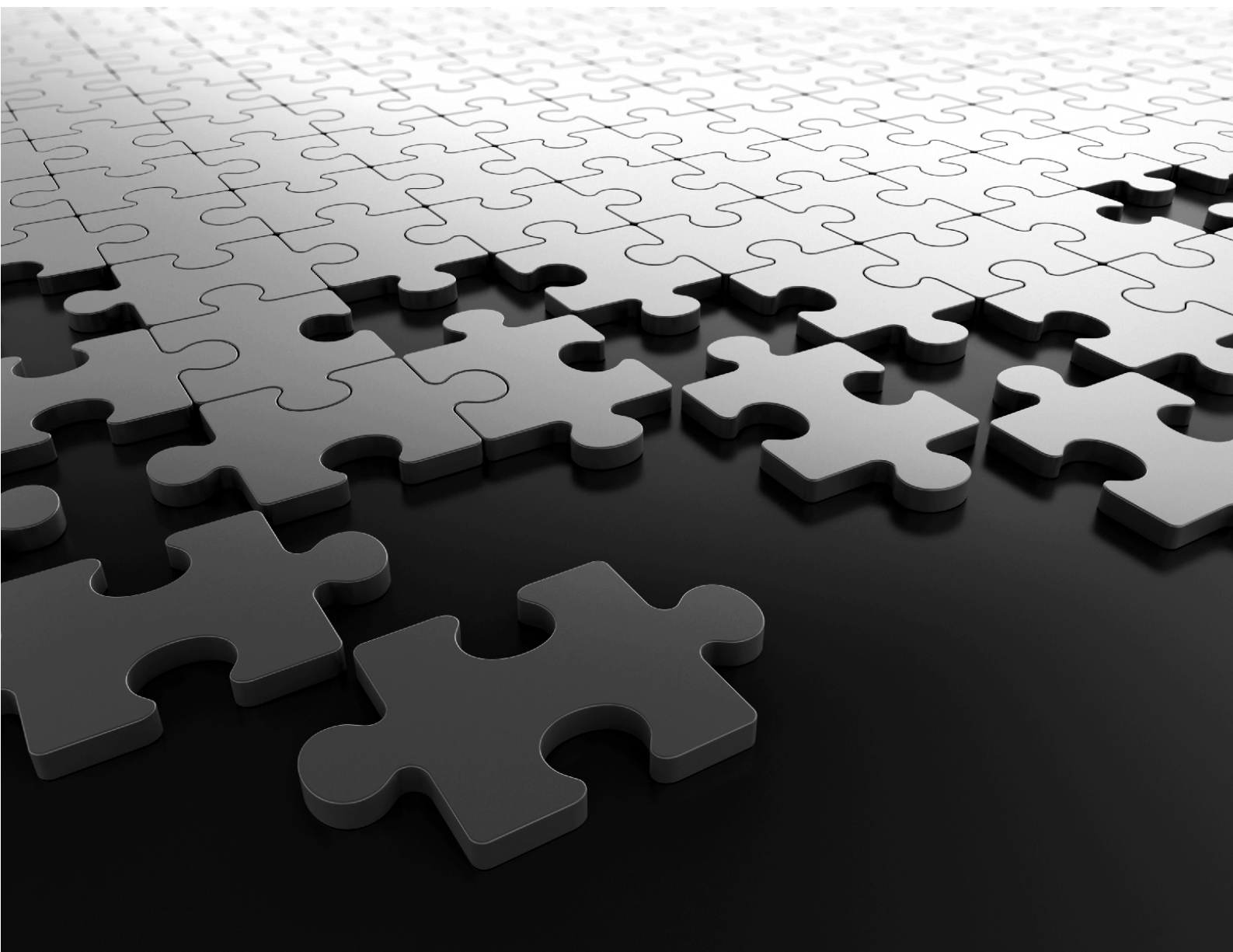


**SETU VTEP
System Manual**



SETU VTEP
Multi-Port SIP Based VoIP to T1/E1 PRI Gateway

System Manual



Documentation Disclaimer

Matrix Comsec reserves the right to make changes in the design or components of the product as engineering and manufacturing may warrant. Specifications are subject to change without notice.

This is a general documentation for all models of the product. The product may not support all the features and facilities described in the documentation.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise information in this publication for any reason without prior notice. Matrix Comsec makes no warranties with respect to this documentation and disclaims any implied warranties. While every precaution has been taken in the preparation of this system manual, Matrix Comsec assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Neither Matrix Comsec nor its affiliates shall be liable to the purchaser of this product or third parties for damages, losses, costs or expenses incurred by the purchaser or third parties as a result of: accident, misuse or abuse of this product or unauthorized modifications, repairs or alterations to this product or failure to strictly comply with Matrix Comsec's operating and maintenance instructions.

Copyright

All rights reserved. No part of this system manual may be copied or reproduced in any form or by any means without the prior written consent of Matrix Comsec.

Version 2

Release date: January 27, 2021



Contents

Introduction	1
Welcome	1
About this System Manual	1
Know Your SETU VTEP	4
Overview of SETU VTEP	4
LEDs	5
Applications	6
Installing SETU VTEP	7
Getting Started	7
Protecting SETU VTEP and Yourself	7
Connecting SETU VTEP	9
Accessing Jeeves	15
Basic Settings	19
Region	20
Network	22
LAN	24
WAN	26
Virtual WAN	33
Dynamic DNS (DynDNS.org)	39
Clone MAC Address for WAN	40
SIP Trunk	41
E1 Port	75
T1 Port	123
Login Password	173
Date-Time Settings	175
Advanced Settings	181
System Parameters	181
Dial Plan	193
Number Lists	196
Automatic Number Translation (ANT)	201
SIP Network Profile	205
SIP VoIP Profile	220
Codec Profile	224
Destination Port Determination	226
Group	241

Peer-to-Peer Dialing	245
PIN Authentication	250
Digest Authentication	253
Static Routing	255
Access Code	259
Emergency Number	260
Certificate Manager	264
(CDR)	274
Features	281
Making a New Call using Access Code	281
Disconnecting a Call using Access Code	281
Maintenance	282
Firmware Upgrade	282
Configuration Upgrade	284
Logs	290
System Debug	291
System Activity Log	296
System Fault Log	301
Network Diagnosis	304
Simple Network Management Protocol (SNMP)	306
PCAP Trace	312
Manual Call Test	314
Default System	315
Soft Restart	317
T1E1 Port Alarm/ Performance Monitoring	318
Status	322
System Detail	322
NX DBM Vocoder Detail	324
NX DBM Vocoder 1 status is displayed on this page.	324
System Performance	325
Configuration	325
Network	327
SIP Trunk	330
T1E1 Port	332
Appendix	333
Acronyms	333
Default Region Table	336
Call Progress Tones	339
Product Specifications	342
Features at Glance	345
Warranty Statement	346
Disposal of Products/Components after End-Of-Life	347
E-Waste Management and Handling Rules	348
Open Source Licensing Terms and Conditions	352

Welcome

Thank you for choosing SETU VTEP! We hope you will make optimum use of this intelligent, feature-packed VoIP to T1E1 gateway. Please read this document carefully to get acquainted with the product before installing and operating it.

About this System Manual

This document contains detailed information and instructions for installing and operating SETU VTEP.

You may also refer to the *SETU VTEP Quick Start* for quick installation. To view or download the Quick Start, scan the QR Code printed on the Product Label/Packaging Label.

You may also view or download the Quick Start from <https://www.matrixtelesol.com/product-manuals.html>

For product registration and warranty related details, please visit <https://www.matrixcomsec.com/product-registration-form.html>

Intended Audience

This system manual is meant for:

- **Network and System Engineers (SE)**, who will install, configure and maintain SETU VTEP. System Engineers are persons who customize the system configuration to meet the requirements of the organizations/users. It is assumed that System Engineers have some experience in installing and programming gateways, and are familiar with various technical terms and functions associated with it.

The System Engineer has full access to the system. Only the System Engineer is permitted to make any alterations in the configurations of SETU VTEP.

- **Users**, are individuals/organizations who will actually use SETU VTEP. Users are not expected to configure the system or program its features. The parts of this document that contain instructions for operating the features of SETU VTEP are relevant for users.

Organization of this Document

This system manual contains the following chapters:

Introduction: Gives information about this system manual.

Know Your SETU VTEP: Provides an overview of SETU VTEP.

Installing SETU VTEP: Contains information on how to install SETU VTEP, how to configure the device using the web-based programming tool, Jeeves.

Basic Settings: Provides instructions for configuring the basic parameters of SETU VTEP, which are sufficient to get the system into operation.

Advanced Settings: Contains instructions for configuring the more advanced features and facilities of SETU VTEP.

Features: Describes the features of SETU VTEP, namely, Making New Calls using Access Code, Call Disconnection using Access Code, IP Dialing and Knowing Network Information using Access Codes.

Maintenance: Provides instructions for back-up, generating reports and debugging.

Status: Describes the indicators of System, Network, SIP Trunks and T1/E1 port status.

How to read this System Manual

This System Manual is structured such that you become familiar with the product, learn how to install it, connect its interfaces to the networks, configure the system and use it.

This system manual is presented in a manner that will help you to find all the information you need, quickly and easily. You may use the Table of Contents and the Index to look up topics you want. You may also use the hyper linked cross-references (in blue font color) in the text to navigate through this document and find the related information.

Conventions used in this System Manual

The following symbols have been used for notices to draw your attention to important things:



Note: indicates something that requires your special attention or to remind you of something you need to do when you are using SETU VTEP.



Caution: indicates an action or condition that is likely to result in malfunction or damage to SETU VTEP or your property.



Warning: indicates a hazard or an action that will cause damage to SETU VTEP or cause bodily harm to the user.

Terminology used in this System Manual

The technical terms and acronyms used in this system manual are standard terms, commonly used in telecommunication and data communication industry. Considering the group of intended users of this manual, wherever possible use of jargon has been avoided.

In this manual, words '**SETU VTEP**', '**Gateway**', '**System**' are used interchangeably to mean SETU VTEP.

Some of the terms specific to this System Manual that you will encounter are defined below:

Term	Usage in the document
System Engineer (SE)	The person who installs, configures and maintains SETU VTEP.
User	The person who uses SETU VTEP.
Caller / Calling party	The person who make calls to SETU VTEP.
Callee / Called party	The person to whom calls are made by SETU VTEP user.
Source / Originating Port	A port from which a call originates.
Destination / Terminating Port	A port on which a call terminates.
Ethernet Port / Network Port	The port used for LAN or WAN connectivity.

Using this System Manual, we hope you will be able to install, operate and make optimum use of your SETU VTEP. However, if you encounter any technical problems, please contact your dealer/reseller or the Matrix Customer Care.

Overview of SETU VTEP

SETU VTEP is a SIP-based VoIP Gateway that offers connectivity to the ISDN Network. Using its intelligent Least Cost Routing logic, SETU VTEP diverts your calls through the most appropriate, cost-effective network, resulting in major savings in call costs.

With its excellent voice quality and optimized packet voice streaming over IP Network, SETU VTEP is an effective and flexible solution for accessing internet-based telephony services and corporate intranet systems across established local area networks.



Key Features

- Allowed and Denied Numbers
- Automatic Number Translation
- Call Detail Records (CDR)
- Call Progress Tone
- Daylight Saving Mode
- Digest Authentication
- Dynamic DNS
- Emergency Number Dialing
- Fax over IP
- Least Cost Routing
- NAT and STUN Support
- PCAP Trace
- Peer-to-Peer Calling
- Return Call to Original Caller
- VLAN Tagging
- Web based Programming

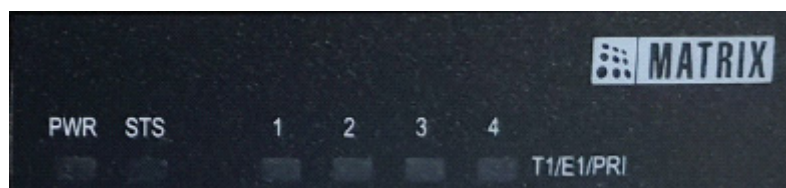
This product is available in following configuration:

Sr. No.	Configuration	Voice Channels	T1E1 Port
1.	SETU VTEP4P	120	4
2.	SETU VTEP3P	90	3
3.	SETU VTEP2P	60	2
4.	SETU VTEP1P	30	1

For a complete list of Hardware features refer [“Product Specifications”](#) in the Appendix.

LEDs¹

SETU VTEP has a Power LED (PWR), Status LED (STS) and 4 T1/E1/PRI Port LEDs. The LEDs indicate the status of the ports, and various events occurring on the ports, including errors.

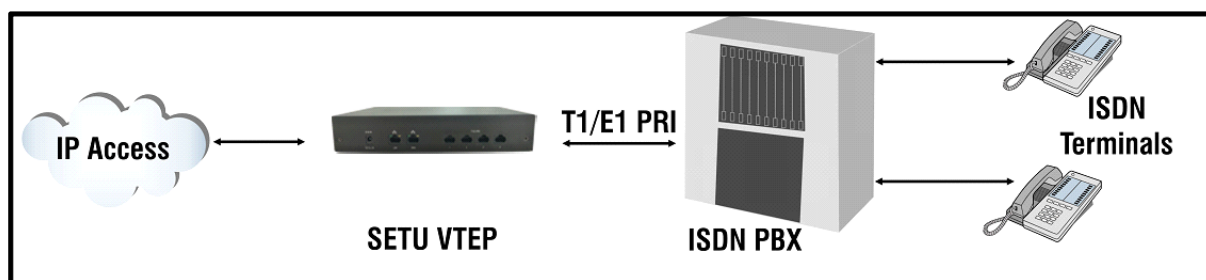


SETU VTEP is easy to install and operate. The built-in web server, JEEVES, allows you to configure the system parameters and features On-site as well as from a remote location.

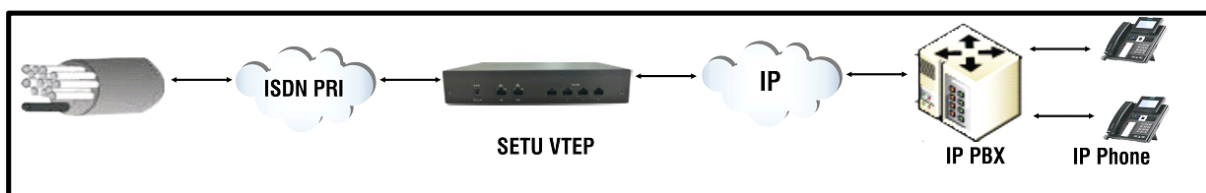
1. Depending on the configuration of your SETU VTEP, the number of T1/E1/PRI Port LEDs may vary.

Applications

VoIP Access Device for Existing PBX



PRI Gateway for an IP-PBX



Getting Started

Before you begin to install and set up the hardware of SETU VTEP, make sure you have the following items:

- Power supply.
- A standalone PC and/or a locally connected host or workstation that can PING the SETU VTEP.
- Appropriate cables and connectors to set up and test the Ethernet interface of the SETU VTEP.
- A SIP Account to test VoIP connectivity.
- An NT1 termination device for the T1/E1 line, where applicable.

Well begun is half done; plan your hardware installation well.

Protecting SETU VTEP and Yourself

For safe and efficient operation, observe the guidelines and all necessary safety precautions given in here. While installing as well as using any electronic appliance, take every safety precaution to reduce the risk of fire, electric shock and injury to persons.

Protecting the system while installing

Take these preventive steps while installing SETU VTEP:

- Do not install the system at any of the below locations:
 - in any area where it is directly exposed to sunlight, excessive cold or humid atmosphere.
 - any area where sulfuric gases are produced and where there are thermal springs.
 - at any place which is sensitive to vibrations or frequent and strong shocks.
 - at dusty places or places where it comes in direct contact with oil or water.
 - near any water source like a wash bowl, kitchen sink, bath tub or near a swimming pool.
 - on movable or unstable surfaces, which may cause the product to fall and get damaged.

Safety Instructions

It is recommended that you follow the safety instructions given below and adhere to it while handling this electronic appliance. Your safety and that of the others lies in your hands.

- Read and understand all the instructions given in the manual properly.
- Unplug the product from the wall outlet before cleaning and do not use liquid cleaners. Use only dry and soft cloth.
- Do not open the system in power ON condition.
- Interfacing cables should not touch the exposed power line cable.
- The product should be operated with proper power voltage supply.
- Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
- To reduce the risk of electric shock or damage to the system, take the product to the qualified serviceman, when some repair work or servicing is required. Removing covers or opening the system or incorrect reassembly may cause electric shock when used subsequently.

Unplug the system from the wall outlet and contact the qualified service personnel under the following conditions:

- If liquid has been spilled into the product.
- If the product has been exposed to rain or water.
- If the product does not operate normally by following the operating instructions. Adjust only those controls which are covered by the operating instructions because improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to normal operation.
- If the product has been dropped or the cabinet has been damaged.
- If the product exhibits a distinct change in the performance.

Battery

SETU VTEP contains a 3VDC/18mAh (Li-Al) alloy-Manganese Dioxide Coin Battery (ML 1220 - Rechargeable) of diameter 12.5mm and height 2.0mm. The Battery should be replaced only by authorized dealers of Matrix. End Users must not attempt to replace it.



There is risk of explosion if the Battery is replaced in an incorrect manner. Please dispose-off used Batteries.

Disposal

This product must be disposed off according to the national laws and regulations prevailing in the country where it is installed.

Connecting SETU VTEP

Verify contents of the package shipped to you with the contents listed below. If any of the items is missing or damaged, contact your Dealer/Reseller.

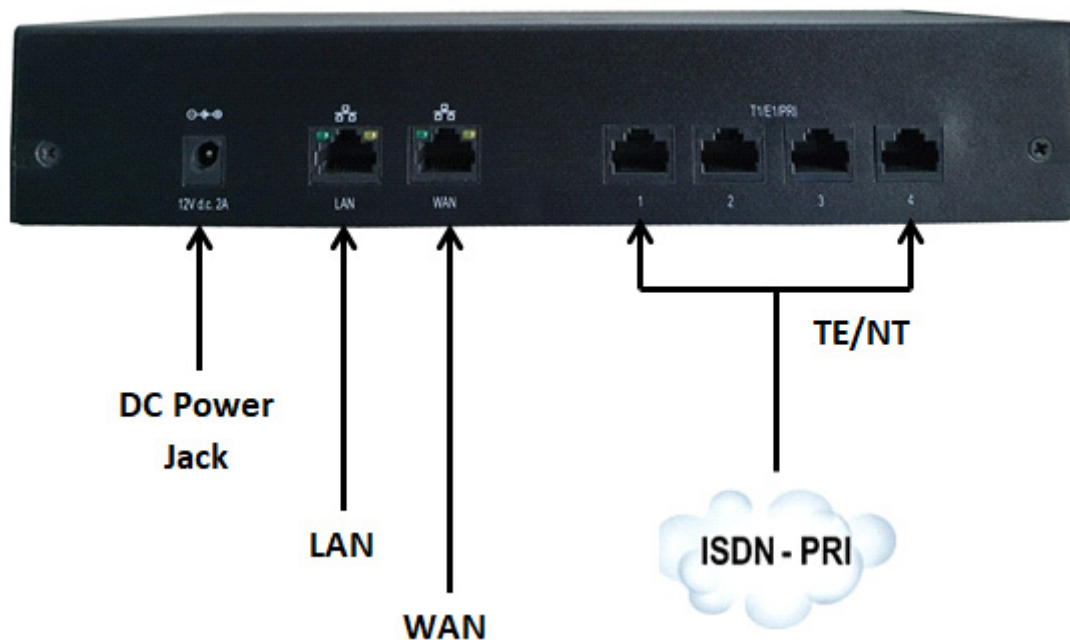
You can view the documentation of the following product by scanning the QR code printed on the Product Label/ Packaging Label of the product.

Package Contents

Sr. No.	Item Name	Quantity	Remarks
01	SETU VTEP unit	1	
02	Power Adapter	1	Power adapter will be supplied with country specific plug
03	Ethernet Cable RJ45	2	1 for LAN+1 for WAN
04	PRI Cross Cable	4	

If any of these items is missing or damaged, please contact the dealer/reseller from whom you purchased the system.

SETU VTEP has 125 SIP Trunks, 4 T1/E1 Port, 1 LAN Port, 1 WAN Port, a Power Adapter and LEDs.



- Place the system at the selected site.
- Connect the system, refer to the diagram above.

Connecting SETU VTEP to the VoIP Network

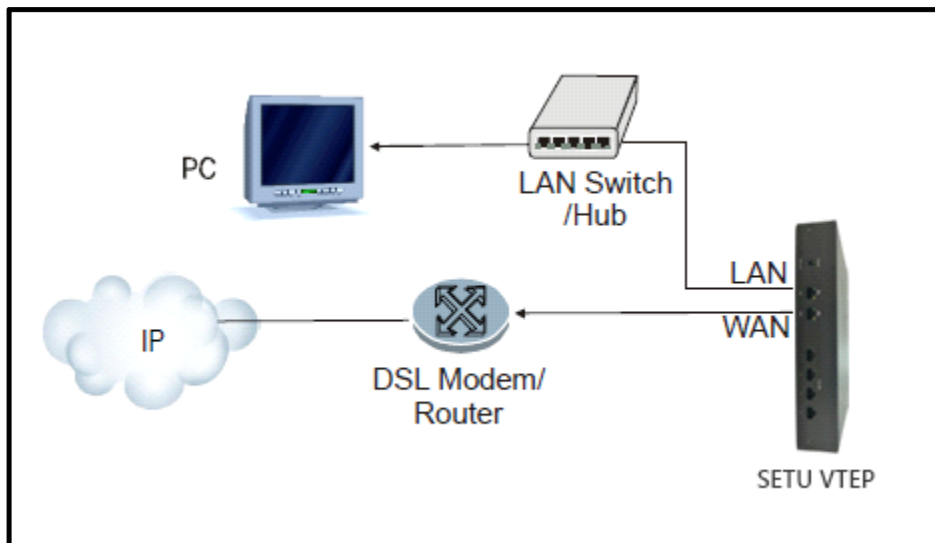


Before you connect the system to WAN, we recommend that you first connect a computer to the LAN Port of SETU VTEP, configure the Basic Settings, and then connect to WAN.

- Use the Ethernet cable supplied for the LAN port of SETU VTEP to connect the system to the IP network, which may be Public Internet or a LAN.

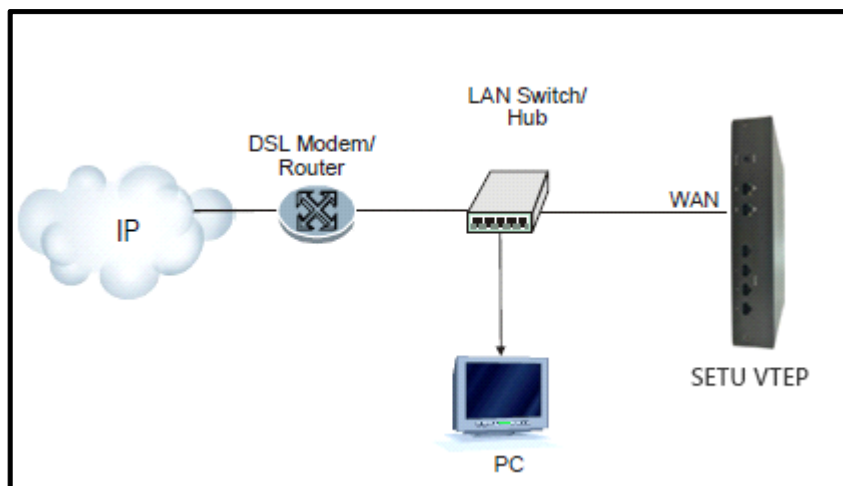
If connecting to the Public IP Network,

- Plug one end of the Ethernet cable into the WAN Port of SETU VTEP and the other end into the DSL modem/Router.



If connecting to a Private Network (Behind a NAT Router),

- Plug one end of the Ethernet cable into the WAN Port of SETU VGFX and the other end into the LAN Switch/Hub.



Connecting SETU VTEP to the ISDN PRI Network

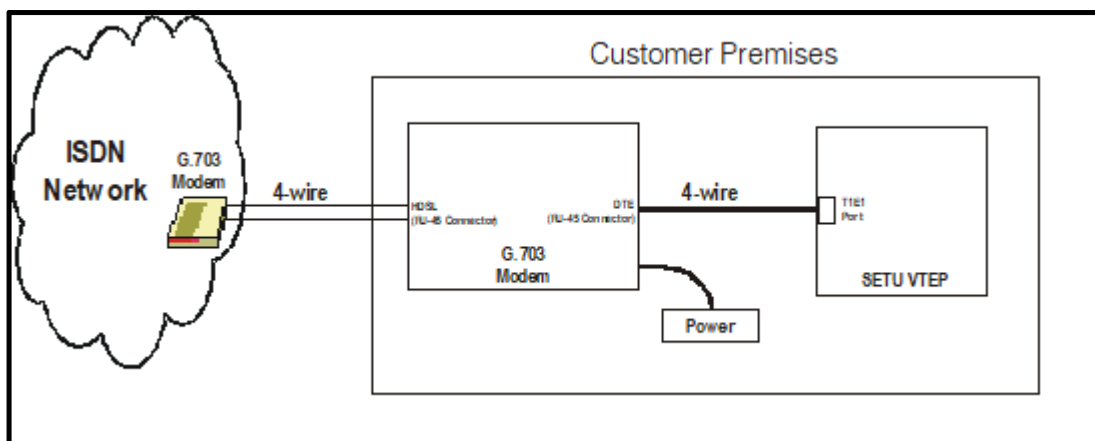
On T1 carrier lines, the system supports the following signaling types:

- PRI
- Robbed Bit Signaling (RBS)

On E1 carrier lines, the system supports the signal types:

- PRI
- Channel Associated Signaling (CAS)
- Select the type of carrier line according to your requirement.
- By default, the T1/E1 Port is set for E1 Line connectivity.
- Use the cable supplied in the package for the T1/E1 Port to connect to the T1/E1 network interface equipment (modem), as shown in the figure below.

The modem is usually supplied by the ISDN Service Provider along with the T1/E1 line.



Most Service Providers insist on connecting an ISDN modem at both the ends of the T1/E1 line, i.e. one at the Local Exchange and other at the Customer's Premises.

At the Customer's Premises, the T1/E1 line is terminated on the HDSL interface of the modem.

The DTE interface of the modem is to be connected to the T1/E1 port of the system.

Refer the following pin details for connecting the Network Termination Unit with the T1/E1 Port of SETU VTEP.

Pin details of HDSL Interface of the G.703 Modem. (HDSL Network Termination Unit)

Pin Number	Pin Details
1	Line A
2	Line A
3	Not used
4	Line B

Pin Number	Pin Details
5	Line B
6	Not used
7	Not used
8	Not used

Pin details of DTE Interface of G.703 Modem. (HDSL Network Interface Unit)

Pin Number	Pin Details
1	TX1 (Tip)
2	TX2 (Ring)
3	Not used
4	RX1 (Ring)
5	RX2 (Tip)
6	Not used
7	Not used
8	Not used



- *The pin out details of the HDSL interface and DTE interface are of a stand-alone HDSL Network Termination Unit: the Model HTU-E from RAD Data Communication.*
- *Most of the HDSL Network Termination Unit manufacturers use these connectors. But you are advised to read the installation guide of the HDSL Network Termination Unit being used by you.*

Pin details of the T1/E1 Port of SETU VTEP

Pin	Function
1	Receive Data Input Rx1
2	Receive Data Input Rx2
3	Not connected
4	Transmit Data Output Tx1
5	Transmit Data Output Tx2
6	Not connected
7	Not connected
8	Not connected



You may use PRI Cross cable depending on the pin out of the DTE Interface of the terminal.

- Accordingly, plug in one end of the cable supplied with the system into the T1/E1 port connector. Plug the other end of the cable into the Network Termination Unit.

- If you have completed all other installation tasks. Power the system, and observe the Reset Cycle.

Connecting the Power Supply

- Power on the SETU VTEP by connecting the 12V DC, 2A Power Adapter to the Power jack.
- Observe the Reset cycle.

Reset Cycle

- Reset Cycle (Power-ON Self Test) takes about 2 minutes to finish.

System LED Indication (STS)

System Status	LED Indication	Comment
Gateway started successfully	Green Blinks 1000ms ON - 1000ms OFF	Gateway Started Successfully
MM_Up_SIP_down	Red Blinks 500ms ON -3500ms OFF	Media Manager is Up SIP stack is down
MM_down_SIP_Up	Red Blinks 500ms ON - 500ms OFF 500msON - 2500ms OFF	Media Manager is down SIP stack is Up
MM_down_SIP_down	Red Blinks 500 ms ON - 500ms OFF 500 ms ON - 500ms OFF 500 ms ON - 1500ms OFF	Media Manager is down SIP stack is down

T1E1 Port LED Indication

1. Port Active Mode

Signaling Type: E1-PRI

LED Pattern:

Port Status	Color	Cadence
Layer 1 established successfully	GREEN	Continuous ON
CRC4 Alarm	GREEN	100ms ON-100 ms OFF
BFA Alarm	RED	500ms ON-500 ms OFF
LOS Alarm	RED	Continuous ON

Signaling Type: E1-CAS

LED Pattern:

Port Status	Color	Cadence
Layer 1 established successfully	GREEN	Continuous ON
CRC4 Alarm	GREEN	100ms ON-100 ms OFF
MFA Alarm	RED	100ms ON-100 ms OFF
BFA Alarm	RED	500ms ON-500 ms OFF
LOS Alarm	RED	Continuous ON

Signaling Type: T1-RBS or T1-PRI

LED Pattern:

Port Status	Color	Cadence
No Alarm	GREEN	Continuous ON
TFA Alarm or MFA Alarm	RED	500ms ON-500 ms OFF
AIS Alarm	RED	100ms ON-100 ms OFF
LOS Alarm	RED	Continuous ON

2. *Port Disable Mode*

LED Pattern:

Port Status	Color	Cadence
Port Disable	RED	Continuous ON

Accessing Jeeves

SETU VTEP provides an embedded web server with a graphic user Interface (GUI), *Jeeves*, for configuration.

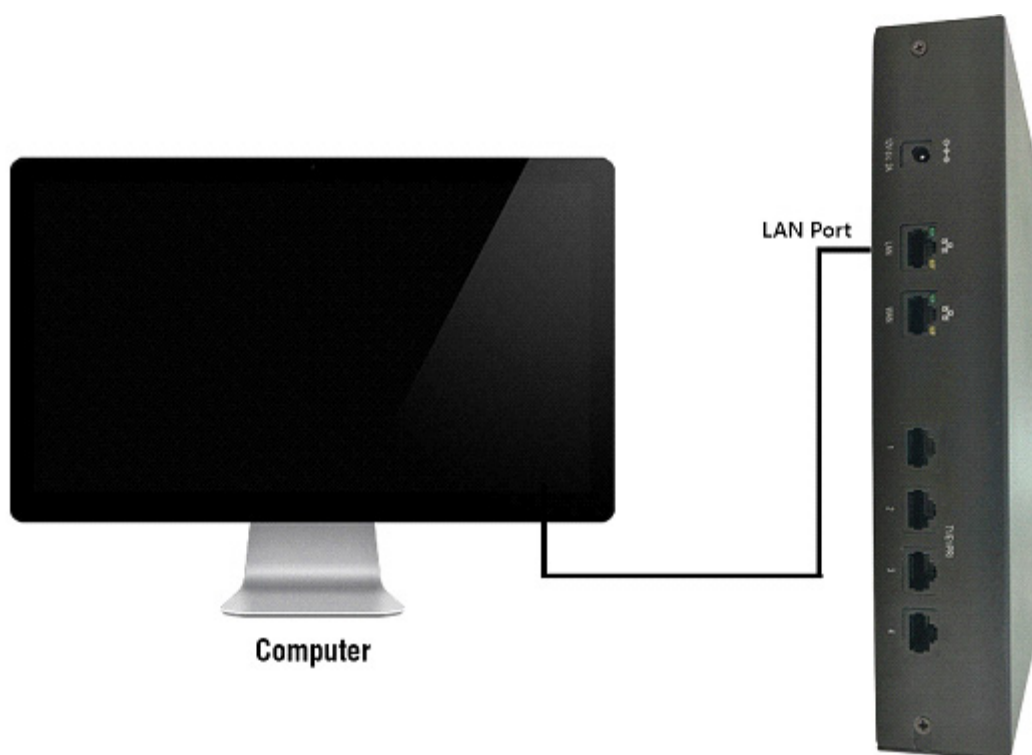
To access Jeeves, you will need to connect a computer to SETU VTEP.

Connecting a Computer

You may connect a standalone computer to SETU VTEP or grab any computer connected in the same LAN as SETU VTEP.



Connect a standalone computer to SETU VTEP, when installing the system for the very first time. You may connect it to a computer on LAN at a later stage, once you have finished installation and configuration of the system.



To connect a standalone computer,

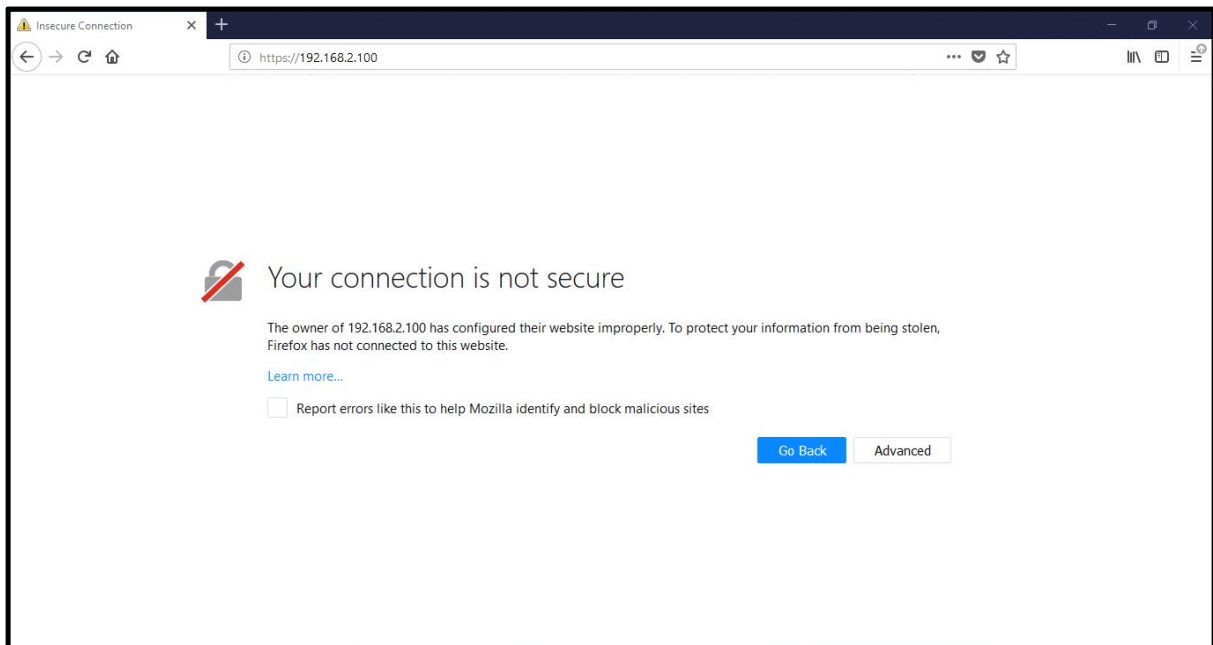
- Plug one end of the Ethernet cable, supplied with the system, into the LAN Port of SETU VTEP. Plug the other end into the LAN port of the computer.
- Make sure the IP Address of the computer and the LAN Port of SETU VTEP do not conflict, and that both are in the same Subnet.

The default IP Address of the LAN Port of SETU VTEP is: **192.168.2.100**

The default Subnet Mask of the LAN Port of SETU VTEP is: **255.255.255.0**

Change the Subnet of the computer, if necessary.

- Make sure a web-browser, either Internet Explorer (Version 7 or higher) or Mozilla Firefox (Version 3.5 or higher), is installed on the computer.
- Open the browser (Internet Explorer or Mozilla Firefox) on the computer.
- Enter the default IP address **192.168.2.100** of the LAN Port of SETU VTEP in the address bar of the browser.
- You will be redirected to the HTTPS protocol for security reasons.
- Click on **Advanced**.
- Click on the **Proceed with <https://192.168.2.100>**.



- The **Login** page will open.

MATRIX SETU VTEP

Login Password

Matrix ComSec Pvt. Ltd.
Visit Us: www.MatrixComSec.com

WARNING: No part of the system should be copied or reproduced in any form or by any means without the prior written consent of Matrix ComSec Pvt. Ltd.
Copyright © 2013 Matrix ComSec Pvt. Ltd.

- In **Login Password**, enter **M@rXt3ID4\$**, the default SE Password.
- Click the **Login** button.



Before you start configuring the system, if you wish to view or download the SETU VTEP Quick Start, you can scan the QR Code present on the login page of Jeeves.

- You will be prompted to change the default SE Password.

Password Change

Login through default password is not allowed. Change the password to login.

Current Password

New Password

Confirm New Password

Note :

Password must follow following requirements:

- Minimum length must be 6 characters.
- Password must include atleast 1 uppercase, 1 lowercase , 1 number and 1 special character.
- Allowed characters are 0-9, a-z, A-Z, all special characters except %, =, #, +, &, \, <, >, ' , ' and space.

- In **Current Password**, enter the default SE Password.
- Enter the **New Password**. All ASCII characters (except Percentage %, Hash #, Equal to =, Plus +, And &, Backslash \, Less than <, Greater than >, Apostrophe ' , Double Quote " and **Space**) and digits 0 to 9 are allowed. The new password must be:
 - a minimum of 6 characters to a maximum of 16 characters.

- include atleast one upper-case, one lower-case, one number and one special character.
- In **Confirm New Password**, re-enter the new password to confirm.
- Click **Submit**. You will be re-directed to the Login page again.
- In **Login Password**, enter the new password.

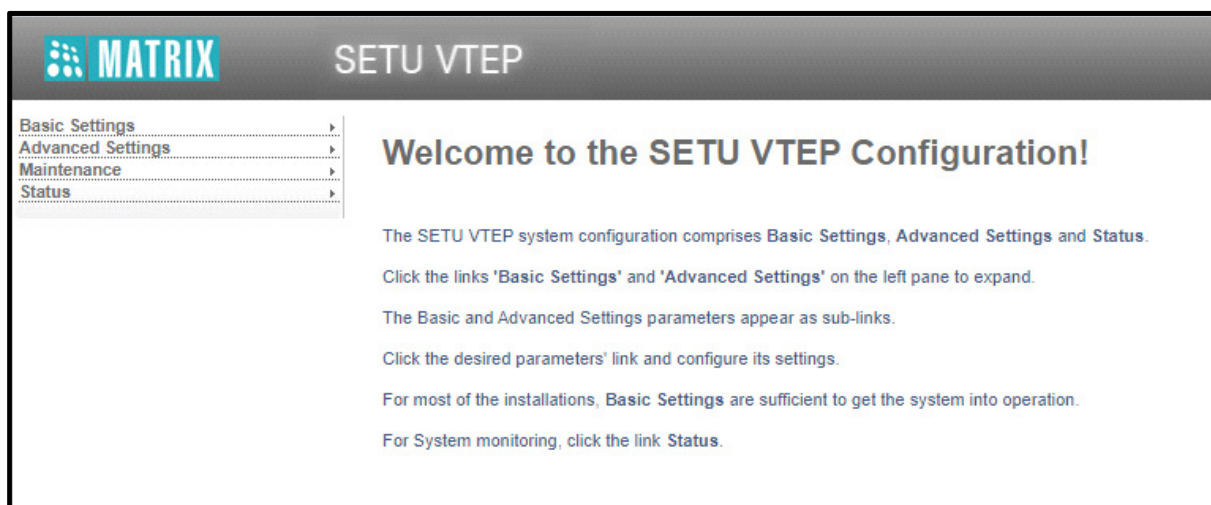


As this password is meant for restricting access to the SE mode, we strongly recommend you to:

- *Keep the password secret.*
- *Select a complex password that cannot be easily guessed.*
- *Change the password regularly. See [“Login Password”](#) for instructions.*

On successful login, the **Home** page of Jeeves opens.

The left pane shows the links **Basic Settings**, **Advanced Settings**, **Maintenance** and **Status**.



Basic Settings break down the complexities of configuration and are sufficient to get your system into operation.

Advanced Settings enable you to configure the advanced features and facilities of SETU VTEP.

Maintenance allows you to carry out system maintenance and monitoring like uploading configuration and firmware, system debug, system restart.

Status allows you to view the system details and status of all the SIP trunks, T1/E1 layer and the Network port.

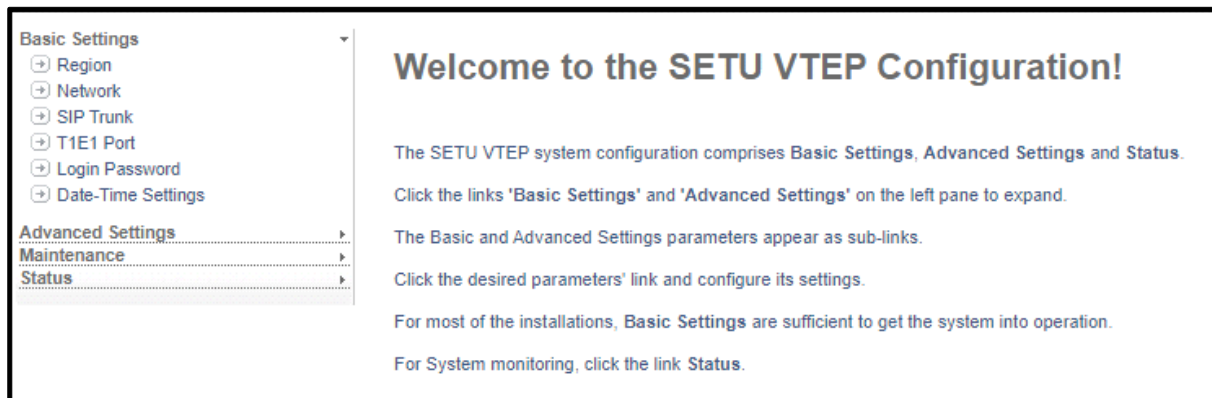
You may now configure the Basic Settings of SETU VTEP.




The Basic Settings lets you configure the basic parameters of SETU VTEP. Configuring these, you will be able to operate the system efficiently.


To configure Basic Settings,

- Click the **Basic Settings** link to expand.

The links to the different basic parameters appear on the left navigation bar.



- Click the sub link of the required parameter: **Region, Network, SIP Trunk, T1E1 Port, Login Password** and **Date -Time Settings**.
- The selected parameter page opens.
 - Click **Expand**  to expand a link and display all parameters under the link.
 - Click **Collapse**  to collapse a link and hide all parameters under the link.
 - Click **Settings**  to configure / edit the settings of a parameter further.
 - Click the **Submit** button to save changes made on the page.
 - Click the **Default** button to assign factory set values to all the parameters on the page.
 - Click the **Add** button to add a new record.
 - Click the **Delete** button to delete a record.

- Click the **Close** button to exit a window.
- Click **Logout**  to end the login session and exit Jeeves. You will return to the login page of Jeeves.

Region

To configure Region and other region specific parameters,

- Click the **Region** link.



The screenshot displays the 'Region' configuration page. On the left, a sidebar under 'Basic Settings' lists 'Region', 'Network', 'SIP Trunk', 'T1/E1 Port', 'Login Password', and 'Date-Time Settings'. The 'Region' option is selected. The main content area is titled 'Region' and contains the following fields:

- Region:** A dropdown menu currently showing 'India'.
- PCM Companding Type:** A dropdown menu currently showing 'A-law'.
- Call Progress Tone:** A dropdown menu currently showing 'India'.
- Country Code:** A text input field containing '91'.

 At the bottom of the form are two buttons: 'Submit' (with a checkmark icon) and 'Default' (with a reset icon).

Region

- In **Region**, select the name of the country where SETU VTEP is installed. Default: India.
- When you change Region, an alert message will appear on the screen **“Changing Region shall assign default values to all parameters of the system. Do you want to continue?”** Click OK. All country specific parameters will be assigned default values. See [“Default Region Table”](#) in the Appendix for country specific default values.

PCM Companding Type

- SETU VTEP automatically sets the **PCM Companding Type** according to the Region you select. You can change the PCM Companding Type—A-law or μ -law as per your requirement. Default: A-law (for India).

Call Progress Tones

- Select **Call Progress Tone**. SETU VTEP supports country specific Call Progress Tone Generation (CPTG) to simulate the same tones of the local PSTN to which it is connected. The Call Progress Tones supported by SETU VTEP for different countries is presented in the *Appendix*. For details, see [“Call Progress Tones”](#).

- To match the call progress tone of the country where SETU VTEP is installed, select the Country accordingly. Default: India

The screenshot shows a configuration window titled 'Region'. It contains several dropdown menus and buttons. The 'Region' dropdown is set to 'India'. The 'PCM Companding Type' dropdown is set to 'A-law'. The 'Call Progress Tone' dropdown is open, displaying a list of countries: Argentina, Australia, Brazil, Canada, China, Egypt, France, Germany, Greece, India (highlighted), Indonesia, Iran, Iraq, Israel, Italy, Japan, and Kenya. The 'Country Code' field is empty. At the bottom left, there are two buttons: 'Submit' (with a checkmark icon) and 'Default' (with a plus icon).

Country Code

- SETU VTEP automatically sets the **Country Code** according to the Region you select. You can change the Country Code as per your requirement. Default: 91 (India).

If you have kept **Remove Country Code from CLI received** check box enabled in the *System Parameters*, the system will remove the Country Code configured here from the CLI received on the source port.

- Click the **Submit** button to save.

Network

SETU VTEP may be installed typically, in a Public IP Network or in a Private network, behind a NAT Router.

When SETU VTEP is installed in a Public IP Network,

- the WAN Port of SETU VTEP is connected to a Broadband Router/Modem.
- Public IP is assigned to the WAN Port.

When SETU VTEP is installed in a Private Network, behind a NAT Router,

- the WAN Port of SETU VTEP is connected to the LAN Switch/Hub.
- Private IP is assigned to the WAN Port.

Depending on your installation scenario, configure the Network Port Parameters.

To configure Network parameters,

- Click the **Basic Settings** link to expand.
- Click the **Network** link. The Network Parameters page opens.

The screenshot shows the 'Network' configuration page. On the left is a sidebar with a tree view containing 'Basic Settings' (expanded), 'Advanced Settings', 'Maintenance', and 'Status'. Under 'Basic Settings', 'Region', 'Network' (selected), 'SIP Trunk', 'T1E1 Port', 'Login Password', and 'Date-Time Settings' are listed. The main content area is titled 'Network' and contains the following settings:

- Virtual WAN**: A checkbox labeled 'Enable' which is checked.
- IP Addressing mode for LAN**: A dropdown menu set to 'IPv4 only'.
- IP Addressing mode for WAN**: A dropdown menu set to 'IPv4 and IPv6'.
- IP Addressing mode for Virtual WAN**: A dropdown menu set to 'IPv4 and IPv6'.

Below these settings are expandable sections for 'LAN', 'WAN', 'Virtual WAN', 'Dynamic DNS (DynDNS.org)', and 'Clone MAC Address for WAN'. At the bottom are two buttons: 'Submit' (with a checkmark icon) and 'Default' (with a reset icon).

- **Virtual WAN:** Enable Virtual WAN if your system uses it and configure the respective parameters related to Virtual WAN.
Virtual WAN will be applicable only for SIP.
- **IP Addressing mode for LAN:** Select the IP version you want the system to use for LAN. You may select — IPv4 only or IPv4 and IPv6. Default: IPv4 only.

If you select IPv4 only, you can configure the IPv4 parameters only.

If you select IPv6 only, you can configure the IPv6 parameters only.

If you select IPv4 and IPv6, you can configure both IPv4 and IPv6 parameters.
- **IP Addressing mode for WAN:** Select the IP version you want the system to use for WAN. You may select — IPv4 only or IPv4 and IPv6. Default: IPv4 and IPv6.

If you select IPv4 only, you can configure the IPv4 parameters only.

If you select IPv6 only, you can configure the IPv6 parameters only.

If you select IPv4 and IPv6, you can configure both IPv4 and IPv6 parameters.

- **IP Addressing mode for Virtual WAN:** Select the IP version you want the system to use for Virtual WAN. You may select — IPv4 only or IPv4 and IPv6. Default: IPv4 and IPv6.

If you select IPv4 only, you can configure the IPv4 parameters only.

If you select IPv6 only, you can configure the IPv6 parameters only.

If you select IPv4 and IPv6, you can configure both IPv4 and IPv6 parameters.



IP Addressing mode for LAN depends on the IP Addressing mode for WAN and VWAN.

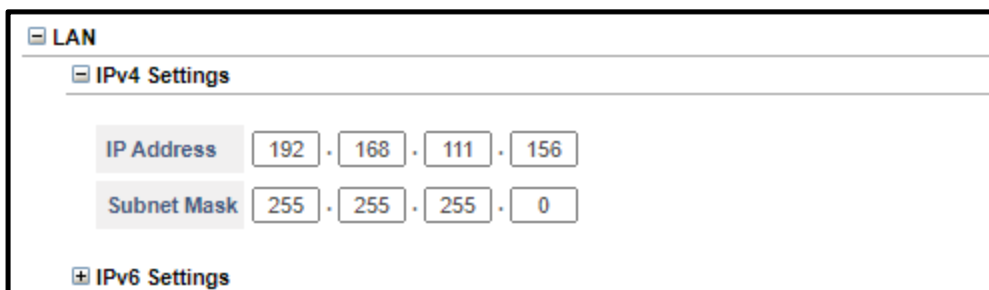
If IP Addressing mode for either WAN and/or VWAN is selected as either IPv6 or both IPv4 & IPv6, then IP Addressing mode for LAN will be disabled and by default the mode will be set as IPv4 and IPv6.

Network	
Virtual WAN	<input checked="" type="checkbox"/> Enable
IP Addressing mode for LAN	IPv4 and IPv6 ▼
IP Addressing mode for WAN	IPv4 and IPv6 ▼
IP Addressing mode for Virtual WAN	IPv6 only ▼

LAN

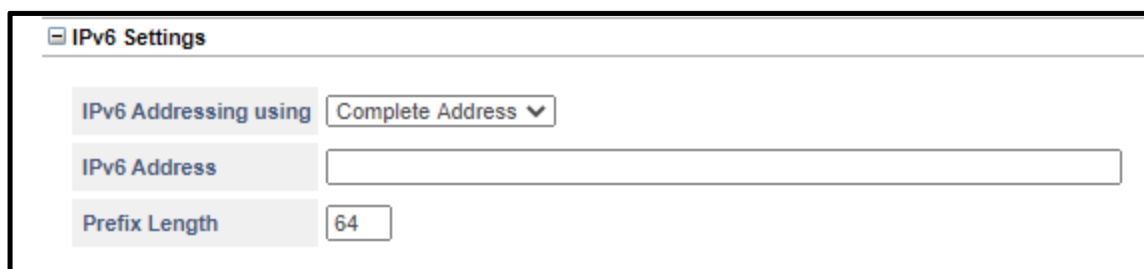
Click **LAN** to expand.

