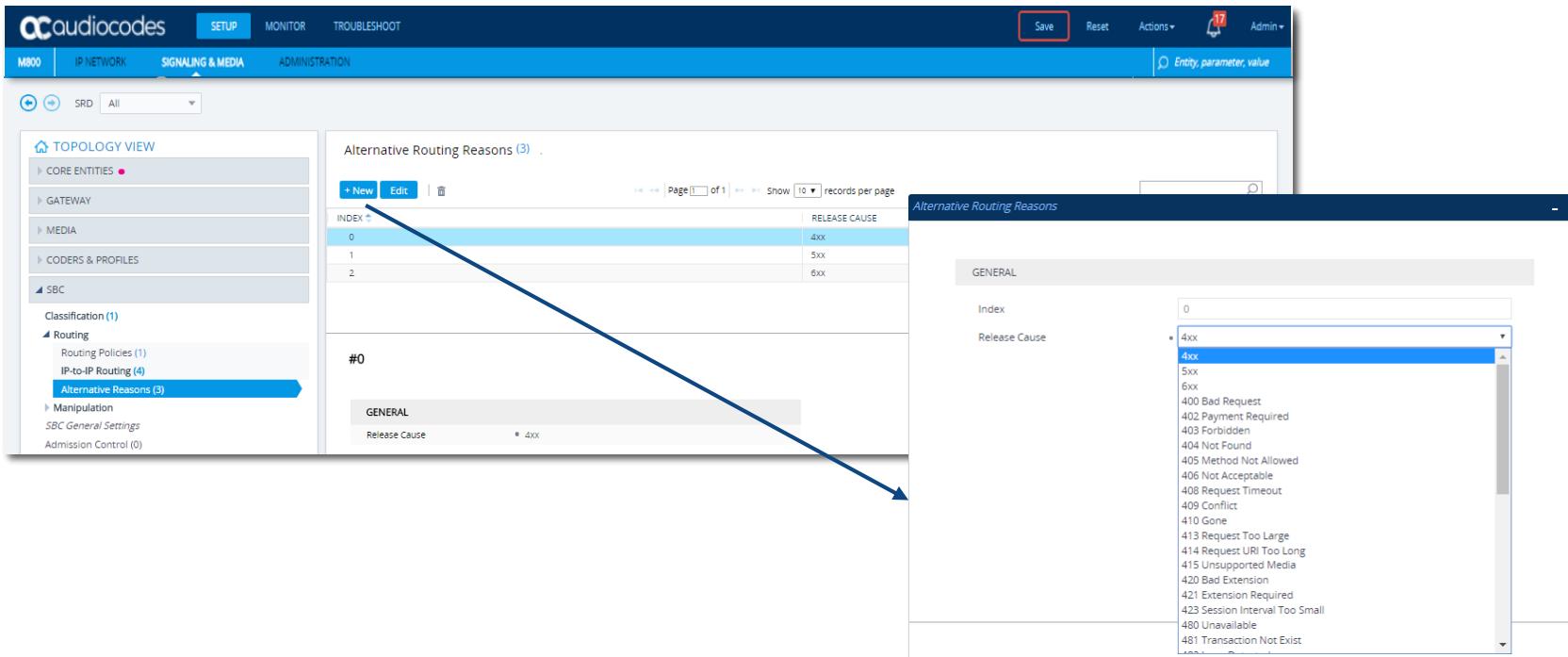
INDEX #	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	LAN Users -> Hosted IP-PBX	Default_SBCRout	Route Row	LAN Users	All	*	*	IP Group	Hosted IP-PBX	--	
1	LAN Users -> Alternative Hosted IP-PBX	Default_SBCRout	Alternative Route	LAN Users	All	*	*	IP Group	Alternative Hosted IP-PBX	--	
2	Internal LAN User -> Hosted IP-PBX	Default_SBCRout	Alternative Route	LAN Users	All	*	*	IP Group	LAN Users	--	
3	Hosted IP-PBX -> LAN Users	Default_SBCRout	Route Row	Hosted IP-PBX	All	*	*	IP Group	LAN Users	--	
4	Alternative Hosted IP-PBX -> LAN Users	Default_SBCRout	Route Row	Alternative Hosted IP-PBX	All	*	*	IP Group	LAN Users	--	

Below the table, the details for row #4 are shown:

GENERAL		ACTION	
Name	#4 [Alternative Hosted IP-PBX -> LAN Users]	Destination Type	IP Group
Alternative Route Options	Route Row	Destination IP Group	#3 [LAN Users]
		Destination SIP Interface	--
		Destination Address	
		Destination Port	0
		Destination Transport Type	
		Call Setup Rules Set ID	* -1
		Group Policy	Sequential
		Cost Group	--

# Define Alternative Routing Reasons

- Enables defining up to 20 different call release reasons for call releases
- If no response, or ICMP or SIP 408 response is received, the SBC attempts to use the alternative route even if no entries are configured in the 'Alternative Routing Reasons'



The screenshot shows the audiocodes M800 web interface. The left sidebar navigation includes sections like TOPOLOGY VIEW, CORE ENTITIES, GATEWAY, MEDIA, CODERS & PROFILES, SBC, Classification (1), Routing (1), IP-to-IP Routing (4), Alternative Reasons (3), Manipulation, SBC General Settings, and Admission Control (0). The 'Alternative Reasons (3)' link is highlighted.