- **For IPv4 Settings:**



The screenshot shows the 'LAN' configuration window. Under the 'IPv4 Settings' tab, there are two rows of input fields. The first row is labeled 'IP Address' and contains four boxes with the values '192', '168', '111', and '156', separated by dots. The second row is labeled 'Subnet Mask' and contains four boxes with the values '255', '255', '255', and '0', also separated by dots. Below these fields, there is a collapsed 'IPv6 Settings' section.

- In **IP Address**, the current IP Address of the LAN Port is displayed. Example: **192.168.111.156**. You can assign only Static IP to the LAN Port.
- In **Subnet Mask**, the current Subnet Mask of the LAN Port is displayed. Example: **255.255.255.0**. If required, you may change the LAN Port IP Address and Subnet Mask.
- **For IPv6 Settings:**



The screenshot shows the 'IPv6 Settings' configuration window. It contains three rows of settings. The first row is 'IPv6 Addressing using' with a dropdown menu currently set to 'Complete Address'. The second row is 'IPv6 Address' with a large, empty text input field. The third row is 'Prefix Length' with a text input field containing the value '64'.

- **IPv6 Addressing using:** You can select — Complete Address or Prefix. Default: Complete Address.

If you select Complete Address,

- Configure the **IPv6 Address** and the **Prefix Length**. The IP Address configured will be considered as the complete IPv6 address.

For example: 2001:0:3238:DFE1:63::FEFB

The Prefix Length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

Valid Range of the IPv6 Address is A to F, a to f, 0 to 9,:(colon). It can be a maximum of 39 characters. Default: Blank.

The Prefix Length range is from 1 to 128 bits. Default: 64.

If you select Prefix,

- Configure the **IPv6 Prefix**. The system will consider the configured value as 64 bit Prefix of the IPv6 Address. Then the system will generate the complete IPv6 Address from it. Default: Blank.

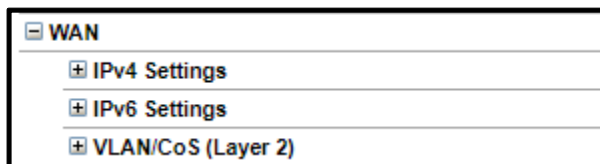
Valid characters 0 to 9, a to f, A to F and : (colon). It can be a maximum of 21 characters.



When your SETU VTEP is installed in a Private Network, make sure the LAN Port and the WAN Port are connected in different subnets.

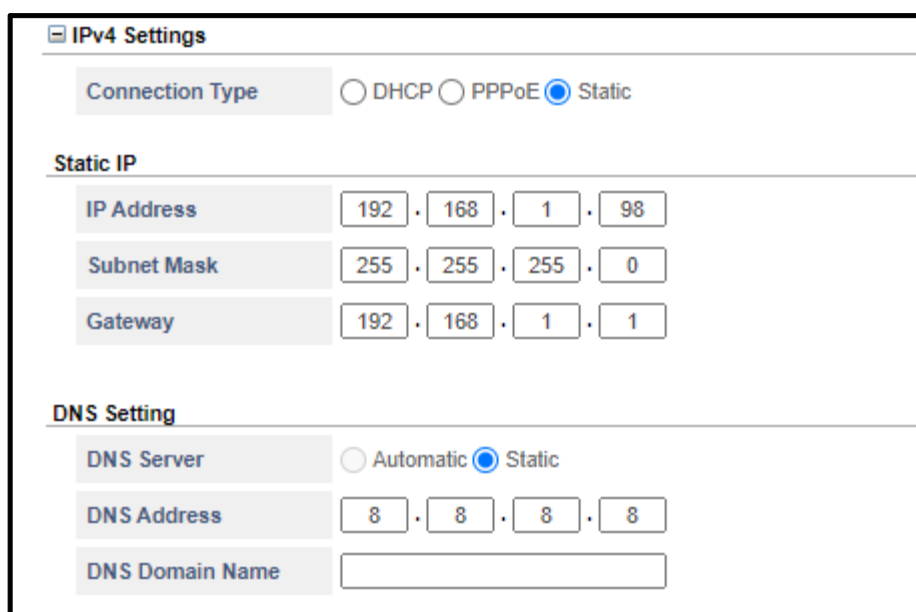
WAN

- Click **WAN** to expand.



A screenshot of a web interface showing the 'WAN' section expanded. It contains three sub-items: 'IPv4 Settings', 'IPv6 Settings', and 'VLAN/CoS (Layer 2)', each with a plus icon to its left.

For IPv4 Settings:



A screenshot of the 'IPv4 Settings' configuration page. At the top, 'Connection Type' has three radio buttons: 'DHCP', 'PPPoE', and 'Static' (which is selected). Below this is a 'Static IP' section with three rows of input fields: 'IP Address' (192, 168, 1, 98), 'Subnet Mask' (255, 255, 255, 0), and 'Gateway' (192, 168, 1, 1). At the bottom is a 'DNS Setting' section with 'DNS Server' set to 'Static' (selected over 'Automatic'), 'DNS Address' (8, 8, 8, 8), and an empty 'DNS Domain Name' field.

Connection Type

- Select the network connection type, that is, the IP Addressing Scheme used by your network to assign the IP address to the WAN Port: Static, DHCP, PPPoE. Default: Static.
- Static:** Select **Static**, if your network uses **Static IP addressing** and configure the following parameters.
 - In **IP Address**, enter the IP Address you obtained from your Network Administrator for the WAN Port of SETU VTEP. Make sure that the IP Address does not conflict with that of any other device on the LAN. Default: 192.168.1.98
 - In **Subnet Mask**, enter the Subnet Mask you obtained from your Network Administrator for the WAN Port. Default: 255.255.255.0
 - In **Gateway**, enter the IP Address of the Router's LAN Interface as the Default Gateway IP Address. Default: 192.168.1.1

- **DHCP:** Select **DHCP**, if your network uses DHCP Addressing. Whenever SETU VTEP is restarted, the DHCP server will dynamically assign an IP Address, Subnet Mask and Gateway Address to the WAN Port.
- You have to configure the Domain Name Server (DNS) Address only, if not already provided by your Internet Service Provider.

The screenshot shows the 'IPv4 Settings' window. Under 'Connection Type', the 'DHCP' radio button is selected. The 'DNS Setting' section is visible, showing 'DNS Server' set to 'Static', 'DNS Address' set to '8.8.8.8', and 'DNS Domain Name' as an empty text box.

- **PPPoE:** Select **PPPoE**, if your network uses PPPoE addressing. The PPPoE server will automatically assign an IP Address, Subnet Mask and Gateway Address to the WAN Port of SETU VTEP.
- You need to configure the following parameters provided by your Internet Service Provider:

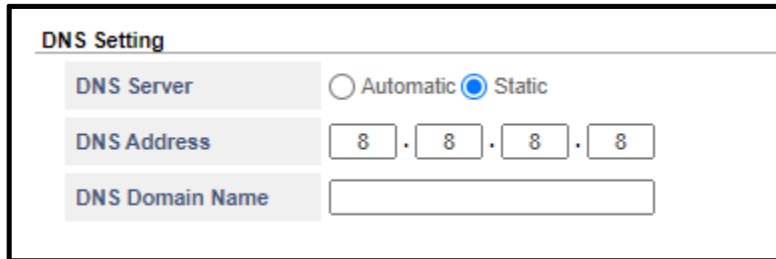
The screenshot shows the 'IPv4 Settings' window. Under 'Connection Type', the 'PPPoE' radio button is selected. The 'PPPoE' section is visible, showing 'User ID', 'Password', and 'Service Name' as empty text boxes. The 'DNS Setting' section is also visible, showing 'DNS Server' set to 'Static', 'DNS Address' set to '8.8.8.8', and 'DNS Domain Name' as an empty text box.

- In **PPPoE User ID**, enter the User Name provided by the Internet Service Provider. The User ID can be a maximum of 64 characters.
- In **PPPoE Password**, enter the User Password provided by the Internet Service Provider. The password can be a maximum of 64 characters.

- In **PPPoE Service Name**, enter the Service Name, if provided by your Internet Service Provider. The Service Name may be a maximum of 64 characters.
- If Service Name is not provided, leave this blank.

DNS Setting

Configure the Domain Name Server (DNS) settings as provided by your Internet Service Provider. You may consult your Network Administrator.



- Select **DNS Server** as **Automatic** or **Static** according to the Connection Type (IP Addressing scheme) used by the network.
- Select **Static** if:
 - your network uses Static IP Addressing.
 - your network uses DHCP or PPPoE, but the DHCP/ PPPoE server does not provide DNS Address automatically.
- In **DNS Address**, enter the DNS Server Address. In **DNS Domain Name**, enter the DNS Domain Name if provided to you by your Network Administrator.
- Select **Automatic** if:
 - your network uses DHCP or PPPoE IP Addressing.
 - the DHCP/ PPPoE server of your network assigns the DNS Address automatically.

For IPv6 Settings:

IPv6 Settings

Connection Type ☐ Statefull DHCPv6 ☐ Stateless Auto-Configuration ☒ Static

Static

IPv6 Addressing using Complete Address ▼

IPv6 Address 4001::192:168:1:156

Prefix Length 64

Gateway 4001::1

DNS Setting

DNS Server ☐ Automatic ☒ Static

DNS Address 2001::2001:2001:2001:2001

Connection Type

- Select the network connection type, that is, the IP Addressing Scheme used by your network to assign the IP address to the WAN Port: Static, Statefull DHCPv6, Stateless Auto-Configuration. Default: **Static**.
- Select **Static**, if your network uses **Static IP addressing** and configure the following parameters.
 - Select the **IPv6 Addressing** either using **Complete Address** or **Prefix**.
 - Enter the **IPv6 Address**.
- **Prefix Length:** Configure the Prefix Length. Valid Range: 1 to 128 bits. Default: 064.

The Prefix Length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

The Prefix Length range is from 1 to 128 bits. Default: 64.

- In **Gateway**, enter the IP Address of the Router's LAN Interface as the Default Gateway IP Address. Example: 4001::1.

- **Statefull DHCPv6:** Select this option as the connection type, if your network uses DHCP to obtain various necessary parameters from DHCP Servers so the DHCP clients can operate in an Internet Protocol (IP) network.
- Statefull DHCP is centrally managed on a DHCP server(s); and the DHCP clients use Statefull DHCP to obtain an IP address(es) and other useful configuration information from the DHCP server(s).

The screenshot shows the 'IPv6 Settings' window. Under 'Connection Type', 'Statefull DHCPv6' is selected with a radio button. Below this, the 'Statefull DHCPv6' section is active, showing 'Prefix Length' set to '64'. The 'DNS Setting' section shows 'DNS Server' set to 'Static' and 'DNS Address' set to '2001::2001:2001:2001:2001'.

- **Prefix Length:** Configure the Prefix Length. Valid Range: 1 to 128 bits. Default: 064.
- The Prefix Length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
- The Prefix Length range is from 1 to 128 bits. Default: 64.

The screenshot shows the 'IPv6 Settings' window. Under 'Connection Type', 'Stateless Auto-Configuration' is selected with a radio button. Below this, the 'Stateless Auto-Configuration' section is active, showing 'IPv6 Scope Preference' set to 'Global' (via a dropdown) and 'Prefix Length' set to '64'. The 'DNS Setting' section shows 'DNS Server' set to 'Static' and 'DNS Address' set to '2001::2001:2001:2001:2001'.

- **Stateless Auto-Configuration:** Select this option as the connection type, if your network uses DHCP to obtain various necessary parameters from DHCP Servers so the DHCP clients can operate in an Internet Protocol (IP) network.
- DHCPv6 for stateless configuration parameters allows a stateless or statefull DHCPv6 client to export configuration parameters (DHCPv6 options) to a local DHCPv6 server pool.

- The local DHCPv6 server can then provide the imported configuration parameters to other DHCPv6 clients.
- **IPv6 Scope Preference:** IPv6 includes support of Global as well as Non-Global Addresses. Select the scope of preference — Global or Unique. Default: Global.
- **Prefix Length:** Configure the Prefix Length. Valid Range: 1 to 128 bits. Default: 064.

The Prefix Length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

The Prefix Length range is from 1 to 128 bits. Default: 64.

DNS Setting

Configure the Domain Name Server (DNS) settings as provided by your Internet Service Provider. You may consult your Network Administrator.

The screenshot shows a configuration window titled "DNS Setting". It contains two main sections. The first section is labeled "DNS Server" and has two radio buttons: "Automatic" and "Static". The "Static" radio button is selected. The second section is labeled "DNS Address" and contains a text input field with the value "2001::2001:2001:2001:2001".

- Select **DNS Server** as **Automatic** or **Static** according to the Connection Type (IP Addressing scheme) used by the network.
- Select **Static** if:
 - your network uses Static IP Addressing.
 - your network uses Statefull DHCPv6 and Statefull Auto-Configuration, but the server does not provide DNS Address automatically.
- In **DNS Address**, enter the DNS Server Address. In **DNS Domain Name**, enter the DNS Domain Name if provided to you by your Network Administrator.

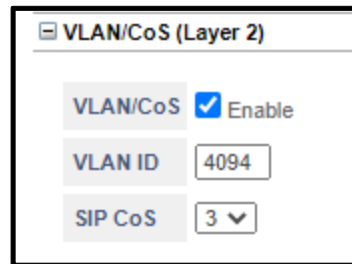
The screenshot shows a configuration window titled "DNS Setting". It contains two main sections. The first section is labeled "DNS Server" and has two radio buttons: "Automatic" and "Static". The "Automatic" radio button is selected. The second section is labeled "DNS Address" and contains an empty text input field.

- Select **Automatic** if:
 - your network uses Statefull DHCPv6 and Statefull Auto-Configuration IP Addressing.
 - the Statefull DHCPv6 and Statefull Auto-Configuration server of your network assigns the DNS Address automatically.

VLAN/CoS

If SETU VTEP is connected in a VLAN, configure the **VLAN/CoS**. This parameter enables the SETU VTEP to add VLAN header to the packets generated by it. The VLAN header consists of the VLAN ID (12-bit) and Class of Service (CoS, 3-bit) for prioritization of traffic.

- Click **VLAN/CoS (Layer 2)** to expand.
- Select the **VLAN/CoS** check box to enable VLAN ID tagging on all packets generated by the system.
Default: Disabled.

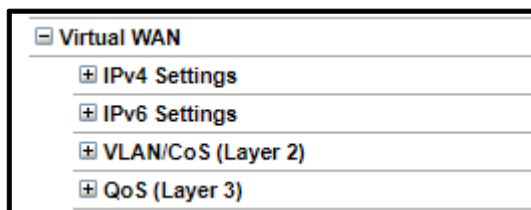


VLAN/CoS (Layer 2)	
VLAN/CoS	<input checked="" type="checkbox"/> Enable
VLAN ID	4094
SIP CoS	3 ▼

- Enter the **VLAN ID** that you have assigned to the VLAN in which the SETU VTEP is connected. Valid range is 0 to 4094. Default: 4094.
- For **SIP CoS**, define the CoS (priority) bits which will be added in all SIP packets. Valid range is 0 to 7.

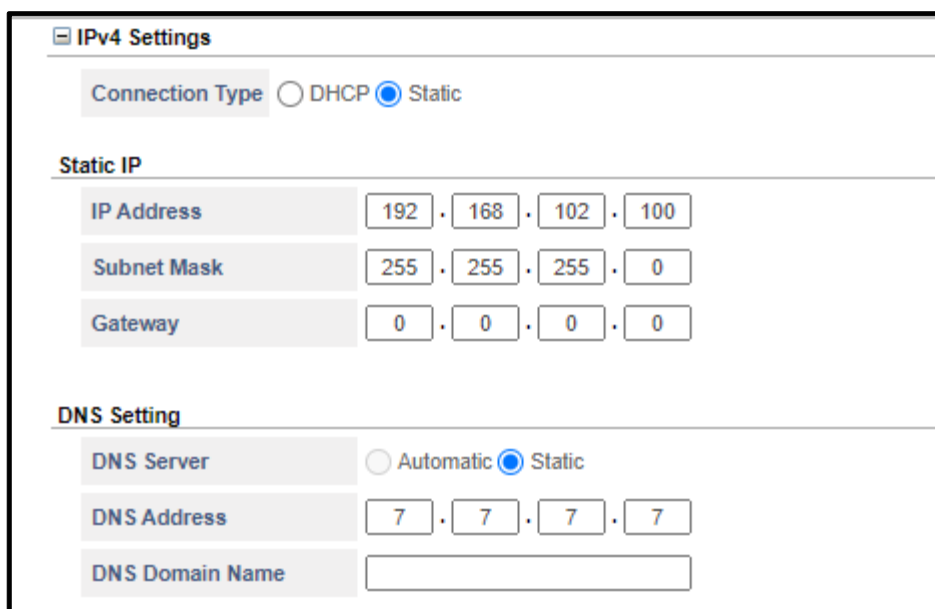
Virtual WAN

- Click on Virtual WAN to expand it.



A screenshot of a web interface showing a sidebar menu. The menu is titled "Virtual WAN" and is expanded, showing four sub-items: "IPv4 Settings", "IPv6 Settings", "VLAN/CoS (Layer 2)", and "QoS (Layer 3)". Each item has a plus icon to its left.

For IPv4 Settings:



A screenshot of the "IPv4 Settings" configuration page. The page has a title bar "IPv4 Settings". Below it, there is a "Connection Type" section with two radio buttons: "DHCP" and "Static". The "Static" radio button is selected. Below this is a "Static IP" section with three rows of input fields: "IP Address" (192, 168, 102, 100), "Subnet Mask" (255, 255, 255, 0), and "Gateway" (0, 0, 0, 0). Below that is a "DNS Setting" section with two rows: "DNS Server" (Automatic, Static) where "Static" is selected, and "DNS Address" (7, 7, 7, 7). There is also a "DNS Domain Name" input field.

Connection Type

- Select the network connection type, that is, the IP Addressing Scheme used by your network to assign the IP address to the WAN Port: Static, DHCP, PPPoE. Default: Static.
- **Static:** Select **Static**, if your network uses **Static IP addressing** and configure the following parameters.
 - In **IP Address**, enter the IP Address you obtained from your Network Administrator for the WAN Port of SETU VTEP. Make sure that the IP Address does not conflict with that of any other device on the LAN. Default: 192.168.1.98
 - In **Subnet Mask**, enter the Subnet Mask you obtained from your Network Administrator for the WAN Port. Default: 255.255.255.0
 - In **Gateway**, enter the IP Address of the Router's LAN Interface as the Default Gateway IP Address. Default: 192.168.1.1

- **DHCP:** Select **DHCP**, if your network uses DHCP Addressing. Whenever SETU VTEP is restarted, the DHCP server will dynamically assign an IP Address, Subnet Mask and Gateway Address to the WAN Port.
- You have to configure the Domain Name Server (DNS) Address only, if not already provided by your Internet Service Provider.

The screenshot shows the 'IPv4 Settings' window. Under 'Connection Type', the 'DHCP' radio button is selected. Under 'DNS Setting', the 'Static' radio button is selected for 'DNS Server'. The 'DNS Address' field is populated with '7.7.7.7' using a four-part numeric input. The 'DNS Domain Name' field is empty.

DNS Setting

Configure the Domain Name Server (DNS) settings as provided by your Internet Service Provider. You may consult your Network Administrator.

This is a close-up of the 'DNS Setting' section. It shows the 'DNS Server' section with 'Automatic' and 'Static' radio buttons, where 'Static' is selected. Below it, the 'DNS Address' is set to '7.7.7.7' in a four-part numeric input. The 'DNS Domain Name' field is empty.

- Select **DNS Server** as **Automatic** or **Static** according to the Connection Type (IP Addressing scheme) used by the network.
- Select **Static** if:
 - your network uses Static IP Addressing.
 - your network uses DHCP but the DHCP server does not provide DNS Address automatically.
- In **DNS Address**, enter the DNS Server Address. Default: **7.7.7.7**
- In **DNS Domain Name**, enter the DNS Domain Name if provided to you by your Network Administrator.

DNS Setting

DNS Server ☒ Automatic ☐ Static

- Select **Automatic** if:
 - your network uses DHCP IP Addressing.
 - the DHCP server of your network assigns the DNS Address automatically.

For IPv6 Settings:

IPv6 Settings

Connection Type ☐ Statefull DHCPv6 ☐ Stateless Auto-Configuration ☒ Static

Static

IPv6 Addressing using Complete Address ▾

IPv6 Address 1001::192:168:112:154

Prefix Length 64

Gateway

DNS Setting

DNS Server ☐ Automatic ☒ Static

DNS Address 901::1

Connection Type

- Select the network connection type, that is, the IP Addressing Scheme used by your network to assign the IP address to the WAN Port: Static, Statefull DHCPv6, Stateless Auto-Configuration. Default: **Stateless Auto-Configuration**.
- Select **Static**, if your network uses **Static IP addressing** and configure the following parameters.
 - **IPv6 Addressing using:** You can select — **Complete Address** or **Prefix**.

If you select Complete Address,

- Configure the **IPv6 Address** and the **Prefix Length**. The IP Address configured will be considered as the complete IPv6 Address.

The Prefix Length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

Valid Range of the IPv6 Address is A to F, a to f, 0 to 9,:(colon). It can be a maximum of 39 characters. Default: Blank.

The Prefix Length range is from 1 to 128 bits. Default: 64.

- **Gateway:** Configure the Gateway IP Address for the WAN Port. It can be a maximum of 39 characters.

If you select Prefix,

- Configure the **IPv6 Prefix**. The system will consider the configured value as 64 bit Prefix of the IPv6 Address. Then the system will generate the complete IPv6 Address from it. Default: Blank.

Valid characters 0 to 9, a to f, A to F and : (colon). It can be a maximum of 21 characters.

- **Statefull DHCPv6:** Select this option as the connection type, if your network uses DHCP to obtain various necessary parameters from DHCP Servers so the DHCP clients can operate in an Internet Protocol (IP) network.
- Statefull DHCP is centrally managed on a DHCP server(s); and the DHCP clients use Statefull DHCP to obtain an IP address(es) and other useful configuration information from the DHCP server(s).

The screenshot shows the 'IPv6 Settings' configuration window. It contains three main sections: 'Connection Type' with three radio button options ('Statefull DHCPv6' is selected), 'Statefull DHCPv6' with a 'Prefix Length' input field set to '64', and 'DNS Setting' with two radio button options ('Automatic' and 'Static', with 'Static' selected) and a 'DNS Address' input field containing '901::1'.

- **Prefix Length:** Configure the Prefix Length. Valid Range: 1 to 128 bits. Default: 64.
- The Prefix Length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

IPv6 Settings

Connection Type ☐ Statefull DHCPv6 ☒ Stateless Auto-Configuration ☐ Static

Stateless Auto-Configuration

IPv6 Scope Preference Unique ▾

Prefix Length 64

DNS Setting

DNS Server ☐ Automatic ☒ Static

DNS Address 901::1

- **Stateless Auto-Configuration:** Select this option as the connection type, if your network uses DHCP to obtain various necessary parameters from DHCP Servers so the DHCP clients can operate in an Internet Protocol (IP) network.
- DHCPv6 for stateless configuration parameters allows a stateless or statefull DHCPv6 client to export configuration parameters (DHCPv6 options) to a local DHCPv6 server pool.
- The local DHCPv6 server can then provide the imported configuration parameters to other DHCPv6 clients.
- **IPv6 Scope Preference:** IPv6 includes support of Global as well as Non-Global Addresses. Select the scope of preference — **Global** or **Unique**. Default: **Unique**.
- **Prefix Length:** Configure the Prefix Length. Valid Range: 1 to 128 bits. Default: 64.

The Prefix Length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

DNS Setting

Configure the Domain Name Server (DNS) settings as provided by your Internet Service Provider. You may consult your Network Administrator.

DNS Setting

DNS Server ☐ Automatic ☒ Static

DNS Address 901::1

- Select **DNS Server** as **Automatic** or **Static** according to the Connection Type (IP Addressing scheme) used by the network.

- Select **Static** if:
 - your network uses Static IP Addressing.
 - your network uses Statefull DHCPv6 and Statefull Auto-Configuration, but the server does not provide DNS Address automatically.
- In **DNS Address**, enter the DNS Server Address. In **DNS Domain Name**, enter the DNS Domain Name if provided to you by your Network Administrator.



DNS Setting

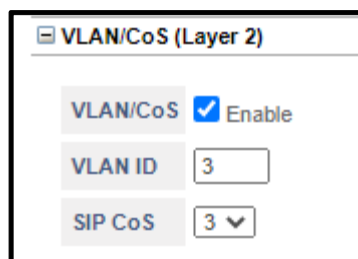
DNS Server ☒ Automatic ☐ Static

- Select **Automatic** if:
 - your network uses Statefull DHCPv6 and Statefull Auto-Configuration IP Addressing.
 - the Statefull DHCPv6 and Statefull Auto-Configuration server of your network assigns the DNS Address automatically.

VLAN/CoS

If SETU VTEP is connected in a VLAN, configure the **VLAN/CoS**. This parameter enables the SETU VTEP to add VLAN header to the packets generated by it. The VLAN header consists of the VLAN ID (12-bit) and Class of Service (CoS, 3-bit) for prioritization of traffic.

- Click **VLAN/CoS (Layer 2)** to expand.
- Select the **VLAN/CoS** check box to enable VLAN ID tagging on all packets generated by the system. Default: Disabled.



VLAN/CoS (Layer 2)

VLAN/CoS ☒ Enable

VLAN ID 3

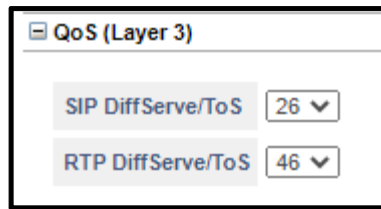
SIP CoS 3

- Enter the **VLAN ID** that you have assigned to the VLAN in which the SETU VTEP is connected. Valid range is 0 to 4094. Default: 3.

For **SIP CoS**, define the CoS (priority) bits which will be added in all SIP packets. Valid range is 0 to 7.

QoS (Layer 3)

Click QoS (Layer 3) to expand.



- SETU VTEP will send all SIP messages using SIP QoS setting, enter the **SIP DiffServe/ ToS** as per your requirement. Valid range is 00 to 63. Default: 26.
- SETU VTEP will send all the RTP packets with RTP QoS setting, enter the **RTP DiffServe/ ToS** as per your requirement. Valid range is 00 to 63. Default: 46.

Dynamic DNS (DynDNS.org)

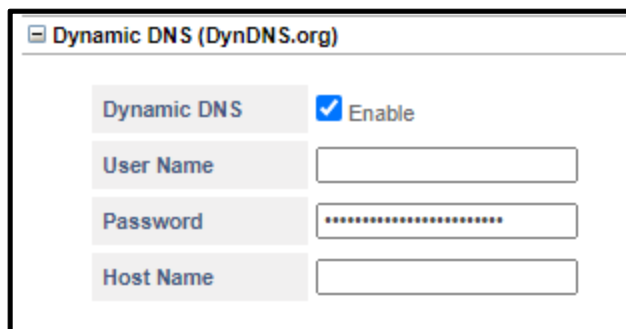
Dynamic DNS (DDNS) is a service that maps internet domain names to IP addresses. DDNS Service Provider provides the host name/domain name to the internet devices and also embeds DDNS client in the internet device. By doing so, whenever a new IP Address is assigned to the internet host, the DDNS client running in the internet host updates its new IP address in the Dynamic DNS server.

When the WAN Port of SETU VTEP is assigned a dynamic IP, its new IP Address needs to be updated regularly with the various devices or networks which utilise the WAN Port settings to function. Dynamic DNS resolves this by mapping a domain name to the WAN Port IP Address, which SETU VTEP can update in the Dynamic DNS Server.

Once the IP Address of the system is updated in the DNS server, any caller on the IP network can reach the system by dialing the host name/domain of the system.

SETU VTEP supports Dynamic DNS Server client of the Service Provider Dynamic DNS.org. To use this service, you must first register with DynDNS.org and then do the following:

- Click **Dynamic DNS (DynDNS.org)** to expand.
- Select the **Dynamic DNS Enable** check box.



- Enter the **User Name** you created on DynDNS.org. The name can be a maximum of 40 characters.

- Enter the **Password** you created for the User Name on DynDNS.org. The password can be a maximum of 24 characters.
- Enter the **Host Name** you created on the DynDNS.org here. The Host Name can be a maximum of 40 characters.

Clone MAC Address for WAN

- Click **Clone MAC Address for WAN** to expand.
- **LAN MAC Address:** This displays the LAN MAC Address.
- **WAN MAC Address:** This displays the WAN MAC Address.
- If you want to clone the MAC address, select the **Clone MAC Address for WAN** check box.



In **MAC Address (Cloned)**, enter the desired MAC address you want to clone in hexadecimal format, e.g. 00:50:c2:55:b0:10.

Restoring Default LAN IP Address

You may restore the Default LAN IP Address by changing the position of Jumper **J13** on the PCB.

To do this,

- Make sure you are wearing an electrostatic discharge preventive wrist strap or belt and have a grounding mat.
- Switch off the power supply
- Remove the top cover of the enclosure.
- Locate and change the position of the Jumper **J13** from **AB** to **BC**.
- Switch ON the system and wait for 15 seconds.
- Switch OFF the system.
- Change the Jumper position from **BC** to the original position **AB**.
- Replace the enclosure cover.
- Switch ON the system.

The LAN IP Address will be restored to default, **192.168.2.100**



When you restore the default LAN IP Address (192.168.2.100) by changing the Jumper position, a few other parameters will also be set to default. See "Restoring Default Settings by changing the Jumper Position" for details.

SIP Trunk

SETU VTEP supports 125 SIP Trunks. You can register all SIP Trunks with the same ITSP or with different ITSPs. These SIP Trunks may be configured as Proxy or Peer-to-Peer (non-proxy).

- Click the **Basic Settings** link to expand.
- Click the **SIP Trunk** link.

Trunk	Enable	Name	Status	SIP ID	SIP Registration	SIP Network Profile	Incoming Call Routing
SIP-1	<input checked="" type="checkbox"/>		Disabled	5656	<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)
SIP-2	<input checked="" type="checkbox"/>		Disabled		<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)
SIP-3	<input checked="" type="checkbox"/>		Disabled		<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)
SIP-4	<input checked="" type="checkbox"/>		Disabled		<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)
SIP-5	<input type="checkbox"/>		Disabled		<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)
SIP-6	<input type="checkbox"/>		Disabled		<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)
SIP-7	<input type="checkbox"/>		Disabled		<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)
SIP-8	<input type="checkbox"/>		Disabled		<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)
SIP-9	<input type="checkbox"/>		Disabled		<input checked="" type="checkbox"/>	Network Profile 1	Route calls to number received in INVITE message using T1E1 Port 1 (Ch 1 - 30)

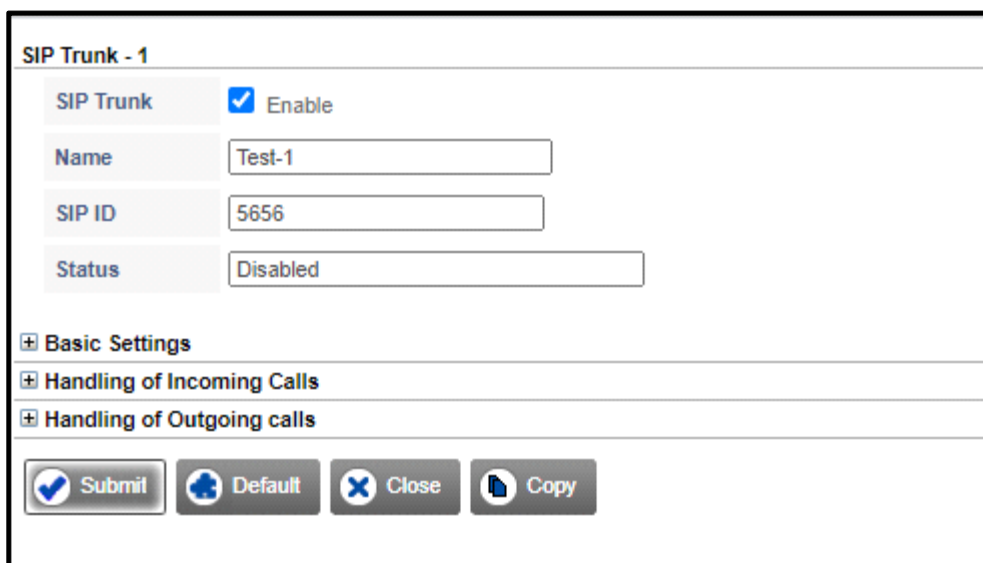
The SIP Trunk page displays the following parameters:

- **Trunk:** It displays the SIP Trunk numbers. Click on the desired SIP Trunk number to configure the SIP Trunk Parameters.
- **Enable:** Click the check box to enable the SIP Trunk.
- **Name:** Assign a Name to the SIP Trunk for identification. The Name can be a maximum of 24 characters.
- **Status:** This displays the status of SIP Trunk.
- **SIP ID:** This displays the SIP ID assigned to the SIP Trunk.
- **SIP Registration:** Keep the **SIP Registration** enabled. Clear this check box only if you do not want to enable SIP Registration for the respective SIP Trunk. Default: Enabled.
- **SIP Network Profile:** It displays the Network Profile you select for the SIP Trunk. To configure the Network Profile, click on **Network Profile**.
- **Incoming Call Routing:** It displays the Incoming Call Routing Method selected for the SIP Trunk.

To configure the **SIP Trunk** parameters,

- Click **SIP-1**.

The **SIP Trunk-1** window opens.



SIP Trunk - 1

SIP Trunk ☒ Enable

Name


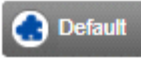


SIP ID

Status

+ **Basic Settings**

+ **Handling of Incoming Calls**

+ **Handling of Outgoing calls**

 **Submit**  **Default**  **Close**  **Copy**

- Select the **SIP Trunk** check box to enable the SIP Trunk. You may disable the SIP Trunk, if you do not want to route calls through this Trunk. Default: Disabled.
- You can assign a **Name** to the SIP Trunk for identification. Default: Blank.

Assign the name of the ITSP with which the trunk is registered, or any other name of your choice. The name will appear on the display of the remote party's phone, when a call is made through this SIP Trunk.

- In **SIP ID**, the SIP ID that you assign under *Basic Settings* is displayed.
- **Status** displays the status of the SIP Trunk.

Basic Settings

Click **Basic Settings** to expand.

Basic Settings	
SIP ID	5656
Authentication ID	89
Authentication Password
SIP Network Profile	Network Profile 1
SIP Registration	<input checked="" type="checkbox"/> Enable
Maximum Calls	128
FAX Protocol	<input checked="" type="radio"/> T.38 <input type="radio"/> Pass Through
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes

- In **SIP ID**, enter the SIP ID provided by your ITSP. For example, if the SIP URI provided by the ITSP is 12345@abc.com, enter 12345 in this field. Default: Blank.

The SIP ID is the number which remote parties will use to call this SIP Trunk.

The SIP ID may be a number or text consisting of a maximum of 40 characters.

- Enter the **Authentication ID** (User ID) provided by your ITSP. Default: Blank.
- Enter the **Authentication Password** provided by your ITSP. Default: Blank.
- In **SIP Network Profile**, you can either select the default **Network Profile 1** or **Add New Network Profile** option.
- Click **Settings** to configure the parameters of the selected Network Profile.

For detailed instructions, see [“SIP Network Profile”](#).

You can also configure the SIP Network Profile from *Advanced Settings*. For instructions, see [“SIP Network Profile”](#) under Advanced Settings.

- Keep the **SIP Registration** check box enabled.

SETU VTEP will send the REGISTER message to Registrar Proxy or Outbound Proxy as applicable.

Clear the check box, only if you want to disable registration. Default: Enabled.

- In **Maximum Calls**, select the number of simultaneous calls you want to allow on this SIP Trunk.

The maximum number of simultaneous SIP calls depend upon the number of Vocoder channels supported.

- Select the desired **Fax Protocol**, to send and receive the Fax over IP:
 - **T.38:** If you select this option, the device you are sending the fax to, must also support this protocol.
 - **Pass Through:** Select this option, if you need to send fax over G.711. The device you are sending fax to must also use G.711.

Default: T.38.

- Select the **Allow Call Disconnection using Access code** check box to enable. Default: Disabled. To know more about the feature, see [“Disconnecting a Call using Access Code”](#).

Handling of Incoming Calls

Click **Handling of Incoming Calls** to expand.

Handling of Incoming Calls	
Block all calls received on this SIP Trunk	<input type="checkbox"/> Yes
Use Called Party Number from	Request-URI ▼
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this SIP Trunk	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ ➔
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply
Display received URI as Calling Name	<input checked="" type="checkbox"/> Apply

- Keep the **Block all calls received on this SIP Trunk** check box disabled.

Select this check box only if you do not want to route calls received on this SIP Trunk.

- By default, SETU VTEP identifies the Called Party Number for routing the incoming call on the SIP Trunk further, by the number received in the **Request-URI** of the INVITE message.

If you want the system to identify the Called Party Number from the 'To Field' of the INVITE message, in the **Use Called Party Number From** parameter, select the **To Field** option.

Destination Number Determination

Select the desired destination number determination method for routing incoming calls *with* and *without* CLI.

- To **Route all Incoming calls (with CLI)**, you may select from any of the following methods:
 - without any Destination Number
 - to a Fixed Destination Number
 - on the basis of Calling Party Number
 - on the basis of DDI Number
 - to the Called Party Number

- after Answering the Call and Collecting the Digits²
Default: to the Called Party Number

Handling of Incoming Calls	
Block all calls received on this SIP Trunk	<input type="checkbox"/> Yes
Use Called Party Number from	Request-URI ▼
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this SIP Trunk	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ ➔
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply
Display received URI as Calling Name	<input checked="" type="checkbox"/> Apply

Read further for instructions on selecting and configuring each of these destination number determination methods.



If the destination number to be dialed out is an IP Address, SETU VTEP will not check the Destination Port Determination Method. Instead, it will route the call using the SIP Trunk / Group programmed for IP Dialing. (See “[IP Dialing](#)” to know more).

Route to a Fixed Destination Number

2. “After Answering the Call and Collecting the Digits” option is supported only for SETU VTEP 1P and SETU VTEP 3P configuration.

In this method, calls received on the SIP Trunk are routed to a fixed destination number, which is configured for the SIP Trunk.

Handling of Incoming Calls

Block all calls received on this SIP Trunk ☐ Yes

Use Called Party Number from Request-URI ▼

Route all Incoming calls (with CLI) to a Fixed Destination Number ▼

Block Calls received without CLI on this SIP Trunk ☐ Yes

Route all Incoming calls (without CLI) to the Called Party Number ▼

Fixed Destination Number

Fixed Destination Number

Select Destination Port for routing calls Fixed ▼ ➡

Allowed-Denied Logic ☐ Apply

Reject Calls from Blacklisted Callers ☐ Apply

Display received URI as Calling Name ☒ Apply

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **to the Fixed Destination Number**.
- In the **Fixed Destination Number** box that appears, enter the desired destination number. The Destination Number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and . (dot/period). Default: Blank.
- Click **Submit** to save your settings.

Route on the basis of Calling Party Number

In this method, a call received on the SIP Trunk is routed to a specific number, as per the calling party's number. You must configure the calling party numbers in the *Calling Party Number Based Table*.

When there is an incoming call on the SIP Trunk, SETU VTEP will match the Calling Party Number with the entries of the Calling Party Number Based Table. If a match is found, the call is routed to the destination number configured for that Calling Party Number.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **on the basis of Calling Party Number**.

- Click **Settings** .

Handling of Incoming Calls


Block all calls received on this SIP Trunk

☐ Yes

Use Called Party Number from

Request-URI ▼

Route all Incoming calls (with CLI)

on the basis of Calling Party Number ▼ 

If no match found in the Calling Party Number Table, route calls

to the Called Party Number ▼


Block Calls received without CLI on this SIP Trunk

☐ Yes

Route all Incoming calls (without CLI)

to the Called Party Number ▼

Select Destination Port for routing calls

Fixed ▼ 

Allowed-Denied Logic

☐ Apply

Reject Calls from Blacklisted Callers

☐ Apply

Display received URI as Calling Name

☒ Apply

- The **SIP Trunk- Destination Number Determination: Calling Number Based** Table window opens.

1-100	101-200	201-300	301-400	401-499
-------	---------	---------	---------	---------

SIP Trunk - Destination Number Determination: Calling Number Based		
Index	Calling Number	Destination Number
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		
013		
014		
015		
016		
017		
018		
019		
020		
021		
022		
023		
024		

☒ Submit
 ☐ Default All

- In **Calling Number**, enter the calling party numbers. The Calling numbers may consist of a maximum of 24 characters. Default: Blank.
- For each calling party number, enter a corresponding destination number in **Destination Number**. Destination numbers may consist of a maximum of 24 characters. Digits 0 to 9, *, # and (.) dot are allowed. Default: Blank.
- Click **Submit** to save your entries. Close the window to return to the main page.

You can also configure the **Calling Number Based** table from *Advanced Settings*. For instructions, see [“Destination Number Determination”](#) under *Advanced Settings*.

- Select a method for routing incoming calls with CLI that *do not match* with any entries in the Calling Party Number Based Table.

In **If no match found in the Calling Party Number Table, route calls**, select the desired method from the following options for processing the call:

- to a Fixed Destination Number
 - to the Called Party Number
 - on the basis of DDI Number
 - after Answering the Call and Collecting the Digits
- Default: to the Called Party Number.

Route on the basis of DDI Number

In this method, incoming calls on the SIP Trunk are routed to specific numbers as per the DDI number received in the SETUP message on the SIP Trunk.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **on the basis of DDI Number**.

The screenshot shows the 'Handling of Incoming Calls' configuration window. It contains several settings:

- Block all calls received on this SIP Trunk**: ☐ Yes
- Use Called Party Number from**: Request-URI ▼
- Route all Incoming calls (with CLI)**: on the basis of DDI Number ▼ (This row is highlighted with a red box)
- Block Calls received without CLI on this SIP Trunk**: ☐ Yes
- Route all Incoming calls (without CLI)**: to the Called Party Number ▼
- Select Destination Port for routing calls**: Fixed ▼
- Allowed-Denied Logic**: ☐ Apply
- Reject Calls from Blacklisted Callers**: ☐ Apply
- Display received URI as Calling Name**: ☒ Apply

- Click **Settings** ➡.

The **SIP Trunk - Destination Number Determination: DDI Number Based** Table opens.

DDI Number Generation

SIP Trunk - Destination Number Determination: DDI Number Based

Index	DDI Number	Destination Number	Reverse DDI	
			Apply	Reference ID
001			<input type="checkbox"/>	1 ▼
002			<input type="checkbox"/>	1 ▼
003			<input type="checkbox"/>	1 ▼
004			<input type="checkbox"/>	1 ▼
005			<input type="checkbox"/>	1 ▼
006			<input type="checkbox"/>	1 ▼
007			<input type="checkbox"/>	1 ▼
008			<input type="checkbox"/>	1 ▼
009			<input type="checkbox"/>	1 ▼
010			<input type="checkbox"/>	1 ▼
011			<input type="checkbox"/>	1 ▼
012			<input type="checkbox"/>	1 ▼
013			<input type="checkbox"/>	1 ▼

- In **DDI Number**, enter the DDI Numbers allotted by your service provider.
- For each DDI Number, enter the corresponding destination number in **Destination Number**.
- To apply **Reverse DDI** for each number, select the check boxes under **Apply** and select the **Reference ID** for the number. Default: Apply Reverse DDI is disabled and Reference ID is 1.
- Click **Submit** to save and close the window to return to the main page.

You can also configure the **DDI Number Based** Table from *Advanced Settings*. For instructions, see [“Destination Number Determination”](#) under *Advanced Settings*.

Route to the Called Party Number

In this method, a call received on the SIP Trunk is routed to a specific number depending upon the called party number received in the SETUP Message on the SIP Trunk.

- To apply this method, in **Route all incoming calls (with CLI)**, select **to the Called Party Number**.

The screenshot shows the 'Handling of Incoming Calls' configuration window. It contains several settings for SIP Trunk call handling. The 'Route all Incoming calls (with CLI)' option is selected and highlighted with a red box, with 'to the Called Party Number' chosen from the dropdown menu. Other settings include 'Block all calls received on this SIP Trunk' (Yes), 'Use Called Party Number from' (Request-URI), 'Block Calls received without CLI on this SIP Trunk' (Yes), 'Route all Incoming calls (without CLI)' (to the Called Party Number), 'Select Destination Port for routing calls' (Fixed), 'Allowed-Denied Logic' (Apply), 'Reject Calls from Blacklisted Callers' (Apply), and 'Display received URI as Calling Name' (checked Apply).

Handling of Incoming Calls	
Block all calls received on this SIP Trunk	<input type="checkbox"/> Yes
Use Called Party Number from	Request-URI ▼
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this SIP Trunk	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ ➔
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply
Display received URI as Calling Name	<input checked="" type="checkbox"/> Apply

Route after Answering the Call and Collecting the Digits³

In this method, the incoming call is answered and dial tone is played to the caller, allowing the caller to dial the desired number. The number dialed by the caller is considered as the destination number.

Handling of Incoming Calls

Block all calls received on this SIP Trunk ☐ Yes

Use Called Party Number from Request-URI ▼

Route all Incoming calls (with CLI) after Answering the Call and Collecting the Digits ▼

Block Calls received without CLI on this SIP Trunk ☐ Yes

Route all Incoming calls (without CLI) to the Called Party Number ▼

Answering the call and collecting the digits

Prompt caller to enter PIN ☐ Enable

Dial Plan 1 ▼ ➡

First Digit Wait Timer 7 Seconds

Inter Digit Wait Timer 5 Seconds

End Of Dialing Digit # ▼

Minimum Number of digits that must be dialed by the caller 02 ▼

Maximum Number of digits that can be dialed by the caller 24 ▼

If No Digit dialed during First Digit Wait Timer Disconnect Call ▼

Allow making New Call using Access code ☐ Yes

Select Destination Port for routing calls Fixed ▼ ➡

Allowed-Denied Logic ☐ Apply

Reject Calls from Blacklisted Callers ☐ Apply

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **after Answering the Call and Collecting the Digits**.

The related parameters of this method appear under **Answering the call and collecting the digits**.


- If you want to enable PIN Authentication on the SIP Trunk, select the **Prompt caller to enter PIN** check box.

If you enable this check box, you must also configure the PIN Authentication Table. To know more about this feature and for detailed instructions, see “PIN Authentication” under *Advanced Settings*.

- SETU VTEP supports 8 Dial Plans with total 64 entries in each table. When a user dials a number, it is compared with the Destination Number configured in the Dial Plan. If a match is found, the system routes the call immediately without waiting for End of Dialing and if a match is not found, the system will wait for the End of Dialing and then route the call as per the Destination Port Selection method configured.

3. Route after Answering the call and Collecting Digits is applicable for STU VTEP 1P and SETU VTEP 3P configurations only.

Select the **Dial Plan** table number you configured for this port. If you have not configured the Dial Plan table you may do so now,

- Click **Settings**  the Dial Plan Table opens.
- Configure the numbers in the table. For detailed instructions, see “Dial Plan”.
- Set the duration of the **First Digit Wait Timer**. This is the duration for which you want the system to wait for the caller to dial the destination number after the dial tone. Valid range is 01 to 99 seconds. Default: 7 seconds
- You may configure the following options as End of Dialing indication:
 - Set the duration of the **Inter Digit Wait Timer**. This is the duration for which you want the system to wait while receiving the digits dialed by the caller to consider it as End of Dialing. You may change this timer, if required. Valid range is 01 to 99 seconds. Default: 05 seconds.
 - In **End of Dialing Digit**, select # or * as termination digit the system should consider to detect end of dialing. Default: #
 - In **Minimum number of digits that can be dialed by the caller**, select the minimum number of digits to be dialed by the user for the system to consider it as a valid number. Valid range is 01 to 24 digits. Default: 2 digits.
 - In **Maximum Number of digits that can be dialed by the caller**, select the maximum number of digits to be dialed by the user for the system to consider it as End of Dialing. Valid range is 01 to 24 digits. Default: 24 digits.

When the caller dials a number, the system will match it with the above End of Dialing indications and accept the one that matches first.

- If the caller fails to dial the number during the First Digit Wait Timer, you can either have the system disconnect the call or route the call to a fixed destination number.

In **If No Digit dialed during First Digit Wait Timer**, select the desired option: **Disconnect the Call** or **Use Fixed Destination Number**. Default: Disconnect Call.

- If you selected **Use Fixed Destination Number**, enter the desired destination number in the **Fixed Destination Number** field. The Destination number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and . (dot/period). Default: Blank.



- *The First Digit Wait Timer is loaded as soon as the system answers the call.*
- *When you dial the first digit, the First Digit Wait Timer is stopped and the system loads the Inter Digit Wait Timer.*
- *SETU VTEP reloads the Inter Digit Wait Timer:*
 - *each time you dial a new digit till the termination digit is detected.*
 - *each time you dial a new digit till the entry is not matched in Dial Plan.*
 - *when you have dialed the maximum number of digits configured as End of Dialing.*

- If you want to enable the feature Making New Call using Access Code on the SIP Trunk, select the **Allow making New Call using Access Code** check box. For further details, see “Making a New Call using Access Code”.
- Click **Submit** to save settings.
- If you do not want to route the incoming calls received without CLI, through this SIP Trunk, select **Block Calls received without CLI on this SIP Trunk** check box.
- To **Route all Incoming calls (without CLI)**, you may select from any of the following methods:
 - to a Fixed Destination Number, see [“Route to a Fixed Destination Number”](#).
 - on the basis of DDI Number, see [“Route on the basis of DDI Number”](#).
 - to the Called Party Number, see [“Route to the Called Party Number”](#).
 - after Answering the Call and Collecting the Digits, see [“Route after Answering the Call and Collecting the Digits”](#).

Default: to the Called Party Number.

Handling of Incoming Calls	
Block all calls received on this SIP Trunk	<input type="checkbox"/> Yes
Use Called Party Number from	Request-URI ▼
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this SIP Trunk	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ ➕
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply
Display received URI as Calling Name	<input checked="" type="checkbox"/> Apply

Destination Port Determination

For the SIP Trunk, select the Destination Port for routing calls from the following options:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number

Default: Fixed.