The main content area displays the 'Alternative Routing Reasons' configuration. It shows three entries in a table:

INDEX	RELEASE CAUSE
0	4xx
1	5xx
2	6xx

A modal window titled 'Alternative Routing Reasons' is open, showing a list of SIP error codes under the 'GENERAL' tab:

- Index 0
- Release Cause 4xx
- 4xx (selected)
- 5xx
- 6xx
- 400 Bad Request
- 402 Payment Required
- 403 Forbidden
- 404 Not Found
- 405 Method Not Allowed
- 406 Not Acceptable
- 408 Request Timeout
- 409 Conflict
- 410 Gone
- 413 Request Too Large
- 414 Request URI Too Long
- 415 Unsupported Media
- 420 Bad Extension
- 421 Extension Required
- 423 Session Interval Too Small
- 480 Unavailable
- 481 Transaction Not Exist

An alternative destination can be:

- A. Only an IP destination
- B. Only an PSTN destination
- C. IP destination or PSTN destination
- D. None of the above



If the alternative reasons table is kept empty then:

- A. Alternative routing will never occur
- B. Alternative routing will occur only if 503 SIP message is received
- C. Alternative routing will occur If no response, or ICMP or SIP 408 response is received
- D. Alternative routing will occur in any case as long the entry is configured in IP to IP routing table

In Hosted IP PBX Survivability Mode:

- A. There will be no intra LAN calls
- B. There will be intra LAN calls only between AudioCodes IP Phones
- C. There will be intra LAN calls only between registered IP Phones
- D. None of the above

When a 4xx SIP message is received it means that:

- A. The call can't be establish because of a network issue
- B. The call can't be establish because of a server issue
- C. The call can't be establish because of a user issue
- D. None of the above





Hands-on Lab 5

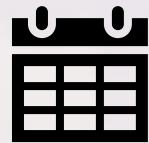
SBC Survivability





## Lesson 15

# SBC High Availability

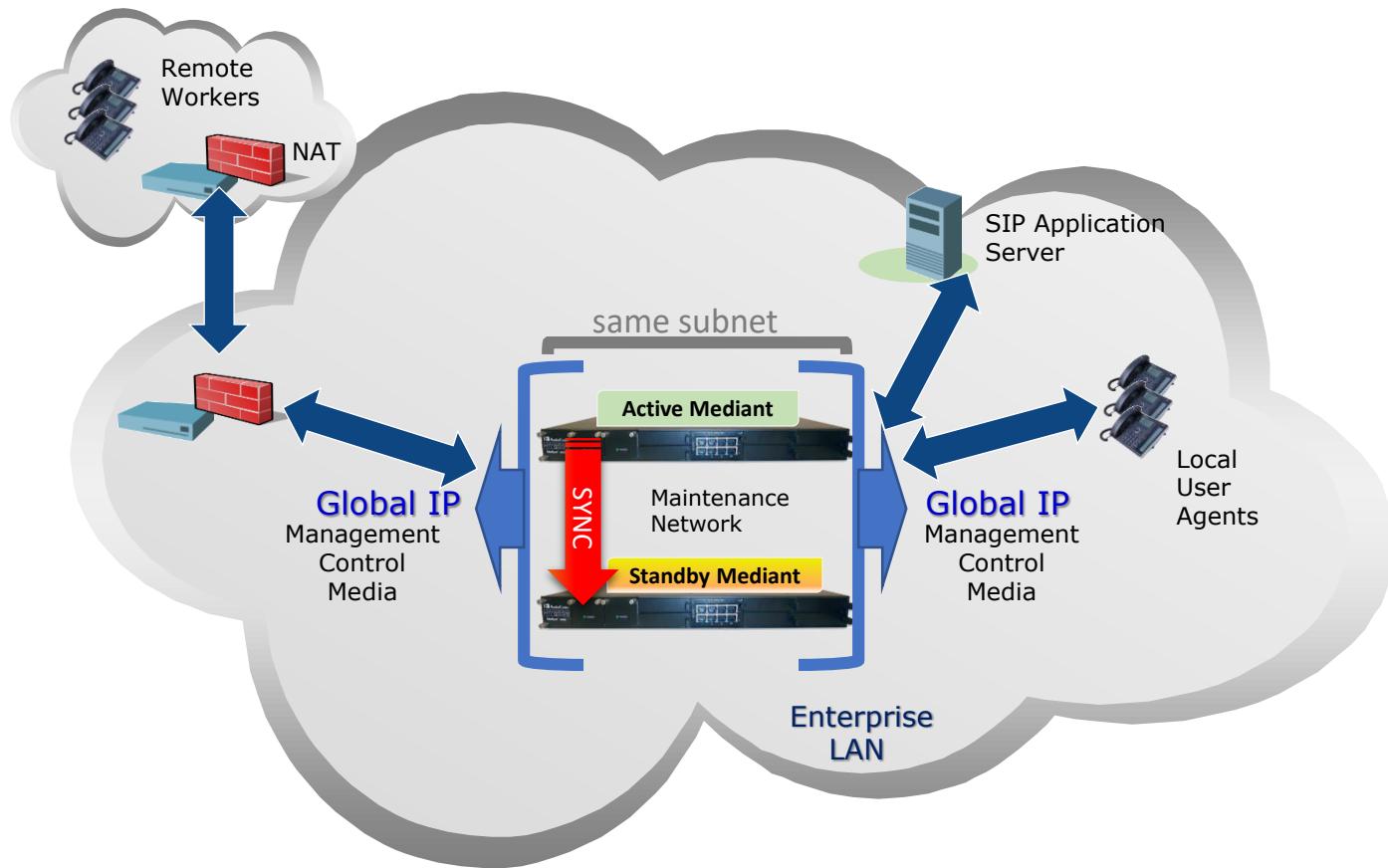


- After completing this lesson you'll be able to:
  - Understand the High Availability (HA) concept
  - Understand the HA architecture
  - Understand how to configure HA

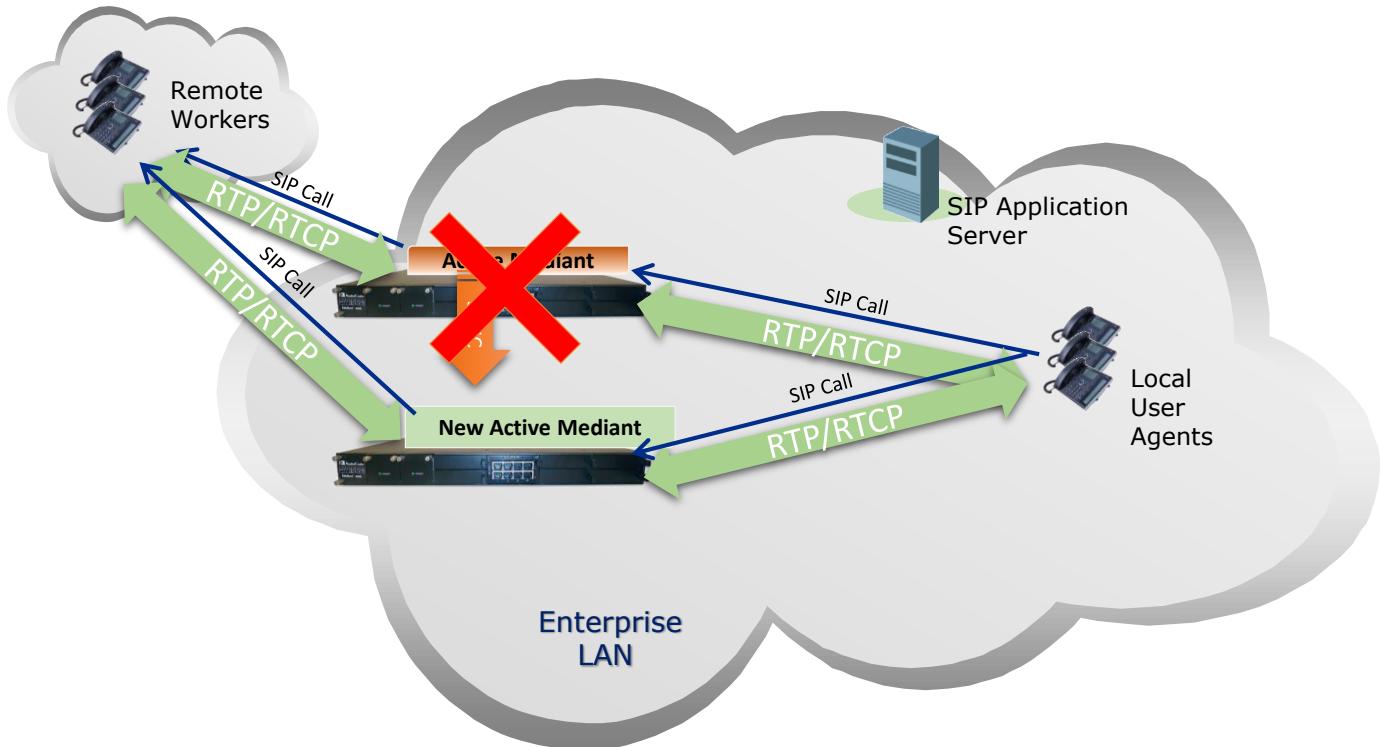
- The device's High Availability (HA) feature provides 1+1 system redundancy using two Mediant devices
- If failure occurs in the active device, a switchover occurs to the redundant device which takes over the call handling process ensuring the continuity of call services
- All active calls (signaling and media) are maintained upon switchover
  - Only IP calls are maintained during a switchover
  - For those devices supporting the Gateway function, PSTN calls are dropped by sending a SIP BYE message to the IP side. This is because only the active device is physically connected to the PSTN interfaces

- Provides full redundancy between the two Mediant devices
- One of the devices is in Active state while the second is in Redundant state
- In the Redundant device, only the Maintenance interface is active
- Management of the HA pair is done only through the Active device
- Upon a major functional failure in the Active device, the Redundant device becomes active
- Supported in:
  - Mediant 500
  - Mediant 800
  - Mediant 2600
  - Mediant 4000
  - Mediant 9000
  - Software SBC