Read the description and follow the instructions for each of these destination port selection methods given below.



If the destination number to be dialed out is an IP Address, SETU VTEP will not check the Destination Port Determination Method. Instead, it will route the call using the SIP Trunk / Group programmed for IP Dialing. (To know more, see the feature description “IP Dialing”).

Fixed

In this method, calls received on the SIP Trunk are routed to a Fixed Destination Port, irrespective of the number dialed on the SIP Trunk.

To apply this method, do the following:

- In **Select Destination Port for routing calls**, select **Fixed** option.

Handling of Incoming Calls

Block all calls received on this SIP Trunk	<input type="checkbox"/> Yes
Use Called Party Number from	Request-URI ▼
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this SIP Trunk	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ ➡
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply
Display received URI as Calling Name	<input checked="" type="checkbox"/> Apply

- Click **Settings** ➡.

The **Destination Port/Group for SIP Trunk** window opens.

Destination Port/Group for SIP Trunk

Edit	Routing Group	Fallback Routing Group
➡	T1E1 Port 1 (Ch 1 - 30) (Ascending)	None

✕ Close

The default **Routing Group** and **Fallback Routing Groups** appear.

- If you wish to change the default Routing Group options, click **Edit** ➡.

The **Edit Selective Port/Group for SIP Trunk** window opens.

Edit Selective Port/Group for SIP Trunk

Routing Group

☒ T1E1 Port 1 and Channel Number from 01 to 30 in Ascending order

☐ T1E1 Group 1

Fallback Routing Group ☐ Apply


☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1



SIP Trunk Group is also supported for SETU VTEP 1P and SETU VTEP 3P configurations.

- Create the **Routing Group**.
 - To create a group of *sequential T1E1 Port* as members,
 - Select the desired **T1E1 Port** numbers as members. Default: 1.
 - In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
 - In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.
 - To create a group of *not-sequential T1E1 Ports* as members,
 - Select a **T1E1 Group**.
 - Select **T1E1 Group** number. Default: 1.
 - Click **Settings** .

- The **T1E1 Port - Group** window opens.

T1E1 Port - Group

T1E1 Group: 1 ▼

Member Selection Method: First Free ▼

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1 ▼	01 ▼	30 ▼	Ascending ▼
2	2 ▼	01 ▼	30 ▼	Ascending ▼
3	None ▼	01 ▼	30 ▼	Ascending ▼
4	None ▼	01 ▼	30 ▼	Ascending ▼

Submit Default Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic “Group” under *Advanced Settings*.
- You may create the **Fallback Routing Group**.

Fallback Routing Group ☒ Apply

☒ T1E1 Port 1 ▼ and Channel Number from 01 ▼ to 01 ▼ in Ascending ▼ order

☐ T1E1 Group 1 ▼

Submit Close

- To do this,
 - Select the **Apply** check box.
 - Follow the same instructions provided earlier for creating *sequential* and *not-sequential* group of T1E1 Ports.
- Click **Submit** to save changes. The **Edit** window closes.
- The entry you edited appears in the **Destination Port/Group for SIP Trunk** window.
- Close the **Destination Port/Group for SIP Trunk** window to return to the main page.

On the basis of Destination Number

In this method, incoming calls on the source port are routed to the destination port on the basis of the destination number (called party number) dialed by the caller.

You must configure the called party numbers in the **Destination Number Based** Table. SETU VTEP will match the called party number dialed by the caller with the entries of this table. If a match is found for the number in the table, the call is routed to the destination.

To apply this method, do the following:

- In **Select Destination Port for routing calls**, select **On the basis of Destination Number** option.

Handling of Incoming Calls

Block all calls received on this SIP Trunk	<input type="checkbox"/> Yes
Use Called Party Number from	Request-URI ▼
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this SIP Trunk	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	On the basis of Destination Number ▼ (+)
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply
Display received URI as Calling Name	<input checked="" type="checkbox"/> Apply

- Click **Settings** (+).

The **SIP Trunk - Destination Port Determination - Destination Number Based** table window opens.

SIP Trunk - Destination Port Determination - Destination Number Based

<input type="checkbox"/>	Edit	Destination Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>	(+)	No Match Found	T1E1 Group 1	None

Total Records : 1 1

Testing

Enter the destination number to know which entry would be selected for routing

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 250 entries.

Add Entry

Destination Number

Routing Group

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

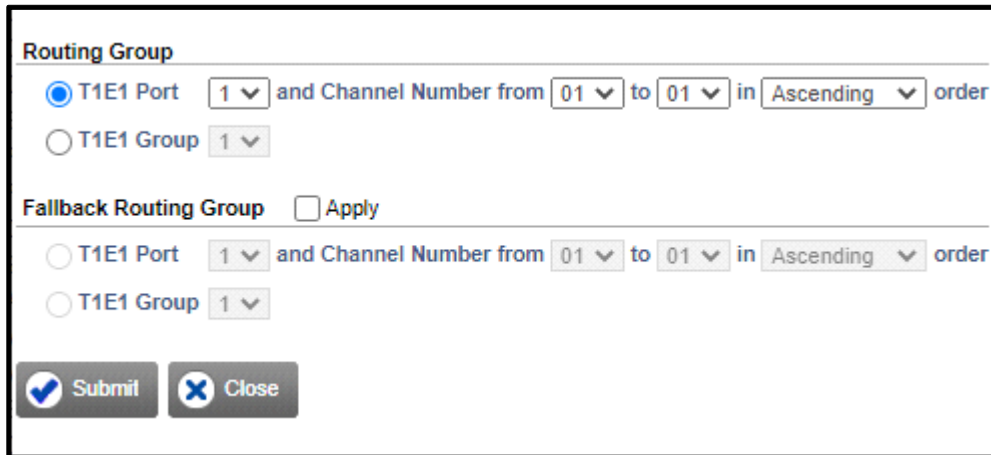
- In **Destination Number**, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters"). Valid characters are 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

Wildcard Characters

SETU VTEP supports following characters.

Character	Description
X (letter X)	X represents any single digit from 0 to 9.
#	When # is configured in a number string, it will not be considered as End of Dialing.
*	When * is configured in a number string, it will not be considered as End of Dialing.
+	+ (plus) can be configured as a first character of the Destination Number string in the <i>SIP Trunk-Destination Port Determination-Destination Number Based</i> table only.
[-]	Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket.
[,]	Comma within a bracket is used as a separator between the groups of numbers.
[^]	Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret.
T (letter T)	Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing.

- Create the **Routing Group**.
- To create a group of *sequential T1E1 Ports* as members,



Routing Group


☒ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

Fallback Routing Group ☐ Apply

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

- Select the desired **T1E1 Port** numbers as members. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In the **in - order** field, select the order in which the system should check for a free member channel to route the call.
- Select **Ascending** to start checking from the first to the last member channel. Select **Descending** to start checking from the last to the first member channel. Default: Ascending.
- To create a group of *not-sequential T1E1 Ports* as members,
 - Select a **T1E1 Group**.
 - Select **T1E1 Group** number. Default: 1.
 - Click **Settings** .

- The **T1E1 Port - Group** window opens.

T1E1 Port - Group

T1E1 Group: 1 ▼

Member Selection Method: First Free ▼

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1 ▼	01 ▼	30 ▼	Ascending ▼
2	2 ▼	01 ▼	30 ▼	Ascending ▼
3	None ▼	01 ▼	30 ▼	Ascending ▼
4	None ▼	01 ▼	30 ▼	Ascending ▼

Submit Default Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic “Group” under *Advanced Settings*.
- You may create the **Fallback Routing Group**.

Fallback Routing Group ☒ Apply

☒ T1E1 Port 1 ▼ and Channel Number from 01 ▼ to 01 ▼ in Ascending ▼ order

☐ T1E1 Group 1 ▼

Submit Close


- To do this,
 - Select the **Apply** check box.
 - Follow the same instructions provided earlier for creating *sequential* and *not-sequential* group of T1E1 Ports.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **SIP Trunk - Destination Port Determination - Destination Number Based** table.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.

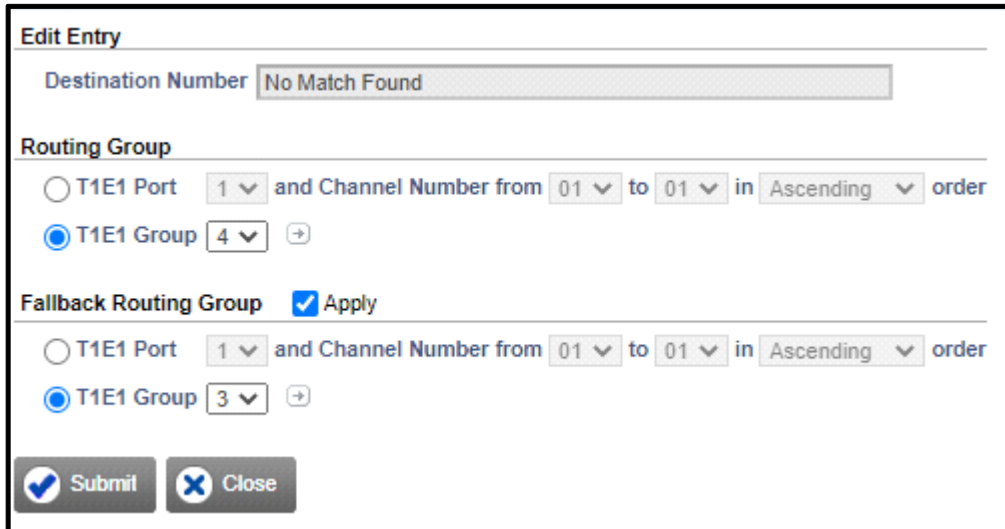


If there are multiple entries in the *Destination Number Based* table, to search a particular entry in the table, under *Testing* enter the desired number to know which entry would be selected for routing search box.

- By default, T1E1 Port 1 - 1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** .




Edit Entry

Destination Number


Routing Group

☐ T1E1 Port and Channel Number from to in order

☒ T1E1 Group 

Fallback Routing Group ☒ Apply

☐ T1E1 Port and Channel Number from to in order

☒ T1E1 Group 

☒ Submit ☒ Close

- The **Edit Entry** window opens.
- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.

You can also configure the **Destination Number Based** Table from *Advanced Settings*. For instructions, see ["Destination Port Determination"](#) under *Advanced Settings*.

On the basis of Calling Party Number

In this method, incoming calls on the SIP Trunk are routed to a specific port as per the calling party's number.

To apply this method, do the following:

- In **Select Destination Port for routing calls**, select **On the basis of Calling Party Number** option.

Handling of Incoming Calls

Block all calls received on this SIP Trunk	<input type="checkbox"/> Yes
Use Called Party Number from	Request-URI ▼
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this SIP Trunk	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	On the basis of Calling Party Number ▼ ➔
Allowed-Denied Logic	<input type="checkbox"/> Apply
Reject Calls from Blacklisted Callers	<input type="checkbox"/> Apply
Display received URI as Calling Name	<input checked="" type="checkbox"/> Apply

- Click **Settings** ➔.

The **SIP Trunk - Destination Port Determination - Calling Number Based** table window opens.

SIP Trunk - Destination Port Determination - Calling Number Based				
<input type="checkbox"/>	Edit	Calling Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>	➔	No Match Found	T1E1 Group 1	None
Total Records : 1		1		
<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Close		

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 499 entries.

Add Entry

Calling Number

Routing Group

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☒ Submit ☐ Close

- In **Calling Number**, enter the number (max. 24 characters) from which you expect calls to be received. Valid digits are 0 to 9, *, #, (dot). Default: Blank.
- Create the **Routing Group**.
 - To create a group of *sequential T1E1 Ports* as members,

Routing Group

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

- Select the desired **T1E1 Port** numbers as members. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member T1E1 Port to route the call.

Select **Ascending** to start hunting from the first to the last member T1E1 Port. Select **Descending** to start hunting from the last to the first member T1E1 Port. Default: Ascending.

- To create a group of *not-sequential T1E1 Ports* as members,
 - Select a **T1E1 Group**.
 - Select **T1E1 Group** number. Default: 1.
 - Click **Settings**

- The **T1E1 Port - Groups** window opens.

T1E1 Port - Group

T1E1 Group: 1 ▼

Member Selection Method: First Free ▼

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1 ▼	01 ▼	14 ▼	Ascending ▼
2	2 ▼	01 ▼	30 ▼	Ascending ▼
3	None ▼	01 ▼	30 ▼	Ascending ▼
4	None ▼	01 ▼	30 ▼	Ascending ▼

Submit Default Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic [“Group”](#) under *Advanced Settings*.
- Click **Submit** to save changes. The **Add Entry** window closes.
- To delete an entry, select the check box and click the **Delete** button.
- By default, T1E1 Port 1 - 1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** ➡.

Edit Entry

Destination Number: No Match Found

Routing Group

☐ T1E1 Port 1 ▼ and Channel Number from 01 ▼ to 01 ▼ in Ascending ▼ order

☒ T1E1 Group 4 ▼ ➡

Fallback Routing Group ☒ Apply

☐ T1E1 Port 1 ▼ and Channel Number from 01 ▼ to 01 ▼ in Ascending ▼ order

☒ T1E1 Group 3 ▼ ➡

Submit Close

- The **Edit Entry** window opens.

- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.

You can also configure the **Calling Number Based** Table from *Advanced Settings*. For instructions, see [“Destination Port Determination”](#) under *Advanced Settings*.

Allowed - Denied Logic

You can apply the Allowed-Denied logic on the SIP Trunk (source port) if you want to allow or restrict the dialing of particular numbers. You can use this feature for Toll Control.

The Allowed-Denied Number Logic makes use of two Number lists:

- **Allowed Numbers List:** This is the list of numbers that can be dialed out from the SIP Trunk.
- **Denied Numbers List:** This list contains the numbers that are to be restricted from being dialed out from the SIP Trunk.

When Allowed-Denied Logic is enabled on a source port, for each number dialed from the port, SETU VTEP uses the best-match-found logic to compare the dialed number with the Allowed Number list and the Denied Number list.

The number is allowed to be dialed, if it:

- matches with both lists.
- matches with Allowed Number list, but not with the Denied Number list.
- matches with neither the Allowed List nor the Denied List.

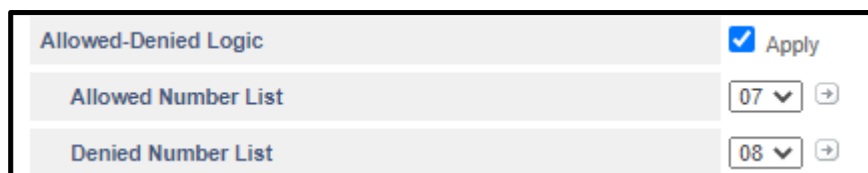
The number is denied, if it matches with the Denied Number list, but not with the Allowed Number list.

The system does not apply the Allowed-Denied Logic:

- When dialed number string matches with any Access Code.
- When dialed number string matches with any Emergency Number.
- When any one of the following is selected to Route all Incoming Calls (with CLI):
 - on the basis of Calling Party Number
 - to a Fixed Destination Number
 - on the basis of DDI Number

To apply Allowed - Denied Logic on the SIP Trunk,


- Select the **Allowed - Denied Logic** check box.

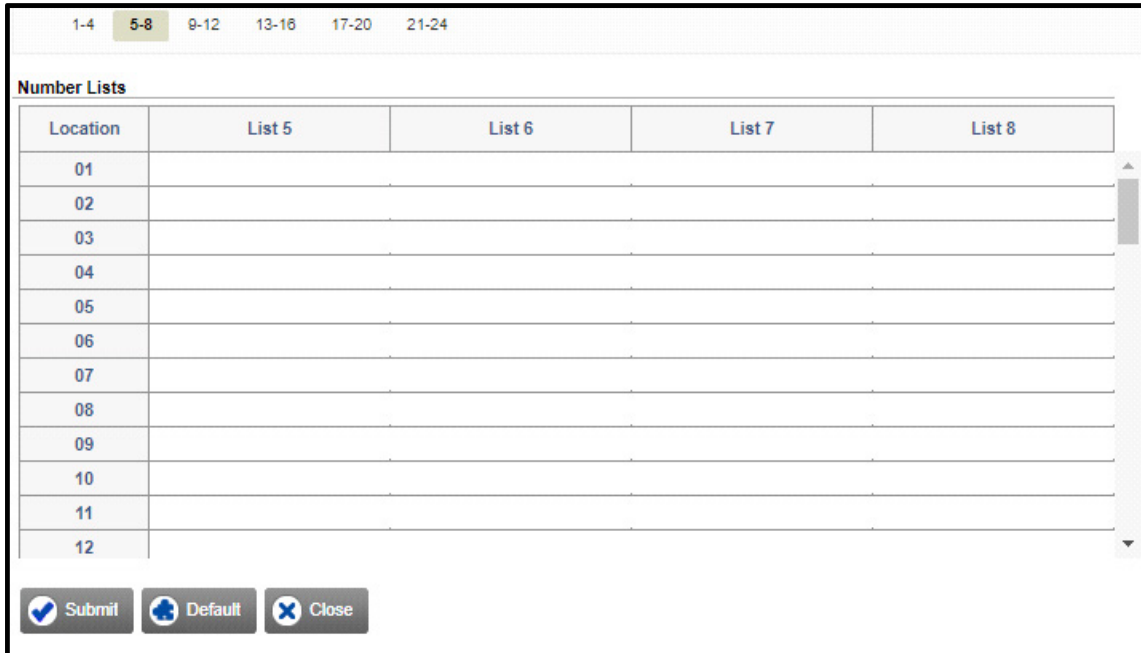


Allowed-Denied Logic	<input checked="" type="checkbox"/> Apply
Allowed Number List	07 ▼ ➕
Denied Number List	08 ▼ ➕

- In the **Allowed Number List**, select the list number you have configured with numbers you want to allow to be dialed out from the SIP Trunk. Default: 07

If you have not configured the Allowed Number List,

- Click **Settings** . The Number Lists window opens.




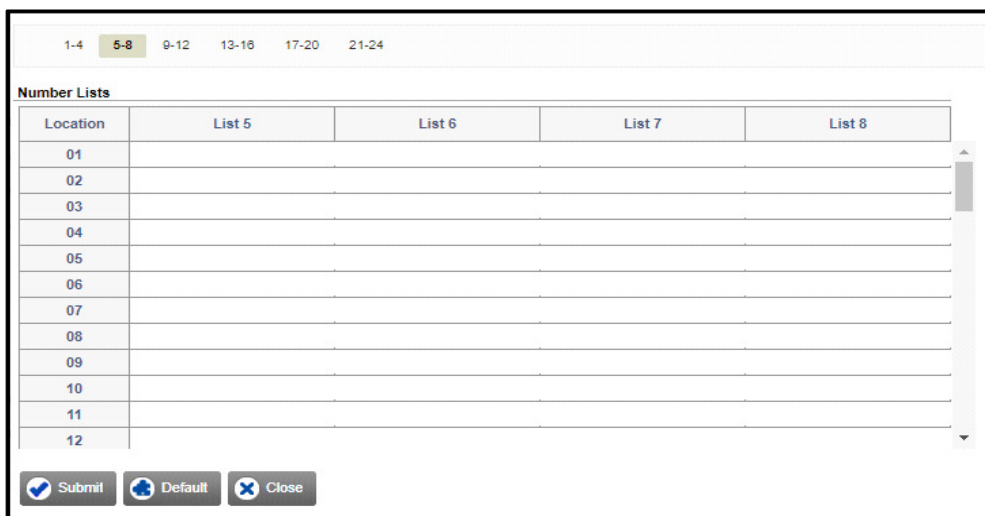
Location	List 5	List 6	List 7	List 8
01				
02				
03				
04				
05				
06				
07				
08				
09				
10				
11				
12				

Submit Default Close

- You may configure the default Allowed Number List or any other list. See [“Number Lists”](#) to configure the allowed numbers.
- Click **Submit** to save the Allowed Number List and close the window.
- In the **Denied Number List**, select the list number you have configured with numbers you want to restrict to be dialed out from the SIP Trunk. Default: 08

If you have not configured the Denied Number List,

- Click **Settings** . The Number Lists window opens.



Location	List 5	List 6	List 7	List 8
01				
02				
03				
04				
05				
06				
07				
08				
09				
10				
11				
12				

Submit Default Close

- You may configure the default Denied Number List or any other list. See [“Number Lists”](#) to configure the restricted numbers.
- Click **Submit** to save the Denied Number List and close the window.


Black Listed Callers


With the Black Listed Callers feature you can block incoming calls from specific addresses/numbers on SIP Trunks. Thus all incoming calls from the numbers you have 'blacklisted' will be automatically rejected by SETU VTEP.

To apply Black Listed Callers on SIP Trunk,

- Select the **Reject Calls from Blacklisted Callers** check box.



- Configure the **Black Listed Callers** table.
- To do this,
 - Click **Settings** .
 - The Number List window opens.



Location	List 9	List 10	List 11	List 12
01				
02				
03				
04				
05				
06				
07				
08				
09				
10				
11				
12				

- By default, Number List 11 is assigned as Black Listed Callers List.
- Enter the numbers of unwanted callers in this list.
- Click **Submit** to save the entries and close the window to return to the main page.

Display Received URI as Calling Name

- Keep the **Display Received URI as Calling Name** check box enabled.

Display received URI as Calling Name	<input checked="" type="checkbox"/> Apply
--------------------------------------	---

When Name is received in the "FROM" header for incoming call on the SIP Trunk, SETU VTEP will display name and received URI as calling name. When Name is not received, SETU VTEP will display only the received URI as calling name.

You may disable this check box, if you do not want the system to display the received URI as calling name on the SIP Trunk.

- Click **Submit**.

Handling of Outgoing Calls

When a SIP Trunk is determined as the destination port, numbers dialed from this port constitute outgoing calls.

Handling of Outgoing calls

Block calls through this SIP Trunk	<input type="checkbox"/> Yes
Route calls through this SIP Trunk without Registration	<input type="checkbox"/> Yes
CLIR	<input type="checkbox"/> Enable
SIP ID in "FROM" header of INVITE message	SIP ID configured ▼
Send Called Party Number in	To, Request URI ▼
Identity header in INVITE message	None ▼
Reverse DDI Reference ID	1 ▼
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Apply
Automatic Number Translation(ANT) for Calling Number	<input type="checkbox"/> Apply
Route calls returned unconnected to Original Caller	<input type="checkbox"/> Yes
Connect Source Port when 183(Session Progress) is received on SIP	<input type="checkbox"/> Yes

Submit Default Close Copy

- Click **Handling of Outgoing calls** to expand.
- If you do not want to route outgoing calls through this SIP Trunk, select the **Block calls through this SIP Trunk** check box.
- To allow the users to make outgoing calls irrespective of whether the SIP Trunk has been successfully registered with the proxy or not, select the **Route Calls through this SIP Trunk without Registration** check box.

By default, the system does not allow outgoing calls to be made if the status of the SIP Trunk is 'not registered'.

- By default, the CLI of the SIP Trunk is sent to the called party when outgoing calls are made using the SIP Trunk. If you do not want to send CLI, enable the **CLIR** check box. Default: Disabled.
- SETU VTEP supports flexible options for sending **SIP ID in "FROM" header of INVITE message** during an outgoing call. You may select the desired option — SIP ID configured, Caller ID received on Source Port, Caller ID after applying Reverse DDI logic, Fixed Number. Default: SIP ID configured.
 - If you select *Caller ID after applying Reverse DDI logic*, SETU VTEP allows you to configure the desired option for **If no match found using Reverse DDI logic** — SIP ID configured, Caller ID received on Source Port, Fixed Number. Default: SIP ID configured.
 - If you select *Fixed Number* option for **SIP ID in "FROM" header of INVITE message** or **If no match found using Reverse DDI logic**, you must configure the **Fixed Number**. The Fixed Number can be a maximum of 24 characters. Characters 0-9, +, * # and dot(.) are allowed. Default: Blank.

- SETU VTEP provides you the option to **Send Called Party Number** in “To” or “Request URI” field. You may select — “To, Request URI”, “To”, “Request URI”. Default: To, Request URI.
- If you select *To*, then the called party number will be sent in “To” field, whereas SIP ID configured on the trunk will be sent in the “Request URI” field.
- If you select *Request URI*, then the called party number will be sent in the “Request URI” field, while SIP ID configured on the trunk will be sent in the “To” field.
- If you select *To, Request URI*, then the called party number will be sent in both the fields.

If the SIP ID is not configured and you select the option — To or Request URI, then the called party number will be sent in both the fields.

If the called party number is not available in any of the above cases then the remote server address will be sent in the selected field.

- SETU VTEP also offers flexible options for sending **Identity header in INVITE message** during an outgoing call. You may select the desired option — None, P-Preferred Identity, P-Asserted Identity— according to the Identity header supported by your service provider. Default: None.
- SETU VTEP supports flexible options for sending **SIP ID in Identity header of INVITE message** during an outgoing call. You may select the desired option — Send SIP ID configured, Send Caller ID received on Source Port, Send Caller ID after applying Reverse DDI logic, Send Fixed Number. Default: Send SIP ID configured.



SIP ID in Identity header of INVITE message can be configured only when you have selected either P-Preferred Identity or P-Asserted Identity as Identity header in INVITE message.

- If you select *Send Caller ID after applying Reverse DDI logic*, SETU VTEP allows you to configure the desired option for **If no match found using Reverse DDI logic** — Send SIP ID configured, Send Caller ID received on Source Port, Send Fixed Number. Default: SIP ID configured.
- If you select *Send Fixed Number* as an option for **SIP ID in Identity header of INVITE message** or **If no match found using Reverse DDI logic**, you must configure the **Fixed Number**. The Fixed Number can be a maximum of 24 digits. Characters 0-9, +, *, # and dot(.) are allowed. Default: Blank.



If you have enabled CLIR and SIP ID in Identity header in INVITE message is configured, then SETU VTEP will add Privacy = ID header in the INVITE message during an outgoing call from the SIP Trunk.

- Select **Reverse DDI Reference ID**, if you have selected either/ both of the following:
 - *Caller ID after applying Reverse DDI logic* option as the **SIP ID in "FROM" header of INVITE message**.
 - *Send Caller ID after applying Reverse DDI logic* option as the **SIP ID in Identity header of INVITE message**.

SETU VTEP will compare the Reference ID configured on the SIP Trunk with the one configured in the SIP Trunk - Destination Number Determination: DDI Number Based Table. If a match is found, SETU VTEP will send the corresponding DDI Number to the Called Party.

- You can apply **Automatic Number Translation logic** on outgoing calls made from the SIP Trunk.
- To apply ANT logic on the Called Numbers, select the **Automatic Number Translation (ANT) for Called Number** check box. Default: Disabled.

Automatic Number Translation(ANT) for Called Number	<input checked="" type="checkbox"/> Enable
Use Automatic Number Translation Table	1 ▼ ➔
Pause Timer	2 ▼ Seconds

- In **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Called Numbers. Default: Table 1.

If you have not configured the Automatic Number Translation Table,

- Click **Settings** ➔.
- The Automatic Number Translation Table window opens.

1
2
3
4
5
6
7
8

Automatic Number Translation Table - 1

Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	
11		0	
12		0	

Examples of Number Pattern

Number	Strip Digit	Add Prefix	Remarks
\$\$\$	0	13152222	System will add the prefix '13152222' to every 3-digit dialed number.
8\$\$\$	1		System will strip off the first digit of all 4-digit dialed numbers that start with 8, and will dial out the remaining 3-digit number.
\$\$\$\$\$\$	0	1315	System will add the prefix '1315' to every 7-digit dialed number.

- You may configure the default Automatic Number Translation Table or any other Table. See [“Automatic Number Translation \(ANT\)”](#) to configure the ANT Table.
- Click **Submit** to save the ANT Table and close the window.
- Return to ANT parameter and assign the ANT Table you configured.

- Click **Submit**.
- Set the duration of the **Pause Timer**, if you have configured ^ (Pause) in the Add Prefix column of the ANT Table. Valid range is 1 to 9 seconds. Default: 2 seconds.
- To apply ANT logic on the Calling Numbers, select the **Automatic Number Translation (ANT) for Calling Number** check box. Default: Disabled.

Automatic Number Translation (ANT) for Calling Number

☒ Enable

Use Automatic Number Translation Table

5 ▼

+

- In **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Calling Numbers. Default: Table 5.

If you have not configured the Automatic Number Translation Table,

- Click **Settings** .
- The Automatic Number Translation Table window opens.

1 2 3 4 5 6 7 8

Automatic Number Translation Table - 5

Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	
11		0	
12		0	

Examples of Number Pattern

Number	Strip Digit	Add Prefix	Remarks
\$\$\$	0	13152222	System will add the prefix '13152222' to every 3-digit dialed number.
8\$\$\$	1		System will strip off the first digit of all 4-digit dialed numbers that start with 8, and will dial out the remaining 3-digit number.
\$\$\$\$\$\$	0	1315	System will add the prefix '1315' to every 7-digit dialed number.

☒ Submit

Default

Close

- You may configure the default Automatic Number Translation Table 5 or any other Table. See [“Automatic Number Translation \(ANT\)”](#) to configure the ANT Table.

- Click **Submit** to save the ANT Table and close the window.
- Return to ANT parameter and assign the ANT Table you configured.
- Click **Submit** to apply List.
- Select the **Route calls returned unconnected to Original Caller** check box, if you want SETU VTEP to route outgoing calls made from this Trunk that return unconnected back to the original caller.

If you enable this feature, when an outgoing call is made using this Trunk, and the Called Party is found busy or does not respond, SETU VTEP stores the number of the calling party, the number of the called party and this trunk (through which the outgoing call was made). A record of each such call is stored for the duration of the Unconnected Calls Record Delete Timer (configurable; default: 999 minutes).

If the called party returns the call before the expiry of this Timer, SETU VTEP checks whether *Apply RCOC only if the caller calls back on the same trunk from which the call was made* is enabled or not, and accordingly places the incoming call to the original calling party. To change the duration of this timer, delete records of such calls and enable/disable the *Apply RCOC only if the caller calls back on the same trunk from which the call was made* check box, see [“System Parameters”](#).

- To connect the Source Port with the Destination Port without waiting for the call on the Destination Port to mature, select the **Connect Source Port when 183 (Session Progress) is received on SIP** check box to enable. Default: Disabled.

In all Destination Number Determination methods except *After Answering the Call and Collecting the Digits*, the Source Port gets connected to the Destination Port only after the call has matured, that is, the called party has answered the call. Until the call matures, the caller hears only Ring Back Tone played by the network.

By connecting the Source Port with the Destination Port immediately after the number is dialed, the caller can know the state of the call; if the called party is busy, not responding, not reachable or is rejecting the call.



*If you enable **Connect Source Port when 183(Session Progress) is received on SIP**, you will not be able to provide the features [“Making a New Call using Access Code”](#) and [“Disconnecting a Call using Access Code”](#) to users.*

- Click **Submit** to save the changes.

Copy SIP Trunk Parameters

- You can also copy the settings of a SIP Trunk to another SIP Trunk using the **Copy** button. To do this,
- Click the **Copy** button. The **Copy SIP Trunk Parameters** window opens.

1-32 33-64 65-96 97-125

Copy SIP Trunk Parameters from SIP Trunk 001 ▼ to

All ☐

SIP Trunk 1	<input type="checkbox"/>	SIP Trunk 2	<input type="checkbox"/>	SIP Trunk 3	<input type="checkbox"/>	SIP Trunk 4	<input type="checkbox"/>
SIP Trunk 5	<input type="checkbox"/>	SIP Trunk 6	<input type="checkbox"/>	SIP Trunk 7	<input type="checkbox"/>	SIP Trunk 8	<input type="checkbox"/>
SIP Trunk 9	<input type="checkbox"/>	SIP Trunk 10	<input type="checkbox"/>	SIP Trunk 11	<input type="checkbox"/>	SIP Trunk 12	<input type="checkbox"/>
SIP Trunk 13	<input type="checkbox"/>	SIP Trunk 14	<input type="checkbox"/>	SIP Trunk 15	<input type="checkbox"/>	SIP Trunk 16	<input type="checkbox"/>
SIP Trunk 17	<input type="checkbox"/>	SIP Trunk 18	<input type="checkbox"/>	SIP Trunk 19	<input type="checkbox"/>	SIP Trunk 20	<input type="checkbox"/>
SIP Trunk 21	<input type="checkbox"/>	SIP Trunk 22	<input type="checkbox"/>	SIP Trunk 23	<input type="checkbox"/>	SIP Trunk 24	<input type="checkbox"/>
SIP Trunk 25	<input type="checkbox"/>	SIP Trunk 26	<input type="checkbox"/>	SIP Trunk 27	<input type="checkbox"/>	SIP Trunk 28	<input type="checkbox"/>
SIP Trunk 29	<input type="checkbox"/>	SIP Trunk 30	<input type="checkbox"/>	SIP Trunk 31	<input type="checkbox"/>	SIP Trunk 32	<input type="checkbox"/>

- In the **Copy SIP Trunk Parameters from SIP Trunk** box, select the number of the trunk you want to copy settings *From*. Select the check box of the respective trunk numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the trunks, select the **All** check box.
- Click the **OK** button.
- Once you have copied the settings, you can again edit the specific parameters of the SIP Trunk you copied the settings to.

E1 Port

SETU VTEP supports the T1/E1 Ports to which you can connect the T1 or E1 line.

- Click the **Basic Settings** link to expand.
- Click the **T1E1 Port** link.

Port	Enable	Name	Status	Line Signaling	Orientation	Call Routing
T1E1-1	<input checked="" type="checkbox"/>		Layer 1 - Down Layer 2 - Down	E1 - PRI ETSI NET5	Terminal	Route calls to number received in SETUP message using SIP Trunk 1 - 1
T1E1-2	<input checked="" type="checkbox"/>		Layer 1 - Down Layer 2 - Down	E1 - PRI ETSI NET5	Terminal	Route calls to number received in SETUP message using SIP Trunk 1 - 1
T1E1-3	<input checked="" type="checkbox"/>		Layer 1 - Down Layer 2 - Down	E1 - PRI ETSI NET5	Terminal	Route calls to number received in SETUP message using SIP Trunk 1 - 1
T1E1-4	<input checked="" type="checkbox"/>		Layer 1 - Down Layer 2 - Down	E1 - PRI ETSI NET5	Terminal	Route calls to number received in SETUP message using SIP Trunk 1 - 1

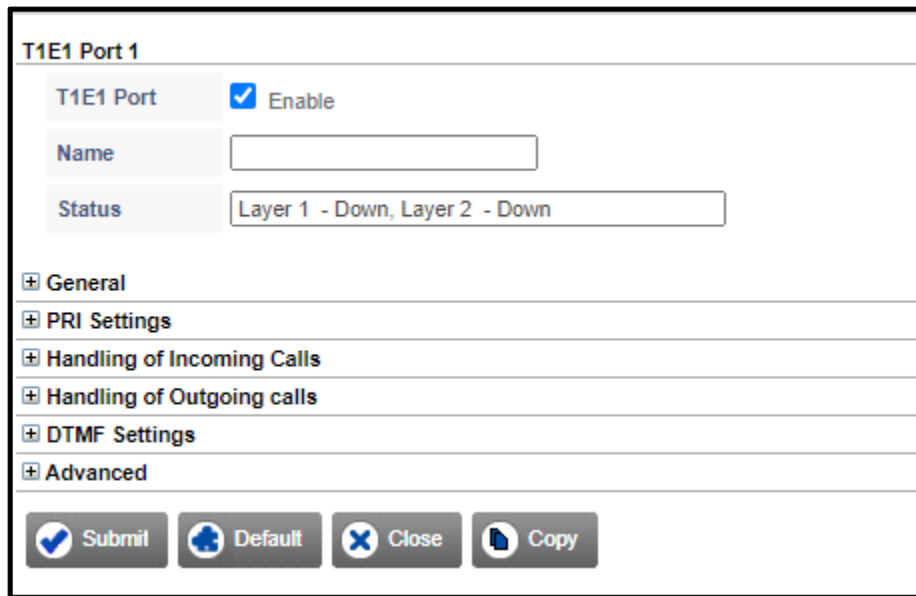
The T1E1 Port page displays the following parameters:

- **Port:** It displays the T1E1 Port numbers. Click on the desired T1E1 Port number to configure the Port Parameters.
- **Enable:** Keep the **T1E1 Ports** enabled. Clear the T1E1 Port **Enable** check box, only if you do not want to use the respective port. Default: Enabled.
- **Name:** Assign a Name to the T1E1 Port for identification. The Name can be a maximum of 24 characters.
- **Status:** This displays the status of Layer 1 and Layer 2, that is, Up or Down.
- **Line Signaling:** It displays the Carrier Type, Signaling Type and the ISDN Switch Variant you select.
- **Orientation:** It displays the type of orientation you select — Network or Terminal.
- **Call Routing:** It displays the Call Routing Method you select.

To configure the **T1E1 Port**,

- Click **T1E1-1**.

The **T1E1 Port 1** window opens.



T1E1 Port 1

T1E1 Port ☒ Enable

Name

Status

+ General





+ PRI Settings

+ Handling of Incoming Calls

+ Handling of Outgoing calls

+ DTMF Settings

+ Advanced

 Submit  Default  Close  Copy

- Keep the **T1E1 Port** check box enabled.

Clear the **T1E1 Port Enable** check box only when you do not want to use this T1E1 Port. Default: Enabled.

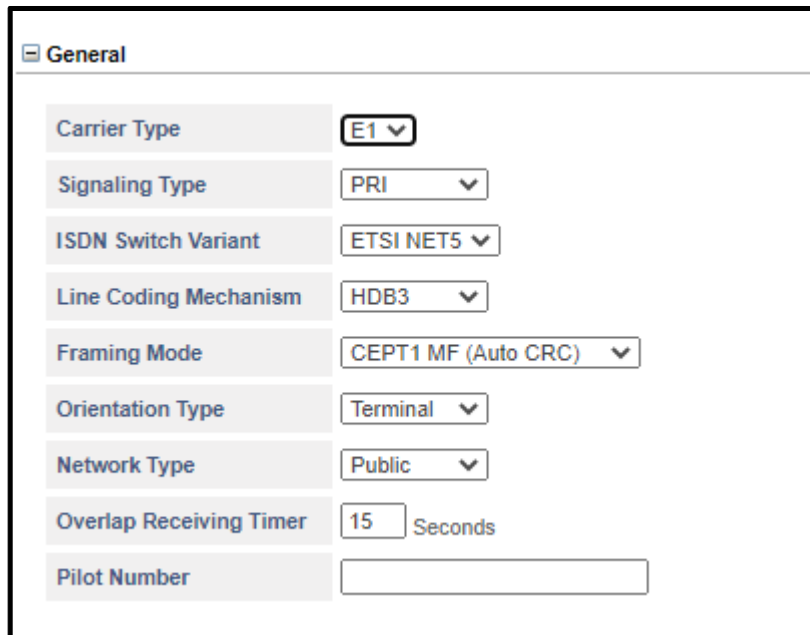
- You can assign a **Name** to the T1E1 Port, which will be displayed to the called party, if the called party telephone instrument supports CLI display.

The name you assign may consist of a maximum of 24 characters. Default: Blank.

- **Status** displays the status of the T1E1 Port.

General

- Click **General** to expand.



The screenshot shows a configuration window titled "General". It contains several settings, each with a label and a corresponding input field or dropdown menu:

- Carrier Type**: A dropdown menu with "E1" selected.
- Signaling Type**: A dropdown menu with "PRI" selected.
- ISDN Switch Variant**: A dropdown menu with "ETSI NET5" selected.
- Line Coding Mechanism**: A dropdown menu with "HDB3" selected.
- Framing Mode**: A dropdown menu with "CEPT1 MF (Auto CRC)" selected.
- Orientation Type**: A dropdown menu with "Terminal" selected.
- Network Type**: A dropdown menu with "Public" selected.
- Overlap Receiving Timer**: A text input field with "15" and a "Seconds" label.
- Pilot Number**: An empty text input field.

- Select **E1** as the **Carrier Type**. Default: E1.
- Select **Signaling Type**. The Signaling Type signifies the type of signaling to be used on the E1 line.
SETU VTEP supports — PRI and CAS signaling for E1 line. Default: PRI.
 - If you select **PRI**, you must configure the PRI parameters. For instructions, see [“PRI Settings”](#)
 - If you select **CAS**, you must configure the CAS parameters. For instructions, see [“CAS Settings”](#).
- ISDN supports a variety of service provider switches. These switches are designed using ISDN standard protocol. The type of switch you select determines various factors — the number of ISDN devices that could be handled, the B-Channel that would support voice, video, data, etc. Each country uses their own specific type of ISDN switch.

The system supports only ETSI NET5 as the **ISDN Switch Variant**. This parameter is applicable only if you select PRI as the Signaling Type.

- Line Coding is a mechanism to code the digital data into electrical pulses for the purpose of transmission over the communication channel.

Select the **Line Coding Mechanism** — AMI Basic or HDB3. Default: AMI Basic.

- Framing** is a formatting resource that splits the digital data into time slots of 8 bits each. Each time slot is treated as single transmission unit. These frames enable the receiver to interpret the data.

Select the **Framing Mode** as per your requirement. You can select — CEPT1 MF (No CRC), CEPT1 MF (Forced CRC) or CEPT1 MF (Auto CRC) Framing Modes. Default: CEPT1 MF (Auto CRC).

- Select the **Orientation Type** for the port as **Terminal** or **Network**, according to your installation scenario. Default: Terminal.

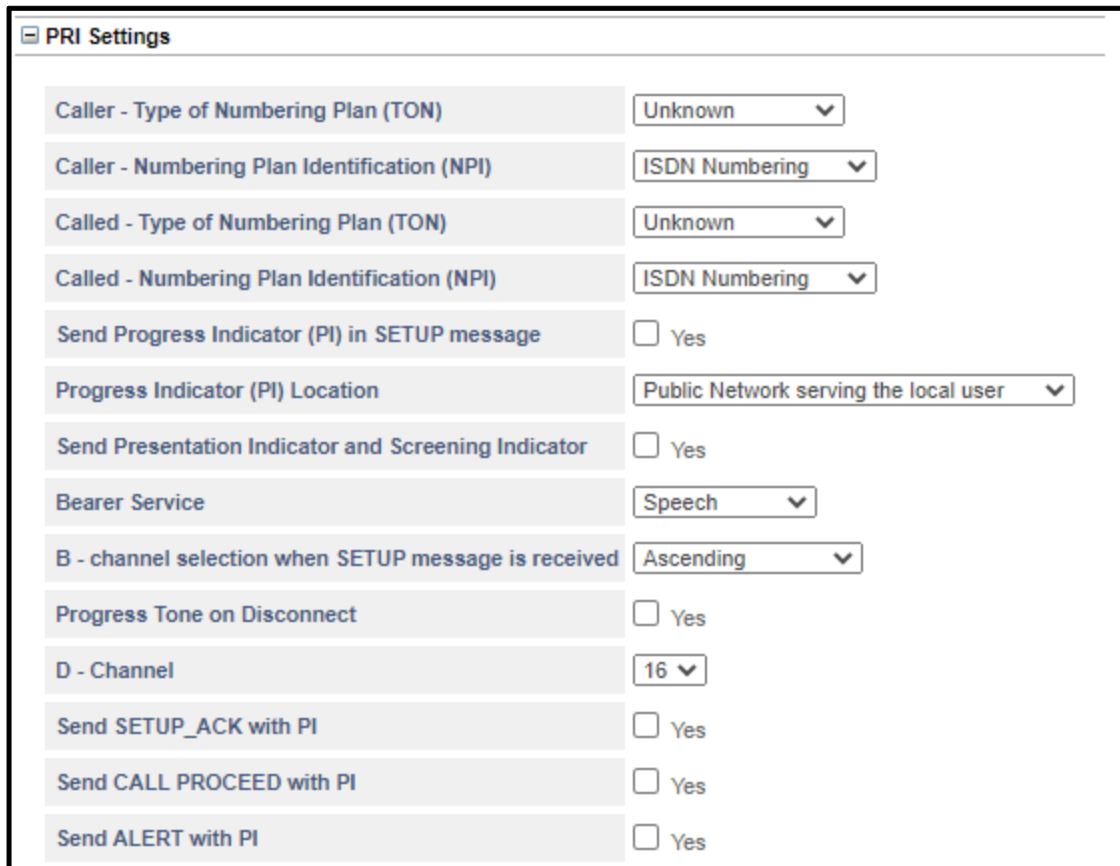
If you have selected *Terminal* as Orientation Type, select the **Network Type** — Public or Private — to specify whether the T1 line is from a **Public** Network (telephone exchange) or from a **Private** Network (to the NT port of a System). Default: Public.

- For **Terminal** as the Orientation Type, configure — [“PRI Settings”](#) and [“Handling of Outgoing Calls”](#).
- Enter the **Pilot Number** provided by your service provider for the E1 line connected to the T1/E1 Port. Pilot Number is necessary for sending the calling party number when the call is routed using T1/E1 Port and Reverse DDI logic is not applied. Valid digits are 0 to 9, #, *. Default: Blank.

PRI Settings

If you have selected **PRI** as **Signaling Type**, configure the PRI parameters.

- Click **PRI Settings**.



The screenshot shows a window titled "PRI Settings" with a list of configuration options. Each option is in a light gray box with a label on the left and a control (dropdown or checkbox) on the right.

Parameter	Value
Caller - Type of Numbering Plan (TON)	Unknown
Caller - Numbering Plan Identification (NPI)	ISDN Numbering
Called - Type of Numbering Plan (TON)	Unknown
Called - Numbering Plan Identification (NPI)	ISDN Numbering
Send Progress Indicator (PI) in SETUP message	<input type="checkbox"/> Yes
Progress Indicator (PI) Location	Public Network serving the local user
Send Presentation Indicator and Screening Indicator	<input type="checkbox"/> Yes
Bearer Service	Speech
B - channel selection when SETUP message is received	Ascending
Progress Tone on Disconnect	<input type="checkbox"/> Yes
D - Channel	16
Send SETUP_ACK with PI	<input type="checkbox"/> Yes
Send CALL PROCEED with PI	<input type="checkbox"/> Yes
Send ALERT with PI	<input type="checkbox"/> Yes

- Select the required option for sending the **Caller-Type of Numbering Plan (TON)** — Unknown, International, National, Network Specific, Subscriber, Abbreviated or Reserved. Default: Unknown.
- Select the required option for sending the **Caller-Numbering Plan Identification (NPI)** — Unknown, ISDN Numbering, Data Numbering, Telex Numbering, National Numbering, Private or Reserved. Default: ISDN Numbering.
- Select the required option for sending the **Called-Type of Numbering Plan (TON)** — Unknown, International, National, Network Specific, Subscriber, Abbreviated or Reserved. Default: Unknown.
- Select the required option for sending the **Called-Numbering Plan Identification (NPI)** — Unknown, ISDN Numbering, Data Numbering, Telex Numbering, National Numbering, Private or Reserved. Default: ISDN Numbering.
- Select the **Send Progress Indicator (PI) in SETUP message** check box if you want the progress indicator value to be sent in SETUP message. Default: Disabled.
- Set the **Progress Indicator (PI) value in SETUP message** to the desired value. You can select — 1 or 3.

Progress indicator 1 indicates that the call is not end-to-end ISDN and further call progress information may be available in-band.

Progress indicator 3 indicates that the origination address is non-ISDN.

This value will be included in the Setup Message to indicate whether the calling party is an ISDN device or not. Default: 1.

- Select the **Progress Indicator (PI) Location** for the SETUP message. The location is a progress indicator information element that indicates from where the message is coming. Default: Public Network serving the local user.
- Select the **Send Presentation Indicator and Screening Indicator** check box, if you want the system to display the presentation and screening information to the remote end. Default: Disabled.
 - Select the required **Presentation Indicator**. This allows remote end to know whether CLI Number should be displayed to user or not. You can select — Presentation Allowed, Presentation Restricted or Received from Source Port. Default: Received from Source Port.
 - Select the required **Screening Indicator**. This indicates whether the information is provided by the user or the network along with the screening details — not screened, verified and passed or verified and failed and Network provided. Default: User-provided, not screened.
- Select the **Bearer Service** supported by your service provider. This will be sent in the SETUP Message. You can select — Speech, 3.1 KHz Audio. Default: Speech
- Select the B - channel selection when SETUP message is received⁴ as per your requirement.
- Select the **Progress Tone on Disconnect** check box, if you want the system to play the progress tone on the port when the call is released by the remote end or disconnected by the system. Default: Disabled.
- Select the **D - Channel** as per your requirement.

You may select — channel 01 to channel 31 — for the signaling.

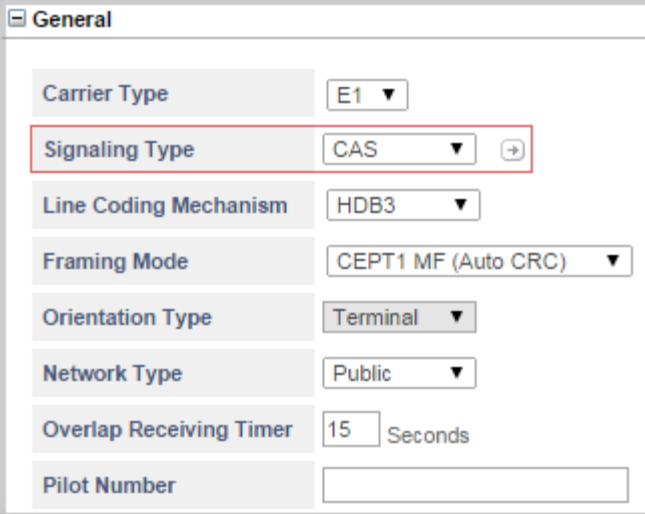
Default: 16.

- Select the **Send SETUP_ACK with PI** check box, if you want the system to send PI (Progress indicator) element in Setup Ack message. Default: Disabled.
- Select the **Send CALL PROCEED with PI** check box, if you want the system to send PI (Progress indicator) in Proceed message. Default: Disabled.
- Select the **Send ALERT with PI** check box, if you want the system to send PI (Progress indicator) in Alert message. Default: Enabled.
- Click **Submit** to save changes.

4. This parameter is not applicable in this version, it is meant for future use.

CAS Settings

If you have selected **CAS** as **Signaling Type**, configure the CAS parameters.



The screenshot shows a 'General' settings window with the following fields:

- Carrier Type**: E1 ▼
- Signaling Type**: CAS ▼ (highlighted with a red box and a settings icon)
- Line Coding Mechanism**: HDB3 ▼
- Framing Mode**: CEPT1 MF (Auto CRC) ▼
- Orientation Type**: Terminal ▼
- Network Type**: Public ▼
- Overlap Receiving Timer**: 15 Seconds
- Pilot Number**: (empty text field)

- Click **Settings** .