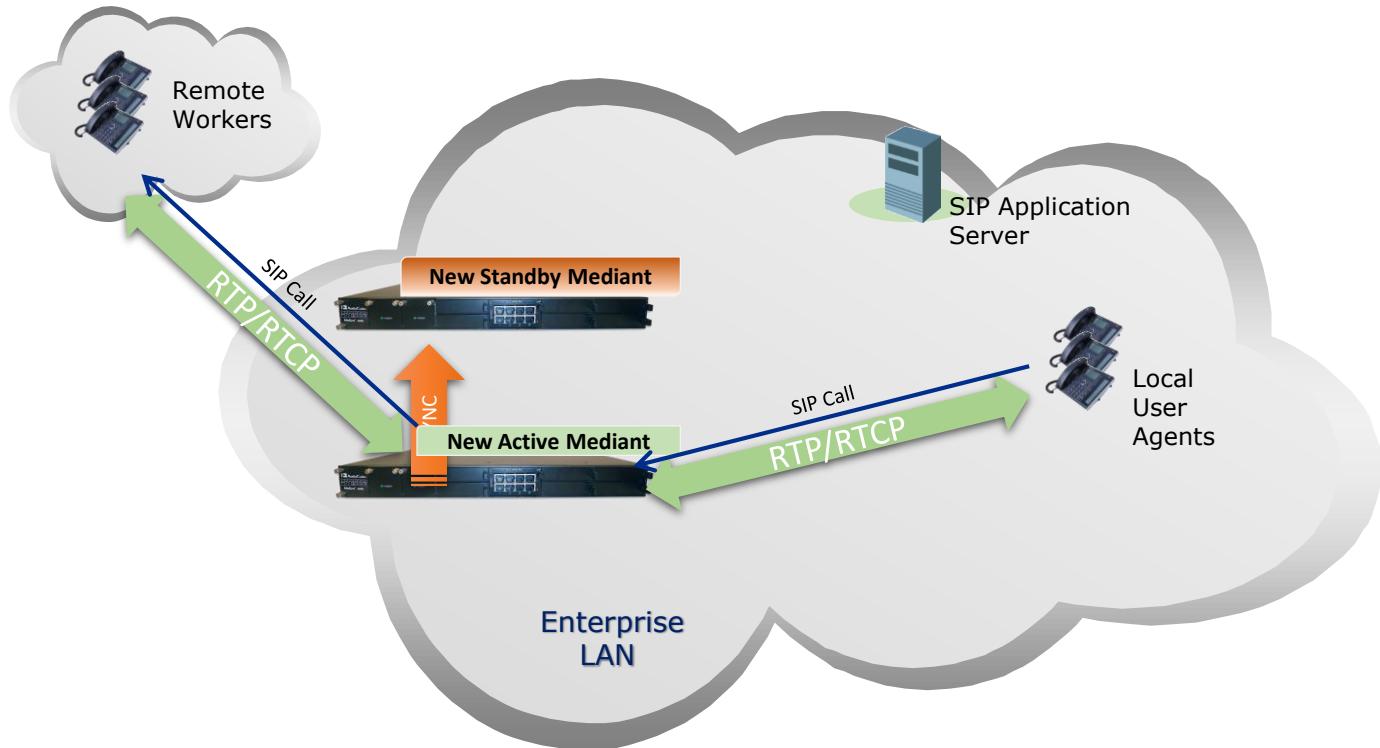
# Two Box Redundancy – Network topology



# Two Box Redundancy flow



# Two Box Redundancy flow



# HA License Key

audiocodes

SETUP MONITOR TROUBLESHOOT

Save Reset Actions ▾ Admin ▾

0

MEDIANTE SBC IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

SRD All

TIME & DATE

WEB & CLI

SNMP

MAINTENANCE

Configuration File

Auxiliary Files

Maintenance Actions

**License Key**

Software Upgrade

High Availability Maintenance

License Key

Product Key	Local FK	53834431404032	79
Mode	Serial Number	Board Type	

GENERAL

High Availability (HA)	200
DSP Channels	9.80
Maximum Supported Software Version	

VOIP SIGNALING PROTOCOLS

SIP	200
MGCP	100

SBC CAPACITY

SBC Sessions	Local 100	Actual 100
Far End Users (FEU)	1000	1000

SKYPE FOR BUSINESS

MSFT	200
------	-----

VOIP FEATURES

Voice Quality Monitoring	200
Test Call	100
Media Enhancement	200

CODERS

Load File

File

Help

- Since both devices have the same IP address, in the initial configuration stage, they cannot both be connected to the network
- To initially configure HA:
  1. Configure HA on the first device
  2. Burn the configuration to flash and power down
  3. Configure HA on the second device
  4. Burn the configuration to flash and reset
  5. Power up the first device

audiocodes

SETUP MONITOR TROUBLESHOOT Save Reset Actions ▾ 0 Admin ▾

MEDIANTE SBC IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entity, parameter, value

All

NETWORK VIEW

CORE ENTITIES

IP Interfaces (3)

Ethernet Devices (2)

Ethernet Groups (15)

Physical Ports (2)

Static Routes (0)

HA Settings

IP Interfaces (3)