- The CAS parameters window opens.

E1-CAS Parameters

E1 Line Signaling Variant

ITU-T Q.400-Q490 ▼

E1 Register Signal Variant

DTMF ▼

Line Signal Parameters

Line Signaling

☒

C and D bit

1 ▼

Invert Bit A Flag

☐

Invert Bit B Flag

☐

Invert Bit C Flag

☐

Invert Bit D Flag

☐

E1 Metering Bit

Bit-A ▼

E1 Metering Pulse Minimum Timer

150

msec

Clear Back Signal

Release Guard ▼

Release Timer

400

msec

Line Seizure Acknowledge Wait Timer

200

msec

Release Guard Timer

200

msec

Submit

Default

Copy

Close

- Configure the following parameters.

E1-CAS Parameters

- Select the appropriate **E1 Line Signaling Variant** — ITU-T Q.400-Q.490, Brazil. Default: ITU-T Q.400-Q.490.

If you select Brazil, all the **CAS Parameters** will be assigned default values as per Brazil.

- Select the appropriate **E1 Register Signal Variant** — DTMF. Default: DTMF.

If you select DTMF, DNIS/ANI is transmitted in the corresponding speech channel using the DTMF signals as per ITU-T Q.23.

Line Signal Parameters

- By default **Line Signaling** check box is enabled. If you are unable to make outgoing calls, check with your Service Provider and disable this option.
- **C and D Bits** indicates the default values of C and D bits when the T1/E1 Port transmits line signals.

CD Bits	Meaning (Binary Value)
0	00 (C=0, D=0)
1	01
2	10
3	11

Default: 01 i.e. C=0 and D=1



The C and D bits received during an IC call should be ignored by the system.

- **Invert Bit A Flag** specifies whether A-bit is to be inverted before transmitting and on receiving. Select the check box to Invert Bit A. Default: Disabled (Do Not Invert Bit A).
- **Invert Bit B Flag** specifies whether B-bit is to be inverted before transmitting and on receiving. Select the check box to Invert Bit B. Default: Disabled (Do Not Invert Bit B1)
- **Invert Bit C Flag** specifies whether C-bit is to be inverted before transmitting and on receiving. Select the check box to Invert Bit C. Default: Disabled (Do Not Invert Bit C).
- **Invert Bit D Flag** specifies whether D-bit is to be inverted before transmitting and on receiving. Select the check box to enable, that is to Invert Bit D. Default: Disabled (Do Not Invert Bit D).
- **E1 Metering Bit** signifies the bit used by the network to signal metering pulses. You can select — None, Bit-A, Bit-B, Bit-C or Bit-D. Default: Bit-A.
- Set the duration of the **E1 Metering Pulse Minimum Timer**. This specifies the minimum time for which the metering bit is changed, to be recognized as a genuine metering pulse subject to E1 Metering Pulse Minimum timer. All Changes occurred for time less than this timer is ignored. Valid range is 20ms to 1000ms. Default: 150ms.
- **Clear Back Signal** is the signal used to signify that the called party has disconnected the line first. This is indicated in two ways: Release Guard (Ab =1) or Forced Release (Bb = 0). This parameter is country specific. Default: Release Guard.
- Set the duration of the **Release Timer**. This specifies the time for which the clear back signal should persist on the line to be recognized as a genuine clear back signal. This is also known as Clear Back timer. Valid range is 20 to 1000 msec. Default: 400 msec.
- Set the duration of the **Line Seizure Acknowledge Wait Timer**. This specifies the time for which the outbound end waits for seizure acknowledgement from the inbound end after sending the line seizure signal. On expiry of this timer, clear forward signal is sent by the outbound end. Alarm is to be generated. This timer is applicable only when acting as outbound end. Valid range is 0001 to 9999 msec. Default: 200msec.

- Set the duration of the **Release Guard Timer**. This specifies the time for which inbound register waits before declaring the channel idle (sending idle signal) when clear forward line signal is received from the outbound end. This timer is applicable for Forced Release signal. This timer is applicable only when acting as inbound end. This timer depends on the speed of switching and processing. Valid range is 0000 to 9999 msec. Default: 200msec.
- Click **Submit** to save changes.
- Close the window to return to the main page.

Copy E1-CAS Parameters

- You can also copy the settings of a E1-CAS from one T1E1 port to the another using the **Copy** button. To do this,
- Click the **Copy** button. The **Copy E1-CAS Parameters** window opens.

The screenshot shows a dialog box titled "Copy E1-CAS Parameters". It contains a "from T1E1 Port to" label with a dropdown menu set to "1", followed by a "to" label. Below this, there are five checkboxes: "All", "T1E1 Port 1", "T1E1 Port 2", "T1E1 Port 3", and "T1E1 Port 4". At the bottom, there are two buttons: "OK" with a checkmark icon and "Cancel" with an "X" icon.

- In the **from T1E1 Port to** box, select the number of the T1E1 Port you want to copy settings *From*. Select the check boxes of the desired port numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the T1E1 Ports, select the **All** check box.
- Click the **OK** button.
- Once you have copied the settings, you can again edit the specific parameters of E1-CAS you copied the settings to.
- Close the **Copy E1-CAS Parameters** window.
- Click **Submit** to save changes.
- Close the window to return to the main page.

Handling of Incoming Calls

Click **Handling of Incoming Calls** to expand.

Select the method to route the incoming calls from the T1E1 Port.

SETU VTEP provides three options for **Handling of Incoming Calls** — Port Wise, Channel Number Wise and MSN/DDI Number Wise. Default: Port Wise.

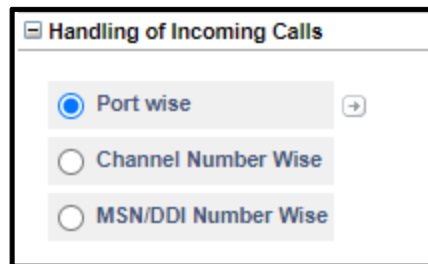


- **Port Wise:** Select this method to apply the call routing method for the entire port.
- **Channel Number Wise:** Select this method to apply a different call routing method for each channel. You can configure a different incoming call routing option for each channel.
- **MSN/DDI Number Wise:** Select this method to apply a different call routing method for each MSN number given by the Service Provider for the E1 Line. SETU VTEP allows you to configure upto 8 MSN Numbers.

Port Wise

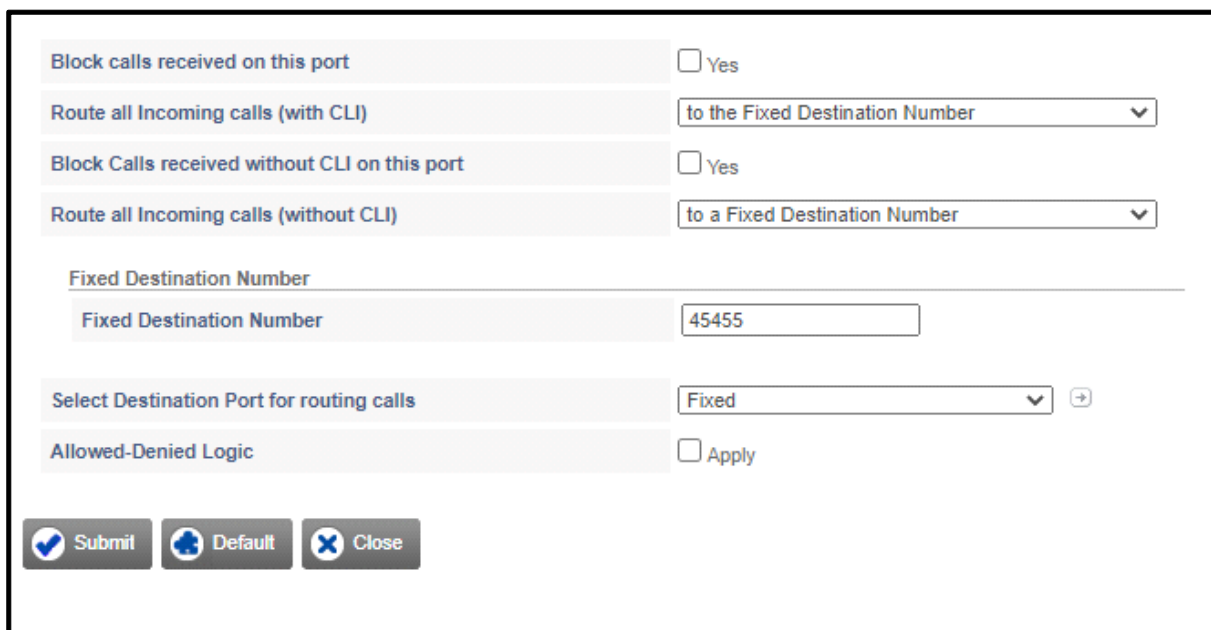
To configure Handling of Incoming Calls Port Wise,

- Select the **Port Wise** check box.




A screenshot of the 'Handling of Incoming Calls' configuration window. It features three radio button options: 'Port wise' (selected), 'Channel Number Wise', and 'MSN/DDI Number Wise'. Each option has a small '+' icon to its right.

- Click **Settings** .
- The **Handling of Incoming Calls - Port Wise** window opens.



A screenshot of the 'Handling of Incoming Calls - Port Wise' configuration window. It contains several settings:

- Block calls received on this port**: ☐ Yes
- Route all Incoming calls (with CLI)**:
- Block Calls received without CLI on this port**: ☐ Yes
- Route all Incoming calls (without CLI)**:
- Fixed Destination Number**:
- Select Destination Port for routing calls**: 
- Allowed-Denied Logic**: ☐ Apply

At the bottom, there are three buttons: **Submit** (with a checkmark icon), **Default** (with a reset icon), and **Close** (with an 'X' icon).

- Keep the **Block calls received on this port** check box disabled.

Select this check box only if you do not want to route calls received on this port.

Destination Number Determination

Select the desired destination number determination method for routing incoming calls *with* and *without* CLI.

- To **Route all Incoming calls (with CLI)**, you may select from any of the following methods:
 - to a Fixed Destination Number
 - on the basis of Calling Party Number
 - on the basis of DDI Number
 - to the Called Party Number
 - after Answering the Call and Collecting the Digits
- Default: to a Fixed Destination Number

Read further for instructions on selecting and configuring each of these destination number determination methods.



If the destination number to be dialed out is an IP Address, SETU VTEP will not check the Destination Port Determination Method. Instead, it will route the call using the SIP Trunk / Group programmed for IP Dialing. (See [“IP Dialing”](#) to know more).

Route to a Fixed Destination Number

In this method, calls received on the T1E1 Port are routed to a fixed destination number, which is configured for the T1E1 Port.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **to the Fixed Destination Number**.
- In the **Fixed Destination Number** box that appears, enter the desired destination number. The Destination Number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and. (dot/period). Default: Blank.
- Click **Submit** to save your settings.

Route on the basis of Calling Party Number

In this method, a call received on the T1E1 Port is routed to a specific number, as per the calling party's number. You must configure the calling party numbers in the *Calling Party Number Based Table*.

When there is an incoming call on the T1E1 Port, SETU VTEP will match the Calling Party Number with the entries of the Calling Party Number Based Table. If a match is found, the call is routed to the destination number configured for that Calling Party Number.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select on the basis of Calling Party Number.

Handling of Incoming Calls - Port Wise

Block calls received on this port

☐ Yes

Route all Incoming calls (with CLI)

on the basis of Calling Party Number

If no match found in the Calling Party Number Table, route calls

after Answering the Call and Collecting the Digits

Block Calls received without CLI on this port

☐ Yes

Route all Incoming calls (without CLI)

to a Fixed Destination Number

Fixed Destination Number

Fixed Destination Number

45455

Answering the call and collecting the digits

Prompt caller to enter PIN

☐ Enable

Dial Plan

1

First Digit Wait Timer

7

Seconds

Inter Digit Wait Timer

5

Seconds

End Of Dialing Digit

#

Minimum Number of digits that must be dialed by the caller

02

Maximum Number of digits that can be dialed by the caller

24

If No Digit dialed during First Digit Wait Timer

Disconnect Call

Allow making New Call using Access code

☐ Yes

Select Destination Port for routing calls

Fixed

Allowed-Denied Logic

☐ Apply

Submit

Default

Close

- Click **Settings**.

- The **T1E1 Port - Destination Number Determination: Calling Number Based** Table window opens.

1-100
101-200
201-300
301-400
401-499

T1E1 Port - Destination Number Determination: Calling Number Based

Index	Calling Number	Destination Number
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		
013		
014		
015		
016		
017		
018		
019		
020		
021		
022		
023		
024		

Submit
 Default All
 Close

- In **Calling Number**, enter the calling party numbers. The Calling numbers may consist of a maximum of 24 characters. Default: Blank.
- For each calling party number, enter a corresponding destination number in **Destination Number**. Destination numbers may consist of a maximum of 24 characters. Digits 0 to 9, *, # and (.) dot are allowed. Default: Blank.
- Click **Submit** to save your entries. Close the window to return to the **Handling of Incoming Calls - Port Wise** window.

You can also configure the **Calling Number Based** table from *Advanced Settings*. For instructions, see [“Destination Number Determination”](#) under *Advanced Settings*.

- Select a method for routing incoming calls with CLI that *do not match* with any entries in the Calling Party Number Based Table.

In the **If no match found in the Calling Party Number Table, route calls** box, select the desired method from the following options for processing the call:

- to a Fixed Destination Number
- on the basis of DDI Number
- to the Called Party Number
- after Answering the Call and Collecting the Digits

Default: after Answering the Call and Collecting the Digits

- If you want to enable PIN Authentication on the T1E1 Port, select the **Prompt caller to enter PIN** check box.

If you enable this check box, you must also configure the PIN Authentication Table. To know more about this feature and for detail instructions, see [“PIN Authentication”](#) under *Advanced Settings*.

- SETU VTEP supports 8 Dial Plans with total 64 entries in each table. When a user dials a number, it is compared with the Destination Number configured in the Dial Plan. If a match is found, the system routes the call immediately without waiting for End of Dialing and if a match is not found, the system will wait for the End of Dialing and then route the call as per the Destination Port Selection method configured.

Select the **Dial Plan** table number you configured for this port. If you have not configured the Dial Plan table you may do so now,

- Click **Settings** ➡ the Dial Plan Table opens.

Dial Plan Table - 1

Index	Destination Number
01	
02	
03	
04	
05	
06	
07	
08	

Testing

Enter the destination number to know which entry would be selected for routing

- Configure the numbers in the table. For detailed instructions, see [“Dial Plan”](#).
- Set the duration of the **First Digit Wait Timer**. This is the duration for which you want the system to wait for the caller to dial the destination number after the dial tone. Valid range is 01 to 99 seconds. Default: 7 seconds

- You may configure the following options as End of Dialing indication:
 - Set the duration of the **Inter Digit Wait Timer**. This is the duration for which you want the system to wait while receiving the digits dialed by the caller to consider it as End of Dialing. You may change this timer, if required. Valid range is 01 to 99 seconds. Default: 05 seconds.
 - In **End of Dialing Digit**, select # or * as termination digit the system should consider to detect end of dialing. Default: #
 - In **Minimum number of digits that can be dialed by the caller**, select the minimum number of digits to be dialed by the user for the system to consider it as a valid number. Valid range is 01 to 24 digits. Default: 2 digits.
 - In **Maximum Number of digits that can be dialed by the caller**, select the maximum number of digits to be dialed by the user for the system to consider it as End of Dialing. Valid range is 01 to 24 digits. Default: 24 digits.

When the caller dials a number, the system will match it with the above End of Dialing indications and accept the one that matches first.

- If the caller fails to dial the number during the First Digit Wait Timer, you can either have the system disconnect the call or route the call to a fixed destination number.

In the **If No Digit dialed during First Digit Wait Timer** box, select the desired option: **Disconnect the Call** or **Use Fixed Destination Number**. Default: Disconnect Call.

- If you selected **Use Fixed Destination Number**, enter the desired destination number in the **Fixed Destination Number** field. The Destination number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and . (dot/period). Default: Blank.



- *The First Digit Wait Timer is loaded as soon as the system answers the call.*
- *When you dial the first digit, the First Digit Wait Timer is stopped and the system loads the Inter Digit Wait Timer.*
- *SETU VTEP reloads the Inter Digit Wait Timer:*
 - *each time you dial a new digit till the termination digit is detected.*
 - *when you have dialed the maximum number of digits configured as End of Dialing.*
- If you want to enable the feature Making New Call using Access Code on the T1E1 Port, select the **Allow making New Call using Access Code** check box. For further details, see [“Making a New Call using Access Code”](#).
- Click **Submit** to save settings.

Route on the basis of DDI Number

In this method, incoming calls on the T1E1 Port are routed to specific numbers as per the DDI number received in the SETUP message on the T1E1 Port.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select on the basis of DDI Number.

Handling of Incoming Calls - Port Wise

Block calls received on this port ☐ Yes

Route all Incoming calls (with CLI) on the basis of DDI Number ▼ ➔

Block Calls received without CLI on this port ☐ Yes

Route all Incoming calls (without CLI) to the Called Party Number ▼

Select Destination Port for routing calls Fixed ▼ ➔

Allowed-Denied Logic ☐ Apply

Submit Default Close

- Click **Settings** ➔.

The **T1E1 Port - Destination Number Determination: DDI Number Based** Table opens.

1-100 101-200 201-300 301-400 401-500 501-600 601-700 701-800 801-900 901-1000

DDI Number Generation

T1E1 Port - Destination Number Determination: DDI Number Based

Index	DDI Number	Destination Number	Reverse DDI	
			Apply	Reference ID
051			<input type="checkbox"/>	1 ▼
052			<input type="checkbox"/>	1 ▼
053			<input type="checkbox"/>	1 ▼
054			<input type="checkbox"/>	1 ▼
055			<input type="checkbox"/>	1 ▼
056			<input type="checkbox"/>	1 ▼
057			<input type="checkbox"/>	1 ▼
058			<input type="checkbox"/>	1 ▼
059			<input type="checkbox"/>	1 ▼
060			<input type="checkbox"/>	1 ▼
061			<input type="checkbox"/>	1 ▼
062			<input type="checkbox"/>	1 ▼
063			<input type="checkbox"/>	1 ▼
064			<input type="checkbox"/>	1 ▼
065			<input type="checkbox"/>	1 ▼
066			<input type="checkbox"/>	1 ▼
067			<input type="checkbox"/>	1 ▼
068			<input type="checkbox"/>	1 ▼
069			<input type="checkbox"/>	1 ▼

Submit Default All Close

- In **DDI Number**, enter the DDI Numbers allotted by your service provider.
- For each DDI Number, enter the corresponding destination number in **Destination Number**.
- To apply **Reverse DDI** for each number, select the check boxes under **Apply** and select the **Reference ID** for the number. Default: Apply Reverse DDI is disabled and Reference ID is 1.
- Click **Submit** to save and close the window to return to the **Handling of Incoming Calls - Port Wise** window.

You can also configure the **DDI Number Based** Table from *Advanced Settings*. For instructions, see [“Destination Number Determination”](#) under *Advanced Settings*.

Route to the Called Party Number

In this method, a call received on the T1E1 Port is routed to a specific number depending upon the called party number received in the SETUP Message on the T1E1 Port.

- To apply this method, in **Route all incoming calls (with CLI)**, select **to the Called Party Number**.

Handling of Incoming Calls - Port Wise

Block calls received on this port ☐ Yes

Route all Incoming calls (with CLI) to the Called Party Number ▼

Block Calls received without CLI on this port ☐ Yes

Route all Incoming calls (without CLI) to the Called Party Number ▼

Select Destination Port for routing calls Fixed ▼ →

Allowed-Denied Logic ☐ Apply

Submit Default Close

Route after Answering the Call and Collecting the Digits

In this method, the incoming call is answered and dial tone is played to the caller, allowing the caller to dial the desired number. The number dialed by the caller is considered as the destination number.

Handling of Incoming Calls - Port Wise

Block calls received on this port ☐ Yes

Route all Incoming calls (with CLI) **after Answering the Call and Collecting the Digits ▼**

Block Calls received without CLI on this port ☐ Yes

Route all Incoming calls (without CLI) to the Called Party Number ▼

Answering the call and collecting the digits

Prompt caller to enter PIN ☐ Enable

Dial Plan 1 ▼ ➡

First Digit Wait Timer 7 Seconds

Inter Digit Wait Timer 5 Seconds

End Of Dialing Digit # ▼

Minimum Number of digits that must be dialed by the caller 02 ▼

Maximum Number of digits that can be dialed by the caller 24 ▼

If No Digit dialed during First Digit Wait Timer Disconnect Call ▼

Allow making New Call using Access code ☐ Yes

Select Destination Port for routing calls Fixed ▼ ➡

Allowed-Denied Logic ☐ Apply

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **after Answering the Call and Collecting the Digits**.

The related parameters of this method appear under **Answering the call and collecting the digits**.

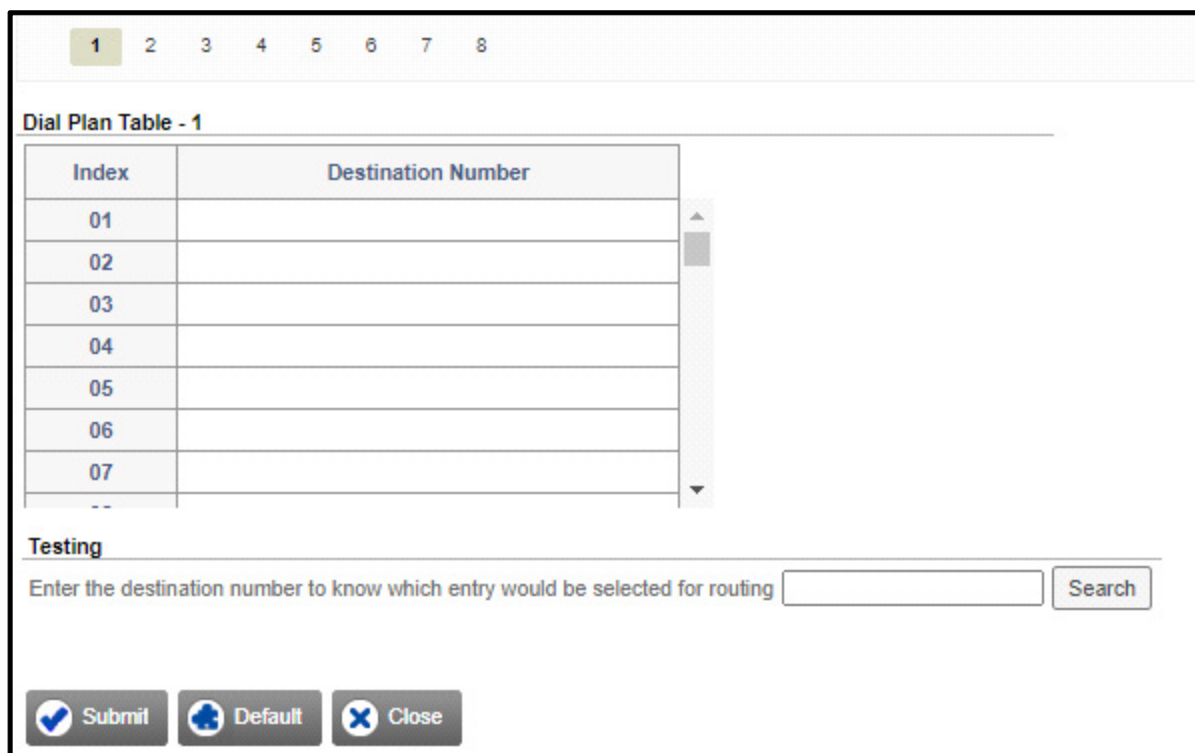
- If you want to enable PIN Authentication on the T1E1 Port, select the **Prompt caller to enter PIN** check box.

If you enable this check box, you must also configure the PIN Authentication Table. To know more about this feature and for detail instructions, see [“PIN Authentication”](#) under *Advanced Settings*.

- SETU VTEP supports 8 Dial Plans with total 64 entries in each table. When a user dials a number, it is compared with the Destination Number configured in the Dial Plan. If a match is found, the system routes the call immediately without waiting for End of Dialing and if a match is not found, the system will wait for the End of Dialing and then route the call as per the Destination Port Selection method configured.

Select the **Dial Plan** table number you configured for this port. If you have not configured the Dial Plan table you may do so now,

- Click **Settings** . The Dial Plan Table opens.



Dial Plan Table - 1

Index	Destination Number
01	
02	
03	
04	
05	
06	
07	
...	

Testing

Enter the destination number to know which entry would be selected for routing

- Configure the numbers in the table. For detailed instructions, see [“Dial Plan”](#).
- Set the duration of the **First Digit Wait Timer**. This is the duration for which you want the system to wait for the caller to dial the destination number after the dial tone. Valid range is 01 to 99 seconds. Default: 7 seconds
- You may configure the following options as End of Dialing indication:
 - Set the duration of the **Inter Digit Wait Timer**. This is the duration for which you want the system to wait while receiving the digits dialed by the caller to consider it as End of Dialing. You may change this timer, if required. Valid range is 01 to 99 seconds. Default: 05 seconds.
 - In **End of Dialing Digit**, select # or * as termination digit the system should consider to detect end of dialing. Default: #
 - In **Minimum number of digits that can be dialed by the caller**, select the minimum number of digits to be dialed by the user for the system to consider it as a valid number. Valid range is 01 to 24 digits. Default: 2 digits.
 - In **Maximum Number of digits that can be dialed by the caller**, select the maximum number of digits to be dialed by the user for the system to consider it as End of Dialing. Valid range is 01 to 24 digits. Default: 24 digits.

When the caller dials a number, the system will match it with the above End of Dialing indications and accept the one that matches first.

- If the caller fails to dial the number during the First Digit Wait Timer, you can either have the system disconnect the call or route the call to a fixed destination number.

In the **If No Digit dialed during First Digit Wait Timer** box, select the desired option: **Disconnect the Call** or **Use Fixed Destination Number**. Default: Disconnect Call.

- If you selected **Use Fixed Destination Number**, enter the desired destination number in the **Fixed Destination Number** field. The Destination number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and . (dot/period). Default: Blank.



- *The First Digit Wait Timer is loaded as soon as the system answers the call.*
- *When you dial the first digit, the First Digit Wait Timer is stopped and the system loads the Inter Digit Wait Timer.*
- *SETU VTEP reloads the Inter Digit Wait Timer:*
 - *each time you dial a new digit till the termination digit is detected.*
 - *when you have dialed the maximum number of digits configured as End of Dialing.*
- If you want to enable the feature Making New Call using Access Code on the T1E1 Port, select the **Allow making New Call using Access Code** check box. For further details, see [“Making a New Call using Access Code”](#).
- Click **Submit** to save settings.
- If you do not want to route the incoming calls received without CLI, through this T1E1 Port, select **Block Calls received without CLI on this Port** check box.
- To **Route all Incoming calls (without CLI)**, you may select from any of the following methods:
 - to a Fixed Destination Number, see [“Route to a Fixed Destination Number”](#).
 - on the basis of DDI Number, see [“Route on the basis of DDI Number”](#).
 - to the Called Party Number, see [“Route to the Called Party Number”](#).
 - after Answering the Call and Collecting the Digits, see [“Route after Answering the Call and Collecting the Digits”](#)

Default: to the Called Party Number.

Handling of Incoming Calls - Port Wise	
Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this port	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ ➔
Allowed-Denied Logic	<input type="checkbox"/> Apply

Destination Port Determination

For the port/channel/MSN number, select the Destination Port for routing calls from the following options:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number

Default: Fixed.

Read the description and follow the instructions for each of these destination port selection methods given below.



If the destination number to be dialed out is an IP Address, SETU VTEP will not check the Destination Port Determination Method. Instead, it will route the call using the SIP Trunk / Group programmed for IP Dialing. (See “[IP Dialing](#)” to know more).

Fixed

In this method, calls received on the T1E1 Port are routed to a Fixed Destination Port, irrespective of the number dialed on the T1E1 Port.

To apply this method, do the following:

- In **Select Destination Port for routing calls**, select **Fixed** option.

Handling of Incoming Calls - Port Wise

Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this port	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ ➔
Allowed-Denied Logic	<input type="checkbox"/> Apply

Submit Default Close

- Click **Settings** ➔.

The **Destination Port/Group for T1E1 Port** window opens.

Destination Port/Group for T1E1 Port

Edit	Routing Group	Fallback Routing Group
➔	SIP Trunk 1 - 1 (Ascending)	None

Close

The default **Routing Group** and **Fallback Routing Groups** appear.

- If you wish to change the default Routing Group options, click **Edit** ➔.

The **Edit Selective Port/Group for T1E1 Port** window opens.

- Create the **Routing Group**.
- To create a routing group of *sequential T1E1 Channels* as members,

- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,

- Select **T1E1 Group**.

Routing Group

☐ T1E1 Port 1 ▾ and Channel Number from 01 ▾ to 01 ▾ in Ascending ▾ order
☒ T1E1 Group 1 ▾ ➔
☐ SIP Trunk 001 ▾ to 001 ▾ in Ascending ▾ order
☐ SIP Group 1 ▾

- Select a **T1E1 Group** number. Default: 1.
- Click **Settings** ➔.
- The **T1E1 Port - Group** window opens.

T1E1 Port - Group

T1E1 Group 1 ▾
 Member Selection Method First Free ▾

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1 ▾	30 ▾	30 ▾	Ascending ▾
2	2 ▾	01 ▾	30 ▾	Ascending ▾
3	3 ▾	01 ▾	30 ▾	Ascending ▾
4	None ▾	01 ▾	30 ▾	Ascending ▾

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic *“Group”* under *Advanced Settings*.
- Similarly, you can create a group of *sequential* and *not-sequential* SIP Trunk.
- You may create the **Fallback Routing Group**.

Fallback Routing Group ☒ Apply

☐ T1E1 Port 1 ▾ and Channel Number from 01 ▾ to 01 ▾ in Ascending ▾ order
☐ T1E1 Group 1 ▾
☒ SIP Trunk 001 ▾ to 001 ▾ in Ascending ▾ order
☐ SIP Group 1 ▾

- To do this,

- Select the **Apply** check box.
- Follow the same instructions provided earlier for creating *sequential* and *not-sequential* groups of T1E1 Ports and SIP Trunks.
- Click **Submit** to save changes. The **Edit** window closes.
- The entry you edited appears in the **Destination Port/Group for T1E1 Port** window.
- Close the **Destination Port/Group for T1E1 Port** window to return to the **Handling of Calls** window.

On the basis of Destination Number

In this method, incoming calls on the source port are routed to the destination port on the basis of the destination number (called party number) dialed by the caller.

You must configure the called party numbers in the **Destination Number Based** Table. SETU VTEP will match the called party number dialed by the caller with the entries of this table. If a match is found for the number in the table, the call is routed to the destination.

To apply this method, do the following:

- In **Select Destination Port for routing calls**, select **On the basis of Destination Number** option.

Handling of Incoming Calls - Port Wise

Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this port	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	On the basis of Destination Number ▼ ➡
Allowed-Denied Logic	<input type="checkbox"/> Apply

- Click **Settings** ➡.

The **T1E1 Port - Destination Port Determination - Destination Number Based** table window opens.

T1E1 Port - Destination Port Determination - Destination Number Based				
<input type="checkbox"/>	Edit	Destination Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>		No Match Found	SIP Trunk 1 - 1 (Ascending)	None

Total Records : 1 1

Testing

Enter the destination number to know which entry would be selected for routing

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 1000 entries.

Add Entry

Destination Number

Routing Group

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☒ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1

Fallback Routing Group ☐ Apply

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☐ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1

- In **Destination Number**, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters") in this field. Valid characters are 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

Wildcard Characters

SETU VTEP supports following characters.

Character	Description
X (letter X)	X represents any single digit from 0 to 9.
#	When # is configured in a number string, it will not be considered as End of Dialing.

*	When * is configured in a number string, it will not be considered as End of Dialing.
+	+ (plus) can be configured as a first character of the Destination Number string in the <i>SIP Trunk-Destination Port Determination-Destination Number Based</i> table only.
[-]	Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket.
[,]	Comma within a bracket is used as a separator between the groups of numbers.
[^]	Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret.
T (letter T)	Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing.

- Create the **Routing Group**.
- To create a routing group of *sequential T1E1 Channels* as members,

The screenshot shows the 'Routing Group' configuration window. The 'T1E1 Port' option is selected with a radio button. The configuration is set to '1' and 'Channel Number from 01 to 01 in Ascending order'.


- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

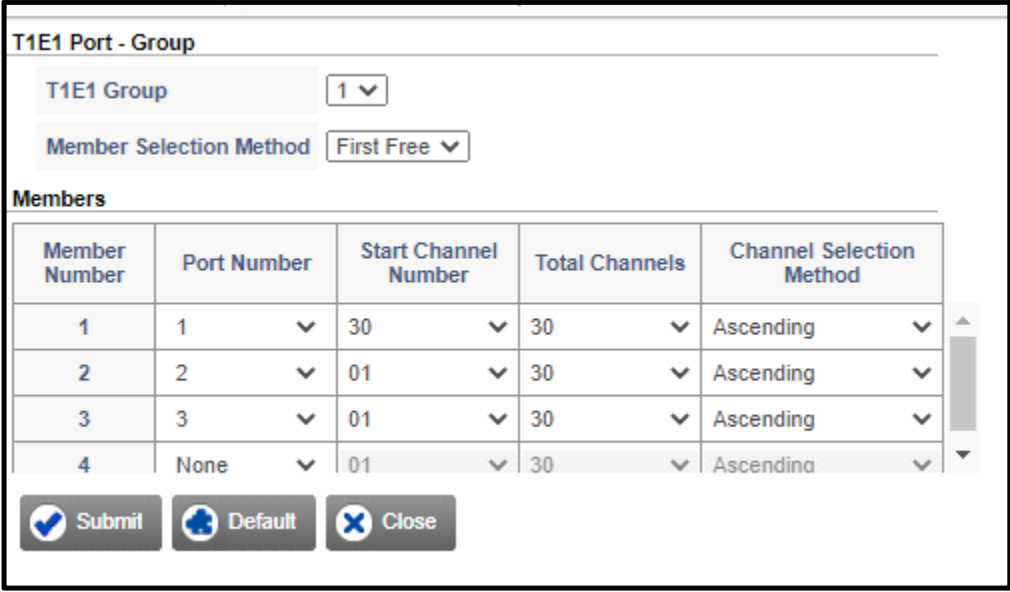
Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,
- Select **T1E1 Group**.

The screenshot shows the 'Routing Group' configuration window. The 'T1E1 Group' option is selected with a radio button. The configuration is set to '1' and 'Channel Number from 01 to 01 in Ascending order'.

- Select a **T1E1 Group** number. Default: 1.

- Click **Settings** .
- The **T1E1 Port - Groups** window opens.



T1E1 Port - Group

T1E1 Group: 1 ▼

Member Selection Method: First Free ▼

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1 ▼	30 ▼	30 ▼	Ascending ▼
2	2 ▼	01 ▼	30 ▼	Ascending ▼
3	3 ▼	01 ▼	30 ▼	Ascending ▼
4	None ▼	01 ▼	30 ▼	Ascending ▼

Submit Default Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic [“Group”](#) under *Advanced Settings*.
- Similarly, you can create a group of *sequential* and *not-sequential* SIP Trunk.
- You may create the **Fallback Routing Group**.



Fallback Routing Group ☒ Apply

☐ T1E1 Port 1 ▼ and Channel Number from 01 ▼ to 01 ▼ in Ascending ▼ order

☐ T1E1 Group 1 ▼

☒ SIP Trunk 001 ▼ to 001 ▼ in Ascending ▼ order

☐ SIP Group 1 ▼


- To do this,
 - Select the **Apply** check box.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **T1E1 Port - Destination Port Determination - Destination Number Based** table.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.

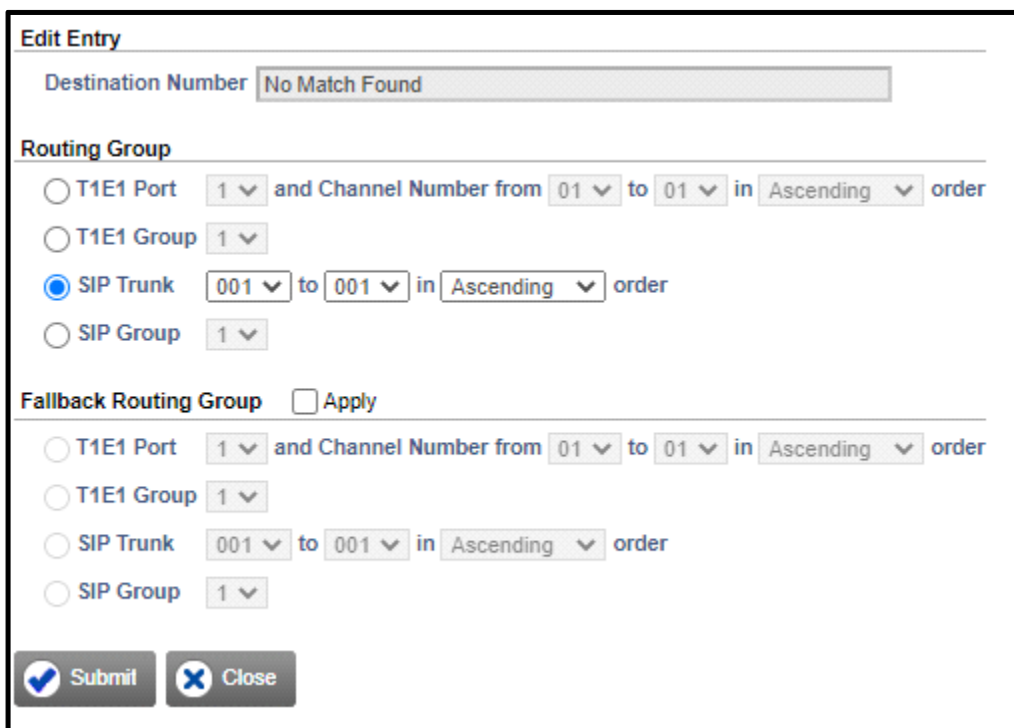


If there are multiple entries in the Destination Number Based table, to search a particular entry in the table, under Testing enter the desired number in the **Enter the destination number to know which entry would be selected for routing** search box.

- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** .



Edit Entry

Destination Number

Routing Group

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☒ SIP Trunk to in order

☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- The **Edit Entry** window opens.
- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.

You can also configure the **Destination Number Based** Table from *Advanced Settings*. For instructions, see [“Destination Port Determination”](#) under *Advanced Settings*.

On the basis of Calling Party Number

In this method, incoming calls on the T1E1 Port are routed to a specific port as per the calling party's number.

To apply this method, do the following:

- In **Select Destination Port for routing calls**, select **On the basis of Calling Party Number** option.

Handling of Incoming Calls - Port Wise

Block calls received on this port

☐ Yes

Route all Incoming calls (with CLI)

to the Called Party Number ▼

Block Calls received without CLI on this port

☐ Yes

Route all Incoming calls (without CLI)

to the Called Party Number ▼

Select Destination Port for routing calls

On the basis of Calling Party Number ▼ ➔

Allowed-Denied Logic

☐ Apply

Submit

Default

Close

- Click **Settings** ➔.

The **T1E1 Port - Destination Port Determination - Calling Number Based** table window opens.

<input type="checkbox"/>	Edit	Calling Number	Routing Group	Fallback Routing Group
	➔	No Match Found	SIP Trunk 1 - 1 (Ascending)	None
<input type="checkbox"/>	➔	3333	T1E1 Port 1 (Ch 1 - 30) (Descending)	T1E1 Port 2 (Ch 1 - 30) (Descending)
<input type="checkbox"/>	➔	4444	T1E1 Group 1	T1E1 Group 8
<input type="checkbox"/>	➔	5555	SIP Group 1	SIP Group 9
<input type="checkbox"/>	➔	6666	SIP Trunk 1 - 1 (Ascending)	SIP Trunk 1 - 1 (Ascending)
<input type="checkbox"/>	➔	6666	SIP Trunk 1 - 125 (Ascending)	SIP Trunk 1 - 125 (Ascending)
<input type="checkbox"/>	➔	8888	SIP Group 9	T1E1 Group 8
<input type="checkbox"/>	➔	8888	SIP Trunk 1 - 1 (Ascending)	None
<input type="checkbox"/>	➔	9999	T1E1 Group 1	None
<input type="checkbox"/>	➔	1212	SIP Group 1	None
<input type="checkbox"/>	➔	3443	T1E1 Port 1 (Ch 1 - 30) (Ascending)	SIP Trunk 5 - 5 (Ascending)
<input type="checkbox"/>	➔	4545	SIP Trunk 1 - 10 (Ascending)	SIP Trunk 100 - 125 (Ascending)
<input type="checkbox"/>	➔	55555555	T1E1 Port 1 (Ch 10 - 10) (Ascending)	T1E1 Port 3 (Ch 15 - 15) (Ascending)
Total Records : 13		1		

Add

Delete

Close

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 499 entries.

Add Entry

Calling Number

Routing Group

☐ T1E1 Port and Channel Number from to in order
☐ T1E1 Group
☒ SIP Trunk to in order
☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order
☐ T1E1 Group
☐ SIP Trunk to in order
☐ SIP Group

- In **Calling Number**, enter the number (max. 24 characters) from which you expect calls to be received. Valid digits are 0 to 9, *, #, (dot). Default: Blank.
- Create the **Routing Group**.
- To create a routing group of *sequential T1E1 Channels* as members,

Routing Group

☒ T1E1 Port and Channel Number from to in order
☐ T1E1 Group
☐ SIP Trunk to in order
☐ SIP Group

- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,

- Select **T1E1 Group**.

Routing Group

☐ T1E1 Port 1 ▾ and Channel Number from 01 ▾ to 01 ▾ in Ascending ▾ order

☒ T1E1 Group 1 ▾ ➕

☐ SIP Trunk 001 ▾ to 001 ▾ in Ascending ▾ order

☐ SIP Group 1 ▾

- Select a **T1E1 Group** number. Default: 1.
- Click **Settings** ➔.
- The **T1E1 Port - Groups** window opens.

T1E1 Port - Group

T1E1 Group 1 ▾

Member Selection Method First Free ▾

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1 ▾	30 ▾	30 ▾	Ascending ▾
2	2 ▾	01 ▾	30 ▾	Ascending ▾
3	3 ▾	01 ▾	30 ▾	Ascending ▾
4	None ▾	01 ▾	30 ▾	Ascending ▾

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic *“Group”* under *Advanced Settings*.
- Similarly, you can create a group of *sequential* and *not-sequential* SIP Trunk.
- You may create the **Fallback Routing Group**.

Fallback Routing Group ☒ **Apply**

☐ T1E1 Port 1 ▾ and Channel Number from 01 ▾ to 01 ▾ in Ascending ▾ order

☐ T1E1 Group 1 ▾

☒ SIP Trunk 001 ▾ to 001 ▾ in Ascending ▾ order

☐ SIP Group 1 ▾

- To do this,


- Select the **Apply** check box.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **T1E1 Port - Destination Port Determination - Destination Number Based** table.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.



*If there are multiple entries in the Destination Number Based table, to search a particular entry in the table, under Testing enter the desired number in the **Enter the destination number to know which entry would be selected for routing** search box.*

- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** .

Edit Entry

Destination Number: No Match Found

Routing Group

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☒ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1

Fallback Routing Group ☐ Apply

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☐ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1

☒ Submit ☐ Close

- The **Edit Entry** window opens.
- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.

You can also configure the **Destination Number Based** Table from *Advanced Settings*. For instructions, see [“Destination Port Determination”](#) under *Advanced Settings*.

Allowed - Denied Logic

You can apply the Allowed-Denied logic on the T1E1 Port (source port) if you want to allow or restrict the dialing of particular numbers. You can use this feature for Toll Control.

The Allowed-Denied Number Logic makes use of two Number lists:

- **Allowed Numbers List:** This is the list of numbers that can be dialed out from the T1E1 Port.
- **Denied Numbers List:** This list contains the numbers that are to be restricted from being dialed out from the T1E1 Port.

When Allowed-Denied Logic is enabled on a source port, for each number dialed from the port, SETU VTEP uses the best-match-found logic to compare the dialed number with the Allowed Number list and the Denied Number list.

The number is allowed to be dialed, if it:

- matches with both lists.
- matches with Allowed Number list, but not with the Denied Number list.
- matches with neither the Allowed List nor the Denied List.

The number is denied, if it matches with the Denied Number list, but not with the Allowed Number list.

The system does not apply the Allowed-Denied Logic:

- When dialed number string matches with any Access Code.
- When dialed number string matches with any Emergency Number.
- When any one of the following is selected to Route all Incoming Calls (with CLI):
 - on the basis of Calling Party Number
 - to a Fixed Destination Number
 - on the basis of DDI Number

To apply Allowed - Denied Logic on the T1E1 Port,

- Select the **Allowed - Denied Logic** check box.



Allowed-Denied Logic	<input checked="" type="checkbox"/> Apply
Allowed Numbers List	01 ▼ ➔
Denied Numbers List	02 ▼ ➔

- In the **Allowed Number List**, select the list number you have configured with numbers you want to allow to be dialed out from the T1E1 Port. Default: 01

If you have not configured the Allowed Number List,


- Click **Settings** ➔.

- The **Number Lists** window opens.

Location	List 1	List 2	List 3	List 4
01	0	0		
02	1	1		
03	2	2		
04	3	3		
05	4	4		
06	5	5		
07	6	6		
08	7	7		
09	8	8		
10	9	9		
11	*	*		
12	#	#		

- You may configure the default Allowed Number List 1 or any other list. See [“Number Lists”](#) to configure the allowed numbers.
- Click **Submit** to save the Allowed Number List and close the window.
- In the **Denied Number List**, select the list number you have configured with numbers you want to restrict to be dialed out from the T1E1 Port. Default: 02


If you have not configured the Denied Number List,

- Click **Settings** . The **Number Lists** window opens.
- You may configure the default Denied Number List 2 or any other list. See [“Number Lists”](#) to configure the restrict numbers.
- Click **Submit** to save the Denied Number List and close the window.


Channel Number Wise

To configure Handling of Incoming Calls for each channel,

- Select the **Channel Number Wise** check box.

 **Handling of Incoming Calls**

☐ Port Wise

☒ **Channel Number Wise** 

☐ MSN/DDI Number Wise

- Click **Settings** .

- The **T1E1 Port 1 - Call Routing - Channel Number Wise** window opens.

T1E1 Port 1 - Call Routing - Channel Number wise

Channel Number	Name	Call Routing
CH-1		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-2		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-3		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-4		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-5		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-6		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-7		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-8		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-9		Route calls to number received in SETUP message using SIP Trunk 1 - 1

- Click the respective channel number to configure the parameters.

T1E1 Port 1 Channel Number 1

Name

Handling of Incoming Calls - Channel Number Wise

Block calls received on this channel

☐ Yes

Route all Incoming calls (with CLI)

to the Called Party Number

Block Calls received without CLI on this channel

☐ Yes

Route all Incoming calls (without CLI)

to a Fixed Destination Number

Fixed Destination Number

Fixed Destination Number

Select Destination Port for routing calls

Fixed

Allowed-Denied Logic

☐ Apply

Submit

Default

Copy

Close

Configure the routing parameters for each channel.

- Block calls received on this channel.
- Route all Incoming Calls (with CLI), see [“Destination Number Determination”](#).
- Block Calls received without CLI on this channel.
- Route all Incoming Calls (without CLI), see [“Destination Number Determination”](#).
- Select the destination port for routing calls, see [“Destination Port Determination”](#).
- Allowed-Denied Logic, see [“Allowed - Denied Logic”](#).
- Handling of Outgoing Calls, see [“Handling of Outgoing Calls”](#).

Copy Channel Based Routing Parameters

- You can also copy the settings of a T1E1 Channel to another T1E1 Channel using the **Copy** button. To do this,
- Click the **Copy** button. The **Copy T1E1 Port Channel based routing parameters from Channel Number** window opens.

Copy T1E1 Port Channel based routing parameters from Channel Number 01 ▼ to

All	<input type="checkbox"/>						
Ch 1	<input type="checkbox"/>	Ch 2	<input type="checkbox"/>	Ch 3	<input type="checkbox"/>	Ch 4	<input type="checkbox"/>
Ch 5	<input type="checkbox"/>	Ch 6	<input type="checkbox"/>	Ch 7	<input type="checkbox"/>	Ch 8	<input type="checkbox"/>
Ch 9	<input type="checkbox"/>	Ch 10	<input type="checkbox"/>	Ch 11	<input type="checkbox"/>	Ch 12	<input type="checkbox"/>
Ch 13	<input type="checkbox"/>	Ch 14	<input type="checkbox"/>	Ch 15	<input type="checkbox"/>	Ch 16	<input type="checkbox"/>
Ch 17	<input type="checkbox"/>	Ch 18	<input type="checkbox"/>	Ch 19	<input type="checkbox"/>	Ch 20	<input type="checkbox"/>
Ch 21	<input type="checkbox"/>	Ch 22	<input type="checkbox"/>	Ch 23	<input type="checkbox"/>	Ch 24	<input type="checkbox"/>
Ch 25	<input type="checkbox"/>	Ch 26	<input type="checkbox"/>	Ch 27	<input type="checkbox"/>	Ch 28	<input type="checkbox"/>
Ch 29	<input type="checkbox"/>	Ch 30	<input type="checkbox"/>				

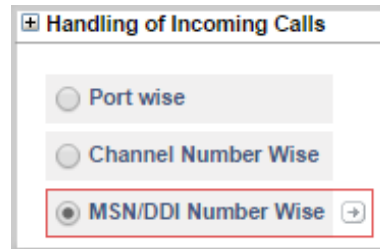
OK Close

- In the **Copy T1E1 Port Channel based routing parameters from Channel Number** box, select the number of the channel you want to copy settings *From*. Select the check boxes of the desired channel numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the channels, select the **All** check box.
- Click the **OK** button.
- Once you have copied the settings, you can again edit the specific parameters of the T1E1 Channel you copied the settings to.
- Close the **T1E1 Port 1 Channel Number 1** window.
- To configure any Channel, click the respective channel number on the **T1E1 Port 1 - Call Routing - Channel Number Wise** window and follow the same instructions as given above.
- Close the **T1E1 Port 1 - Call Routing - Channel Number Wise** window.

MSN/DDI Number Wise

To configure Handling of Incoming Calls for each MSN Number,


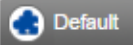
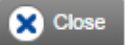

- Select the **MSN/DDI Number Wise** check box.