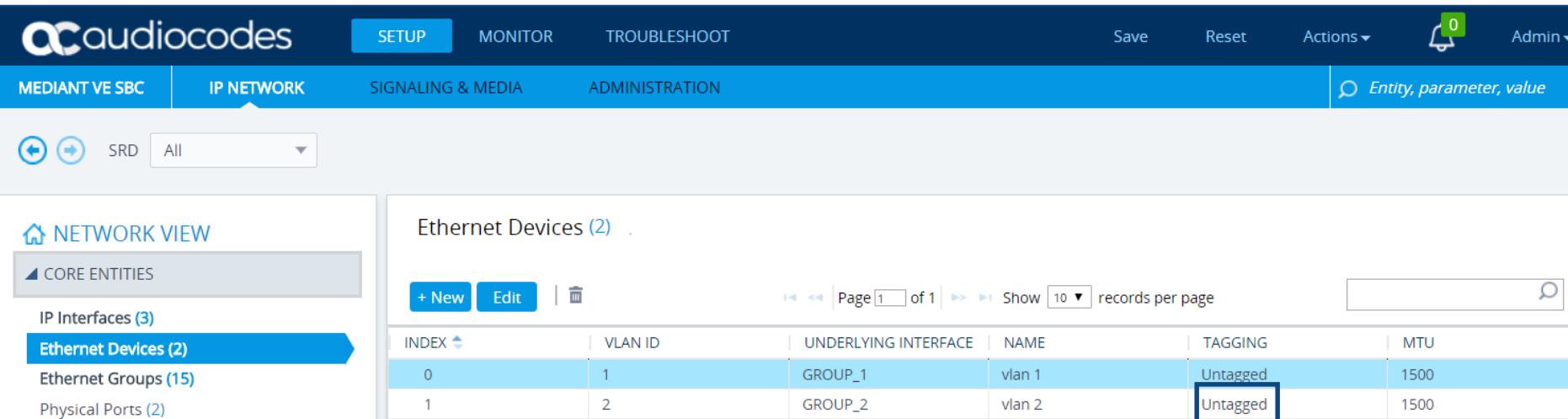
+ New Edit | 0

Page 1 of 1 Show 10 records per page

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN	OAMP + Media	IPv4 Manual	10.8.94.80	16	10.8.0.1	0.0.0.0	0.0.0.0	vlan 1
1	WAN	Media + Control	IPv4 Manual	10.8.95.80	16	10.8.0.1	0.0.0.0	0.0.0.0	vlan 1
2	HA	MAINTENANCE	IPv4 Manual	192.168.0.80	16	192.168.0.1	0.0.0.0	0.0.0.0	vlan 2

Maintenance Interface

- If VLAN tags are not required for the maintenance interface, define the group as 'Untagged'
- This will set the Native VLAN of the group to the same VLAN



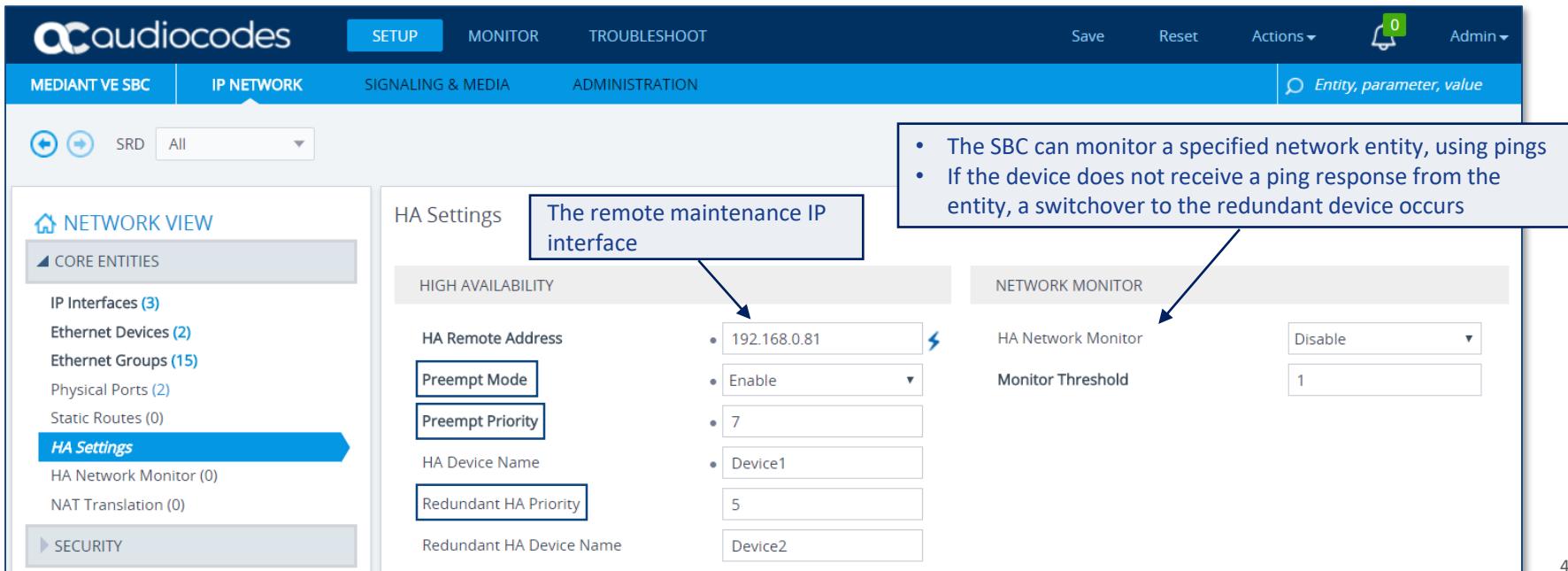
The screenshot shows the audiocodes web interface for managing network entities. The top navigation bar includes links for SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions, and Admin. The main menu on the left lists MEDIANTE SBC, IP NETWORK (which is selected), SIGNALING & MEDIA, and ADMINISTRATION. A search bar at the top right contains the placeholder "Entity, parameter, value".

In the center, under the IP NETWORK tab, there is a "NETWORK VIEW" section with a sidebar containing "CORE ENTITIES" and links for IP Interfaces (3), Ethernet Devices (2) (which is highlighted in blue), Ethernet Groups (15), and Physical Ports (2). The main content area displays "Ethernet Devices (2)" with a table:

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING	MTU
0	1	GROUP_1	vlan 1	Untagged	1500
1	2	GROUP_2	vlan 2	Untagged	1500

The "TAGGING" column for both rows is highlighted with a blue box.

- Enable the HA Preempt feature
- Set the priority level of the device in the 'Preempt Priority' field
  - Typically, you would configure the active device with a higher priority level (number) than the redundant device (range 1-10)



The screenshot shows the audiocodes SBC web interface under the 'IP NETWORK' tab. In the left sidebar, 'HA Settings' is selected. The main panel displays the 'HA Settings' configuration page. A callout box highlights the 'The remote maintenance IP interface' section, which contains the 'HA Remote Address' field set to '192.168.0.81'. Another callout box highlights the 'HIGH AVAILABILITY' section, specifically the 'Preempt Priority' field set to '7'. To the right, a 'NETWORK MONITOR' section is shown with 'HA Network Monitor' set to 'Disable' and 'Monitor Threshold' set to '1'. A callout box also highlights this section.

- The SBC can monitor a specified network entity, using pings
- If the device does not receive a ping response from the entity, a switchover to the redundant device occurs

- On default configuration the system is HA symmetric – each unit that become Active will stay Active
- The system can be configured in Preempt mode which allows specifying one of the units as the favorite/prioritized unit between the two units
- When working in Preempt mode, each unit should be configured with priority and whenever a unit with higher priority is recovering from a failure, it will become active again (performs an Auto-Switchover after HA sync. has ended)

# HA Status in the Monitor Page

Screenshot of the audiocodes Monitor Page showing HA status.

The page has a top navigation bar with tabs: SETUP, MONITOR (selected), and TROUBLESHOOT. Below the tabs are buttons for Save, Reset, Actions, and Admin. A search bar on the right contains the placeholder "Entity, parameter, value".

The main content area shows "Device Information" for a Mediant VE SBC:

Address: 10.8.94.80	Firmware: 7.20A.200.055	Type: Mediant VE SBC	<b>Operational HA Status</b> (boxed)
		S/N: 53834431404032	

Below the device information, there are two sections: "Redundant Device: Device2" (gray background) and "Active Device: Device1" (green background). Each section displays icons for Alarms (red lightbulb), Network (two green ports), and a green progress bar.

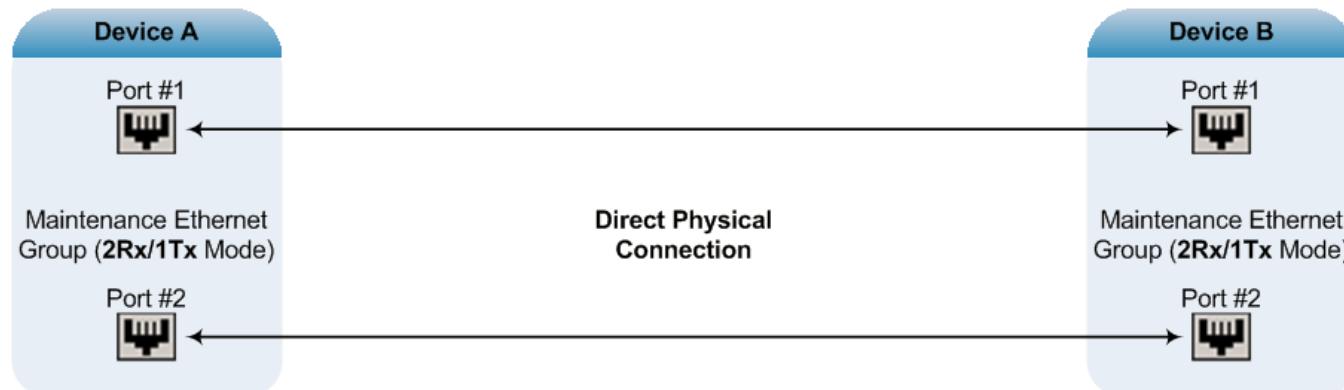
An arrow points from the "Operational HA Status" text in the list below to the "Operational HA Status" box on the device information card.

- **Synchronizing** - Redundant device is synchronizing with Active device
- **Operational** - The device is in HA mode
- **Stand Alone** - HA is configured, but the Redundant device is missing and HA is currently unavailable

- When only one device is running, it is in stand-alone state
- When the second device is loaded, it recognizes the Active device (through the Maintenance network) and acquires the HA Redundant state
- Synchronization between the Active and Redundant devices may take several minutes in which the Active device provides the Redundant device with all its current configuration settings (including loaded files and \*.cmp)
- Once loaded to the Redundant device, the Redundant device reboots to apply the new configuration

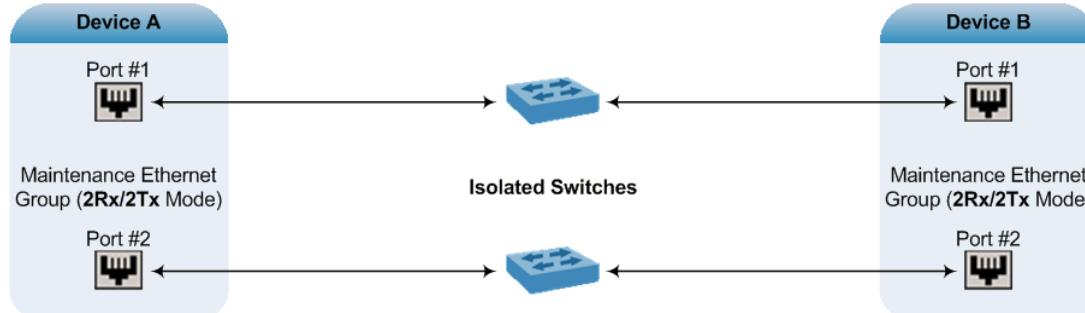
- A dedicated physical group for the Maintenance Interface
- Shared physical group – the physical port group used for the Maintenance Interface is also used for other interfaces (i.e., OAMP, Media, and/or Control) in addition to the Maintenance Interface