A configuration window titled "Handling of Incoming Calls" with a plus icon in the top left corner. It contains three radio button options: "Port wise", "Channel Number Wise", and "MSN/DDI Number Wise". The "MSN/DDI Number Wise" option is selected and highlighted with a red rectangular box. To the right of the "MSN/DDI Number Wise" option is a small square button with a right-pointing arrow.

- Click **Settings** .
- The **T1E1 Port 1 - Call Routing - MSN/DDI Number Wise** window opens.

T1E1 Port 1 - Call Routing - MSN/DDI Number wise				
MSN Number	Name	Number	Total DDI Number	Call Routing
MSN-1			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-2			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-3			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-4			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-5			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-6			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-7			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-8			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1

- Click the respective MSN number to configure the parameters.

T1E1 Port 1 MSN Number 1

Name

Handling of Incoming Calls - Msn Number Wise

MSN Number 1	<input type="text"/>
Total DDI Numbers	<input type="text" value="100"/>
Block calls received on this MSN number	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	<input type="text" value="to the Called Party Number"/> ▼
Block Calls received without CLI on this MSN number	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	<input type="text" value="to the Called Party Number"/> ▼
Select Destination Port for routing calls	<input type="text" value="Fixed"/> ▼
Allowed-Denied Logic	<input type="checkbox"/> Apply

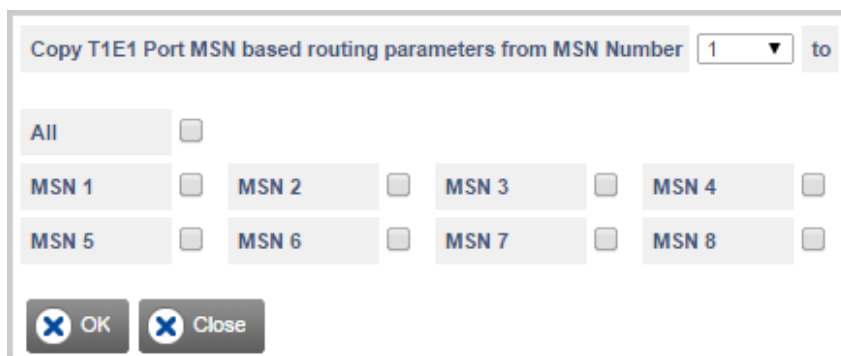
Submit
 Default
 Copy
 Close

Configure the routing parameters for each MSN number:

- **MSN Number 1:** Enter the first **MSN Number** (max. 24 digits) provided by your Service Provider. Valid digits are 0-9, # and *. Default: Blank.
- **Total DDI Number:** Specify **Total DDI Numbers** provided by your Service Provider. Valid range is 1 to 9999. Default: 0100.
- **Name:** Assign a Name for identification.
- Block calls received on this MSN Number.
- Route all Incoming Calls (with CLI), see [“Destination Number Determination”](#).
- Block Calls received without CLI on this MSN number.
- Route all Incoming Calls (without CLI), see [“Destination Number Determination”](#).
- Select the destination port for routing calls, see [“Destination Port Determination”](#).
- Allowed-Denied Logic, see [“Allowed - Denied Logic”](#).
- Handling of Outgoing Calls, see [“Handling of Outgoing Calls”](#).

Copy MSN Based Routing Parameters

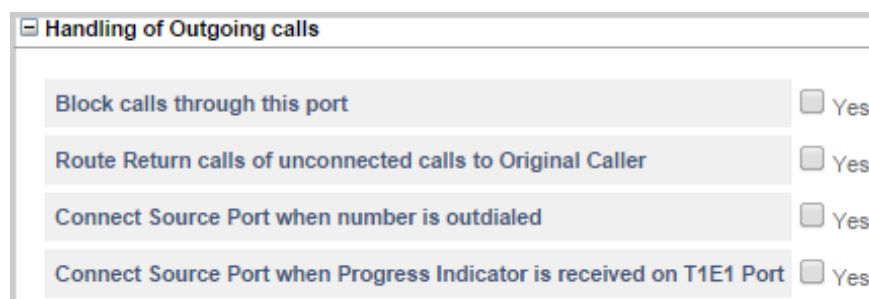
- You can also copy the settings of a MSN Number to another MSN Number using the **Copy** button. To do this,
- Click the **Copy** button. The **Copy T1E1 Port MSN based routing parameters from MSN Number** window opens.



- In the **Copy T1E1 Port MSN based routing parameters from MSN Number** box, select the MSN Number you want to copy settings *From*. Select the check boxes of the desired MSN Numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the MSN Numbers, select the **All** check box.
- Click the **OK** button.
- Once you have copied the settings, you can again edit the specific parameters of the MSN Number you copied the settings to.
- Close the **T1E1 Port 1 MSN Number 1** window.
- To configure any MSN Number, click the respective MSN Number on the **T1E1 Port 1 - Call Routing - MSN/DDI Number Wise** window and follow the same instructions as given above.
- Close the **T1E1 Port 1 - Call Routing - MSN/DDI Number Wise** window.

Handling of Outgoing Calls

Click **Handling of Outgoing Calls** to expand.



When T1/E1 Port is determined as the destination port, numbers dialed from this port constitute outgoing calls.

For outgoing calls from T1/E1 Port, you can apply the features Automatic Number Translation (ANT) and Route Calls Returned Unconnected to Original Caller.

- Select the **Block calls through this port** check box, if you do not want to route outgoing calls through this port.
- Enable **Route Return calls of unconnected calls to Original Caller** check box, if you want SETU VTEP to route outgoing calls made from this port that return unconnected back to the original caller. Default: Disabled.

If you enable this feature, when an outgoing call is made using this port, and the Called Party is found busy or does not respond, SETU VTEP stores the number of the calling party, the number of the called party and this port (through which the outgoing call was made). A record of each such call is stored for the duration of the Unconnected Calls Record Delete Timer (configurable; default: 999 minutes).

If the called party returns the call before the expiry of this Timer, SETU VTEP checks whether *Apply RCOC only if the caller calls back on the same trunk from which the call was made* is enabled or not, and accordingly places the incoming call to the original calling party. To change the duration of this timer, delete records of such calls and enable/disable the *Apply RCOC only if the caller calls back on the same trunk from which the call was made* check box, see [“System Parameters”](#).

- To connect the Source Port with the Destination Port without waiting for the call on the Destination Port to mature, enable the **Connect Source Port when number is outdialed** check box. Default: Disabled.

In all Destination Number Determination methods except *After Answering the Call and Collecting the Digits*, the Source Port gets connected to the Destination Port only after the call has matured, that is, the called party has answered the call. Until the call matures, the caller hears only Ring Back Tone played by the network.

By connecting the Source Port with the Destination Port immediately after the number is dialed, the caller can know the state of the call; if the called party is busy, not responding, not reachable or is rejecting the call.

- Enable **Connect Source Port when Progress Indicator is received on T1E1 Port** check box, to connect Source Port with the Destination Port as soon as Progress Indicator is received on T1E1 Port without waiting for the call on the Destination Port to mature. Default: Disabled.

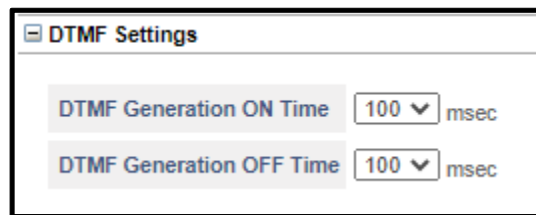


If you enable Connect Source Port when Progress Indicator is received on T1E1 Port, you will not be able to provide the features [“Making a New Call using Access Code”](#) and [“Disconnecting a Call using Access Code”](#) to users.

- Click **Submit** to save settings.

DTMF Settings

- Click **DTMF Settings** to expand.



DTMF Settings

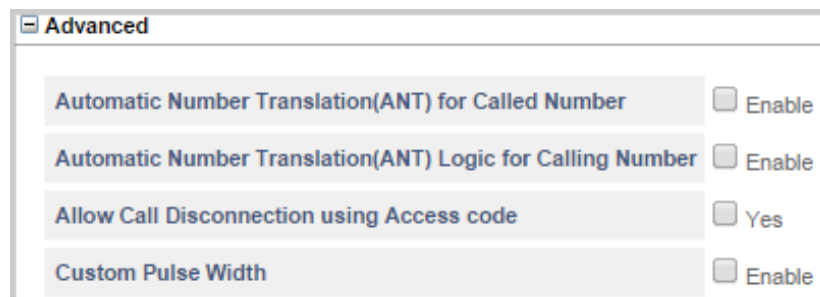
DTMF Generation ON Time 100 msec

DTMF Generation OFF Time 100 msec

- Select the appropriate **DTMF Generation ON Time** for the T1E1 Port. This is the time for which the DTMF digit which is to be outdialed remains ON. Valid range is 50 to 250 msec. Default: 100 msec.
- Select the appropriate **DTMF Generation OFF Time** for the T1E1 Port. This is the time for which system should wait before dialing the successive DTMF digits so that the T1E1 network can detect the dialed digits. Valid range is 50 to 250 msec. Default: 100 msec.

Advanced

- Click **Advanced**.



Advanced

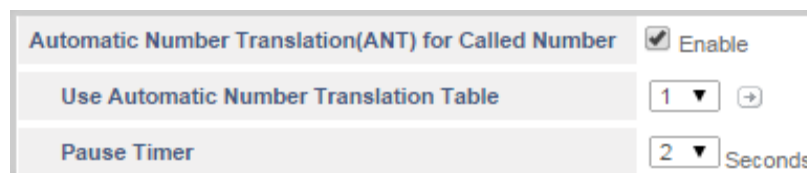
Automatic Number Translation(ANT) for Called Number ☐ Enable

Automatic Number Translation(ANT) Logic for Calling Number ☐ Enable

Allow Call Disconnection using Access code ☐ Yes

Custom Pulse Width ☐ Enable

- You can apply **Automatic Number Translation logic** on outgoing calls made from the T1E1 Port.
- To apply ANT logic on the Called Numbers, select the **Automatic Number Translation (ANT) for Called Number** check box. Default: Disabled.



Automatic Number Translation(ANT) for Called Number ☒ Enable

Use Automatic Number Translation Table 1

Pause Timer 2 Seconds

- In **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Called Numbers. Default: Table 1.

If you have not configured the Automatic Number Translation Table,

- Click **Settings** .

- The **Automatic Number Translation Table** window opens.

1
2
3
4
5
6
7
8

Automatic Number Translation Table - 1

Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	
11		0	
12		0	

Examples of Number Pattern

Number	Strip Digit	Add Prefix	Remarks
\$\$\$	0	13152222	System will add the prefix '13152222' to every 3-digit dialed number.
8\$\$\$	1		System will strip off the first digit of all 4-digit dialed numbers that start with 8, and will dial out the remaining 3-digit number.
\$\$\$\$\$\$	0	1315	System will add the prefix '1315' to every 7-digit dialed number.

Submit
 Default
 Close

- You may configure the default Automatic Number Translation Table or any other Table. See [“Automatic Number Translation \(ANT\)”](#) to configure the ANT Table.
- Click **Submit** to save the ANT Table and close the window.
- Return to ANT parameter and assign the ANT Table you configured.
- Click **Submit**.
- Set the duration of the **Pause Timer**, if you have configured ^ (Pause) in the Add Prefix column of the ANT Table. Valid range is 1 to 9 seconds. Default: 2 seconds.
- To apply ANT logic on the Calling Numbers, click the **Automatic Number Translation (ANT) for Calling Number** check box. Default: Disabled.

Automatic Number Translation (ANT) for Calling Number
☒ Enable

Use Automatic Number Translation Table

5
▼
+

- In the **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Calling Numbers. Default: Table 5.

If you have not configured the Automatic Number Translation Table,

- Click **Settings** .
- The **Automatic Number Translation Table** window opens.




12345678

Automatic Number Translation Table - 5

Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	
11		0	
12		0	

Examples of Number Pattern

Number	Strip Digit	Add Prefix	Remarks
\$\$\$	0	13152222	System will add the prefix '13152222' to every 3-digit dialed number.
8\$\$\$	1		System will strip off the first digit of all 4-digit dialed numbers that start with 8, and will dial out the remaining 3-digit number.
\$\$\$\$\$\$	0	1315	System will add the prefix '1315' to every 7-digit dialed number.

 Submit
 Default
 Close

- You may configure the default Automatic Number Translation Table or any other Table. See [“Automatic Number Translation \(ANT\)”](#) to configure the ANT Table.
- Click **Submit** to save the ANT Table and close the window.
- Return to ANT parameter and assign the ANT Table you configured.
- To enable the feature Disconnect Call using Access Code on the T1E1 Port, select the **Allow Call Disconnection using Access code** check box. To know more about this feature, see [“Disconnecting a Call using Access Code”](#).
- To customize the pulse width option and set the pulse shapes configure the **Custom Pulse** parameters. SETU VTEP generates pulse shapes which match the country standard, where it is installed. However, if the standard pulse shape does not match, SETU VTEP enables you to customize the pulse width to match your exact requirements.

To use customize pulse width option and set the pulse shape in 1 to 4 phases,

- Select the **Custom Pulse Width** check box.
- In **Custom Pulse Width Word 1**, set the pulse width for setting pulse shape in the 1st phase. Valid range is 0 to 127. Default: 63.

- In **Custom Pulse Width Word 2**, set the pulse width for setting pulse shape in the 2nd phase. Valid range is 001 to 127. Default: 58.
- In **Custom Pulse Width Word 3**, set the pulse width for setting pulse shape in the 3rd phase. Valid range is 001 to 127. Default: 76.
- In **Custom Pulse Width Word 4**, set the pulse width for setting pulse shape in the 4th phase. Valid range is 001 to 127. Default: 0.

Copy T1E1 Port Parameters

- You can also copy the settings of a T1E1 Port to another T1E1 Port using the **Copy** button. To do this,
- Click the **Copy** button. The **Copy T1E1 Port Parameters** window opens.



Copy T1E1 Port Parameters from T1E1 Port 1 to

☐ All

☐ T1E1 Port 1 ☐ T1E1 Port 2 ☐ T1E1 Port 3 ☐ T1E1 Port 4

☒ OK ☐ Close

- In the **Copy T1E1 Port Parameters from T1E1 Port** box, select the number of the port you want to copy settings *From*. Select the check box of the respective port numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the ports, select the **All** check box.
- Click the **OK** button.

Once you have copied the settings, you can again edit the specific parameters of the **T1E1** Port you copied the settings to.

T1 Port

SETU VTEP supports the T1/E1 Ports to which you can connect the T1 or E1 line.

- Click the **Basic Settings** link to expand.
- Click the **T1E1 Port** link.

T1E1 Port						
Port	Enable	Name	Status	Line Signaling	Orientation	Call Routing
T1E1-1	<input checked="" type="checkbox"/>		Layer 1 - Down Layer 2 - Down	T1 - PRI DMS	Network	Channel wise
T1E1-2	<input checked="" type="checkbox"/>		Layer 1 - Down Layer 2 - Down	T1 - PRI ATT 5ESS	Network	Channel wise
T1E1-3	<input checked="" type="checkbox"/>		Layer 1 - Down Layer 2 - Down	T1 - PRI US NI2	Network	Channel wise
T1E1-4	<input checked="" type="checkbox"/>		Layer 1 - Down Layer 2 - N.A.	T1 - RBS	Terminal	Channel wise

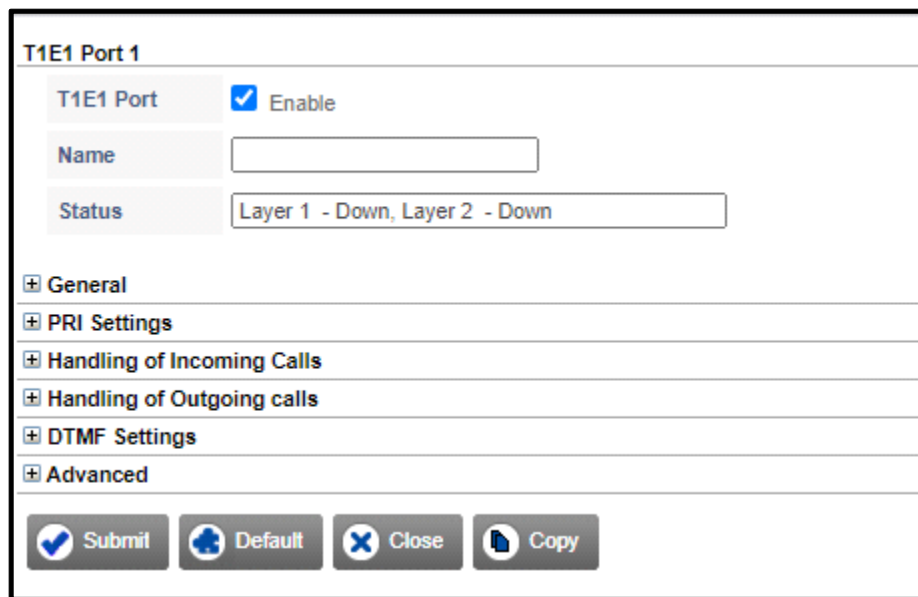
The T1E1 Port page displays the following parameters:

- **Port:** It displays the T1E1 Port numbers. Click on the desired T1E1 Port number to configure the Port Parameters.
- **Enable:** Keep the **T1E1 Ports** enabled. Clear the T1E1 Port **Enable** check box, only if you do not want to use the respective port. Default: Enabled.
- **Name:** Assign a Name to the T1E1 Port for identification. The Name can be a maximum of 24 characters.
- **Status:** This displays the status of Layer 1 and Layer 2, that is, Up or Down.
- **Line Signaling:** It displays the Carrier Type, Signaling Type and the ISDN Switch Variant you select.
- **Orientation:** It displays the type of orientation you select — Network or Terminal.
- **Call Routing:** It displays the Call Routing Method you select.

To configure the **T1E1 Port**,

- Click **T1E1-1**.

The **T1E1 Port-1** window opens.



T1E1 Port 1

T1E1 Port ☒ Enable

Name

Status

+ General

+ PRI Settings

+ Handling of Incoming Calls

+ Handling of Outgoing calls

+ DTMF Settings

+ Advanced

- Keep the **T1E1 Port** check box enabled.

Clear the **T1E1 Port Enable** check box only when you do not want to use this T1E1 Port. Default: Enabled.

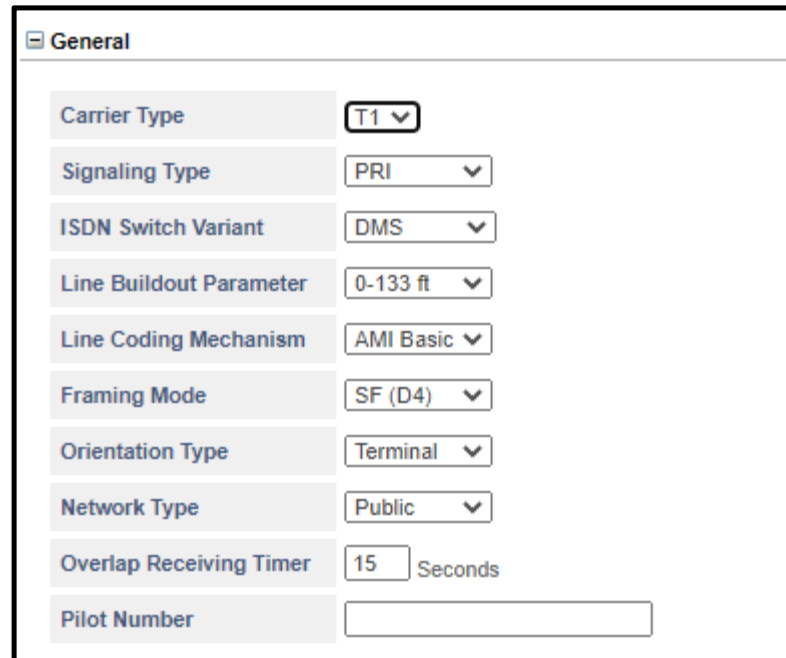
- You can assign a **Name** to the T1E1 Port, which will be displayed to the called party, if the called party telephone instrument supports name display.

The name you assign may consist of a maximum of 24 characters. Default: Blank.

- **Status** displays the status of the T1E1 Port.

General

- Click **General** to expand.
- Select **T1** as the **Carrier Type**. Default: E1.



General	
Carrier Type	T1
Signaling Type	PRI
ISDN Switch Variant	DMS
Line Buildout Parameter	0-133 ft
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Orientation Type	Terminal
Network Type	Public
Overlap Receiving Timer	15 Seconds
Pilot Number	

- Select **Signaling Type**. The Signaling Type signifies the type of signaling to be used on the T1 line.
SETU VTEP supports — PRI and RBS signaling for T1 line. Default: PRI.
 - If you select **PRI**, you must configure the PRI parameters. For instructions, see [“PRI Settings”](#).
 - If you select **RBS**, you must configure the RBS parameters. For instructions, see [“RBS Settings”](#).
- ISDN supports a variety of service provider switches. These switches are designed using ISDN standard protocol. The type of switch you select determines various factors — the number of ISDN devices that could be handled, the B-Channel that would support voice, video, data, etc. Each country uses their own specific type of ISDN switch.

In **ISDN Switch Variant**, select — DMS, US NI2 or ATT 5ESS — as the ISDN Switch Variant. Default: DMS. This parameter is applicable only if you select PRI as the Signaling Type.

- Select the T1 **Line Buildout Parameter** for T1E1 Port. You may select — 0-133 ft., 133-266 ft., 266-399 ft., 399-533 ft., 533-655 ft., -7.5 dB,-16 dB, -22.5 dB. Default: 0-133 ft.
- Line Coding is a mechanism to code the digital data into electrical pulses for the purpose of transmission over the communication channel.

Select the **Line Coding Mechanism** — AMI Basic or B8ZS. Default: AMI Basic.

- **Framing** is a formatting resource that splits the digital data into time slots of 8 bits each. Each time slot is treated as single transmission unit. These frames enable the receiver to interpret the data.

Select the **Framing Mode** as per your requirement. You can select SF (D4) or ESF. Default: SF (D4)

- **SF (D4)** refers to the Superframe with 12 concatenated frames.
- **ESF** refers to the Extended Superframe with 24 concatenated frames. This type of framing mode also has cyclic redundancy checking, a maintenance channel and is used for Common Channel Signaling (CCS).
- Select the **Orientation Type** for the port as **Terminal** or **Network**, according to your installation scenario. Default: Terminal.

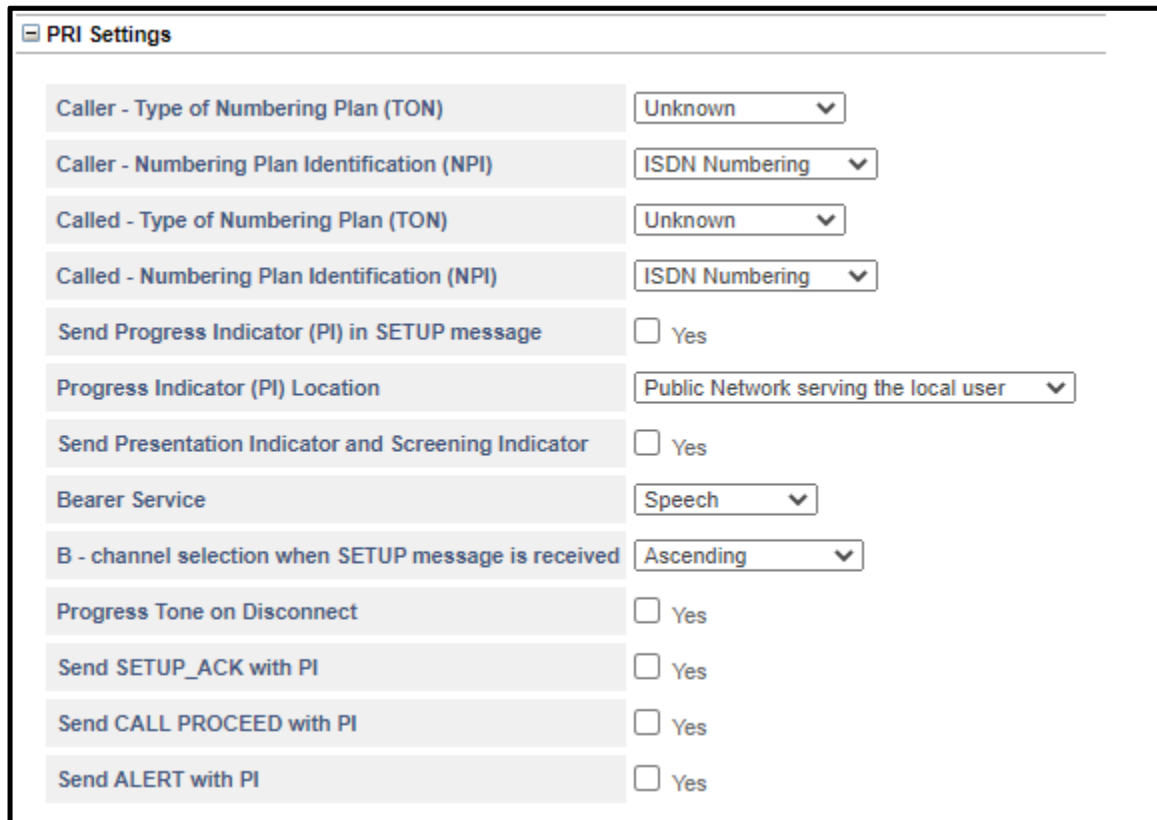
If you select *Terminal* as Orientation Type, select the **Network Type** — Public or Private — to specify whether the T1 line is from a **Public** Network (telephone exchange) or from a **Private** Network (to the NT port of a System). Default: Public.

- For **Terminal** as the Orientation Type, configure — [“Handling of Incoming Calls”](#) and [“Handling of Outgoing Calls”](#).
- For **Network** as the Orientation Type, configure [“DTMF Settings”](#).
- Enter the **Pilot Number** provided by your service provider for the T1 line connected to the T1/E1 Port. Pilot Number is necessary for sending the calling party number when the call is routed using T1/E1 Port and Reverse DDI logic is not applied. Valid digits are 0 to 9, #, *. Default: Blank.

PRI Settings

If you have selected **PRI** as **Signaling Type**, configure the PRI parameters.

- Click **PRI Settings** to expand.



The screenshot shows a configuration window titled "PRI Settings". It contains several rows of settings, each with a label on the left and a control on the right. The controls include dropdown menus and checkboxes.

Setting	Value
Caller - Type of Numbering Plan (TON)	Unknown
Caller - Numbering Plan Identification (NPI)	ISDN Numbering
Called - Type of Numbering Plan (TON)	Unknown
Called - Numbering Plan Identification (NPI)	ISDN Numbering
Send Progress Indicator (PI) in SETUP message	<input type="checkbox"/> Yes
Progress Indicator (PI) Location	Public Network serving the local user
Send Presentation Indicator and Screening Indicator	<input type="checkbox"/> Yes
Bearer Service	Speech
B - channel selection when SETUP message is received	Ascending
Progress Tone on Disconnect	<input type="checkbox"/> Yes
Send SETUP_ACK with PI	<input type="checkbox"/> Yes
Send CALL PROCEED with PI	<input type="checkbox"/> Yes
Send ALERT with PI	<input type="checkbox"/> Yes

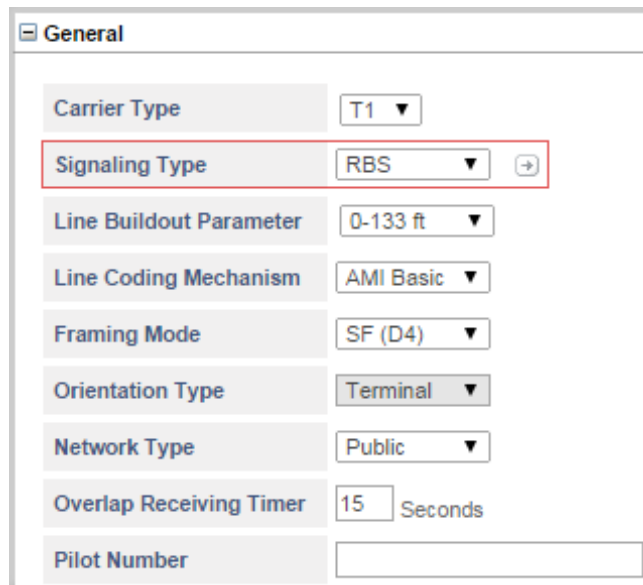
- Select the required option for sending the **Caller-Type of Numbering Plan (TON)** — Unknown, International, National, Network Specific, Subscriber, Abbreviated or Reserved. Default: Unknown.
- Select the required option for sending the **Caller-Numbering Plan Identification (NPI)** — Unknown, ISDN Numbering, Data Numbering, Telex Numbering, National Numbering, Private or Reserved. Default: ISDN Numbering.
- Select the required option for sending the **Called-Type of Numbering Plan (TON)** — Unknown, International, National, Network Specific, Subscriber, Abbreviated or Reserved. Default: Unknown.
- Select the required option for sending the **Called-Numbering Plan Identification (NPI)** — Unknown, ISDN Numbering, Data Numbering, Telex Numbering, National Numbering, Private or Reserved. Default: ISDN Numbering.
- Select the **Send Progress Indicator (PI) in SETUP message** check box if you want the progress indicator value to be sent in SETUP message. Default: Disabled.
 - Set the **Progress Indicator (PI) value in SETUP message** to the desired value. You can select — 1 or 3.
 - Progress indicator 1 indicates that the call is not end-to-end ISDN and further call progress information may be available in-band.

- Progress indicator 3 indicates that the origination address is non-ISDN.
- This value will be included in the Setup Message to indicate whether the calling party is an ISDN device or not. Default: 1.
- Select the **Progress Indicator (PI) Location** for the SETUP message. The location is a progress indicator information element that indicates from where the message is coming. Default: Public Network serving the local user.
- Select the **Send Presentation Indicator and Screening Indicator** check box, if you want the system to display the presentation and screening information to the remote end. Default: Disabled.
- Select the required **Presentation Indicator**. This allows remote end to know whether CLI Number should be displayed to user or not. You can select — Presentation Allowed, Presentation Restricted or Received from Source Port. Default: Received from Source Port.
- Select the required **Screening Indicator**. This indicates whether the information is provided by the user or the network along with the screening details — not screened, verified and passed or verified and failed. Default: User-provided, not screened.
- Select the **Bearer Service** supported by your service provider. This will be sent in the SETUP Message. You can select — Speech, 3.1 KHz Audio. Default: Speech
- Select the **B - channel selection when SETUP message is received**⁵ as per your requirement.
- Select the **Progress Tone on Disconnect** check box, If you want the system to play the progress tone on the T1E1 Port when call is released by the remote end or released by the system. Default: Disabled.
- Select the **Send SETUP_ACK with PI** check box, if you want the system to send PI (Progress indicator) element in Setup Ack message. Default: Disabled.
- Select the **Send CALL PROCEED with PI** check box, if you want the system to send PI (Progress indicator) in Proceed message. Default: Disabled.
- Select the **Send ALERT with PI** check box, if you want the system to send PI (Progress indicator) in Alert message. Default: Disabled.
- Click **Submit** to save changes.

5. This parameter is not applicable in this version, it is meant for future use.

RBS Settings

If you have selected **RBS** as **Signaling Type**, configure the RBS parameters.



The screenshot shows a 'General' settings window with the following fields and values:

Field	Value
Carrier Type	T1
Signaling Type	RBS
Line Buildout Parameter	0-133 ft
Line Coding Mechanism	AMI Basic
Framing Mode	SF (D4)
Orientation Type	Terminal
Network Type	Public
Overlap Receiving Timer	15 Seconds
Pilot Number	

The 'Signaling Type' dropdown is highlighted with a red box, and a red arrow points to the 'Settings' icon next to it.

- Click **Settings**  .

- RBS parameters window opens.

The screenshot shows a configuration window titled 'RBS parameters'. It is divided into three main sections:

- Line Signaling Variables:**
 - Line Signaling Variant: E&M Wink Start FGD (dropdown)
 - Wink Timer: 160 msec (input field)
 - Wink Wait Timer: 30 msec (input field)
 - Wait Wink Timer: 5000 msec (input field)
 - Delay Duration: 100 msec (input field)
 - Start Delay Timer: 20 Seconds (input field)
- Register Signaling Variables:**
 - Register Signaling Variant: DTMF (dropdown)
 - Inbound ANIS/DNIS Format: ?ANI?DNIS? (dropdown)
 - Inbound Delimiter (?) Character: * (dropdown)
 - Outbound ANIS/DNIS Format: ?ANI?DNIS? (dropdown)
 - Outbound Delimiter (?) Character: * (dropdown)
- Maintenance:**
 - FDL Flag: ☐ Enable
 - FDL Protocol: Ansi T1 403 (dropdown)

At the bottom, there are four buttons: Submit (with a checkmark icon), Default (with a circular arrow icon), Copy (with a document icon), and Close (with an X icon).

Line Signaling Variables

- Select the **Line Signaling Variant**. You can select — FXS Loop Start, FXO Loop Start, FXS Ground Start, FXO Ground Start, E&M Immediate Dial/Start, E&M Wink Start or E&M Wink Start FGD. Default: E&M Wink Start FGD.
- Set the duration of the **Wink Timer**. This signifies the momentary Off-Hook condition to acknowledge end of an outgoing call. Valid range is 0001 to 9999 msec. Default: 160 msec.
- Set the duration of the **Wink Wait Timer**. This signifies the maximum time the system should wait before sending a wink start signal after an incoming seizure is detected. Valid range is 0001 to 9999 msec. Default: 30 msec.



Ensure that this timer is greater than the Wink Wait Timer of the other end.

- Set the duration of the **Wait Wink Timer**. This signifies the time for which SETU VTEP will wait for receiving the DNIS after sending the outgoing seizure signal. Valid range is 0001 to 9999 msec. Default: 5000 msec.



Make sure that this timer is greater than the Wait Wink Timer of the other end.

- Set the duration of the **Delay Duration**. This signifies the time after which the DNIS information is to be sent while making an outgoing call. Valid range is 0001 to 9999 msec. Default: 100 msec.
- Set the duration of the **Start Delay Timer**. This signifies the time for which SETU VTEP waits for receiving DNIS from the network. This timer is loaded on receiving the Off-hook (I/C Seizure) on the receive channel (while receiving an incoming call). Valid range is 0001 to 9999 msec. Default: 20 msec.

Register Signaling Variant

- Select the **Register Signaling Variant** for T1/E1 Ports. You can select — DTMF Default: DTMF.
- Select the **Inbound ANI/DNIS Format** for T1/E1 Ports. You can select — ANI, DNIS, ?ANI?, ?DNIS?, ?ANI?DNIS? or ?DNIS?ANI?. Default: ?ANI?DNIS?.
- Enter **Inbound Delimiter (?) Character** as per your requirement. Characters supported in this field are 0-9, #, *, A, B, C and D. Default: *
- Select the **Outbound ANI/DNIS Format** for T1/E1 Port. You can select — ANI, DNIS, ?ANI?, ?DNIS?, ?ANI?DNIS? or ?DNIS?ANI?. Default: ?ANI?DNIS?.
- Enter **Outbound Delimiter (?) Character** as per your requirement. Characters supported in this field are 0-9, #, *, A, B, C and D. Default: *

Maintenance

- FDL is used for communicating general maintenance information for transmitting user defined information within the T1 link. General maintenance information is in the form of Performance Message Report which is generated by SETU VTEP. Depending upon the FDL Protocol, the Performance Message Report is sent every second, or sent on request.
- Select the **FDL Flag** check box to enable, if the Network (Public or Private) to which SETU VTEP is connected supports FDL. Default: Disabled.
- After enabling the FDL Flag, select the **FDL Protocol** — ANSI T1 403 or AT&T 54016 — for reporting the performance monitoring. Default: ANSI T1 403.

Copy T1-RBS Parameters

- You can also copy the settings of a T1-RBS from one T1E1 port to the another using the **Copy** button. To do this,

- Click the **Copy** button. The **Copy T1-RBS Parameters** window opens.



Copy T1-RBS Parameters

from T1E1 Port to 1 to

☐ All

☐ T1E1 Port 1 ☐ T1E1 Port 2 ☐ T1E1 Port 3 ☐ T1E1 Port 4

☒ OK ☐ Cancel

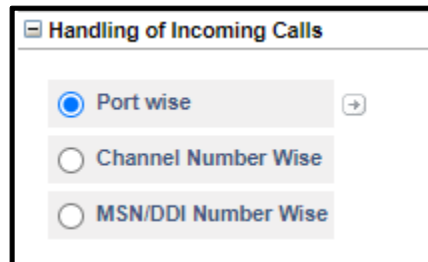
- In the **from T1E1 Port to** box, select the number of the T1-E1 Port you want to copy settings *From*. Select the check boxes of the desired port numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the T1E1 Ports, select the **All** check box.
- Click the **OK** button.
- Once you have copied the settings, you can again edit the specific parameters of T1-RBS you copied the settings to.
- Close the **Copy T1-RBS Parameters** window.
- Click **Submit** to save changes.
- Close the window to return to the main page.

Handling of Incoming Calls

Click **Handling of Incoming Calls** to expand.

Select the method to route the incoming calls from the T1E1 Port.

SETU VTEP provides three options for **Handling of Incoming Calls** — Port Wise, Channel Number Wise and MSN/DDI Number Wise. Default: Port Wise.



- **Port Wise:** Select this method to apply the call routing method for the entire port.
- **Channel Number Wise:** Select this method to apply a different call routing method for each channel. You can configure a different incoming call routing option for each channel.
- **MSN/DDI Number Wise:** Select this method to apply a different call routing method for each MSN number given by the Service Provider for the T1 Line. SETU VTEP allows you to configure upto 8 MSN Numbers.

Port Wise

To configure Handling of Incoming Calls Port Wise,

- Select the **Port Wise** check box.



- Click **Settings**  .

- The **Handling of Incoming Calls - Port Wise** window opens.

Handling of Incoming Calls - Port Wise	
Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this port	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ (+)
Allowed-Denied Logic	<input type="checkbox"/> Apply

- Keep the **Block calls received on this port** check box disabled.

Select this check box only if you do not want to route calls received on this port.

Destination Number Determination

Select the desired destination number determination method for routing incoming calls *with* and *without* CLI.

- To **Route all Incoming calls (with CLI)**, you may select from any of the following methods:
 - to a Fixed Destination Number
 - on the basis of Calling Party Number
 - on the basis of DDI Number
 - to the Called Party Number
 - after Answering the Call and Collecting the Digits
 Default: to the Called Party Number

Read further for instructions on selecting and configuring each of these destination number determination methods.



If the destination number to be dialed out is an IP Address, SETU VTEP will not check the Destination Port Determination Method. Instead, it will route the call using the SIP Trunk / Group programmed for IP Dialing. (See “[IP Dialing](#)” to know more).

Route to a Fixed Destination Number

In this method, calls received on the T1E1 Port are routed to a fixed destination number, which is configured for the T1E1 Port.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **to the Fixed Destination Number**.
- In the **Fixed Destination Number** box that appears, enter the desired destination number. The Destination Number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and. (dot/period). Default: Blank.
- Click **Submit** to save your settings.

Route on the basis of Calling Party Number

In this method, a call received on the T1E1 Port is routed to a specific number, as per the calling party's number. You must configure the calling party numbers in the *Calling Party Number Based Table*.

When there is an incoming call on the T1E1 Port, SETU VTEP will match the Calling Party Number with the entries of the Calling Party Number Based Table. If a match is found, the call is routed to the destination number configured for that Calling Party Number.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select on the basis of Calling Party Number.

Handling of Incoming Calls - Port Wise

Block calls received on this port

☐ Yes

Route all Incoming calls (with CLI)

on the basis of Calling Party Number

If no match found in the Calling Party Number Table, route calls

after Answering the Call and Collecting the Digits

Block Calls received without CLI on this port

☐ Yes

Route all Incoming calls (without CLI)

to the Called Party Number

Answering the call and collecting the digits

Prompt caller to enter PIN

☐ Enable

Dial Plan

1

First Digit Wait Timer

7

Seconds

Inter Digit Wait Timer

5

Seconds

End Of Dialing Digit

#

Minimum Number of digits that must be dialed by the caller

02

Maximum Number of digits that can be dialed by the caller

24

If No Digit dialed during First Digit Wait Timer

Disconnect Call

Allow making New Call using Access code

☐ Yes

Select Destination Port for routing calls

Fixed

Allowed-Denied Logic

☐ Apply

Submit

Default

Close

- Click **Settings** .

- The **T1E1 Port - Destination Number Determination: Calling Number Based** Table window opens.

1-100
101-200
201-300
301-400
401-499

T1E1 Port - Destination Number Determination: Calling Number Based

Index	Calling Number	Destination Number
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		
013		
014		
015		
016		
017		
018		
019		
020		
021		
022		
023		
024		

Submit
 Default All
 Close

- In **Calling Number**, enter the calling party numbers. The Calling numbers may consist of a maximum of 24 characters. Default: Blank.
- For each calling party number, enter a corresponding destination number in **Destination Number**. Destination numbers may consist of a maximum of 24 characters. Digits 0 to 9, *, # and (.) dot are allowed. Default: Blank.
- Click **Submit** to save your entries. Close the window to return to the **Handling of Incoming Calls - Port Wise** window.

You can also configure the **Calling Number Based** table from *Advanced Settings*. For instructions, see [“Destination Number Determination”](#) under *Advanced Settings*.

- Select a method for routing incoming calls with CLI that *do not match* with any entries in the Calling Party Number Based Table.

In the **If no match found in the Calling Party Number Table, route calls** box, select the desired method from the following options for processing the call:

- to a Fixed Destination Number
- on the basis of DDI Number
- to the Called Party Number
- after Answering the Call and Collecting the Digits


Default: after Answering the Call and Collecting the Digits

- If you want to enable PIN Authentication on the T1E1 Port, select the **Prompt caller to enter PIN** check box.

If you enable this check box, you must also configure the PIN Authentication Table. To know more about this feature and for detail instructions, see [“PIN Authentication”](#) under *Advanced Settings*.

- SETU VTEP supports 8 Dial Plans with total 64 entries in each table. When a user dials a number, it is compared with the Destination Number configured in the Dial Plan. If a match is found, the system routes the call immediately without waiting for End of Dialing and if a match is not found, the system will wait for the End of Dialing and then route the call as per the Destination Port Selection method configured.

Select the **Dial Plan** table number you configured for this port. If you have not configured the Dial Plan table you may do so now,

- Click **Settings**  the Dial Plan Table opens.
- Configure the numbers in the table. For detailed instructions, see [“Dial Plan”](#).
- Set the duration of the **First Digit Wait Timer**. This is the duration for which you want the system to wait for the caller to dial the destination number after the dial tone. Valid range is 01 to 99 seconds. Default: 7 seconds
- You may configure the following options as End of Dialing indication:
 - Set the duration of the **Inter Digit Wait Timer**. This is the duration for which you want the system to wait while receiving the digits dialed by the caller to consider it as End of Dialing. You may change this timer, if required. Valid range is 01 to 99 seconds. Default: 05 seconds.
 - In **End of Dialing Digit**, select # or * as termination digit the system should consider to detect end of dialing. Default: #
 - In **Minimum number of digits that can be dialed by the caller**, select the minimum number of digits to be dialed by the user for the system to consider it as a valid number. Valid range is 01 to 24 digits. Default: 2 digits.
 - In **Maximum Number of digits that can be dialed by the caller**, select the maximum number of digits to be dialed by the user for the system to consider it as End of Dialing. Valid range is 01 to 24 digits. Default: 24 digits.

When the caller dials a number, the system will match it with the above End of Dialing indications and accept the one that matches first.

- If the caller fails to dial the number during the First Digit Wait Timer, you can either have the system disconnect the call or route the call to a fixed destination number.

In the **If No Digit dialed during First Digit Wait Timer** box, select the desired option: **Disconnect the Call** or **Use Fixed Destination Number**. Default: Disconnect Call.

- If you selected **Use Fixed Destination Number**, enter the desired destination number in the **Fixed Destination Number** field. The Destination number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and . (dot/period). Default: Blank.



- *The First Digit Wait Timer is loaded as soon as the system answers the call.*
- *When you dial the first digit, the First Digit Wait Timer is stopped and the system loads the Inter Digit Wait Timer.*
- *SETU VTEP reloads the Inter Digit Wait Timer:*
 - *each time you dial a new digit till the termination digit is detected.*
 - *when you have dialed the maximum number of digits configured as End of Dialing.*
- If you want to enable the feature Making New Call using Access Code on the T1E1 Port, select the **Allow making New Call using Access Code** check box. For further details, see [“Making a New Call using Access Code”](#).
- Click **Submit** to save settings.

Route on the basis of DDI Number

In this method, incoming calls on the T1E1 Port are routed to specific numbers as per the DDI number received in the SETUP message on the T1E1 Port.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **on the basis of DDI Number**.

Handling of Incoming Calls - Port Wise

Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	on the basis of DDI Number ▼
Block Calls received without CLI on this port	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼
Allowed-Denied Logic	<input type="checkbox"/> Apply

- Click **Settings**  .




The **T1E1 Port - Destination Number Determination: DDI Number Based** Table opens.

1-100
101-200
201-300
301-400
401-500
501-600
601-700
701-800
801-900
901-1000

DDI Number Generation

T1E1 Port - Destination Number Determination: DDI Number Based

Index	DDI Number	Destination Number	Reverse DDI	
			Apply	Reference ID
001			<input type="checkbox"/>	01 ▼
002			<input type="checkbox"/>	01 ▼
003			<input type="checkbox"/>	01 ▼
004			<input type="checkbox"/>	01 ▼
005			<input type="checkbox"/>	01 ▼
006			<input type="checkbox"/>	01 ▼
007			<input type="checkbox"/>	01 ▼
008			<input type="checkbox"/>	01 ▼
009			<input type="checkbox"/>	01 ▼
010			<input type="checkbox"/>	01 ▼
011			<input type="checkbox"/>	01 ▼

 Submit
 Default All
 Close

- In **DDI Number**, enter the DDI Numbers allotted by your service provider.
- For each DDI Number, enter the corresponding destination number in **Destination Number**.
- To apply **Reverse DDI** for each number, select the check boxes under **Apply** and select the **Reference ID** for the number. Default: Apply Reverse DDI is disabled and Reference ID is 1.
- Click **Submit** to save and close the window to return to the **Handling of Incoming Calls - Port Wise** window.

You can also configure the **DDI Number Based** Table from *Advanced Settings*. For instructions, see [“Destination Number Determination”](#) under *Advanced Settings*.




Route to the Called Party Number

In this method, a call received on the T1E1 Port is routed to a specific number depending upon the called party number received in the SETUP Message on the T1E1 Port.

- To apply this method, in **Route all incoming calls (with CLI)**, select **to the Called Party Number**.

Handling of Incoming Calls - Port Wise

Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	to the Called Party Number ▼
Block Calls received without CLI on this port	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Select Destination Port for routing calls	Fixed ▼ ➔
Allowed-Denied Logic	<input type="checkbox"/> Apply

 Submit  Default  Close

Route after Answering the Call and Collecting the Digits

In this method, the incoming call is answered and dial tone is played to the caller, allowing the caller to dial the desired number. The number dialed by the caller is considered as the destination number.

Handling of Incoming Calls - Port Wise	
Block calls received on this port	<input type="checkbox"/> Yes
Route all Incoming calls (with CLI)	after Answering the Call and Collecting the Digits ▼
Block Calls received without CLI on this port	<input type="checkbox"/> Yes
Route all Incoming calls (without CLI)	to the Called Party Number ▼
Answering the call and collecting the digits	
Prompt caller to enter PIN	<input type="checkbox"/> Enable
Dial Plan	1 ▼ ➡
First Digit Wait Timer	7 Seconds
Inter Digit Wait Timer	5 Seconds
End Of Dialing Digit	# ▼
Minimum Number of digits that must be dialed by the caller	02 ▼
Maximum Number of digits that can be dialed by the caller	24 ▼
If No Digit dialed during First Digit Wait Timer	Disconnect Call ▼
Allow making New Call using Access code	<input type="checkbox"/> Yes
Select Destination Port for routing calls	Fixed ▼ ➡
Allowed-Denied Logic	<input type="checkbox"/> Apply

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, select **after Answering the Call and Collecting the Digits**.


The related parameters of this method appear under **Answering the call and collecting the digits**.

- If you want to enable PIN Authentication on the T1E1 Port, select the **Prompt caller to enter PIN** check box.

If you enable this check box, you must also configure the PIN Authentication Table. To know more about this feature and for detail instructions, see [“PIN Authentication”](#) under *Advanced Settings*.

- SETU VTEP supports 8 Dial Plans with total 64 entries in each table. When a user dials a number, it is compared with the Destination Number configured in the Dial Plan. If a match is found, the system routes the call immediately without waiting for End of Dialing and if a match is not found, the system will wait for the End of Dialing and then route the call as per the Destination Port Selection method configured.

Select the **Dial Plan** table number you configured for this port. If you have not configured the Dial Plan table you may do so now,

- Click **Settings**  the Dial Plan Table opens.
- Configure the numbers in the table. For detailed instructions, see ["Dial Plan"](#).
- Set the duration of the **First Digit Wait Timer**. This is the duration for which you want the system to wait for the caller to dial the destination number after the dial tone. Valid range is 01 to 99 seconds. Default: 7 seconds
- You may configure the following options as End of Dialing indication:
 - Set the duration of the **Inter Digit Wait Timer**. This is the duration for which you want the system to wait while receiving the digits dialed by the caller to consider it as End of Dialing. You may change this timer, if required. Valid range is 01 to 99 seconds. Default: 05 seconds.
 - In **End of Dialing Digit**, select # or * as termination digit the system should consider to detect end of dialing. Default: #
 - In **Minimum number of digits that can be dialed by the caller**, select the minimum number of digits to be dialed by the user for the system to consider it as a valid number. Valid range is 01 to 24 digits. Default: 2 digits.
 - In **Maximum Number of digits that can be dialed by the caller**, select the maximum number of digits to be dialed by the user for the system to consider it as End of Dialing. Valid range is 01 to 24 digits. Default: 24 digits.

When the caller dials a number, the system will match it with the above End of Dialing indications and accept the one that matches first.

- If the caller fails to dial the number during the First Digit Wait Timer, you can either have the system disconnect the call or route the call to a fixed destination number.

In the **If No Digit dialed during First Digit Wait Timer** box, select the desired option: **Disconnect the Call** or **Use Fixed Destination Number**. Default: Disconnect Call.

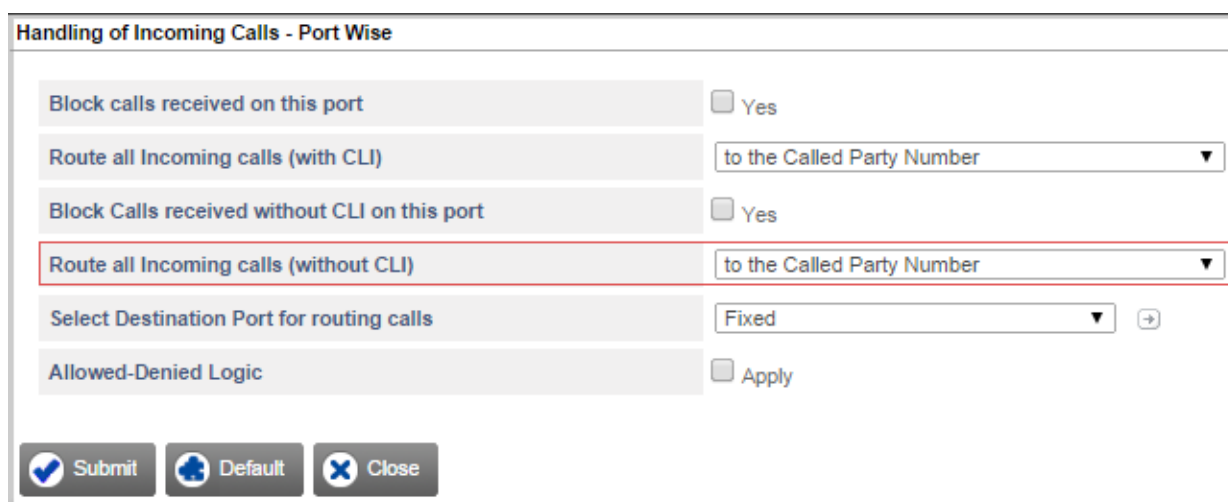
- If you selected **Use Fixed Destination Number**, enter the desired destination number in the **Fixed Destination Number** field. The Destination number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and . (dot/period). Default: Blank.



- *The First Digit Wait Timer is loaded as soon as the system answers the call.*
- *When you dial the first digit, the First Digit Wait Timer is stopped and the system loads the Inter Digit Wait Timer.*
- *SETU VTEP reloads the Inter Digit Wait Timer:*
 - *each time you dial a new digit till the termination digit is detected.*
 - *when you have dialed the maximum number of digits configured as End of Dialing.*
- If you want to enable the feature Making New Call using Access Code on the T1E1 Port, select the **Allow making New Call using Access Code** check box. For further details, see ["Making a New Call using Access Code"](#).

- Click **Submit** to save settings.
- If you do not want to route the incoming calls received without CLI, through this T1E1 Port, select **Block Calls received without CLI on this Port** check box.
- To **Route all Incoming calls (without CLI)**, you may select from any of the following methods:
 - to a Fixed Destination Number, see .
 - on the basis of DDI Number, see [“Route on the basis of DDI Number”](#).
 - to the Called Party Number, see [“Route to the Called Party Number”](#).
 - after Answering the Call and Collecting the Digits, see [“Route after Answering the Call and Collecting the Digits”](#)

Default: to the Called Party Number.



Destination Port Determination

For the port/channel/MSN number, select the Destination Port for routing calls from the following options:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number

Default: Fixed.

Read the description and follow the instructions for each of these destination port selection methods given below.



If the destination number to be dialed out is an IP Address, SETU VTEP will not check the Destination Port Determination Method. Instead, it will route the call using the SIP Trunk / Group programmed for IP Dialing. (To know more, see the feature description [“IP Dialing”](#)).

Fixed

In this method, calls received on the T1E1 Port are routed to a Fixed Destination Port, irrespective of the number dialed on the T1E1 Port.

To apply this method, do the following:

- In **Select Destination Port for routing calls**, select **Fixed** option.

Handling of Incoming Calls - Port Wise

Block calls received on this port ☐ Yes

Route all Incoming calls (with CLI) to the Called Party Number ▼

Block Calls received without CLI on this port ☐ Yes

Route all Incoming calls (without CLI) to the Called Party Number ▼

Select Destination Port for routing calls Fixed ▼ ➔

Allowed-Denied Logic ☐ Apply

Submit Default Close

- Click **Settings** ➔ .

The **Destination Port/Group for T1E1 Port** window opens.

Destination Port/Group for T1E1 Port

Edit	Routing Group	Fallback Routing Group
(+)	SIP Trunk 1 - 1 (Ascending)	None

Close

The default **Routing Group** and **Fallback Routing Groups** appear.

- If you wish to change the default Routing Group options, click **Edit** ➔ .

The **Edit Selective Port/Group for T1E1 Port** window opens.

Edit Selective Port/Group for T1E1 Port

Routing Group

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☒ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1

Fallback Routing Group ☐ Apply

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☐ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1

- Create the **Routing Group**.
- To create a routing group of *sequential T1E1 Port* as members,

Routing Group

☒ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☐ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1

- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,

- Select **T1E1 Group**. Default: 1.

Edit Selective Port/Group for T1E1 Port

Routing Group

☐ T1E1 Port 3 and Channel Number from 01 to 01 in Ascending order
☒ T1E1 Group 1
☐ SIP Trunk 001 to 001 in Ascending order
☐ SIP Group 1

Fallback Routing Group ☐ Apply

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order
☐ T1E1 Group 1
☐ SIP Trunk 001 to 001 in Ascending order
☐ SIP Group 1

- Click **Settings** .
- The **T1E1 Port - Groups** window opens.

T1E1 Port - Group

T1E1 Group 1
 Member Selection Method First Free

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1	01	30	Ascending
2	2	01	30	Ascending
3	3	01	30	Ascending
4	4	01	30	Ascending

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic [“Group”](#) under *Advanced Settings*.

- You may create the **Fallback Routing Group**.

- To do this,
 - Select the **Apply** check box.
 - Follow the same instructions provided earlier for creating *sequential* and *not-sequential* groups of T1E1 Ports and SIP Trunks.
- Click **Submit** to save changes. The **Edit** window closes.
- The entry you edited appears in the **Destination Port/Group for T1E1 Port** window.
- Close the **Destination Port/Group for T1E1 Port** window to return to the **Handling of Calls** window.

On the basis of Destination Number

In this method, incoming calls on the source port are routed to the destination port on the basis of the destination number (called party number) dialed by the caller.

You must configure the called party numbers in the **Destination Number Based** Table. SETU VTEP will match the called party number dialed by the caller with the entries of this table. If a match is found for the number in the table, the call is routed to the destination.

To apply this method, do the following:

- In **Select Destination Port** for routing calls, select **On the basis of Destination Number** option.

Handling of Incoming Calls - Port Wise

Block calls received on this port

☐ Yes

Route all Incoming calls (with CLI)

to the Called Party Number ▼

Block Calls received without CLI on this port

☐ Yes

Route all Incoming calls (without CLI)

to the Called Party Number ▼

Select Destination Port for routing calls

On the basis of Destination Number ▼ ➡

Allowed-Denied Logic

☐ Apply

Submit

Default

Close

- Click **Settings** ➡ .

The **T1E1 Port - Destination Port Determination - Destination Number Based** table window opens.

T1E1 Port - Destination Port Determination - Destination Number Based

<input type="checkbox"/>	Edit	Destination Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>	➡	No Match Found	SIP Trunk 1 - 1 (Ascending)	None

Total Records : 1
1

Testing

Enter the destination number to know which entry would be selected for routing

Add

Delete

Close

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 1000 entries.

- In **Destination Number**, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + *Wildcard Characters*) in this field. Valid characters are 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

Wildcard Characters

SETU VTEP supports following characters.

Character	Description
X (letter X)	X represents any single digit from 0 to 9.
#	When # is configured in a number string, it will not be considered as End of Dialing.
*	When * is configured in a number string, it will not be considered as End of Dialing.
+	+ (plus) can be configured as a first character of the Destination Number string in the <i>SIP Trunk-Destination Port Determination-Destination Number Based</i> table only.
[-]	Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket.
[,]	Comma within a bracket is used as a separator between the groups of numbers.
[^]	Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret.
T (letter T)	Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing.

- Create the **Routing Group**.

- To create a routing group of *sequential T1E1 Channels* as members,

Add Entry

Destination Number

Routing Group

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,
- Select **T1E1 Group**.

Routing Group

☐ T1E1 Port and Channel Number from to in order

☒ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- Select a **T1E1 Group** number. Default: 1.
- Click **Settings** .

- The **T1E1 Port - Group** window opens.

T1E1 Port - Group

T1E1 Group: 1

Member Selection Method: First Free

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1	01	30	Ascending
2	2	01	30	Ascending
3	3	01	30	Ascending
4	4	01	30	Ascending

Submit Default Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic “Group” under *Advanced Settings*.
- Similarly, you can create a group of *sequential* and *not-sequential* SIP Trunk Port.
- You may create the **Fallback Routing Group**.

Fallback Routing Group ☒ Apply

☒ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☐ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1


- To do this,
 - Select the **Apply** check box.
 - Follow the same instructions provided earlier for creating *sequential* and *not-sequential* groups of SIP Trunks.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **T1E1 Port - Destination Port Determination - Destination Number Based** table.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.

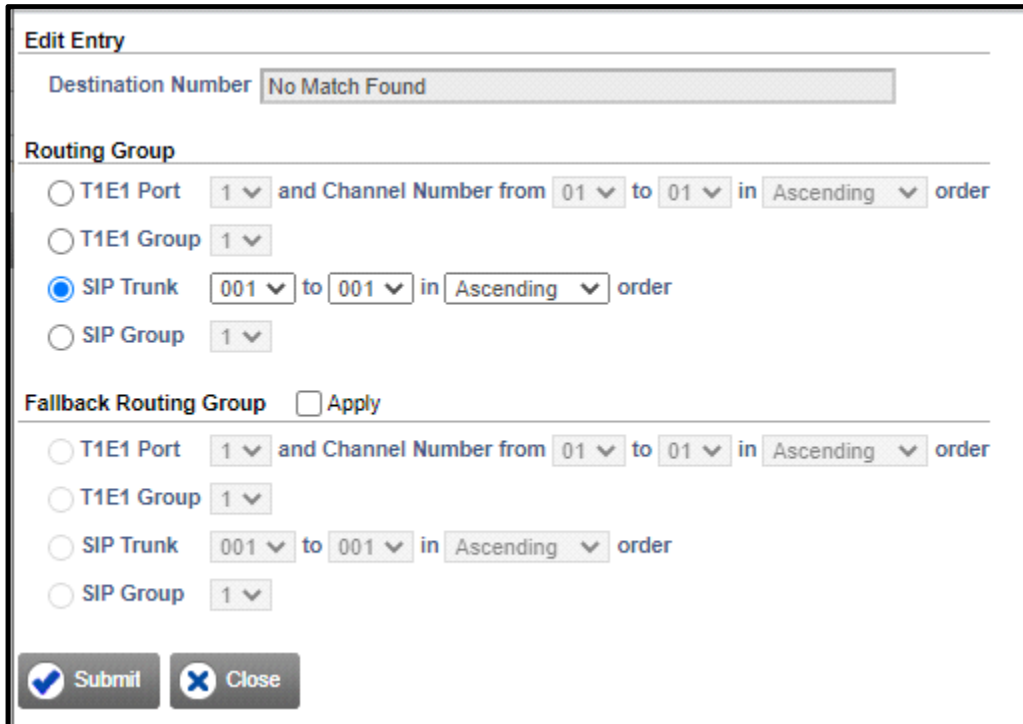


If there are multiple entries in the Destination Number Based table, to search a particular entry in the table, under *Testing* enter the desired number to know which entry would be selected for routing.

- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** .



Edit Entry

Destination Number

Routing Group

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☒ SIP Trunk to in order

☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

☒ Submit ☐ Close

- The **Edit Entry** window opens.
- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.

You can also configure the **Destination Number Based** Table from *Advanced Settings*. For instructions, see [“Destination Port Determination”](#) under *Advanced Settings*.

On the basis of Calling Party Number

In this method, incoming calls on the T1E1 Port are routed to a specific port as per the calling party's number.

To apply this method, do the following:

- In **Select Destination Port for routing calls**, select **On the basis of Calling Party Number** option.

Handling of Incoming Calls - Port Wise

Block calls received on this port

☐ Yes

Route all Incoming calls (with CLI)

to the Called Party Number ▼

Block Calls received without CLI on this port

☐ Yes

Route all Incoming calls (without CLI)

to the Called Party Number ▼

Select Destination Port for routing calls

On the basis of Calling Party Number ▼ ➡

Allowed-Denied Logic

☐ Apply

Submit

Default

Close

- Click **Settings** ➡ .

The **T1E1 Port - Destination Port Determination - Calling Number Based** table window opens.

T1E1 Port - Destination Port Determination - Calling Number Based				
<input type="checkbox"/>	Edit	Calling Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>	➡	No Match Found	SIP Trunk 1 - 1 (Ascending)	None
Total Records : 1		1		
+	Add	⊖	Delete	✕
Close				

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 499 entries.

Add Entry

Calling Number

Routing Group

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☒ SIP Trunk to in order

☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

☒ Submit ☐ Close

- In **Calling Number**, enter the number (max. 24 characters) from which you expect calls to be received. Valid digits are 0 to 9, *, #, (dot). Default: Blank.
- Create the **Routing Group**.
 - To create a routing group of *sequential T1E1 Channels* as members,

Routing Group

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.


Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,

- Select **T1E1 Group**.


Routing Group

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☒ T1E1 Group 1 

☐ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1

- Select a **T1E1 Group** number. Default: 1.
- Click **Settings**  .
- The **T1E1 Port - Group** window opens.




T1E1 Port - Group

T1E1 Group 1

Member Selection Method First Free

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1	01	30	Ascending
2	2	01	30	Ascending
3	3	01	30	Ascending
4	4	01	30	Ascending

 Submit
  Default
  Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic *“Group”* under *Advanced Settings*.
- You may create the **Fallback Routing Group**.

Fallback Routing Group ☒ Apply

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1


☒ SIP Trunk 001 to 001 in Ascending order

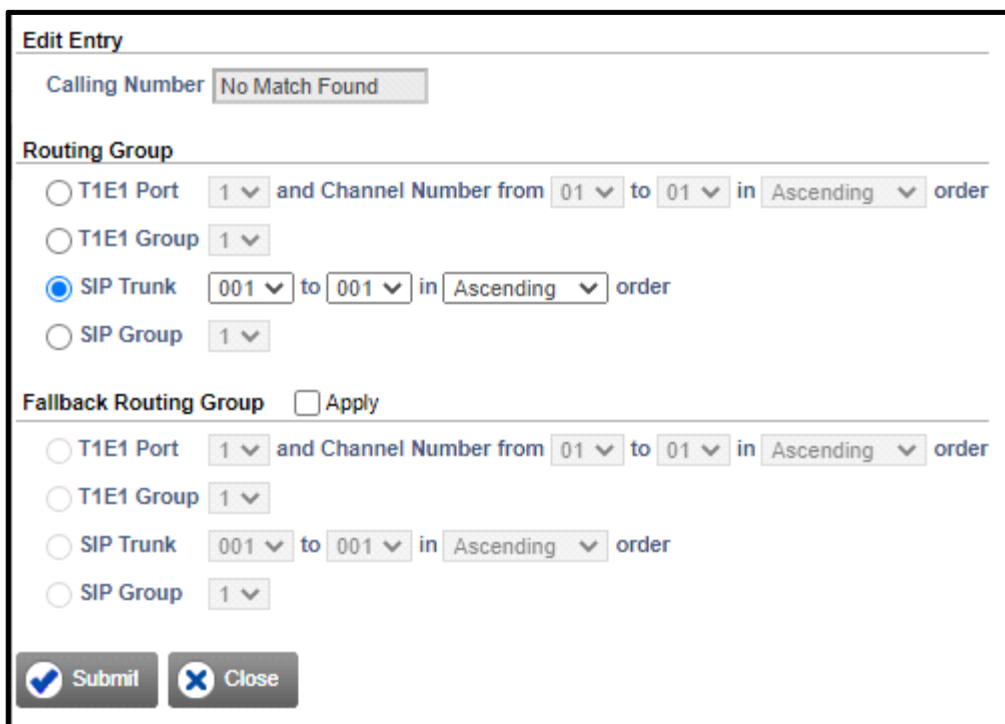
☐ SIP Group 1

- To do this,
- Select the **Apply** check box.

- Follow the same instructions provided earlier for creating *sequential* and *not-sequential* groups of T1E1 Ports and SIP Trunks.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **T1E1 Port - Destination Port Determination - Calling Number Based** table.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.
- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** .



Edit Entry

Calling Number

Routing Group

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☒ SIP Trunk to in order

☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- The **Edit Entry** window opens.
- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.

You can also configure the **Calling Number Based** Table from *Advanced Settings*. For instructions, see [“Destination Port Determination”](#) under *Advanced Settings*.

Allowed - Denied Logic

You can apply the Allowed-Denied logic on the T1E1 Port (source port) if you want to allow or restrict the dialing of particular numbers. You can use this feature for Toll Control.

The Allowed-Denied Number Logic makes use of two Number lists:

- **Allowed Numbers List:** This is the list of numbers that can be dialed out from the T1E1 Port.
- **Denied Numbers List:** This list contains the numbers that are to be restricted from being dialed out from the T1E1 Port.

When Allowed-Denied Logic is enabled on a source port, for each number dialed from the port, SETU VTEP uses the best-match-found logic to compare the dialed number with the Allowed Number list and the Denied Number list.

The number is allowed to be dialed, if it:

- matches with both lists.
- matches with Allowed Number list, but not with the Denied Number list.
- matches with neither the Allowed List nor the Denied List.

The number is denied, if it matches with the Denied Number list, but not with the Allowed Number list.

The system does not apply the Allowed-Denied Logic:

- When dialed number string matches with any Access Code.
- When dialed number string matches with any Emergency Number.
- When any one of the following is selected to Route all Incoming Calls (with CLI):
 - on the basis of Calling Party Number
 - to a Fixed Destination Number
 - on the basis of DDI Number

To apply Allowed - Denied Logic on the T1E1 Port,

- Select the **Allowed - Denied Logic** check box.



Allowed-Denied Logic	<input checked="" type="checkbox"/> Apply
Allowed Numbers List	01 ▼ ➔
Denied Numbers List	02 ▼ ➔

- In the **Allowed Number List**, select the list number you have configured with numbers you want to allow to be dialed out from the T1E1 Port. Default: 01

If you have not configured the Allowed Number List,


- Click **Settings** ➔.

- The **Number Lists** window opens.

Location	List 1	List 2	List 3	List 4
01	0	0		
02	1	1		
03	2	2		
04	3	3		
05	4	4		
06	5	5		
07	6	6		
08	7	7		
09	8	8		
10	9	9		
11	*	*		
12	#	#		

- You may configure the default Allowed Number List 1 or any other list. See [“Number Lists”](#) to configure the allowed numbers.
- Click **Submit** to save the Allowed Number List and close the window.
- In the **Denied Number List**, select the list number you have configured with numbers you want to restrict to be dialed out from the T1E1 Port. Default: 02

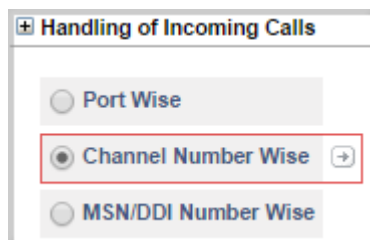
If you have not configured the Denied Number List,

- Click **Settings** . The **Number Lists** window opens.
- You may configure the default Denied Number List 2 or any other list. See [“Number Lists”](#) to configure the restrict numbers.
- Click **Submit** to save the Denied Number List and close the window.

Channel Number Wise

To configure Handling of Incoming Calls for each channel,

- Select the **Channel Number Wise** check box.



- Click **Settings**  .

- The **T1E1 Port 1 - Call Routing - Channel Number Wise** window opens.

Channel Number	Name	Call Routing
CH-1		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-2		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-3		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-4		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-5		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-6		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-7		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-8		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-9		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-10		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-11		Route calls to number received in SETUP message using SIP Trunk 1 - 1
CH-12		Route calls to number received in SETUP message using SIP Trunk 1 - 1

Submit
 Default
 Close
 Copy

- Click the respective channel number to configure the parameters.

T1E1 Port 1 Channel Number 1

Name

Handling of Incoming Calls - Channel Number Wise

Block calls received on this channel

☐ Yes

Route all Incoming calls (with CLI)

to the Called Party Number

Block Calls received without CLI on this channel

☐ Yes

Route all Incoming calls (without CLI)

to the Called Party Number

Select Destination Port for routing calls

Fixed

Allowed-Denied Logic

☐ Apply

Submit

Default

Copy

Close

Configure the routing parameters for each channel.

- Block calls received on this channel.
- Route all Incoming Calls (with CLI), see [“Destination Number Determination”](#).
- Block Calls received without CLI on this channel.
- Route all Incoming Calls (without CLI), see [“Destination Number Determination”](#).
- Select the destination port for routing calls, see [“Destination Port Determination”](#).
- Allowed-Denied Logic, see [“Allowed - Denied Logic”](#).
- Handling of Outgoing Calls, see [“Handling of Outgoing Calls”](#).

Copy Channel Based Routing Parameters

- You can also copy the settings of a T1E1 Channel to another T1E1 Channel using the **Copy** button. To do this,
- Click the **Copy** button. The **Copy T1E1 Port Channel based routing parameters from Channel Number** window opens.

Copy T1E1 Port Channel based routing parameters from Channel Number 01 to

All	<input type="checkbox"/>						
Ch 1	<input type="checkbox"/>	Ch 2	<input type="checkbox"/>	Ch 3	<input type="checkbox"/>	Ch 4	<input type="checkbox"/>
Ch 5	<input type="checkbox"/>	Ch 6	<input type="checkbox"/>	Ch 7	<input type="checkbox"/>	Ch 8	<input type="checkbox"/>
Ch 9	<input type="checkbox"/>	Ch 10	<input type="checkbox"/>	Ch 11	<input type="checkbox"/>	Ch 12	<input type="checkbox"/>
Ch 13	<input type="checkbox"/>	Ch 14	<input type="checkbox"/>	Ch 15	<input type="checkbox"/>	Ch 16	<input type="checkbox"/>
Ch 17	<input type="checkbox"/>	Ch 18	<input type="checkbox"/>	Ch 19	<input type="checkbox"/>	Ch 20	<input type="checkbox"/>
Ch 21	<input type="checkbox"/>	Ch 22	<input type="checkbox"/>	Ch 23	<input type="checkbox"/>	Ch 24	<input type="checkbox"/>
Ch 25	<input type="checkbox"/>	Ch 26	<input type="checkbox"/>	Ch 27	<input type="checkbox"/>	Ch 28	<input type="checkbox"/>
Ch 29	<input type="checkbox"/>	Ch 30	<input type="checkbox"/>				

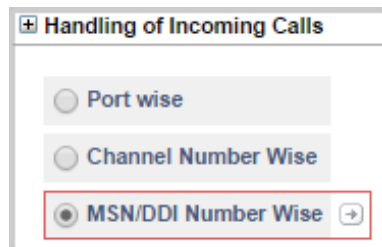
OK Close

- In the **Copy T1E1 Port Channel based routing parameters from Channel Number** box, select the number of the channel you want to copy settings *From*. Select the check boxes of the desired channel numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the channels, select the **All** check box.
- Click the **OK** button.
- Once you have copied the settings, you can again edit the specific parameters of the T1E1 Channel you copied the settings to.
- Close the **T1E1 Port 1 Channel Number 1** window.
- To configure any Channel, click the respective channel number on the **T1E1 Port 1 - Call Routing - Channel Number Wise** window and follow the same instructions as given above.
- Close the **T1E1 Port 1 - Call Routing - Channel Number Wise** window.

MSN/DDI Number Wise

To configure Handling of Incoming Calls for each MSN Number,

- Select the **MSN/DDI Number Wise** check box.



A configuration window titled "Handling of Incoming Calls" with three radio button options: "Port wise", "Channel Number Wise", and "MSN/DDI Number Wise". The "MSN/DDI Number Wise" option is selected and highlighted with a red rectangular box. A small right-pointing arrow icon is located to the right of the selected option.

- Click **Settings**  .
- The **T1E1 Port 1 - Call Routing - MSN/DDI Number Wise** window opens.

T1E1 Port 1 - Call Routing - MSN/DDI Number wise				
MSN Number	Name	Number	Total DDI Number	Call Routing
MSN-1			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-2			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-3			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-4			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-5			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-6			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-7			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1
MSN-8			100	Route calls to number received in SETUP message using SIP Trunk 1 - 1

- Click the respective MSN number to configure the parameters.

T1E1 Port 1 MSN Number 1

Name

Handling of Incoming Calls - Msn Number Wise

MSN Number 1

Total DDI Numbers

100

Block calls received on this MSN number

☐ Yes

Route all Incoming calls (with CLI)

to the Called Party Number

Block Calls received without CLI on this MSN number

☐ Yes

Route all Incoming calls (without CLI)

to the Called Party Number

Select Destination Port for routing calls

Fixed

Allowed-Denied Logic

☐ Apply

Submit

Default

Copy

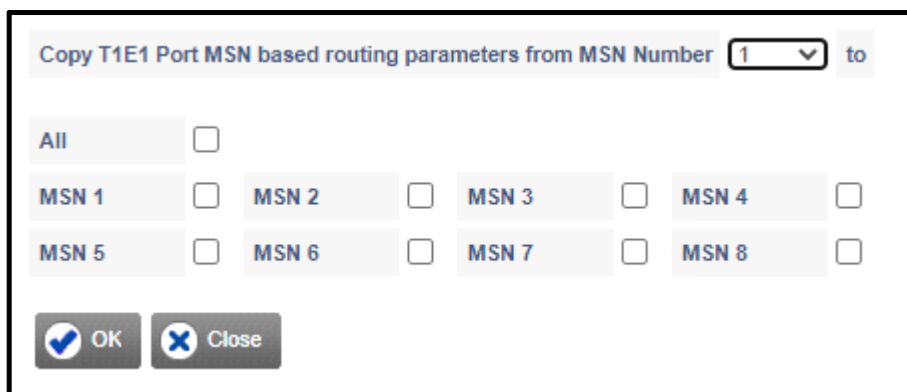
Close

Configure the routing parameters for each MSN number:

- **Name:** Assign a Name for identification.
- **MSN Number 1:** Enter the first **MSN Number** (max. 24 digits) provided by your Service Provider. Valid digits are 0-9, # and *. Default: Blank.
- **Total DDI Number:** Specify **Total DDI Numbers** provided by your Service Provider. Valid range is 1 to 9999. Default: 0100.
- Block calls received on this MSN Number.
- Route all Incoming Calls (with CLI), see [“Destination Number Determination”](#).
- Block Calls received without CLI on this MSN number.
- Route all Incoming Calls (without CLI), see [“Destination Number Determination”](#).
- Select the destination port for routing calls, see [“Destination Port Determination”](#).
- Allowed-Denied Logic, see [“Allowed - Denied Logic”](#).

Copy MSN Based Routing Parameters

- You can also copy the settings of a MSN Number to another MSN Number using the **Copy** button. To do this,
- Click the **Copy** button. The **Copy T1E1 Port MSN based routing parameters from MSN Number** window opens.

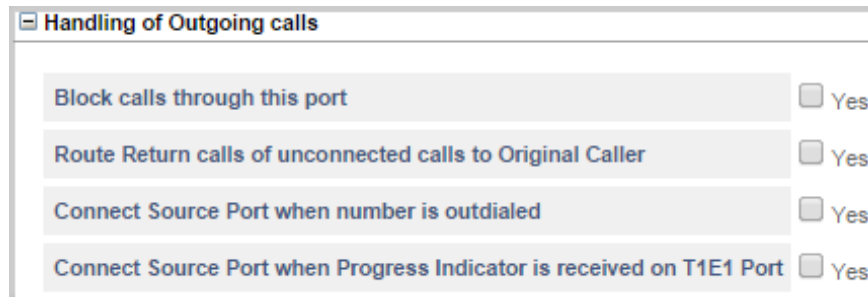


The screenshot shows a dialog box titled "Copy T1E1 Port MSN based routing parameters from MSN Number". At the top, there is a text field containing "1" followed by a dropdown arrow and the word "to". Below this, there are eight checkboxes arranged in two rows of four. The first row contains "All", "MSN 1", "MSN 2", "MSN 3", and "MSN 4". The second row contains "MSN 5", "MSN 6", "MSN 7", and "MSN 8". At the bottom of the dialog box, there are two buttons: "OK" with a checkmark icon and "Close" with an 'X' icon.

- In the **Copy T1E1 Port MSN based routing parameters from MSN Number** box, select the MSN Number you want to copy settings *From*. Select the check boxes of the desired MSN Numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the MSN Numbers, select the **All** check box.
- Click the **OK** button.
- Once you have copied the settings, you can again edit the specific parameters of the MSN Number you copied the settings to.
- Close the **T1E1 Port 1 MSN Number 1** window.
- To configure any MSN Number, click the respective MSN Number on the **T1E1 Port 1 - Call Routing - MSN/DDI Number Wise** window and follow the same instructions as given above.
- Close the **T1E1 Port 1 - Call Routing - MSN/DDI Number Wise** window.

Handling of Outgoing Calls

Click **Handling of Outgoing Calls** to expand.



Handling of Outgoing calls	
Block calls through this port	<input type="checkbox"/> Yes
Route Return calls of unconnected calls to Original Caller	<input type="checkbox"/> Yes
Connect Source Port when number is outdialed	<input type="checkbox"/> Yes
Connect Source Port when Progress Indicator is received on T1E1 Port	<input type="checkbox"/> Yes

When T1/E1 Port is determined as the destination port, numbers dialed from this port constitute outgoing calls.

For outgoing calls from T1/E1 Port, you can apply the features Automatic Number Translation (ANT) and Route Calls Returned Unconnected to Original Caller.

- Select the **Block calls through this port** check box, if you do not want to route outgoing calls through this port.
- Enable **Route Return calls of unconnected calls to Original Caller** check box, if you want SETU VTEP to route outgoing calls made from this port that return unconnected back to the original caller. Default: Disabled.

If you enable this feature, when an outgoing call is made using this port, and the Called Party is found busy or does not respond, SETU VTEP stores the number of the calling party, the number of the called party and this port (through which the outgoing call was made). A record of each such call is stored for the duration of the Unconnected Calls Record Delete Timer (configurable; default: 999 minutes).

If the called party returns the call before the expiry of this Timer, SETU VTEP checks whether *Apply RCOC only if the caller calls back on the same trunk from which the call was made* is enabled or not, and accordingly places the incoming call to the original calling party. To change the duration of this timer, delete records of such calls and enable/disable the *Apply RCOC only if the caller calls back on the same trunk from which the call was made* check box, see [“System Parameters”](#).

- To connect the Source Port with the Destination Port without waiting for the call on the Destination Port to mature, enable the **Connect Source Port when number is out-dialed** check box. Default: Disabled.

In all Destination Number Determination methods except *After Answering the Call and Collecting the Digits*, the Source Port gets connected to the Destination Port only after the call has matured, that is, the called party has answered the call. Until the call matures, the caller hears only Ring Back Tone played by the network.

By connecting the Source Port with the Destination Port immediately after the number is dialed, the caller can know the state of the call; if the called party is busy, not responding, not reachable or is rejecting the call.

- Enable **Connect Source Port when Progress Indicator is received on T1E1 Port** check box, to connect Source Port with the Destination Port as soon as Progress Indicator is received on T1E1 Port without waiting for the call on the Destination Port to mature. Default: Disabled.



If you enable **Connect Source Port** when **Progress Indicator** is received on **T1E1 Port**, you will not be able to provide the features *“Making a New Call using Access Code”* and *“Disconnecting a Call using Access Code”* to users.

- Click **Submit** to save settings.

DTMF Settings

- Click **DTMF Settings** to expand.

DTMF Settings	
DTMF Generation ON Time	100 msec
DTMF Generation OFF Time	100 msec

- Select the appropriate **DTMF Generation ON Time** for the T1E1 Port. This is the time for which the DTMF digit which is to be outdialed remains ON. Valid range is 50 to 250 msec. Default: 100 msec.
- Select the appropriate **DTMF Generation OFF Time** for the T1E1 Port. This is the time for which system should wait before dialing the successive DTMF digits so that the T1E1 network can detect the dialed digits. Valid range is 50 to 250 msec. Default: 100 msec.

Advanced

- Click **Advanced** to expand.

Advanced	
Automatic Number Translation(ANT) for Called Number	<input type="checkbox"/> Enable
Automatic Number Translation(ANT) Logic for Calling Number	<input type="checkbox"/> Enable
Allow Call Disconnection using Access code	<input type="checkbox"/> Yes
Custom Pulse Width	<input type="checkbox"/> Enable

- You can apply **Automatic Number Translation logic** on outgoing calls made from the T1E1 Port.

- To apply ANT logic on the Called Numbers, select the **Automatic Number Translation (ANT) for Called Number** check box. Default: Disabled.

Automatic Number Translation(ANT) for Called Number

☒ Enable

Use Automatic Number Translation Table

1 ▾ ➔

Pause Timer

2 ▾ Seconds

- In **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Called Numbers. Default: Table 1.

If you have not configured the Automatic Number Translation Table,

- Click **Settings** ➔.
- The **Automatic Number Translation Table** window opens.

1 2 3 4 5 6 7 8

Automatic Number Translation Table - 1

Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	
11		0	
12		0	

Examples of Number Pattern

Number	Strip Digit	Add Prefix	Remarks
\$\$\$	0	13152222	System will add the prefix '13152222' to every 3-digit dialed number.
8\$\$\$	1		System will strip off the first digit of all 4-digit dialed numbers that start with 8, and will dial out the remaining 3-digit number.
\$\$\$\$\$\$	0	1315	System will add the prefix '1315' to every 7-digit dialed number.

- You may configure the default Automatic Number Translation Table or any other Table. See [“Automatic Number Translation \(ANT\)”](#) to configure the ANT Table.
- Click **Submit** to save the ANT Table and close the window.
- Return to ANT parameter and assign the ANT Table you configured.
- Click **Submit**.

- Set the duration of the **Pause Timer**, if you have configured ^ (Pause) in the Add Prefix column of the ANT Table. Valid range is 1 to 9 seconds. Default: 2 seconds.
- To apply ANT logic on the Calling Numbers, click the **Automatic Number Translation (ANT) for Calling Number** check box. Default: Disabled.

Automatic Number Translation (ANT) for Calling Number
☒ Enable

Use Automatic Number Translation Table
5

- In the **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Calling Numbers. Default: Table 5.

If you have not configured the Automatic Number Translation Table,

- Click **Settings** .
- The **Automatic Number Translation Table** window opens.

1 2 3 4 **5** 6 7 8

Automatic Number Translation Table - 5

Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	
11		0	
12		0	

Examples of Number Pattern

Number	Strip Digit	Add Prefix	Remarks
\$\$\$	0	13152222	System will add the prefix '13152222' to every 3-digit dialed number.
8\$\$\$	1		System will strip off the first digit of all 4-digit dialed numbers that start with 8, and will dial out the remaining 3-digit number.
\$\$\$\$\$\$	0	1315	System will add the prefix '1315' to every 7-digit dialed number.

- You may configure the default **Automatic Number Translation Table - 5** or any other Table. See [“Automatic Number Translation \(ANT\)”](#) to configure the ANT Table.
- Click **Submit** to save the ANT Table and close the window.

- Return to ANT parameter and assign the ANT Table you configured.
- To enable the feature Disconnect Call using Access Code on the T1E1 Port, select the **Allow Call Disconnection using Access code** check box. To know more about this feature, see [“Disconnecting a Call using Access Code”](#).
- To customize the pulse width option and set the pulse shapes configure the **Custom Pulse** parameters. SETU VTEP generates pulse shapes which match the country standard, where it is installed. However, if the standard pulse shape does not match, SETU VTEP enables you to customize the pulse width to match your exact requirements.

To use customize pulse width option and set the pulse shape in 1 to 4 phases, keep the T1/E1 Custom Pulse Width (CPW) flag enabled.

Custom Pulse Width	<input checked="" type="checkbox"/> Enable
Custom Pulse Width Word 1	<input type="text" value="79"/>
Custom Pulse Width Word 2	<input type="text" value="79"/>
Custom Pulse Width Word 3	<input type="text" value="64"/>
Custom Pulse Width Word 4	<input type="text" value="64"/>

- In **Custom Pulse Width Word 1**, set the pulse width for setting pulse shape in the 1st phase. Valid range is 0 to 127. Default: 63.
- In **Custom Pulse Width Word 2**, set the pulse width for setting pulse shape in the 2nd phase. Valid range is 001 to 127. Default: 58.
- In **Custom Pulse Width Word 3**, set the pulse width for setting pulse shape in the 3rd phase. Valid range is 001 to 127. Default: 76.
- In **Custom Pulse Width Word 4**, set the pulse width for setting pulse shape in the 4th phase. Valid range is 001 to 127. Default: 0.

Copy T1E1 Port Parameters

- You can also copy the settings of a T1E1 Port to another T1E1 Port using the **Copy** button. To do this,

- Click the **Copy** button. The **Copy T1E1 Port Parameters** window opens.



Copy T1E1 Port Parameters from T1E1 Port 1 to

All ☐

T1E1 Port 1 ☐ T1E1 Port 2 ☐ T1E1 Port 3 ☐ T1E1 Port 4 ☐

☒ OK ☐ Close

- In the **Copy T1E1 Port Parameters from T1E1 Port** box, select the number of the port you want to copy settings *From*. Select the check box of the respective port numbers you want to copy the settings *To*.
- If you want to copy the settings *To* all the ports, select the **All** check box.
- Click the **OK** button.

Once you have copied the settings, you can again edit the specific parameters of the **T1E1** Port you copied the settings to.

Login Password

Login Password for Jeeves

To configure the system, you must log into the Jeeves using the Jeeves Password.



The default Jeeves Password is M@rXt3ID4\$. When you login for the first time, you will be prompted to change the password.

The password must be as per the specifications given below:

- It must not be less than 6 characters and can be of maximum 12 characters.
- Digits 0 to 9 and all ASCII characters are allowed, except Percentage %, Hash #, Equal to =, Plus +, And &, Backslash \, Less than <, Greater than >, Apostrophe ' , Double Quote " and Space.
- It must include atleast one upper-case, one lower-case, one number and one special character.



To provide additional security, if you enter a wrong password five times consecutively within 10 minutes, the system will block the source IP Address for 10 minutes. The notification (Warning) will be sent for this event to the SNMP Manager. See ["Simple Network Management Protocol \(SNMP\)"](#) for more details.

To change the Jeeves Password,

- Click the **Basic Settings** link to expand.
- Click the **Login Password** link.

Password Change

Jeeves

Current Password

New Password

Confirm New Password

Note :

Password must follow following requirements:

Minimum length must be 6 characters.

Maximum 16 characters

Password must include atleast 1 uppercase , 1 lowercase , 1 number and 1 special character.

Allowed characters are 0-9, a-z, A-Z, all special characters except %, =, #, +, &, \, <, >, " , ' and space.

Submit

Under **Jeeves**

- Enter **Current Password**.
- Enter **New Password**. Digits 0 to 9 and all ASCII characters are allowed, except Percentage %, Hash #, Equal to =, Plus +, And &, Backslash \, Less than <, Greater than >, Apostrophe ', Double Quote " and Space.

The new password must be:

- a minimum of 6 characters to a maximum of 12 characters.
- include atleast one upper-case, one lower-case, one number and one special character.
- In **Confirm New Password**, re-enter the new password to confirm.
- Click **Submit** button to save your new password.



- *Password for Jeeves is case-sensitive.*
- *When you default the system, Jeeves Password will not be set to default.*

Forgot the Login Password?

If you have already changed the default Jeeves Password (M@rXt3lD4\$) and are unable to recall or locate it, you can restore the default Jeeves Password using the Jumper.

Restoring Default Login Password

You may restore the Default Login Password by changing the position of Jumper **J13** on the PCB.

To do this,

- Make sure you are wearing an electrostatic discharge preventive wrist strap or belt and have a grounding mat.
- Switch off the power supply
- Remove the top cover of the enclosure.
- Locate and change the position of the Jumper **J13** from **AB** to **BC**.
- Switch ON the system and wait for 15 seconds.
- Switch OFF the system.
- Change the Jumper position from **BC** to the original position **AB**.
- Replace the enclosure cover.
- Switch ON the system.



When you change the jumper positions to restore default Jeeves Password (M@rXt3lD4\$), a few other parameters will also be set to default. See [“Restoring Default Settings by changing the Jumper Position”](#) for details.

Date-Time Settings

Real Time Clock

SETU VTEP has a Real Time Clock (RTC) to store date and time. When you select the Region, the RTC parameters are set automatically.


However, the RTC can drift over a long period. So, you may check and reset the RTC values at regular intervals to correct this drift.

To set the Real Time Clock,

- Click the **Basic Settings** link to expand.
- Click the **Date-Time Settings** link.
- The **Real Time Clock** parameters appear on your screen.


Real Time Clock (RTC)

Current Date: 25-Sep-2020

Current Time (HH:MM:SS): 14:43:34 


Current Day: Friday

Daylight Saving Time


DST Type: Disable 

SNTP Settings

SNTP Server Address:

Time Zone: India(GMT+05:30) 

Auto Date & Time Sync with SNTP During Power ON? ☐ Yes

 Submit

- Under **Real Time Clock (RTC)**, click **Settings**  of the **Current Time (HH:MM:SS)**.

- A new window opens.

- Set the **Current Date** in date-month-year format.
- Set the **Current Time** in hours-minutes-seconds format.

The current day will be displayed automatically for the date and time you set.

- Close the window.
- Click **Submit** to save RTC settings.
- Click the **Sync Date-Time with PC** button, if you want to sync the system's date and time with that of your PC.

Daylight Saving Time

Daylight Saving Time (DST) is the practice of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

Many countries of the world⁶ use it, though the start and end dates of DST vary by location and year.

SETU VTEP supports Daylight Saving Time adjustment to enable you to set the Date and Time⁷ of SETU VTEP forward and backward according to the DST convention followed in your country.

You can set DST by: **Day and Month** or **Date and Month**.



When SETU VTEP is set to default, your DST settings will remain unchanged.

To configure DST,

- Click the **Basic Settings** link to expand.
- Click the **Date and Time Settings** link.
- Go to **Daylight Saving Time** and do the following:

6. In most countries in Asia and Africa, and in certain countries of South America, DST is not observed.

7. SETU VTEP sets its Date and Time according to the **Time Zone** you selected, and synchronizes the time according to the **SNTP Server** you selected. See ["Region"](#).

- Select the **DST Type**. You may select **Auto** or **Custom**. If you do not want to apply DST select Disable. Default: Disabled.
- If you select **Auto**, you must select the **Region**. DST will be set automatically for the region you select.

Real Time Clock (RTC)

Current Date

22-Oct-2020

Current Time (HH:MM:SS)

10:05:07

→

Current Day

Thursday

Sync Date-Time with PC

Daylight Saving Time

DST Type

Auto

Region

Australia (Perth)

SNTP Settings

SNTP Server Address

Time Zone

Ireland(GMT)

Auto Date & Time Sync with SNTP During Power ON?

☐ Yes

Sync Date-Time with SNTP Server

Submit

- If you select **Custom**, you must configure the Time Offset and choose whether you want the DST to be applied by Day and Month or by Date and Month and define the DST Start and End time.

Real Time Clock (RTC)

Current Date

22-Oct-2020

Current Time (HH:MM:SS)

10:05:07

+

Current Day

Thursday

Sync Date-Time with PC

Daylight Saving Time

DST Type

Custom

Time Offset (Minutes)

0

Type

Day-Month wise

	Ordinal	Days	Month	Time	
				Hours	Minutes
DST Start	1st	Sunday	January	00	00
DST End	1st	Sunday	January	00	00

SNTP Settings

SNTP Server Address

Time Zone

Ireland(GMT)

Auto Date & Time Sync with SNTP During Power ON?

☐ Yes

Sync Date-Time with SNTP Server

Submit

- In **Time Offset**, enter the time in minutes which the system should consider to forward the clock at the start of DST and to set the clock back when DST ends. Default: 60 minutes.
- Select the desired **Type** of DST as:
 - **Day-Month Wise**, if the DST in your country starts and ends on a particular day of the month. For example, if DST starts on the Second Sunday of March and ends on the First Sunday of October.
 - or–
 - **Date-Month Wise**, if the DST in your country starts and ends on a particular date of the month. For example, if DST starts on October 12 and ends on March 15.

Default: Day-Month Wise.

- If you select **Day-Month Wise** option, you need to configure the Start and End time for DST.

DST Start

- Select the **Ordinal** day of the month when DST begins: 1st, 2nd, 3rd, 4th or 5th.
- Select the **Day** of the month when DST begins: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
- Select the **Month** when DST begins: January to December.
- Set the **Time** when you want DST to begin in 24 hours format.

Default: 1st Sunday March, Time 00 hours and 00 minutes.

DST End

- Select the **Ordinal** day of the month when DST ends: 1st, 2nd, 3rd, 4th or 5th.
- Select the **Day** of the month when DST ends: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
- Select the **Month** when DST ends: January to December.
- Set the **Time** when you want DST to end in 24 hours format.

Default: 1st Sunday September, Time 00 hours and 00 minutes.



When the DST of a particular country starts or ends on the Last Sunday or any other day, for instance, the last Tuesday, last Friday of the month, always set the Ordinal Number as '5th'.

- If you select **Date-Month Wise** option, configure the following parameters:

DST Start

- Select the **Month** when DST begins — January to December.
- Select the **Date** on which DST begins — 1 to 31.
- Set the **Time** when DST begins in 24 hours format.

DST End

- Select the **Month** when DST ends — January to December.
- Select the **Date** on which DST ends — 1 to 31.
- Set the **Time** when DST ends in 24 hours format.

- Click **Submit** to save your DST settings.

Example: If you are installing SETU VTEP in a country in the European Union, as per the European Summer Time, the DST would start on the Last Sunday in March and end on the Last Sunday in October each year. Clocks are advanced by one hour at 01:00 hours GMT at the start of DST and set back by one hour at 01:00 hours GMT when DST ends. Let us take the example of setting DST, if SETU VTEP were installed in Berlin, Germany. In the year 2011, the DST in Berlin starts on Sunday, 27 March at 02:00:00 hours and ends on Sunday 30 October at 03:00:00 hours. To set DST you must do the following:

1. Select the **DST Type** as **Custom**.
2. Set the **Time Offset** as 60 minutes.
3. Select the option **Date-Month Wise** as **Type**⁸.
4. Configure the **DST Start** as follows:
 - Select **March** as the **Month**.
 - Select **27th** as the **Date**.
 - Set **Time** to 01:59:59
5. Now, go to the option **DST End**, and configure as follows.
 - Select **October** as the **Month**.
 - Select **30th** as the **Date**.
 - Set **Time** to 02:59:59.

8. You can also select Day-Month-wise as Type.

6. Click **Submit** to save DST settings.

On Sunday 27 March at 01:59:59 the SETU VTEP will set the clock forward by 1 hour. On Sunday 30 October, SETU VTEP sets the clock back by 1 hour at 02:59:59.

SNTP Settings

To use SNTP for synchronizing with the Real Time Clock,

- Under **Basic Settings**, click the **Date and Time Settings** link.
- Go to **SNTP Settings** on this page.



SNTP Settings	
SNTP Server Address	<input type="text"/>
Time Zone	India(GMT+05:30) ▼
Auto Date & Time Sync with SNTP During Power ON?	<input type="checkbox"/> Yes <input type="button" value="Sync Date-Time with SNTP Server"/>

- In **SNTP Server Address**, enter the Time Server Address. The SNTP Server address can be of maximum 40 characters. Default: Blank.
- By default, the time zone for the country/region where SETU VTEP is installed is automatically selected when you select 'Region'. If required you may change the time zone by selecting the desired country/region from the **Time Zone** list. Default: India (GMT+05:30).
- If you want the system to synchronize date and time with the SNTP server automatically at Power On, select the **Auto Date and Time Sync with SNTP during Power ON?** check box. At every power ON, SETU VTEP will synchronize its date and time with the Time Server address you have entered as SNTP Server Address.

By default, Auto Date and Time Sync with SNTP during Power ON is disabled.

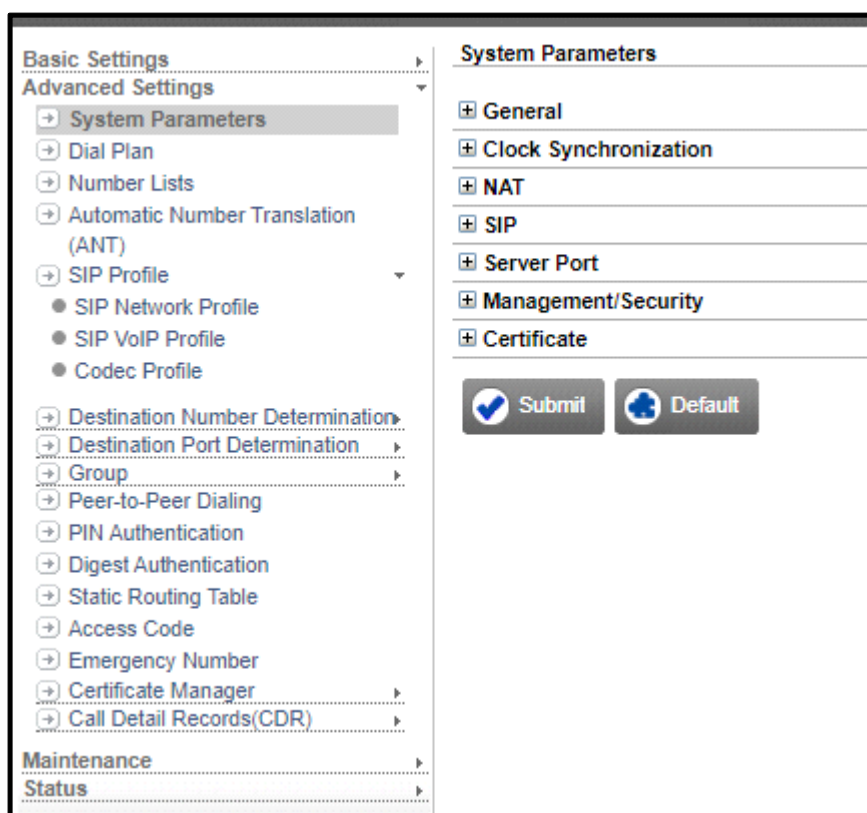
- To synchronize date and time of SETU VTEP with the SNTP server whenever required, click the **Sync Date and Time Server with SNTP** button.
- Click **Submit** to save the changes.

System Parameters

System Parameters are general parameters, related to features and facilities that are applied system-wide, such as System Name, NAT and SIP related parameters, Server Port, Certificates, DMZ etc.

To configure the System Parameters,

- Click the **Advanced Settings** link to expand.
- Click the **System Parameters** link.
- The **System Parameters** page opens.



General Parameters

- Click **General** to expand and configure the following.

System Name	<input type="text"/>
SIP Trunk for IP Dialing	SIP Group ▼ 1 ▼
Play Routing Tone	<input type="checkbox"/> Yes
Call Release Timer	<input checked="" type="checkbox"/> Apply
Release Timer	999 Minutes
Routing Group Busy Wait Timer	1 Seconds
Error Tone Timer	7 Seconds
Error Tone Delay Timer	0 Seconds
Unconnected Calls Record Delete Timer	999 Minutes <input type="button" value="Clear Unconnected Call Records"/>
Remove Country Code from CLI received	<input type="checkbox"/> Yes
Apply RCOC only if the caller calls back on the same trunk from which the call was made	<input type="checkbox"/> Yes

- In **System Name**, enter a name that you wish to assign to SETU VTEP. Naming SETU VTEP will serve as an identifier when there are more than one SETU VTEPs connected in the same LAN network.

Valid range is 40 characters. Default: Blank.

- To use the IP Dialing feature, that is, to directly dial IP Addresses, in **SIP Trunk for IP Dialing** select a SIP Trunk or SIP Group for routing the call to the IP Address.

The valid range for the SIP Trunk is 001 to 125 and for SIP Group is 1 to 9.

When you assign a SIP Trunk, make sure you have enabled the SIP Trunk and configured its necessary parameters. For further details, see [“SIP Trunk”](#) under *Basic Settings*.

When you assign a SIP Group, make sure you have configured the SIP Group. For further details, see [“Group”](#).

Default: SIP Group 1

To know more about this feature, see [“IP Dialing”](#).

- Select the **Play Routing Tone** check box, if you want the system to play routing tone while routing the call to the destination port. During an outgoing call, the routing tone indicates that the call is in progress. Default: Disabled.
- Select the **Call Release Timer** check box, if you want the system to release the ports involved in a call after a definite time period. Default: Enabled.

This timer is loaded when a call gets matured and stops whenever a port involved in a call is released.

- Set the duration of the **Release Timer**. Valid range is 001 to 999 minutes. Default: 999 minutes.
- Set the duration of the **Routing Group Busy Wait Timer**. This timer defines the duration for which you want SETU VTEP to search for a free destination port in the Routing Group and the Fallback Routing

Group in order to route and place the call. This timer is loaded when no destination port is free in both the Routing Group and the Fallback Routing Group. Valid range is 1 to 99 seconds. Default: 1 second.

This timer is loaded when a user performs a transfer activity. The user (transferor) is notified of the status of the transfer activity within the time period you have set for this timer.

Valid range is 1 to 999 seconds. Default: 60 seconds.

- Set the duration of the **Error Tone Timer**. This timer defines the duration for which you want SETU VTEP to will play the Error Tone. Valid range is 0 to 9 seconds. Default: 7 seconds.
- Set the duration of the **Error Tone Delay Timer**. This timer defines the duration for which you want SETU VTEP to play the Error Tone whenever a call is disconnected during speech. Valid range is 00 to 99 seconds. Default: 0 seconds.
- **Unconnected Calls Record Delete Timer**: SETU VTEP offers a feature on the T1/E1 port and SIP trunks whereby outgoing calls made from these ports that return unconnected are routed to the original caller.

To use this feature on a T1/E1 port or SIP Trunk, you must enable **Route calls returned unconnected to Original Caller** under *Handling of Outgoing Calls* on the port.

When an outgoing call is made using the port on which this feature is enabled, and the Called Party is found busy or does not respond, SETU VTEP stores the number of the Calling Party, the number of the Called Party and the source port through which the outgoing call was made. A record of each such call is stored for the duration of the *Unconnected Calls Record Delete Timer* (configurable; default: 999 minutes). If the called party returns the call before the expiry of this Timer, this incoming call is placed to the original calling party.

The records of 200 such Unconnected Calls are stored using FIFO method, and deleted on the expiry of the Record Delete Timer, or when the call returned by the called party is returned to the original caller and answered by the caller.

By default, the Unconnected Calls Record Delete Timer is set to 999 minutes. If required, you may change, this timer to the desired duration.

You can also delete the records of unconnected calls any time, without waiting for this timer, by clicking the **Clear Unconnected Call Records** button.

- Select the **Remove Country Code from CLI received** check box, if you want the system to remove the country code from the CLI received on the source port before presenting it to the destination port. Default: Disabled.

Make sure you have configured the **"Country Code"** under *Region* in the *Basic Settings*.

- **Apply RCOC only if the caller calls back on the same trunk from which the call was made**: If you want SETU VTEP to match the Trunk Port Parameters (Trunk Port Number and Type) of an incoming call with the entry in the RCOC table while applying RCOC logic on the **"SIP Trunk"**, **"E1 Port"** and **"T1 Port"**, select this check box. Default: Disabled.

If this check box is enabled, SETU VTEP will match Trunk port parameters of the incoming call with

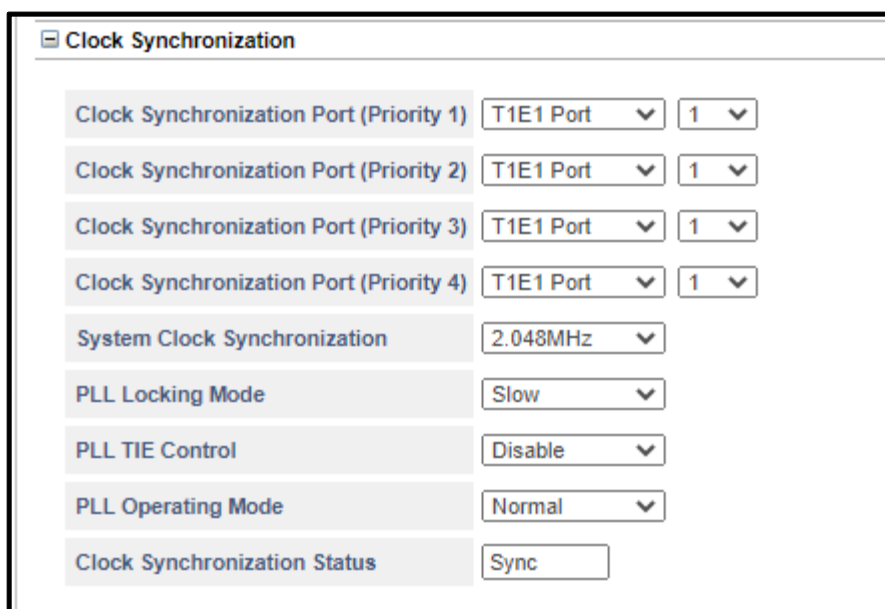
- the entry stored in RCOC table. If a match is found, it will route the incoming call to original caller.

Clock Synchronization

When SETU VTEP transmits or receives the data from the external lines, there must be proper synchronization between the transmitter and receiver. In case of improper synchronization, clock slips can occur. A clock slip can alter the data stream which could result in either the loss of data or the addition of unwanted noise in the data.

Clock Synchronization can be done in three ways— using the data clock, using the external clock (clock is sent by the network on a dedicated cable pair) or using the internal clock. SETU VTEP does not support the external clock. When the SETU VTEP is connected to the PSTN, then it is recommended to extract the clock from the incoming data whereas if the SETU VTEP is used to form a part of a private network, you are recommended to use the internal clock. For example, if a private network is formed by connecting three SETU VTEP, then one system should be programmed as master clock whereas other two should be programmed in the slave mode. If two or more T1E1 Port is connected to the PSTN (or a Private Network) then in such case, clock will be extracted from the first T1E1 port.

- Click **Clock Synchronization** to expand and configure the following.



The screenshot shows the 'Clock Synchronization' configuration window. It contains several settings:

Setting	Value
Clock Synchronization Port (Priority 1)	T1E1 Port 1
Clock Synchronization Port (Priority 2)	T1E1 Port 1
Clock Synchronization Port (Priority 3)	T1E1 Port 1
Clock Synchronization Port (Priority 4)	T1E1 Port 1
System Clock Synchronization	2.048MHz
PLL Locking Mode	Slow
PLL TIE Control	Disable
PLL Operating Mode	Normal
Clock Synchronization Status	Sync

- In **Clock Synchronization Port (Priority 1)**, select the desired T1E1 or None — which you want as the first priority and also select the respective Port Number.

Similarly, configure the **Clock Synchronization Port (Priority 2)**, **Clock Synchronization Port (Priority 3)** and **Clock Synchronization Port (Priority 4)**.

- In **System Clock Synchronization**, select the desired frequency for the synchronization. You can select — 8 KHz Derived, 8 KHz, 2.048 MHz or 1.54 MHz.

Select System Clock Synchronization option as **8 KHz**.

Select System Clock Synchronization option as **2.048 MHz**, only for T1E1 Port (E1 line).

Select System Clock Synchronization option as **1.54 MHz**, only for T1E1 Port (T1 line).

Default: 2.048 MHz for all the countries excluding USA. For USA, it is 1.54 MHz.



The system will restart when the frequency is changed.

- In **PLL Locking Mode**, select the speed required for clock synchronization. You can select — Fast or Slow. Default: Slow.
- In **PLL TIE Control**, you can select — Enable or Disable — as per your requirement. Default: Disabled.
- In **PLL Operating Mode**, you can select — Normal, Hold Over or Free Run — as the operating mode as per your requirement. Default: Normal
- In **Clock Synchronization Status**, the synchronization status of the clock is displayed.

NAT

- Click **NAT** to expand and configure the following.

- In **STUN Server Address: Port** (for WAN and Virtual WAN), enter the STUN Server Address and the Listening Port of the STUN Server.

STUN (Simple Traversal of UDP through NAT) server facilitates the traversing through most of the NATs, except the symmetric NATs. Configure this only when SETU VTEP is located behind a NAT router which is not symmetric.

The STUN Server Address can have maximum 40 characters.

Valid range is 1024 to 65535. Default: 3478.

- Clear the **Use SIP Port Fetched using STUN** check box, if SETU VTEP is located behind the NAT router and you have forwarded the SIP Listening Port of the SETU VTEP in the router.

Keep the **SIP Port fetched using STUN** check box enabled, if you have *not* forwarded the SIP Listening Port in the router.



*Make sure you have selected **NAT Type** as **STUN** in the SIP Trunk. See [“SIP Network Profile”](#).*

- In **Router's Public IP Address** (for WAN and Virtual WAN), enter the public IP address of the NAT router behind which the system is located. Default: Blank.

Configure this only when the system is located behind the NAT router and a Static IP Address is assigned as the Public IP Address of the Router.



*Make sure you have selected **NAT Type** as **Router's IP Address** in the SIP Trunk. See "[SIP Network Profile](#)".*

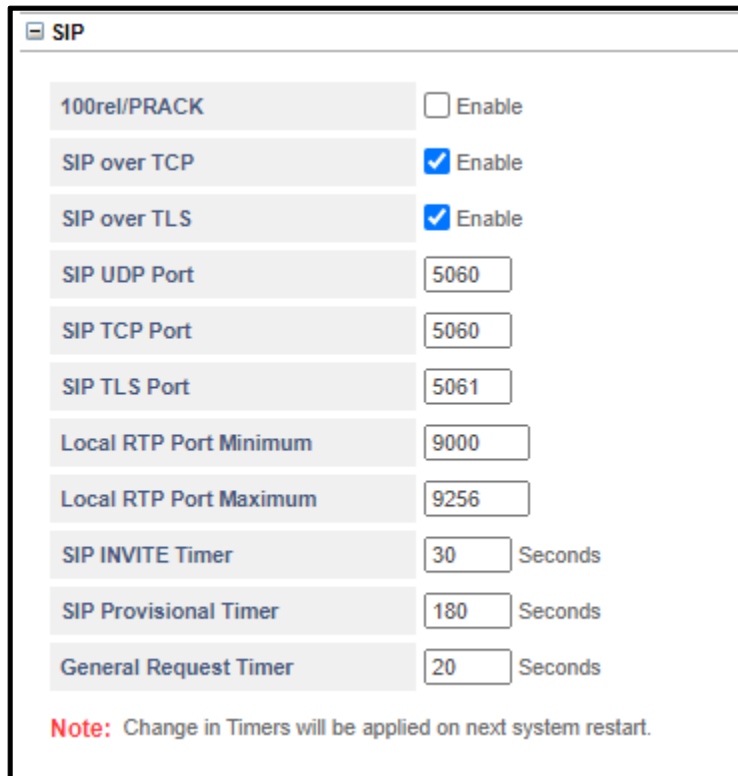
- Select the **UDP NAT Keep Alive** check box, if you want NAT Keep Alive messages to be sent to refresh the binding in the NAT router when SETU VTEP is connected behind a NAT router and the SIP messages are transported over UDP. Default: Disabled.

UDP NAT Keep Alive	<input checked="" type="checkbox"/> Enable
Keep Alive Message	<input checked="" type="radio"/> NOTIFY <input type="radio"/> REGISTER
Interval	<input type="text" value="120"/> Seconds

- Select the type of **Keep Alive Message** to be sent. You can select — REGISTER or NOTIFY as per your requirement. Default: NOTIFY.
- In **Interval**, set the time period after which you want the system to send Keep Alive messages. This time period should be less than the NAT binding timer of the router. Valid range is 001 to 999 seconds. Default: 120 seconds.
- Select the **TCP NAT Keep Alive** check box, if you want NAT Keep Alive messages to be sent to refresh the binding in the NAT router when SETU VTEP is connected behind a NAT router and the SIP messages are transported over TCP. Default: Disabled.
- In **Interval**, set the time period after which you want the system to send Keep Alive messages. This time period should be less than the NAT binding timer of the router. Valid range is 001 to 999 seconds. Default: 120 seconds.
- Click **Submit** to save changes.

SIP

- Click **SIP** to expand and configure the following.



The screenshot shows a configuration window titled "SIP" with a list of settings. Each setting has a label and a corresponding input field or checkbox. The settings are as follows:

Setting	Value
100rel/PRACK	<input type="checkbox"/> Enable
SIP over TCP	<input checked="" type="checkbox"/> Enable
SIP over TLS	<input checked="" type="checkbox"/> Enable
SIP UDP Port	5060
SIP TCP Port	5060
SIP TLS Port	5061
Local RTP Port Minimum	9000
Local RTP Port Maximum	9256
SIP INVITE Timer	30 Seconds
SIP Provisional Timer	180 Seconds
General Request Timer	20 Seconds

Note: Change in Timers will be applied on next system restart.

- Select **100rel/PRACK** check box, if you want SETU VTEP to use 100rel SIP trunk for reliable transmission of SIP provisional responses and PRACK for Provisional Acknowledgement. Default: Disabled.
- Select **SIP Over TCP** check box, if you want SETU VTEP to receive SIP messages over TCP. Default: Enabled.

SETU VTEP supports transporting of SIP messages over User Datagram Protocol (UDP) as well as Transfer Control Protocol (TCP) connection.

Despite the advantages that SIP Over TCP offers, it is more common to use UDP to transport the SIP messages.

Make sure that you have selected *TCP* as the *SIP Transport* option and have enabled the *TCP (Fallback to UDP)* check box. See [“Advanced”](#) in [“SIP Network Profile”](#).

- Select **SIP Over TLS** check box, if you want SETU VTEP to receive SIP messages over TLS. Default: Enabled.

SETU VTEP supports transporting of SIP messages over TLS. TLS protects SIP signaling against loss of integrity, confidentiality and replay.

Make sure that you have selected *TLS* as the *SIP Transport* option. See [“Advanced”](#) in [“SIP Network Profile”](#).

- Configure the **SIP UDP Port**. This is the port on which SETU VTEP listens for SIP messages transported over UDP.
 - This port is also used as the source port for sending SIP messages to the remote peer. Valid range is 1031 to 65534. Default: 5060.
- Configure the **SIP TCP Port**. This is the port on which SETU VTEP listens for SIP messages transported over TCP.
 - This port is also used as the source port for sending SIP messages to the remote peer. Valid range is 1031 to 65534. Default: 5060.
- Configure the **SIP TLS Port**. This is the port on which the SETU VTEP listens for SIP messages transported over TLS.
 - This port is also used as the source port for sending SIP messages to the remote peer. Valid range is 1031 to 65534. Default: 5061.
- In **Local RTP Port Minimum**, enter the desired minimum RTP Port Number. Valid range is 1032 to 65535. Default: 8000.
- In **Local RTP Port Maximum**, enter the desired maximum RTP Port Number. Valid range is 1032 to 65535. By default, the **Local RTP Port Maximum = Local RTP Port Minimum + [Maximum calls⁹ supported by the product x 2]**.
- Set the duration of the **SIP INVITE Timer**. This timer defines the time period for which you want SETU VTEP to wait for the response from the called party after sending the INVITE message. This timer starts after sending INVITE message to the called party and stops after receiving the provisional or the final response or when the call gets disconnected.

On expiry of the timer, SETU VTEP terminates the call process and gives an error tone to the user. Valid range is 10 to 200 seconds. Default: 30 seconds.

- Set the duration of the **SIP Provisional Timer**. This timer defines the time period for which you want SETU VTEP to wait for the final response after receiving the provisional response from the called party. This timer starts when provisional response is received from the called party and stops after receiving the final response from the called party or when then call gets disconnected.

On the expiry of the timer, SETU VTEP terminates the call process and gives error tone to the user. Valid range is 10 to 200 seconds. Default: 180 seconds.

- Set the duration of the **General Request Timer**. This timer defines the time period for which you want SETU VTEP to wait for the response to the transaction request. This timer starts when a transaction is initiated and stops after receiving the response to the request. On expiry of the timer, the SETU VTEP clears the transaction. Valid range is 10 to 60 seconds. Default: 20 seconds.
- Click **Submit** to save changes.

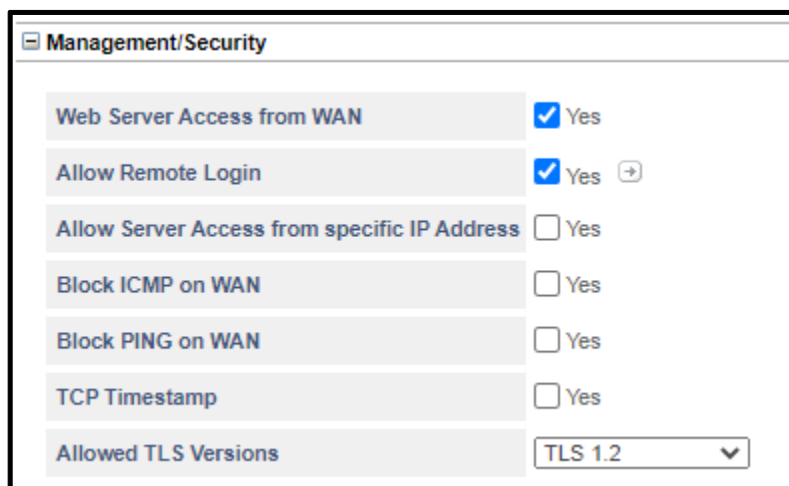


If you have made any changes in the NAT or SIP Parameters, all the ongoing calls will be disconnected when you submit the page to save the changes.

9. The maximum number of calls depends upon the number of Vocoder Channels supported.

Management/Security

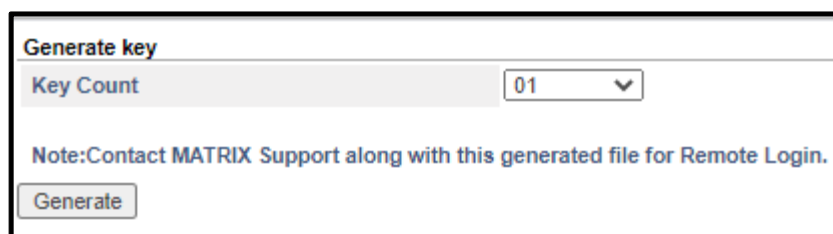
- Click **Management/Security** to expand and configure the following.



The screenshot shows the 'Management/Security' configuration panel. It contains several settings with checkboxes or dropdown menus:

Setting	Value
Web Server Access from WAN	<input checked="" type="checkbox"/> Yes
Allow Remote Login	<input checked="" type="checkbox"/> Yes (+)
Allow Server Access from specific IP Address	<input type="checkbox"/> Yes
Block ICMP on WAN	<input type="checkbox"/> Yes
Block PING on WAN	<input type="checkbox"/> Yes
TCP Timestamp	<input type="checkbox"/> Yes
Allowed TLS Versions	TLS 1.2 (dropdown)

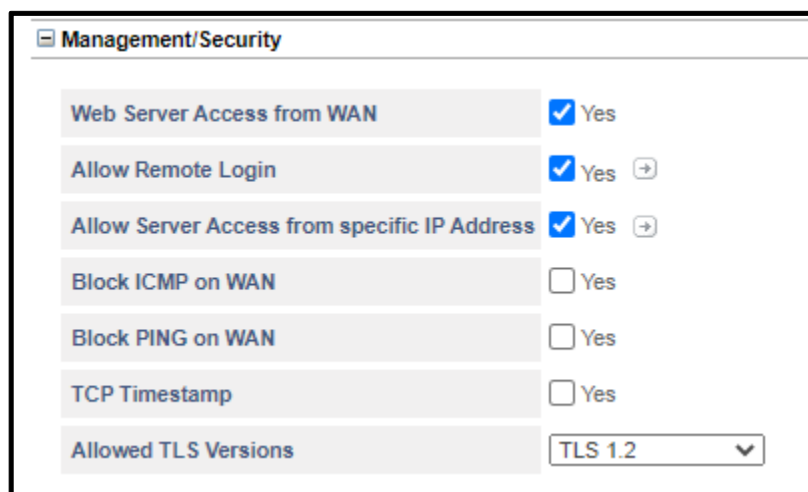
- Select the **Web Server Access from WAN** check box, if you want to allow users to access the system's Web Server (Jeeves) from the WAN Port. Default: Enabled.
- Allow Remote Login:
 - Click **Settings** (+)



The screenshot shows the 'Generate key' dialog box. It has a 'Key Count' dropdown menu set to '01'. Below the dropdown is a note: 'Note: Contact MATRIX Support along with this generated file for Remote Login.' At the bottom is a 'Generate' button.

- In **Key Count**, select the number of keys you wish to generate. You can generate maximum 10 keys.


- Click **Generate**.
- The number of keys you selected are generated and saved in a file. Using these keys you can remotely login into the system.
- For further assistance for Remote Login, along with this file contact Matrix Technical Support Team.
- Select the **Allow Server access from specific IP Address** check box, if you want to allow access of the system to specific users only. Default: Disabled.



The screenshot shows a configuration window titled "Management/Security". It contains several settings, each with a checkbox and a "Yes" label. The "Allow Server Access from specific IP Address" setting is checked. Below the checkboxes is a dropdown menu for "Allowed TLS Versions" set to "TLS 1.2".

Setting	Value
Web Server Access from WAN	<input checked="" type="checkbox"/> Yes
Allow Remote Login	<input checked="" type="checkbox"/> Yes →
Allow Server Access from specific IP Address	<input checked="" type="checkbox"/> Yes →
Block ICMP on WAN	<input type="checkbox"/> Yes
Block PING on WAN	<input type="checkbox"/> Yes
TCP Timestamp	<input type="checkbox"/> Yes
Allowed TLS Versions	TLS 1.2 ▼

If you enable this parameter, you must configure the IP Address table for Server Access.

To configure the IP Address table, Click **Settings** .



IP Address List for Server Access

IPv4 Addresses

Index	IP Address	Subnet Mask
1	192.168.101.198	255.255.255.0
2		
3		
4		
5		
6		
7		
8		
9		
10		

IPv6 Addresses

Index	IPv6 Address	Prefix Length
1		64
2		64
3		64
4		64
5		64
6		64
7		64
8		64
9		64
10		64

The **IP Address List for Server Access** window opens. You can store 10 entries in this table.

- Enter the IP Addresses and their respective Subnet Mask in the table.
- Click **Submit** and close the window.

SETU VTEP will allow system access only to those users whose IP Address matches with the one configured in the IP Address List for Server Access.

- Select the **Block ICMP on WAN** check box, if you want the system to discard the ICMP packets received on WAN. Default: Disabled.
- Select the **Block PING on WAN** check box, if you want the system to discard the PING request received on WAN. Default: Disabled.

Blocking of PING on WAN will prevent your network from being pinged or detected by other Internet users to acquire your IP Address.

- Select the **TCP Timestamp** check box if you want to send Date and Time of SARVAM UCS in response to the TCP request received from the remote device. By default, it is enabled.

- In **Allowed TLS Versions**, select the TLS Version you want the system to use to establish a secure connection with the clients. You may select — TLS 1.0 & Above, TLS 1.1 & Above or TLS 1.2 as per your requirement. Default: TLS 1.0 & Above.
- If the TLS version of the server and the client is not compatible, then secure connection will not be established.



Changing the TLS Version may result in drop of all ongoing TLS connections.

Certificate

- Click **Certificate** to expand and select the certificate for each of the following.

Certificate	
Local Certificate for TLS	DefaultServerCert_Setu ▼
Local Certificate for WebServer	anmol_test_Setu ▼
Local Certificate for Configuration Upgrade	DefaultServerCert_Setu ▼

- In **Local Certificate for TLS**, select the certificate to be used by the system for TLS.

In **Local Certificate for Web Server**, select the certificate to be used by the system for accessing the Web Server.

- In **Local Certificate for Configuration Upgrade**, select the certificate to be used by the system for Configuration Upgrade.

To create as well as Upload/ Download Certificates, see [“Certificate Manager”](#).

Dial Plan

SETU VTEP supports 8 Dial Plans with total 64 entries in each table. The Dial Plan contains a series of digits and/or wildcard characters.

When a user dials a number, it is compared with the Destination Number configured in the Dial Plan. If a match is found, the system routes the call immediately without waiting for End of Dialing and if a match is not found, the system will wait for the End of Dialing and then route the call as per the Destination Port Selection method configured.

Dial Plan will be applied on the — SIP Trunk and T1E1 Port (Terminal) — when,

- the Destination Number Selection method used for routing the call is **Answering the call and collecting the digits**.

and

- the Destination Port Selection method is either **Fixed** or **Calling Number Based**.

Dial Plan will be applied on the — T1E1 Port (Network) — when,

- the Destination Port Selection method is either **Fixed** or **Calling Number Based**.

Configuring Dial Plan Table

- Click the **Advanced Settings** link.
- Click the **Dial Plan** link.

Index	Destination Number
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	
12	
13	
14	
15	

Testing

Enter the destination number to know which entry would be selected for routing

The Dial Plan Table allows you to configure upto 64 entries. Each entry is stored against an Index number.

For each entry,

- In **Destination Number**, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + “[Wildcard Characters](#)”) in this field. Valid characters are 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.
- Click **Submit** to save.



If there are multiple entries in the Dial Plan table, to search a particular entry in the table, under Testing enter the desired number to know which entry would be selected for routing.

Wildcard Characters

SETU VTEP supports following characters.

Character	Description
X (letter X)	X represents any single digit from 0 to 9.
#	When # is configured in a number string, it will not be considered as End of Dialing.
*	When * is configured in a number string, it will not be considered as End of Dialing.
+	+ (plus) can be configured as a first character of the Destination Number string in the <i>SIP Trunk-Destination Port Determination-Destination Number Based</i> table only.
[-]	Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket.
[,]	Comma within a bracket is used as a separator between the groups of numbers.
[^]	Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret.
T (letter T)	Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing.

Refer the following table to understand how a Dial Plan can be configured.

Dial Plan Entry	Description
1XX	Allows you to dial any number in a range from 100 to 199.
[2-5]XX	Allows you to dial any 3 digit number in a range from 200-599.
[2,3,8]XX	Allows you to dial any 3 digit number in the range from 200-299, 300-399, 800-899.
[2-9]XXXXXX	Allows you to dial any 7 digit number in the range from 2000000-9999999.
23[^2]1	Allows you to dial a 4 digit number: 2301, 2311, 2331, 2341, 2351, 2361, 2371, 2381, 2391.
2630[500-550]	Allows you to dial a 7 digit number in the range from 2630500-2630550.
[^6-7]X	Allows you to dial a 2 digit number in the range from 00 to 99 except the numbers from 60 to 79.
1234	Allows you to dial 1234 number only.

011T	Allows you to dial any number starting with 011. The number must be of minimum 3 digits and maximum digits must be as configured for the port.
------	--

Number Lists

A Number List is a data structure that constitutes digit and character strings which must be configured for the system to support the features described in the following.

SETU VTEP supports 24 Number Lists. Each Number List can contain upto 64 entries of a maximum of 24 characters each.

You need to configure Number Lists for the features described in the following. By default, each of these features is assigned particular Number Lists. You may retain the Number List assigned by default, or configure another Number List and assign this list to the feature.

Allowed - Denied Logic

You can apply the Allowed-Denied logic on a source port—SIP and T1E1—if you want to allow or restrict the dialing of particular numbers. You can use this feature for Toll Control.

The Allowed-Denied logic makes use of two Number Lists:

- **Allowed Number List:** This is the list of numbers that can be dialed out from the source port.
- **Denied Number List:** This is the list of numbers that are to be restricted from being dialed out from the source port.

Both the lists must be first programmed separately for each port and then assigned to the respective port.

When Allowed-Denied Logic is enabled on a source port, for each number dialed from the port, SETU VTEP uses the best-match-found logic to compare the dialed number with the Allowed Number List and the Denied Number List.

The number is allowed to be dialed, if the dialed number:

- matches with both lists.
- matches with Allowed Number List, but not with the Denied Number List.
- matches with neither the Allowed List nor the Denied List.

The number is denied, if it matches with the Denied Number List, but not with the Allowed Number List.

Allowed-Denied Number feature is not applicable in following cases:

- Destination number string matches with any Access Code.
- Destination number string matches with any Emergency Number.
- *Route all Incoming Calls (with CLI)* option selected is:
 - Fixed Destination Number
 - or -
 - on basis of Calling Party Number.

To apply this feature,

- you must configure the numbers you want to allow and restrict from being dialed out in the Allowed and Denied Number Lists.

By default, the following Number Lists are assigned for Allowed Denied Logic for each port type:

Port Type	Default Allowed Numbers List	Default Denied Numbers List
SIP Trunks	List 07	List 08
T1E1 Ports	List 01	List 02

You may retain these lists or configure any other Number List from 01 to 24.

- enable **Allowed-Denied Logic** on the port type—SIP and T1E1 — on which you want to apply this feature.
- configure the numbers you want to allow and the numbers you want to restrict in the default **Allowed Number List** and **Denied Number List** assigned to the port.

For instructions, see the following topics under *Basic Settings*:

[“Handling of Incoming Calls” on “SIP Trunk”](#)

[“Handling of Incoming Calls” on “T1 Port”](#)

[“Handling of Incoming Calls” on “E1 Port”](#)

If you do not want to use the default Number Lists assigned to the ports, you may select a different List Number and configure it. In this case, you must select the List Number you configured as the Allowed Number List/Denied Number List for the port.

Black Listed Callers

The Black Listed Callers feature enables you to block incoming calls from specific numbers and addresses on SIP Trunks. You can apply this feature on the Source Port only.

To use this feature,

- you must configure the numbers of unwanted callers in a Number List.



Make sure you have configured the full SIP URI (for example: 12345@abc.com) of the unwanted callers in the Blacklisted Callers Number List.

- enable the **Reject Calls from Blacklisted Callers** check box on the SIP Trunks on which you want to apply this feature.
- select the Number List you configured as **Black Listed Callers Number List**.

For instructions, see the following topics under *Basic Settings*:

- [“Handling of Incoming Calls” on “SIP Trunk”](#)

Now, whenever there is an incoming call on the SIP Trunk you have applied this feature, the SETU VTEP will match the number with the Blacklisted Callers' Number list you have assigned. If the number matches with any of the numbers you have blacklisted, the system will reject the call.

Make a list of numbers that you want to black list. Configure these numbers in a Number List. By default, Number List 16 is assigned as the Black Listed Callers List and Number List 11 is assigned as the Black Listed Callers List for the SIP Trunks.

You may retain this list and configure all the numbers you want to black list in this list or you may configure different Number Lists for different ports and assign the lists to the ports.



Each number string in the List can have a maximum of 24 characters. If the callers' number exceeds 24 characters, the first 24 characters of the number will be checked. If the first 24 characters of the callers' number match perfectly with any of the numbers programmed in Blacklisted Callers List, the call will be rejected.

Call Detail Record Filters

SETU VTEP enables you to generate reports of Call Detail Records using different filters. You can generate Call Detail Record report of calls made to specific numbers (Called Party Numbers) and calls received from specific numbers (Calling Party Numbers).

When you want to sort calls by Called Party and Calling Party Numbers, you must configure a Number list for each of these.

To generate Call Detail Records using Called Party and Calling Party Numbers as filters,

- make a list of Called Party Numbers and another list of Calling Party Numbers.
- configure a Number List with the Called Party Numbers and another Number List with the Calling Party Numbers.

By default, Number list 01 is assigned for both Called Party and Calling Party numbers. You may retain this list and configure Called Party and Calling Party numbers in this list, or you may retain this for Called Party Numbers and configure another list number for Calling Party numbers. In this case you must assign the list you configured to the respective filter.

- assign the Called Party Number list you configured to the CDR filter **Called Party Number Matching with Number List**.
- assign the Calling Party Number list you configured to the CDR filter **Calling Party Number Matching with Number List**.

For instructions, see [“Call Detail Records \(CDR\)”](#).

Configuring Number Lists

You must determine the purpose for which the list is required and accordingly prepare them.

To configure Number lists,

- Click the **Advanced Settings** link to expand.

- Click the **Number List** link.

Basic Settings
Advanced Settings
System Parameters
Dial Plan
Number Lists
Automatic Number Translation (ANT)
SIP Profile
SIP Network Profile
SIP VoIP Profile
Codec Profile
Destination Number Determination
Destination Port Determination
Group
Peer-to-Peer Dialing
PIN Authentication
Digest Authentication
Static Routing Table
Access Code
Emergency Number
Certificate Manager
Call Detail Records(CDR)
Maintenance
Status

1-4 5-8 9-12 13-16 17-20 21-24

Number Lists

Location	List 1	List 2	List 3	List 4
01	0	0		
02	1	1		
03	2	2		
04	3	3		
05	4	4		
06	5	5		
07	6	6		
08	7	7		
09	8	8		
10	9	9		
11	*	*		
12	#	#		
13	+	+		
14	a	a		
15	b	b		
16	c	c		
17	d	d		
18	e	e		
19	f	f		
20	g	g		
21	h	h		

Submit Default

- List 1 to 4 appears on the page. To select another List number, click the tab on the top of the table.
- Select the list number you want to configure.
- Enter the numbers strings in each list.
- Click **Submit** to save entries.
- Assign the list to the respective features for which you configured them on the various port types.

For example, if you configured Number List 22 with black listed numbers for the Black Listed Callers feature on SIP Trunk 2,

- Click the **Basic Settings** link to expand.
- Click the **SIP Trunk** link.
- Click **SIP-2**.

- Under Handling of Incoming Calls, select the **Reject Calls from Blacklisted Callers** check box.

SIP Trunk - 2

SIP Trunk

☐ Enable

Name

SIP ID

7002

Status

Disabled

Basic Settings

Handling of Incoming Calls

Block all calls received on this SIP Trunk

☐ Yes

Use Called Party Number from

Request-URI

Route all Incoming calls (with CLI)

to the Called Party Number

Block Calls received without CLI on this SIP Trunk

☐ Yes

Route all Incoming calls (without CLI)

to the Called Party Number

Select Destination Port for routing calls

Fixed

Allowed-Denied Logic

☐ Apply

Reject Calls from Blacklisted Callers

☒ Apply

Blacklisted Callers Number List

11

Display received URI as Calling Name

☒ Apply

Handling of Outgoing calls

Submit

Default

Close

Copy

- In **Blacklisted Callers Number List**, select **22**.
- Click **Submit**.

You can also configure the Number lists on the respective SIP Trunk and T1E1 Port pages under the [“Basic Settings”](#) link of Jeeves.

Automatic Number Translation (ANT)

Automatic Number Translation (ANT) is used to modify the number string—entire number or part thereof—into the desired number string as per your requirement. ANT is useful when you need to modify the Called/Calling number, before the system routes the call further.

For example, in India the PSTN requires you to dial the prefix 00 for calling international numbers, whereas the ITSP you have subscribed the SIP Trunk with, restricts the dialing of the prefix 00. If you dial this prefix, your call will be rejected by the ITSP. The ANT Table will enable you to modify the Number string as per your requirement so that the calls routed through the SIP Trunk are not rejected.

The Automatic Number Translation feature can be applied on all the SIP Trunks and T1E1 Ports.

Automatic Number Translation makes use of Automatic Number Translation Table. The ANT Table consists of three columns:

- **Number:** In this column, enter the numbers that you want the system to modify.
- **Strip Digit:** In this column, enter the number of digit(s) to be stripped off by the system from the Called/ Calling number string. If you do not want any digits to be stripped, enter '0'.
- **Add Prefix:** In this column, enter the digit(s) which are to be added as prefix to the Called/ Calling number string by the system before routing it further.

To apply this feature on the desired port,

- on a piece of paper make a table, in the first column note down the numbers that needs to be modified. In the second column enter the number of digits you want the system to strip off (if required), and in the third column, enter the number you want the system to add as prefix (if required).
- configure the **Automatic Number Translation Table**. You can configure upto 8 different ANT Tables.
- enable **Automatic Number Translation (ANT) for Called Number** and/or **Automatic Number Translation (ANT) for Calling Number** on the respective ports/trunks, on which you want to apply this feature.
- assign the **Automatic Number Translation Table** you configured.
- configure the **Pause Timer**, if applicable.

For instructions, see:

- [“Advanced”](#) under [“T1 Port”](#)
- [“Advanced”](#) under [“E1 Port”](#)
- [“Handling of Outgoing Calls”](#) under [“SIP Trunk”](#)

Now, whenever there is a call on/ from the Port for which you have applied this feature, SETU VTEP will match the Called/ Calling number with the Number configured in the Automatic Number Translation Table using the best match found logic.

- If a match is found, the system will check whether and how many digits to strip off. It will strip off digits according to the number you have entered in the Strip Digit column. If '0' is configured in the Strip Digit column, it will check the Add Prefix column. If configured, the system will add that prefix. If no prefix is configured, the system will route the same number string further.

If ~ (Wait for Answer) is configured in the Add Prefix column, the system will wait for the call to mature. Similarly, if ^ (Pause) is configured in the Add Prefix column, the system will wait for the Pause timer and then route the call further.

- If no match is found for the Called/ Calling number in the ANT Table, the system will route the number string, without modifying it.



Automatic Number Translation feature will not be applied when Emergency Numbers are dialed.

Automatic Number Translation also forms the basis of Multi-Stage Dialing. Using of Calling Card for making international calls is the most common example of Multi-Stage Dialing.

While using a Calling Card, you have to dial the digits in the following sequence:

1. Dial the number for using the Calling Card, for example, 160223.
2. After the call is matured, dial the PIN number printed on the Calling Card, for example, 113212.
3. At last, dial the international number you want to call. For example, 0014162357896.

Thus, you will have to dial the Calling Card number and the PIN number every time before dialing the international number. To avoid repetitive dialing of these fixed digits for making a call, you can configure the ANT table as under.

- In **Number**, configure '00', the prefix for international numbers.
- In **Add Prefix**, configure the Calling Card server number and the PIN Number.

As the system must wait for the Calling Card server to answer before dialing the PIN, you must configure Wait for Answer (~) between the Calling Card server number and the PIN number.

You must also insert a delay by configuring the Pause Timer (^) after the PIN number.

- Keep Strip Digit as 00.
- The Automatic Number Translation table would look like this:

Index	Number	Strip Digit	Add Prefix
1	00	00	160223~113212^
2			
3			
4			
5			
6			
:			
24			

- When the Automatic Number Translation table is configured, the user must simply dial the destination number, say, 0014125126508.
- The system matches the Called number with the Number configured in the ANT table. The number matches with the entry '00' stored in the table.
- The system dials the Add Prefix number string 160223 (number of the calling card server). It waits for the calling card server to answer the call.
- When the call is matured, i.e. the calling card server has answered the call, the system dials the PIN number 113212 and waits for the Pause Timer before dialing the destination number.

Thus, the user can directly dial the desired destination number and the system dials the rest using the ANT table.

Configuring Automatic Number Translation Table

- Click the **Advanced Settings** link to expand.
- Click the **Automatic Number Translation (ANT)** link.

The screenshot shows the 'Automatic Number Translation (ANT)' configuration window. On the left is a sidebar with a tree view containing 'Basic Settings', 'Advanced Settings' (expanded), 'SIP Profile', 'Destination Number Determination', 'Destination Port Determination', 'Group', 'Peer-to-Peer Dialing', 'PIN Authentication', 'Digest Authentication', 'Static Routing Table', 'Access Code', 'Emergency Number', 'Certificate Manager', 'Call Detail Records(CDR)', 'Maintenance', and 'Status'. The main area displays the 'Automatic Number Translation Table - 1' with 24 rows (Index 01 to 24) and 4 columns: Index, Number, Strip Digit, and Add Prefix. Below this table is a section titled 'Examples of Number Pattern' with 3 rows showing patterns like '\$\$\$', '8\$\$\$' and their corresponding Strip Digit and Add Prefix values. At the bottom are 'Submit' and 'Default' buttons.

Index	Number	Strip Digit	Add Prefix
01		0	
02		0	
03		0	
04		0	
05		0	
06		0	
07		0	
08		0	
09		0	
10		0	
11		0	
12		0	
13		0	
14		0	
15		0	

Number	Strip Digit	Add Prefix	Remarks
\$\$\$	0	13152222	System will add the prefix '13152222' to every 3-digit dialed number.
8\$\$\$	1		System will strip off the first digit of all 4-digit dialed numbers that start with 8, and will dial out the remaining 3-digit number.
\$\$\$\$\$\$	0	1315	System will add the prefix '1315' to every 7-digit dialed number.

Submit Default

The Automatic Number Translation Table window opens. In this table, you can store as many as 24 Numbers at Index Numbers 01 to 24.

- In **Number**, enter the Called/ Calling numbers that need to be modified. You can enter maximum 24 digits. Digits 0-9, #, *, + and \$ are allowed. Default: Blank.

To configure a range of numbers you can use the character \$. Here, \$ is any number from 0 to 9.

For example, if you want SETU VTEP to add prefix '1' to all 10 digit numbers dialed by the user, configure Number as \$\$\$\$\$\$\$\$\$\$, Strip Digit as 0 and Add Prefix as 1. Now, when the user dials any number between the range of 0000000000 to 9999999999, say 4161231234, the system will add prefix 1 to it and dials out the number as 14161231234.

- In **Strip Digit**, enter the number of digits you want the system to strip off from the Called/Calling Number. You can configure from 00-24. Default: 0.
- In **Add Prefix**, enter the number string(s) that you want the system to add as prefix to the Called/Calling Number. You can enter maximum 24 characters. Characters 0-9, *, #, +, ~ (Wait for Answer), ^ (Pause) are allowed. Default: Blank.
- Click **Submit** to save your entries.

SIP Network Profile

You can either edit the settings of the default **Network Profile 1** or you can add a new profile. To do so, click **Add New Profile**.

- Click **Advanced Settings** link.
- Click **SIP Network Profile** under **SIP Profile**.
- The **SIP Network Profile** page opens.

The screenshot displays the 'SIP Network Profile' configuration interface. On the left, a navigation menu lists various settings, with 'SIP Network Profile' highlighted. The main panel shows the configuration for 'Network Profile 1'. Key settings include: 'SIP Network Profile' is enabled; the 'Name' is 'Network Profile 1'; the 'Status' is 'Enabled'; the 'Mode' is set to 'Peer-to-Peer'; the 'Allowed IP Address for Incoming SIP Message' is set to 'As per Trusted IP Address table'; and 'Digest Authentication' is not applied. Below these settings are expandable sections for 'Codec', 'VoIP Profile', and 'Advanced'. At the bottom of the panel are four buttons: 'Submit', 'Default', 'Copy', and 'Add New Profile'.


- Configure the following parameters:
 - Keep the **SIP Network Profile** check box enabled, to use this profile.
Clear this check box only if you do not want to use this profile.
 - Assign a **Name** to the Network Profile for identification. The Name can be a maximum of 24 characters.
 - **Status** displays the status of this Network Profile.
 - You can select **Proxy** or **Peer-to-Peer** as the **Mode**. Default: Peer-to-Peer.
 - If you select **Proxy**, you must configure the following parameters:
 - Registrar Settings
 - Redundancy Settings
 - Codec
 - VoIP Profile
 - Advanced
 - Timers
 - If you select **Peer-to-Peer**, you must configure the following parameters:
 - Enable Peer-to Peer option and configure the Peer-to-Peer Dialing table



- Allowed IP Address for Incoming SIP Message
- Digest Authentication
- Codec
- VoIP Profile
- Advanced

Peer-to-Peer Table

By default **Peer-to-Peer** is selected as the SIP Trunk **Mode**. You must configure the Peer-to-Peer Table.

To do so,

- Click **Settings** .
- The **Peer-to-Peer Dialing** table opens.

Peer-to-Peer Dialing				
<input type="checkbox"/>	Edit	Destination Number	Destination Address	Name
<input type="checkbox"/>		No Match Found	192.168.101.108	
<input type="checkbox"/>		1212	2001::192:168:154:11	rs

Total Records : 2
 1

Testing
 Enter the destination number to know which entry would be selected for routing

- You can add maximum 500 entries. Each entry in the table consists of the Destination Number, Destination Address and Name. For detailed instructions, see [“Peer-to-Peer Dialing”](#).

Allowed IP Address for Incoming SIP Message

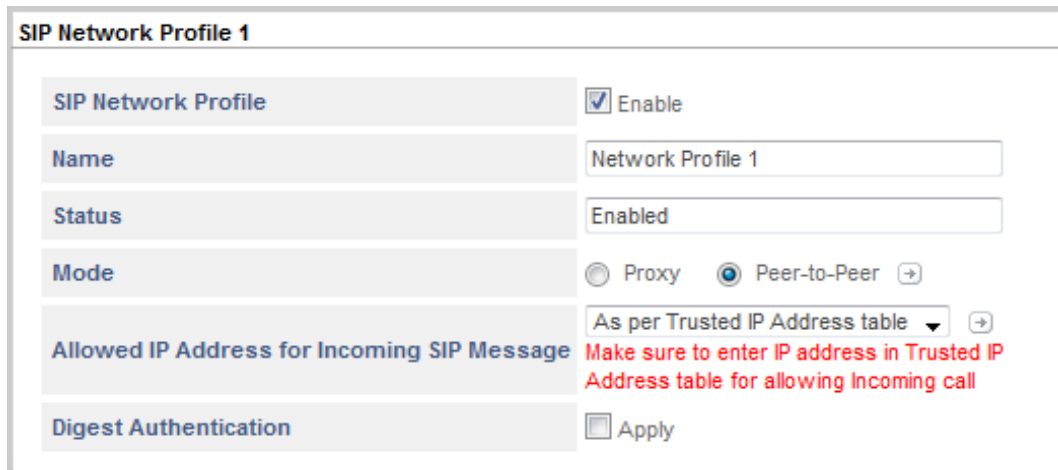
If you have selected the SIP Trunk **Mode** as **Peer-to-Peer**, you must select the desired option in **Allowed IP Address for Incoming SIP Message — As per Trusted IP Address table, As per Peer-to-Peer table** or **Any**.

- If you select **As per Trusted IP Address table** option, the system matches the **IP Address: Port** received in the INVITE message (Source IP address from the Network layer and Source Port from the Transport layer) with the entries configured in the Trusted IP Address table. If a match is found, the call will be routed to the desired destination. Else the call will be rejected.

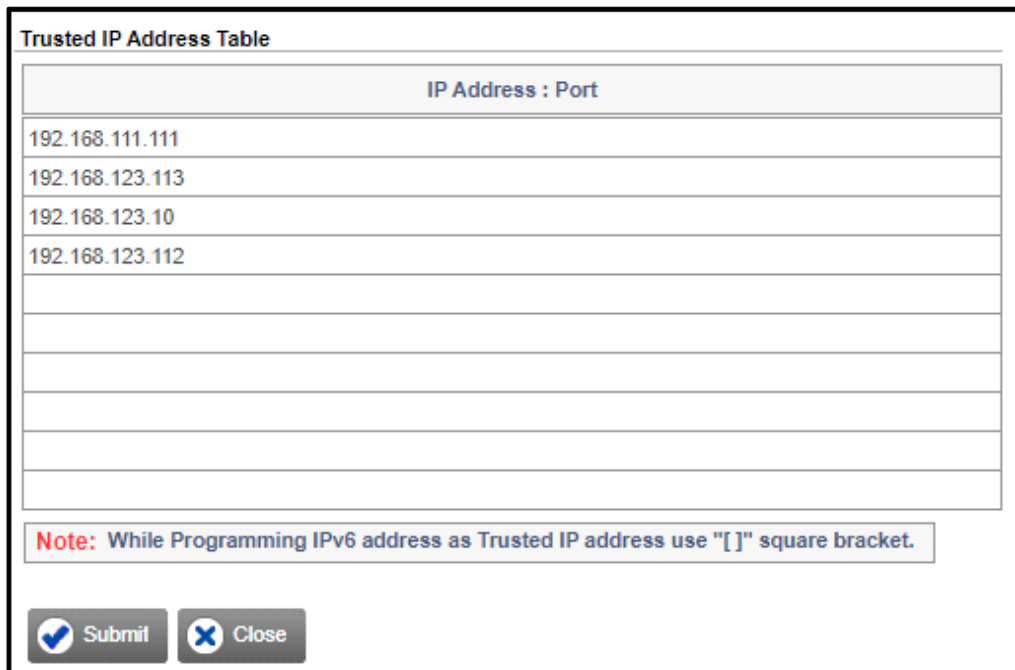
You must configure the **Trusted IP Address Table** to receive incoming calls on this SIP Trunk. If you do not configure this table, incoming calls on this SIP Trunk will be rejected.

You can configure maximum 10 entries in the Trusted IP Address table.

To do so, click **Settings**  .



The **Trusted IP Address Table** opens in a new window.



- Enter the **IP Address** and the corresponding **Port** from which you want to allow incoming calls on this SIP Trunk. You can configure maximum 21 characters. Allowed characters are **0-9**, **dot (.)**, **colon (:)**.

Do not configure the port, if you want to allow incoming calls from all the ports for a particular IP Address.


- Click **Submit** and close the window.
- If you select **As per Peer-to-Peer table** option, the system matches the **IP Address: Port** received in the INVITE message (Source IP address from the Network layer and Source Port from the Transport layer) with the Destination Address configured in the Peer to Peer table. If a match is found, then the call will be routed to the desired destination. Else the call will be rejected.

- If you select **Any** as the option, **Digest Authentication** will be enabled automatically. The system will allow incoming calls only after the callers authenticate themselves with the correct credentials—User ID and Password. The system matches the User ID and Password entered by the callers with the entries stored in the Digest Authentication table. If a match is found, the call will be routed to the desired destination. Else the call will be rejected.

Default: **As per Trusted IP Address Table**

Digest Authentication




If you have selected the SIP Trunk **Mode** as **Peer-to-Peer**,

- you may enable the **Digest Authentication** if you have set *Allowed IP Address for Incoming SIP Message* to *As per Trusted IP Address table* or *As per Peer to Peer table*. Incoming calls on this SIP Trunk will be allowed only after the callers authenticate themselves with their User ID and Password. Default: Disabled.
- Digest Authentication is enabled and you must configure the **Digest Authentication** table, if you have set *Allowed IP Address for Incoming SIP Message* to **Any**.
 - Click **Settings**  .

1-100
101-200
201-300
301-400
401-500

Digest Authentication

Index	User ID	User Password
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		

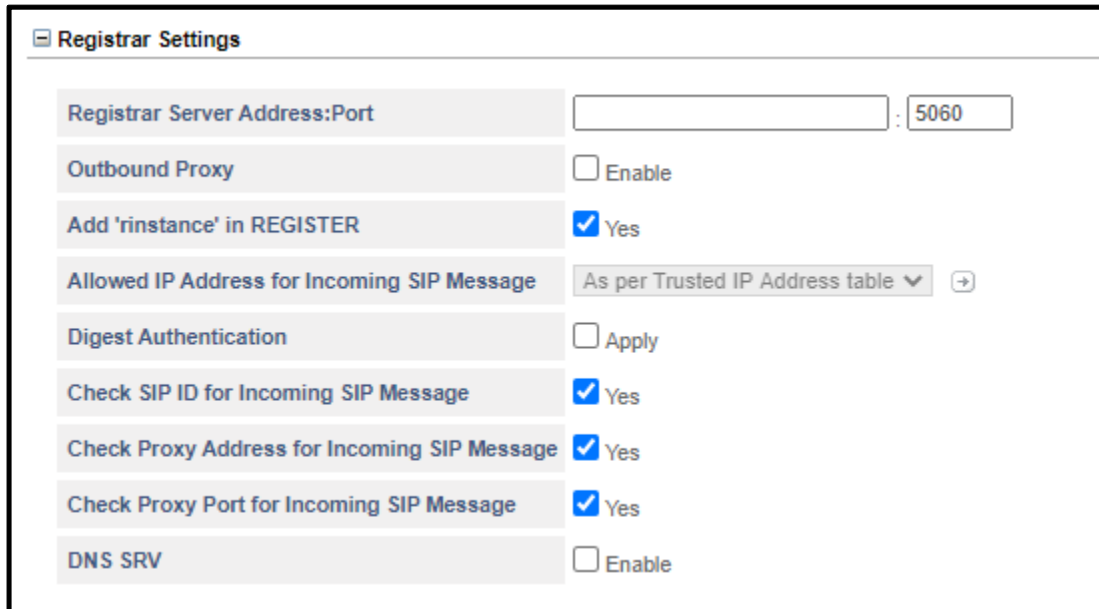
 Submit
 Default All
 Close

For detailed instructions, see [“Digest Authentication”](#). Default: Disabled.

Registrar Settings

If you have selected the SIP Trunk **Mode** as **Proxy**, configure the Registrar Settings.

- Click **Registrar Settings**.



The image shows a 'Registrar Settings' configuration window. It contains several settings:

Setting	Value
Registrar Server Address:Port	[Empty field] : 5060
Outbound Proxy	<input type="checkbox"/> Enable
Add 'rinstance' in REGISTER	<input checked="" type="checkbox"/> Yes
Allowed IP Address for Incoming SIP Message	As per Trusted IP Address table ▼ (+)
Digest Authentication	<input type="checkbox"/> Apply
Check SIP ID for Incoming SIP Message	<input checked="" type="checkbox"/> Yes
Check Proxy Address for Incoming SIP Message	<input checked="" type="checkbox"/> Yes
Check Proxy Port for Incoming SIP Message	<input checked="" type="checkbox"/> Yes
DNS SRV	<input type="checkbox"/> Enable

- In **Registrar Server Address: Port**, enter the Registrar Server Address and the Registrar Server's listening port for SIP messages. The registrar server address may be an IP address or a domain. The Registrar Server Address can be of maximum 64 characters. Valid range is 1025 to 65534. Default: 5060.
- If your Service Provider uses outbound proxy for handling voice calls, select the **Outbound Proxy** check box. Default: Disabled.
- In **Outbound Proxy Server Address: Port**, enter the Outbound Proxy Server's IP Address and the Outbound Proxy Server's Listening Port for SIP. The Outbound Proxy Server Address may be of maximum 64 characters. Valid range is 1025 to 65534. Default: 5060.
- To add 'rinstance' in REGISTER message, keep the **Add 'rinstance' in REGISTER** check box enabled.

'rinstance' is any random value which can be used by SETU VTEP to fetch its own contact binding, that is, to know the Registration Expiry Timer assigned by the server.

When you enable 'rinstance' in Register, SETU VTEP will generate any random value of 'rinstance' and include it in the REGISTER message. The system will use the registration expiry timer of that contact binding.

- By default, the **Allowed IP Address for Incoming SIP Message** is set to **As per Trusted IP Address table** for Proxy SIP Trunk and is non-programmable. You must configure the **Trusted IP Address table** to allow incoming calls from specific IP addresses on this SIP Trunk.

Trusted IP Address table stores upto 13 entries, from which last three entries are uneditable. The last three entries in the table will display the *Registrar Server Address:Port* or *Outbound Proxy Address:Port* and *Fallback Registrar Server Address:Port1* and *2* or *Fallback Outbound Proxy Server*

- Enable **DNS SRV**, if you want the system to send DNS SRV query to the configured domain server. When disabled, the system will send DNS A query to the configured domain server. Default: Disabled.



If you enable DNS SRV, Fallback Server logic will not be applicable.

Redundancy Settings

If you have selected the SIP Trunk **Mode** as **Proxy**, configure the Redundancy Settings.

- Click **Redundancy Settings**.

Redundancy Settings	
Fallback Server	<input type="checkbox"/> Yes
Fallback Event	503 or No Response ▼
No Response Timer	20 Seconds
Registration Behavior	Register with only one Server ▼
Switch Registration to Alternate Server on Fallback	<input checked="" type="checkbox"/> Yes
Load Balancing	Last Call Active ▼

- Select the **Fallback Server** check box, if your Service Provider supports multiple servers in its network. Default: Disabled.

If you have enabled Fallback Server and Outbound Proxy is disabled,

- In the **Fallback Registrar Server Address 1: Port** and **Fallback Registrar Server Address 2: Port** field, enter addresses of the alternate Registrar Servers and their respective listening ports. The Fallback Registrar Server Address can be of maximum 64 characters. Valid range is 1025 to 65534. Default: 5060.

If you have enabled Fallback Server and Outbound Proxy is enabled,

- In **Fallback Outbound Proxy Server Address 1: Port** and **Fallback Outbound Proxy Server Address 2: Port** field, enter addresses of the alternate Outbound Proxy Servers and their respective listening ports. The Fallback Outbound Proxy Server Address can be of maximum 64 characters. Valid range is 1025 to 65534. Default: 5060.
- In the **Fallback Event** list, select the event on occurrence of which SETU VTEP should fallback to an alternate Registrar/Outbound Proxy Server, if available.
 - No Response
 - 503 or No Response
 - 5xx or No Response
 Default: 503 or No Response

In case, the Fallback Server does not respond and the call is not routed to the destination port, the call will be routed to another port type as per the Routing/Fallback Routing Group configured for the SIP Trunk.

- Set the duration of the **No Response Timer**. This timer defines the time period for which SETU VTEP will wait for the response from the server for any request. If no valid response is received before the expiry of this timer, SETU VTEP will fallback to alternate Registrar/Outbound Proxy Server or Routing Group/Fallback Routing Group for further processing of the call. Valid range is 01 to 99 seconds. Default: 20 seconds.



If the SIP General Request Timer configured in the System Parameters is less than the No Response Timer, then SETU VTEP will fallback to alternate Registrar/Outbound Proxy Server or Routing Group/Fallback Routing Group on the expiry of the SIP General Request Timer and the No Response Timer will stop.

- In the **Registration Behavior**, select the desired option:
 - Register with all Servers
 - Register with only one Server

If you select **Register with only one Server**, SETU VTEP will get registered with the Registrar/Outbound Proxy Server. If registration with the Registrar/Outbound Proxy Server fails, it will get registered with Fallback Registrar/Outbound Proxy Server 1 or Fallback Registrar/Outbound Proxy Server 2 respectively for further processing of call.

If you select **Register with all Servers**, SETU VTEP will get registered with Registrar/Outbound Proxy Server as well as Fallback Registrar/Outbound Proxy Servers. It will not apply Fallback logic even if *Fallback Server* is enabled.



*The **Registration Behavior** will be applicable only if, **SIP Registration** is enabled.*

- Keep the **Switch Registration to Alternate Server on Fallback** check box enabled. SETU VTEP will get unregistered with the current server and will register with the alternate server, if fallback occurs while sending the INVITE message.



*The **Switch Registration to Alternate Server on Fallback** will be applicable only if, **SIP Registration** is enabled and **Registration Behavior** is set as **Register with only one Server**.*

- Select the desired option for **Load Balancing** from the following:
 - **Last Call Active**: Each new call will be processed through the Registrar/Outbound Proxy Server through which the last active call has been processed.

For example, if the last call has been processed by Fallback Registrar/Outbound Proxy Server 2, the new call will also be processed through Fallback Registrar/Outbound Proxy Server 2 only.
 - **First Active**: Each new call will be processed through the first active Registrar/Outbound Proxy Server only.
 - **Cyclic**: Each new call will be processed through the next active Registrar/Outbound Proxy Server.

For example, if the last call has been processed by Fallback Registrar/Outbound Proxy Server 1, the new call will be processed through Fallback Registrar/Outbound Proxy Server 2 and the subsequent new call will be processed through the Registrar/Outbound Proxy Server.
Default: Last Call Active.

Codec Profile


If you have selected the SIP Trunk **Mode** as **Proxy** or **Peer-to-Peer**, configure the Codec Profile.

- Click **Codec**.

Codecs are used to compress the data in RTP packets to enable quick transmission. It also decompresses the received data.

The codec profiles supported by SETU VTEP appears in the **Selected Codecs Profiles** list in the following order of preference:

1. G.729 - 20msec - Silencesupp=off
 2. G.723 - 30msec - Silencesupp=off
 3. GSM FR - 20msec - Silencesupp=off
 4. iLBC (30ms) - 30msec - Silencesupp=off
 5. iLBC (20ms) - 20msec - Silencesupp=off
 6. GSM EFR - 20msec - Silencesupp=off
 7. G.711 (u-law) - 20msec - Silencesupp=off
 8. G.711 (A-law) - 20msec - Silencesupp=off
- You can change the order of preference by moving the desired Codecs up or down the list. To move a Codec up or down the list, do the following:
 - In the **Selected Codecs Profiles** list, click the Codec you want to move.
 - Click the UP/DOWN ARROW to move the Codec to the desired position in the list.
 - To remove a Codec from the **Selected Codecs** list, click the Codec you want to remove, and then click the LEFT ARROW. The Codec is moved to the **Available Codecs Profiles** list.

- To move a Codec from the **Available Codecs Profiles** list to the **Selected Codecs Profiles** list, click the Codec you want to move, and then click the RIGHT ARROW.
- You can edit any existing profile or add a new profile. To do so, click **Settings** .
 - The **Codec Profile** window opens. For detailed instructions, see [“Codec Profile”](#).

- Select the desired **Silence Suppression in SDP for G.711 codec** option. SETU VTEP suppresses the *Silence* packets and allows only the *Voice* packets to pass through.

This is used to deactivate certain processes during non-speech section of an audio session to avoid unnecessary coding/ transmission of silence packets in VoIP application. Hence, it results in saving on computation and network bandwidth.

You can select either *Do Not Send*, *Send using Silence Suppression attribute* or *Send using VAD attribute*.

If you select *Do Not Send*, SETU VTEP will not send any “Silence Suppression” media attribute in the SDP offer / answer exchanges. This is not dependant on the Silence Suppression check box.

If the Silence Suppression check box is disabled. and you select *Send using Silence Suppression attribute*, SETU VTEP will send *Silence Suppression=OFF* in the SDP offer / answer exchanges.

If the Silence Suppression check box is enabled. and you select *Send using Silence Suppression attribute*, SETU VTEP will send *Silence Suppression=ON* in the SDP offer / answer exchanges.

If the Silence Suppression check box is disabled. and you select *Send using VAD attribute*, SETU VTEP will send *VAD=NO* in the SDP offer / answer exchanges.

If the Silence Suppression check box is enabled. and you select *Send using VAD attribute*, SETU VTEP will send *VAD=YES* in the SDP offer / answer exchanges.

Default: Send using Silence Suppression attribute

- Select the **Comfort Noise (CN)** check box, if you want SETU VTEP to negotiate the Comfort Noise received in the SDP body with the remote peer. Default: Disabled.
- Select the **Includeptime header in SDP** check box, if you want SETU VTEP to add ptime header in the SDP offer / answer exchanges. Default: Disabled.
- Clear the **Send Re-INVITE when multiple codec is received in 200 (OK)** check box, if you do not want SETU VTEP to send Re-INVITE message and use only the first codec from the multiple codecs received in 200 (OK). Default: Enabled.
- Select the **Send all codecs while sending Offer within the dialog** check box, if you want SETU VTEP to send all the codec configured on SIP Trunk in same order as configured while sending the RE-INVITE message to hold or unhold the call.

When RE-INVITE without SDP is received then the system sends SDP offer in 200 OK response with all the codecs configured for that SIP trunk. The codec order is same as configured for the SIP Trunk.

Default: Disabled.

- Select the **Send multiple codecs in SDP Answer** check box, if you want SETU VTEP to send all the configured codecs in SDP answer. Default: Disabled.

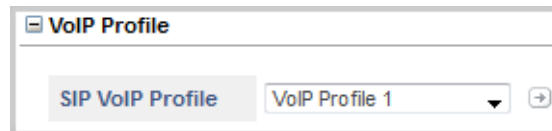
The codecs sent will depend on the option you select in **Codec Priority**.


- When Codec Priority is set as *Local* then system sends all the codecs as per local preference.
- When Codec Priority is set as *Remote* then system sends all the codecs as per the preference received in SDP offered from remote party. Here, the system sends only configured codecs in remote preference.
- Select the desired **Codec Priority** option using which system can decide which codecs — Local or Remote — should be given preference. Default: Local.

VoIP Profile

If you have selected the SIP Trunk **Mode** as **Proxy** or **Peer-to-Peer**, configure the VoIP Profile.

- Click **VoIP Profile**.



- In **SIP VoIP Profile**, you can either select the default **VoIP Profile 1** or **Add New VoIP Profile** option.
- Click **Settings**  to configure the parameters of the selected VoIP Profile.

VoIP Profile 1

SIP VoIP Profile 1

SIP VoIP Profile

☒ Enable

Name

VoIP Profile 1

⊟ RTP

Local RTP Port Minimum

8000

Local RTP Port Maximum

8256

Symmetric RTP

☐ Enable

⊕ SRTCP

⊕ DTMF

⊕ FAX

⊕ T.38 FAX Parameters

⊕ Pass-Through FAX Parameters

☒ Submit

☐ Default

☒ Close

☐ Add New Profile

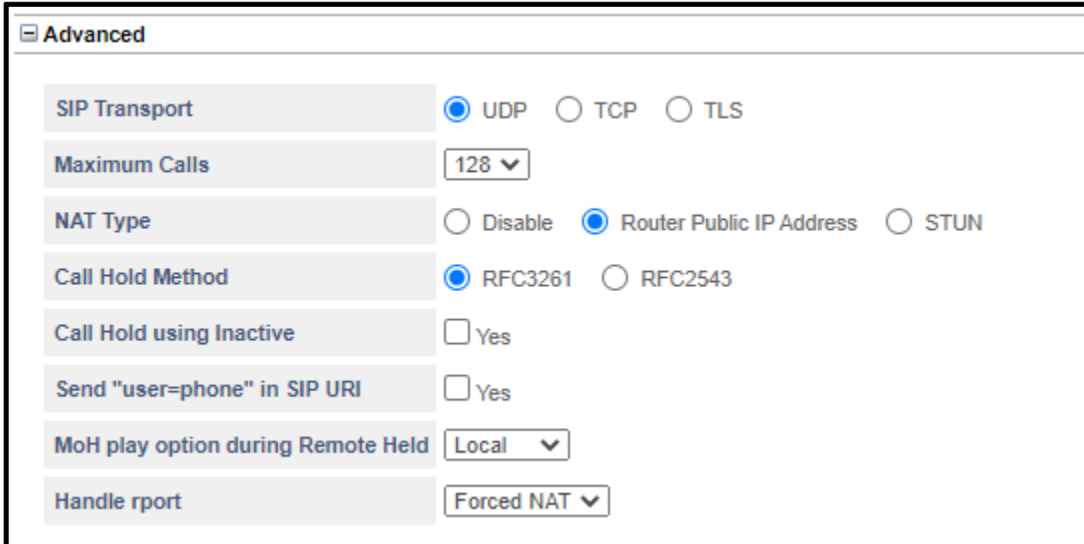
For detailed instructions, see [“SIP VoIP Profile”](#).

You can also configure the **SIP VoIP Profile** under **SIP Profile** from *Advanced Settings*.

Advanced

If you have selected the SIP Trunk **Mode** as **Proxy** or **Peer-to-Peer**, configure the Advanced Settings.

- Click **Advanced**.



The screenshot shows the 'Advanced' settings window for SIP. It contains the following fields and options:

- SIP Transport:** Radio buttons for UDP (selected), TCP, and TLS.
- Maximum Calls:** A dropdown menu showing '128'.
- NAT Type:** Radio buttons for Disable, Router Public IP Address (selected), and STUN.
- Call Hold Method:** Radio buttons for RFC3261 (selected) and RFC2543.
- Call Hold using Inactive:** A checkbox labeled 'Yes' (unchecked).
- Send "user=phone" in SIP URI:** A checkbox labeled 'Yes' (unchecked).
- MoH play option during Remote Held:** A dropdown menu showing 'Local'.
- Handle rport:** A dropdown menu showing 'Forced NAT'.

- Select the default **SIP Transport** for outgoing SIP messages from the following options:
 - **UDP:** Outgoing messages are transported using UDP.
 - **TCP:** Outgoing messages are transported using TCP.
 - **TLS:** Outgoing messages are transported using TLS.

Default: UDP



To use TLS, you must enable **SIP over TLS** in "[System Parameters](#)".

- For the selected Network Profile in **Maximum Calls**, select the number of simultaneous calls you want to allow on the SIP Trunk.

The maximum number of simultaneous SIP calls depend upon the number of Vocoder channels supported.

- When the system is installed behind a NAT Router, select specific NAT traversal mechanism to be used as **NAT Type**. Default: Disabled.
 - Select **Router's IP Address**, if your SETU VTEP is located behind the NAT router (any type).

Make sure you disable Outbound Proxy on SIP Trunk and have configured the same IP Address under NAT settings in the "[System Parameters](#)" page.

- Select **STUN**, if your system is located behind the NAT router other than Symmetric.

Make sure you disable Outbound Proxy on SIP Trunk and have configure the STUN Server Address and port under NAT settings in "[System Parameters](#)".

- In **Call Hold Method** select the desired option — RFC 2543 or RFC 3261 — that is compatible with your ITSP proxy server / remote peer. Default: RFC 3261
- Select the **Call Hold using Inactive** check box, if you want the system to send '*a=inactive*' message instead of '*a=sendonly*' message on the SIP Trunk, when the user puts the call on hold. Default: Disabled.
- Select **Send "user=phone" in SIP URI** check box, if you want SETU VTEP to add user=phone in the Request URI / From / To header of the INVITE message.

SETU VTEP will send user=phone in SIP URI, only if the SIP ID is numeric.

Default: Disabled.

- In **MoH play option during Remote Held**, select the desired option — Local or Remote.

If you select *Local*, SETU VTEP will play Music-On-Hold to the extension that is put on hold.

If you select *Remote*, SETU VTEP will play the Music-On-Hold received from the remote end to the extension that is put on hold.

Default: Local

- In **Handle rport** select the desired option — Forced NAT or RFC 3581.

If you select *Forced NAT*, SETU VTEP will not check Contact/Via header etc. while sending SIP messages and will follow Symmetric Signaling.

If you select *RFC 3581*, the system follows Standard RFC while sending SIP messages.

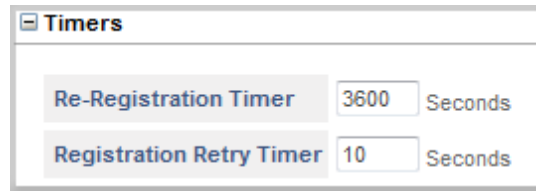
Default: Forced NAT.

- Click **Submit** to save the changes.

Timers

If you have selected the SIP Trunk **Mode** as **Proxy**, configure the Timers.

- Click **Timers**.



The screenshot shows a window titled "Timers" with two configuration rows. The first row is "Re-Registration Timer" with a text input field containing "3600" and the unit "Seconds". The second row is "Registration Retry Timer" with a text input field containing "10" and the unit "Seconds".

Timer Name	Value	Unit
Re-Registration Timer	3600	Seconds
Registration Retry Timer	10	Seconds

- Set the duration of the **Re-registration Timer**. This is the time period after which the SETU VTEP will send registration request to maintain registration binding with the Registrar Server. Valid range is 00001 to 65535 seconds. Default: 3600 seconds.
- Set the duration of the **Registration Retry Timer**. When a registration attempt fails, SETU VTEP will resend registration request to the Registrar Server after the expiry of the Re-registration Timer. Valid range is 00001 to 65535. Default: 10 seconds.



*The above timers will be applicable only if, **SIP Registration** is enabled in **SIP Trunk**.*

SIP VoIP Profile

You can either edit the settings of the default **VoIP Profile 1** or you can add a new profile. To do so, click **Add New Profile**.

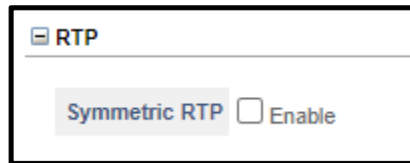
- Click **Advanced Settings** to expand.
- Click **SIP VoIP Profile** under **SIP Profile**.
- The **SIP VoIP Profile** page opens.

The screenshot displays the configuration interface for the SIP VoIP Profile. On the left, a navigation menu shows 'Basic Settings' and 'Advanced Settings'. Under 'Advanced Settings', the 'SIP Profile' section is expanded, and 'SIP VoIP Profile' is selected. The main content area is titled 'VoIP Profile 1'. It contains a 'SIP VoIP Profile' section with an 'Enable' checkbox checked and a 'Name' field set to 'VoIP Profile 1'. Below this are several expandable sections: RTP, SRTP, DTMF, FAX, T.38 FAX Parameters, and Pass-Through FAX Parameters. The 'Pass-Through FAX Parameters' section is expanded, showing a 'Pass-Through FAX Codec' dropdown menu set to 'G.711 (μ-law)'. At the bottom of the page are three buttons: 'Submit' (with a checkmark icon), 'Default' (with a plus icon), and 'Add New Profile' (with a plus icon).

- Configure the following parameters:
 - Keep the **SIP Network Profile** check box enabled to use this profile.
Clear this check box if you do not want to use this profile.
 - Assign a **Name** to the VoIP Profile for identification. The Name can be a maximum of 24 characters.

RTP

- Click **RTP**.

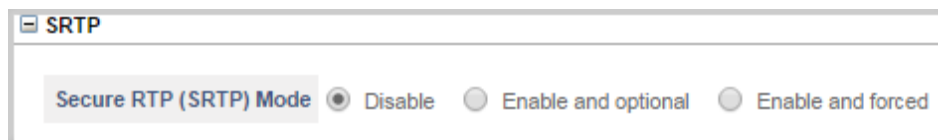


RTP Port is the port on which the SETU VTEP listens for RTP Packets. This port is also used as the source port for sending RTP packets to the remote peer.

- Select the **Symmetric RTP** check box, if you want the system to send RTP packets to original IP and Port from where RTP packets are received. Default: Disabled.

SRTP

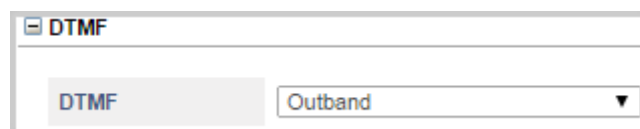
- Click **SRTP**.



- For secure conversations over SIP, SETU VTEP supports the **Secure RTP (SRTP)** mode. Default: Disabled. Select the desired option as per your requirement:
 - Select **Disable**, if you want SETU VTEP to use normal RTP instead of SRTP for transporting the speech packets.
 - Select **Enable and optional**, if you want SETU VTEP to use SRTP for transporting the speech packets. If the remote user does not support SRTP, normal RTP will be used.
 - If you select this option, you must configure the **SRTP Media Type**. You may select *AVP* or *SAVP*. Default: AVP.
 - Select **Enable and forced**, if you want SETU VTEP to use only SRTP (SAVP) for transporting the speech packets. If the remote user does not support SRTP, SETU VTEP will reject incoming calls from and drop outgoing calls made to such users.

DTMF

- Click **DTMF**.



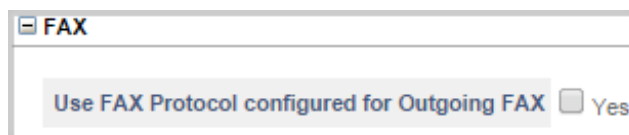
- Select the appropriate **DTMF** sending / receiving mechanism that is compatible with the DTMF sending/ receiving mechanism of your ITSP or remote peer.

- SETU VTEP supports:
 - **In-band:** System will send and detect digits in In-band only.
 - **Outband:** System will send and detect digits in Outband events only.
 - **SIP INFO:** System will send and detect digits in SIP INFO message only.
 - **Outband-->In-band:** System will send and detect digits in Outband, if negotiated in offer / answer else it will use In-band.
 - **SIP INFO-->In-band:** System will send and detect digits in SIP INFO, if negotiated in offer / answer else it will use In-band.
 - **Outband-->SIP INFO-->In-band:** System will send and detect digits in Outband or SIP INFO, if negotiated in offer / answer else it will use In-band. If both Outband and SIP INFO are negotiated, Outband will have priority over SIP INFO.
 - **SIP INFO-->Outband-->In-band:** System will send and detect digits in SIP INFO or Outband, if negotiated in offer / answer else it will use In-band. If both SIP INFO and Outband are negotiated, SIP INFO will have priority over Outband.

Default: Outband.

FAX

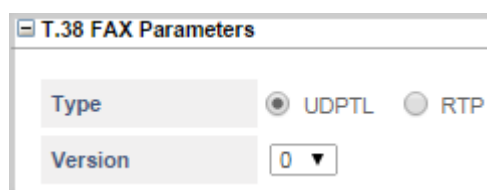
- Click **FAX**.



- Select the **Use FAX Protocol configured for Outgoing FAX** check box, if you want SETU VTEP to use the Fax Protocol configured for outgoing fax for this SIP Trunk and not the one that is received in RE- INVITE message from the remote end. Default: Disabled.

T.38 FAX Parameters

- Click **T.38 FAX Parameters**.



- Select the **Type** of Fax Protocol— UDPTL or RTP — that is compatible with your ITSP proxy server / remote peer. Default: UDPTL.
- For the Type you select, you must select a compatible **Version** — 0, 1, 2 — as supported by your ITSP proxy server / remote peer. Default: 0.

Pass-Through FAX Parameters

- Click **Pass-Through FAX Parameters**.



- Select an appropriate **Pass-Through FAX Codec** — G.711 (μ-law) or G.711 (A-law) — that is compatible with your ITSP proxy server/ remote peer. Default: G.711 (μ-law).

Codec Profile

You can either edit the settings of the **Codec Profiles** numbered from 1 to 8 or you can add a new profile.

- Click **Advanced Settings** to expand.
- Click **Codec** under **SIP Profile**.
- The **Codec Profile** page opens.

Codec Profile	Enable	Codec	p-time	Silence Suppression
1	<input checked="" type="checkbox"/>	G.729	20	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	G.723 (6.3 Kbps)	30	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	GSM FR	20	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	iLBC 30ms	30	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	iLBC 20ms	20	<input type="checkbox"/>
6	<input checked="" type="checkbox"/>	GSM EFR	20	<input type="checkbox"/>
7	<input checked="" type="checkbox"/>	G.711 (u-law)	20	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>	G.711 (A-law)	20	<input type="checkbox"/>

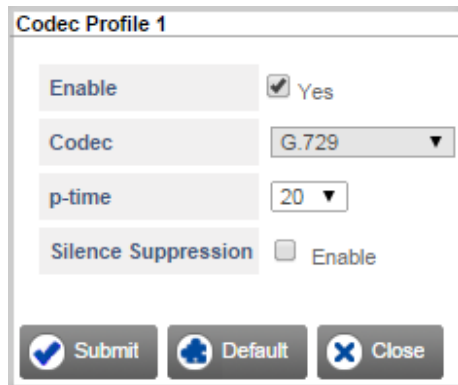
The **Codec Profile** page displays the following parameters:

- **Codec Profile:** It displays the Codec Profile numbers. To configure the Codec Profile Parameters, click on the desired Codec Profile number.
- **Enable:** Click the check box to enable the desired Codec Profile.
- **Codec:** It displays the Codecs assigned to each of the Codec Profile.
- **p-time:** It displays the p-time selected for each of the Codec Profile.
- **Silence Suppression:** It displays whether the Silence Suppression for the respective Codec Profile is enabled or not.

To configure the Codec Profile parameters:

- Click **Add New Profile** to add a new profile.

- To edit the existing profile, click on the **Codec Profile** number you want to edit.
- The respective **Codec Profile** window opens.



- Keep the **Enable** check box enabled to use this profile.

Clear this check box if you do not want to use this profile.

- The **Codec** is fixed for **Codec Profile 1** to **Codec Profile 8**. You can assign the desired **Codec** — G. 729, G.723, GSM FR, iLBC 30ms, iLBC 20ms, G.711 (u - Law), G.711 (A - Law) — only when you add a new Codec Profile.
- Select the desired **p-time** value, if you have selected codec as — G. 729, G.723, GSM FR, G.711 (u - Law), G.711 (A - Law) or GSM EFR.
- If you have selected codec G.723, select the desired **Bit Rate** — 5.3 Kbps or 6.3 Kbps. Default: 6.3kpbs.

When G.723 is negotiated, the selected Bit Rate will be applied only when sending the RTP packets. While receiving the RTP packets from the remote end, both the Bit Rates of G.723 will be accepted.

- For the codecs — G.729, G.723 and G.711 (u - Law) — select the **Silence Suppression** check box, if you want SETU VTEP to suppress the Silence packets and allow only the Voice packets to pass through. Default: Disabled.

Destination Port Determination

The process of routing calls originated on SIP Trunks and T1E1 Ports to the destination port in SETU VTEP takes place in two steps:

- Determination of Destination Number
- Determination of Destination Port

SETU VTEP supports different methods of determining the destination port for the calls originated on SIP Trunks and T1E1 Ports.

Destination Port Determination on SIP Trunks

For SIP Trunks, the system supports the following methods for Destination Port Determination:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number

To apply Destination Port Determination **on the basis of Calling Party Number**, you must configure the **SIP Trunk - Destination Port Determination - Calling Number Based** table.

To apply Destination Port Determination **on the basis of Destination Number**, you must configure the **SIP Trunk - Destination Port Determination - Destination Number Based** table.

Destination Port Determination on T1/E1 Port

For T1/E1 Port with **Orientation Type - Terminal**, the system allows you to configure the following destination port determination methods by Port, Channel and MSN Number/DDI Number:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number

For T1/E1 Port with **Orientation Type - Network**, the system allows you to configure the following destination port determination methods by Port and Channel:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number

To apply Destination Port Determination **On the basis of Calling Party Number**, you must configure the **T1E1 Port - Destination Port Determination - Calling Number Based** table.

To apply Destination Port Determination **On the basis of Destination Number**, you must configure the **T1E1 Port - Destination Port Determination - Destination Number Based** table.

Configuring SIP Trunk & T1E1 Port- Calling Number Based

- Click on SIP Trunk- Destination Port.
- The **SIP Trunk - Destination Port Determination - Calling Number Based** table window opens.

SIP Trunk - Destination Port Determination - Calling Number Based				
<input type="checkbox"/>	Edit	Calling Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>		No Match Found	T1E1 Group 1	None

Total Records : 1 1

Add Delete Close

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 499 entries.

Add Entry

Calling Number

Routing Group

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

Submit Close

- In **Calling Number**, enter the number (max. 24 characters) from which you expect calls to be received. Valid digits are 0 to 9, *, #, (dot). Default: Blank.
- Create the **Routing Group**.
- To create a group of *sequential T1E1 Ports* as members,

Routing Group


☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

- Select the desired **T1E1 Port** numbers as members. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.

- In **in - order**, select the order in which the system should hunt for a free member T1E1 Port to route the call.

Select **Ascending** to start hunting from the first to the last member T1E1 Port. Select **Descending** to start hunting from the last to the first member T1E1 Port. Default: Ascending.

- To create a group of *not-sequential T1E1 Ports* as members,
 - Select a **T1E1 Group**.
 - Select **T1E1 Group** number. Default: 1.
 - Click **Settings** .
 - The **T1E1 Port - Groups** window opens.

T1E1 Port - Group

T1E1 Group


1 ▼


Member Selection Method


First Free ▼

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1 ▼	01 ▼	14 ▼	Ascending ▼
2	2 ▼	01 ▼	30 ▼	Ascending ▼
3	None ▼	01 ▼	30 ▼	Ascending ▼
4	None ▼	01 ▼	30 ▼	Ascending ▼

 Submit

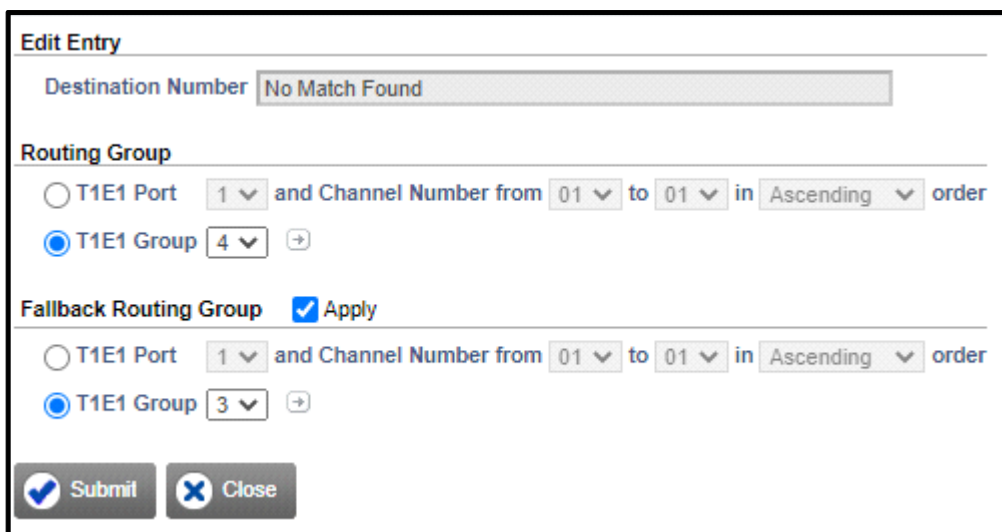
 Default

 Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic [“Group”](#) under *Advanced Settings*.
- Click **Submit** to save changes. The **Add Entry** window closes.
- To delete an entry, select the check box and click the **Delete** button.
- By default, T1E1 Port 1 - 1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** .




Edit Entry

Destination Number


Routing Group

☐ T1E1 Port and Channel Number from to in order

☒ T1E1 Group 

Fallback Routing Group ☒ Apply

☐ T1E1 Port and Channel Number from to in order

☒ T1E1 Group 

☒ Submit ☐ Close

- The **Edit Entry** window opens.
- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.
- You may create the **Fallback Routing Group**.



Fallback Routing Group ☒ Apply

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☒ Submit ☐ Close

- To do this,
 - Select the **Apply** check box.
 - Follow the same instructions provided earlier for creating *sequential* and *not-sequential* group of T1E1 Ports.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **SIP Trunk - Destination Port Determination - Destination Number Based** table.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.



If there are multiple entries in the Destination Number Based table, to search a particular entry in the table, under Testing enter the desired number to know which entry would be selected for routing search box.

- By default, T1E1 Port 1 - 1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- To configure the table for the T1/E1 Port, click **T1E1-Calling Number Based**.

The **T1E1 Port - Destination Port Determination - Calling Number Based** table window opens.

T1E1 Port - Destination Port Determination - Calling Number Based				
<input type="checkbox"/>	Edit	Calling Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>		No Match Found	SIP Trunk 1 - 1 (Ascending)	None

Total Records : 1 1

Add Delete Close

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 499 entries.

Add Entry

Calling Number

Routing Group

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☒ SIP Trunk to in order

☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

Submit Close

- In **Calling Number**, enter the number (max. 24 characters) from which you expect calls to be received. Valid digits are 0 to 9, *, #, (dot). Default: Blank.

- Create the **Routing Group**.
- To create a routing group of *sequential T1E1 Channels* as members,


The screenshot shows the 'Routing Group' configuration window. The 'T1E1 Port' option is selected with a radio button. The configuration is set to '1' and 'Channel Number from 01 to 01' in 'Ascending' order. The other options, 'T1E1 Group', 'SIP Trunk', and 'SIP Group', are not selected.

- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,
- Select **T1E1 Group**.

The screenshot shows the 'Routing Group' configuration window. The 'T1E1 Group' option is selected with a radio button. The configuration is set to '1' and has a '+' icon next to it. The other options, 'T1E1 Port', 'SIP Trunk', and 'SIP Group', are not selected.

- Select a **T1E1 Group** number. Default: 1.
- Click **Settings** .

- The **T1E1 Port - Group** window opens.

T1E1 Port - Group

T1E1 Group

Member Selection Method

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1	01	30	Ascending
2	2	01	30	Ascending
3	3	01	30	Ascending
4	4	01	30	Ascending

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic “[Group](#)” under *Advanced Settings*.
- You may create the **Fallback Routing Group**.

Fallback Routing Group ☒ **Apply**

☐ T1E1 Port and Channel Number from to in order


☐ T1E1 Group

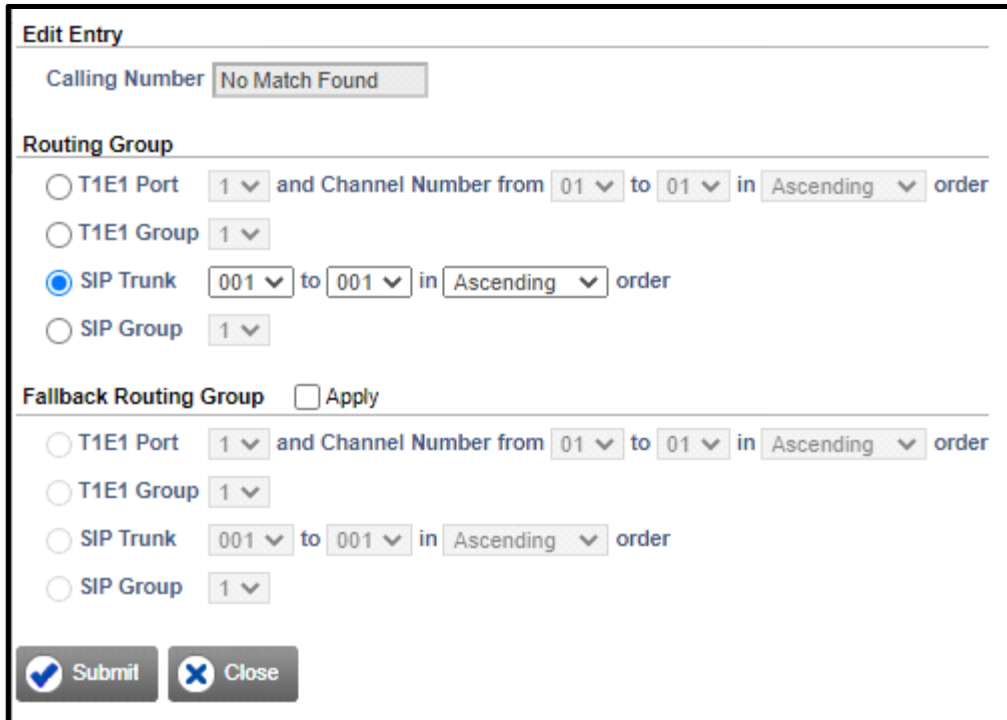
☒ SIP Trunk to in order

☐ SIP Group

- To do this,
 - Select the **Apply** check box.
 - Follow the same instructions provided earlier for creating *sequential* and *not-sequential* groups of T1E1 Ports and SIP Trunks.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **T1E1 Port - Destination Port Determination - Calling Number Based** table.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.
- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** .



Edit Entry

Calling Number

Routing Group

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☒ SIP Trunk to in order

☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- The **Edit Entry** window opens.
- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.

Configuring SIP Trunk & T1E1 Port- Destination Number Based

The **SIP Trunk - Destination Port Determination - Destination Number Based** table window opens.

SIP Trunk - Destination Port Determination - Destination Number Based				
<input type="checkbox"/>	Edit	Destination Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>		No Match Found	T1E1 Group 1	None

Total Records : 1 1

Testing

Enter the destination number to know which entry would be selected for routing

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 250 entries.

Add Entry

Destination Number

Routing Group

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

- In **Destination Number**, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + *Wildcard Characters*). Valid characters are 0 to 9, *, #, X, T, Comma [, Hyphen [-], Caret [^]. Default: Blank.

Wildcard Characters

SETU VTEP supports following characters.

Character	Description
X (letter X)	X represents any single digit from 0 to 9.
#	When # is configured in a number string, it will not be considered as End of Dialing.
*	When * is configured in a number string, it will not be considered as End of Dialing.
+	+ (plus) can be configured as a first character of the Destination Number string in the <i>SIP Trunk-Destination Port Determination-Destination Number Based</i> table only.

[-]	Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket.
[,]	Comma within a bracket is used as a separator between the groups of numbers.
[^]	Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret.
T (letter T)	Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing.

- Create the **Routing Group**.
- To create a group of *sequential T1E1 Ports* as members,

Routing Group

☒ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

Fallback Routing Group ☒ Apply

☐ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

- Select the desired **T1E1 Port** numbers as members. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member T1E1 Port to route the call.

Select **Ascending** to start hunting from the first to the last member T1E1 Port. Select **Descending** to start hunting from the last to the first member T1E1 Port. Default: Ascending.

- To create a group of *not-sequential T1E1 Ports* as members,
 - Select a **T1E1 Group**.
 - Select **T1E1 Group** number. Default: 1.
 - Click **Settings**

- The **T1E1 Port - Group** window opens.

T1E1 Port - Group

T1E1 Group
1

Member Selection Method
First Free

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1	01	30	Ascending
2	2	01	30	Ascending
3	None	01	30	Ascending
4	None	01	30	Ascending

Submit
Default
Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic “Group” under *Advanced Settings*.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.
- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).
- To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,
- To configure the table for the T1/E1 Port, click **T1E1-Destination Number Based**.

The **T1E1 Port - Destination Port Determination - Destination Number Based** table window opens.

T1E1 Port - Destination Port Determination - Destination Number Based

<input type="checkbox"/>	Edit	Destination Number	Routing Group	Fallback Routing Group
<input type="checkbox"/>		No Match Found	SIP Trunk 1 - 1 (Ascending)	None

Total Records : 1
1

Testing

Enter the destination number to know which entry would be selected for routing

Add
Delete
Close

- To add a new entry, click **Add**. The **Add Entry** window opens. You can add upto 1000 entries.

- In **Destination Number**, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + *“Wildcard Characters”*) in this field. Valid characters are 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

Wildcard Characters

SETU VTEP supports following characters.

Character	Description
X (letter X)	X represents any single digit from 0 to 9.
#	When # is configured in a number string, it will not be considered as End of Dialing.
*	When * is configured in a number string, it will not be considered as End of Dialing.
+	+ (plus) can be configured as a first character of the Destination Number string in the <i>SIP Trunk-Destination Port Determination-Destination Number Based</i> table only.
[-]	Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket.
[,]	Comma within a bracket is used as a separator between the groups of numbers.
[^]	Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret.
T (letter T)	Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing.

- Create the **Routing Group**.

- To create a routing group of *sequential T1E1 Channels* as members,

Add Entry

Destination Number

Routing Group

☒ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order

☐ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.
- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,
- Select **T1E1 Group**.

Routing Group

☐ T1E1 Port and Channel Number from to in order

☒ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- Select a **T1E1 Group** number. Default: 1.
- Click **Settings** .

- The **T1E1 Port - Group** window opens.

T1E1 Port - Group

T1E1 Group: 1

Member Selection Method: First Free

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1	01	30	Ascending
2	2	01	30	Ascending
3	3	01	30	Ascending
4	4	01	30	Ascending

Submit Default Close

- Create the T1E1 Group. For detailed instructions on creating groups, see the topic “[Group](#)” under *Advanced Settings*.
- Similarly, you can create a group of *sequential* and *not-sequential* SIP Trunk Port.
- You may create the **Fallback Routing Group**.

Fallback Routing Group ☒ Apply

☒ T1E1 Port 1 and Channel Number from 01 to 01 in Ascending order

☐ T1E1 Group 1

☐ SIP Trunk 001 to 001 in Ascending order

☐ SIP Group 1


- To do this,
 - Select the **Apply** check box.
 - Follow the same instructions provided earlier for creating *sequential* and *not-sequential* groups of SIP Trunks.
- Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **T1E1 Port - Destination Port Determination - Destination Number Based** table.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.

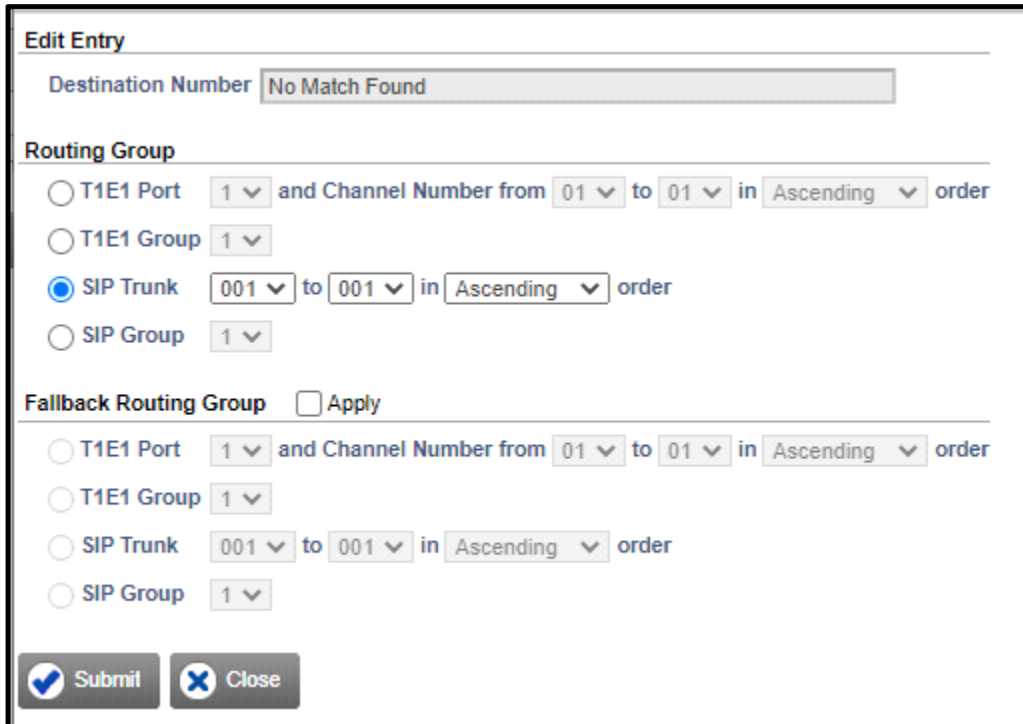


If there are multiple entries in the *Destination Number Based* table, to search a particular entry in the table, under *Testing* enter the desired number to know which entry would be selected for routing.

- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

- For the No Match Found entry in the table, click **Edit** .



Edit Entry

Destination Number

Routing Group

☐ T1E1 Port and Channel Number from to in order
☐ T1E1 Group
☒ SIP Trunk to in order
☐ SIP Group

Fallback Routing Group ☐ Apply

☐ T1E1 Port and Channel Number from to in order
☐ T1E1 Group
☐ SIP Trunk to in order
☐ SIP Group

☒ Submit ☐ Close

- The **Edit Entry** window opens.
- Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
- Click **Submit** and close the window.
- Close the window if you have finished adding/editing entries.

Group

SETU VTEP supports the following methods for determining the destination port for the calls originated on SIP Trunks and T1E1 Ports:

- Fixed
- on the basis of Destination Number
- on the basis of Calling Party Number

A Routing Group may have *sequential* or *not-sequential* ports as members.

A Routing Group of *sequential* ports is formed when you select **SIP Trunk** or **T1E1 Port** as the destination port.

A Routing Group of *not-sequential* ports is formed when you select **SIP - Group** or **T1E1 - Group** as the destination port. The **SIP/T1E1 Group** has members of the same port type, but not in a sequence. For example, a SIP Group can have only SIP Trunks as members.

Configuring Groups

To create a Group,

- Click the **Advanced Settings** link to expand.
- Click **SIP - Group** under **Group**.

The screenshot shows the configuration interface for a SIP Port - Group. On the left is a sidebar with a tree view containing sections: Basic Settings, Advanced Settings (expanded), and Maintenance. Under Advanced Settings, the 'Group' option is selected, and 'SIP - Group' is chosen. The main area is titled 'SIP Port - Group' and contains a dropdown for 'SIP Group' (set to 1), a 'Member Selection Method' dropdown (set to 'First Free'), and a 'Members' table. The table has two columns: 'Member Number' and 'Port Number'. It lists 9 members with port numbers 001 through 009, each with a dropdown arrow. At the bottom are three buttons: 'Submit', 'Default', and 'Default All'.

Member Number	Port Number
1	001
2	002
3	003
4	004
5	005
6	006
7	007
8	008
9	009

- You can create 9 SIP Trunk Groups with 9 members in each group.
- Select a SIP Group Number from **1 to 9**.

- To configure **Members** in the Group,
- For each **Member Number**, select a SIP