- Direct connection (i.e., both devices are connected directly to each other without intermediation of switches), configure the mode to 2RX/1TX:

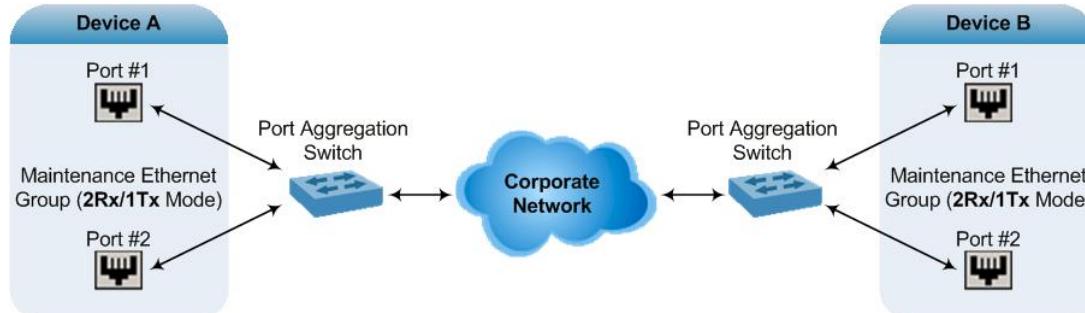


# Indirect Connection

- Two devices are connected through two (or more) isolated LAN switches
  - Configure the mode to 2RX/2TX

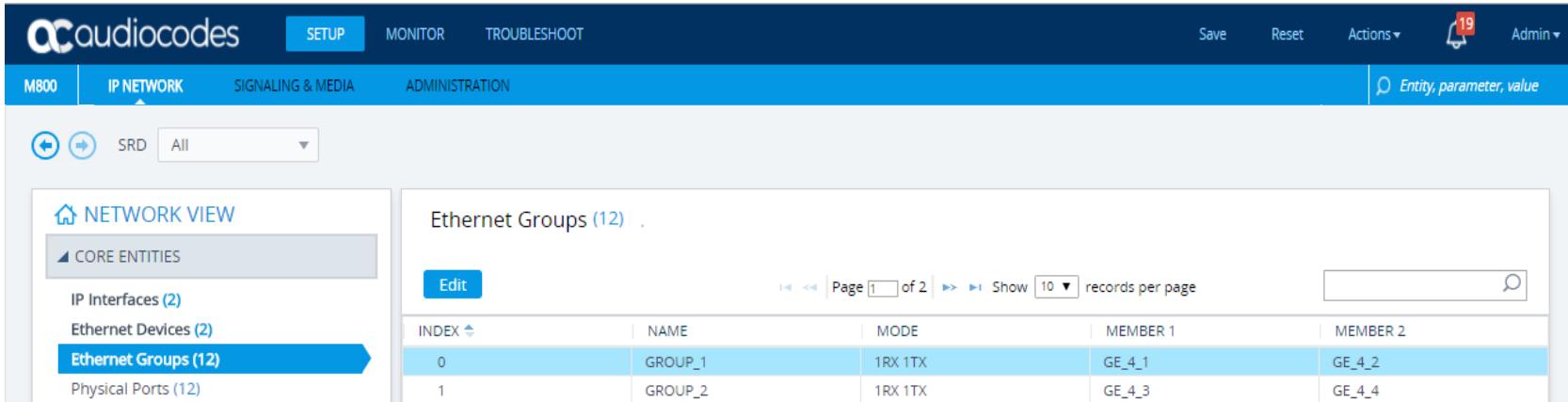


- Two devices are connected to each other through a single LAN switch
  - Configure the mode to 2RX/1TX



# Tx/Rx for Ethernet Port-Pair Groups

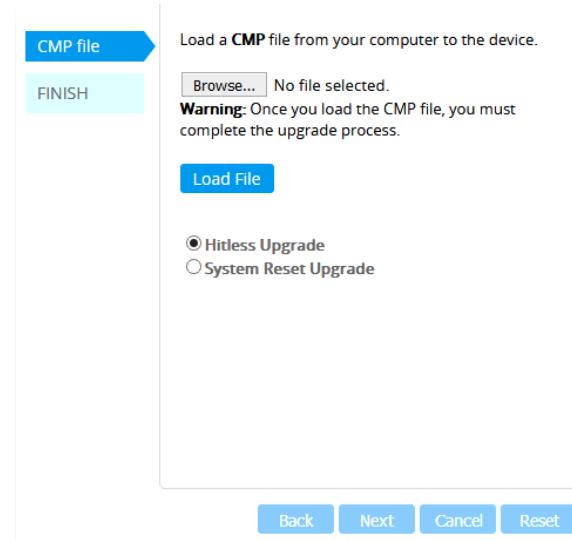
- **1RX/1TX**
  - Only a single port in the group can transmit and receive packets
- **2RX/1TX**
  - Both ports in the group can receive packets
  - Only one port can transmit
- **2RX/2TX**
  - Both ports in the group can receive and transmit packets



The screenshot shows the audiocodes M800 web interface. The top navigation bar includes the audiocodes logo, SETUP (selected), MONITOR, TROUBLESHOOT, Save, Reset, Actions, and Admin. The left sidebar has tabs for M800, IP NETWORK, SIGNALING & MEDIA, and ADMINISTRATION. Under CORE ENTITIES, the IP Interfaces (2) and Ethernet Devices (2) are listed. The Ethernet Groups (12) item is selected and highlighted with a blue arrow. The Physical Ports (12) tab is also visible. The main content area displays the "Ethernet Groups (12)" table with the following data:

INDEX	NAME	MODE	MEMBER 1	MEMBER 2
0	GROUP_1	1RX 1TX	GE_4_1	GE_4_2
1	GROUP_2	1RX 1TX	GE_4_3	GE_4_4

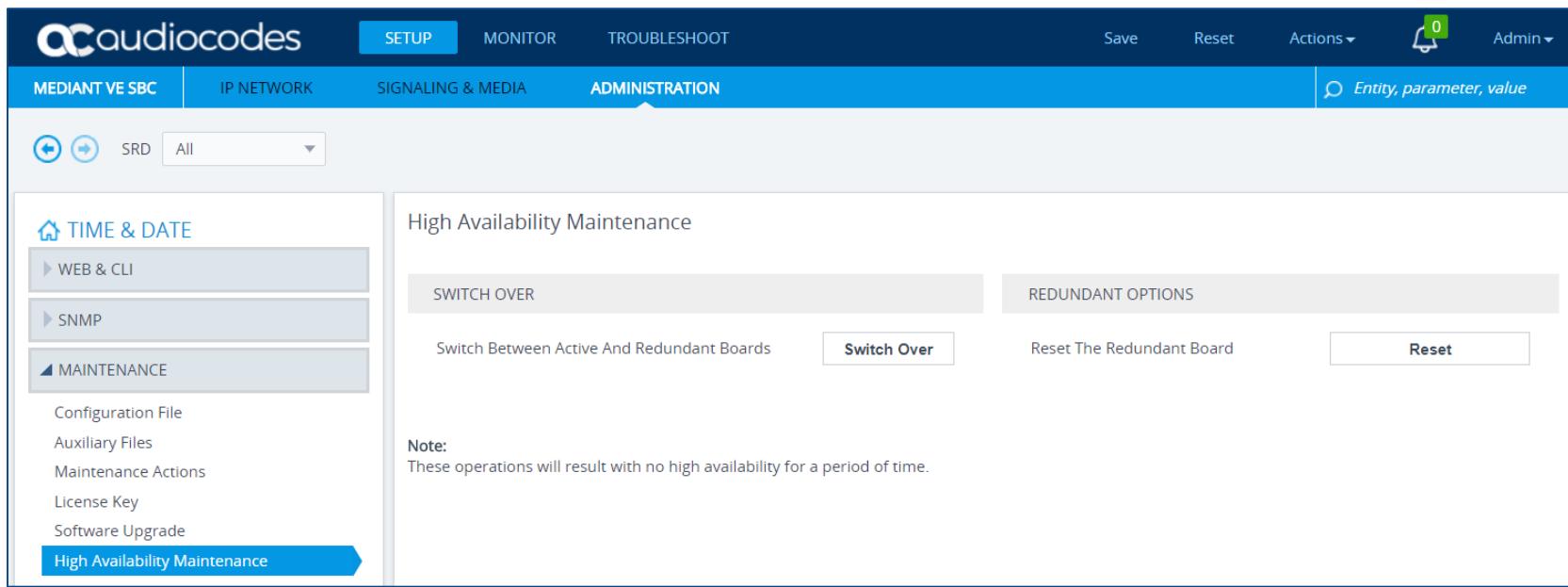
- Two types of software upgrade are available on HA system:
  - **System Reset** – both Active and Redundant units burn and reboot with new software version, this method is quick and simple but it does not preserve service
  - **Hitless** – first the Redundant unit burn and reboot with new software version and a switch over is done, then the other unit is doing the same and a switch back is issued to return to original system setup, this method preserve service but it is more complex and take more time



- Constant keep-alive messages are sent between both devices
- Failure in Active device:
  - The Redundant device issues a switch-over operation
  - The failed device resets and the previously Redundant device becomes Active in stand-alone mode
  - If the failure in the Active device is repaired after reset, it is initialized as the Redundant device and the system returns to HA
- Failure in Redundant device
  - The Active device moves itself into stand-alone mode
  - If the failure in the Redundant device is repaired after reset, it's initialized as the Redundant device once again and the system returns to HA

# High Availability Maintenance

- Manual Switch Over
  - The redundant SBC take over and the active device will reset
- Reset The Redundant Board
  - The redundant SBC resets



The screenshot shows the audiocodes web interface with the following details:

- Header:** audiocodes, SETUP, MONITOR, TROUBLESHOOT, Save, Reset, Actions ▾, Admin ▾.
- Top Navigation:** MEDIANT VE SBC, IP NETWORK, SIGNALING & MEDIA, ADMINISTRATION (highlighted).
- Left Sidebar:** TIME & DATE, WEB & CLI, SNMP, MAINTENANCE (Configuration File, Auxiliary Files, Maintenance Actions, License Key, Software Upgrade), High Availability Maintenance.
- Central Content:**
  - High Availability Maintenance** section.
  - SWITCH OVER** and **REDUNDANT OPTIONS** tabs.
  - Switch Between Active And Redundant Boards** button.
  - Switch Over** button (highlighted in blue).
  - Reset The Redundant Board** button.
  - Reset** button.
- Note:** These operations will result with no high availability for a period of time.



Thank You

*Stay in the loop*

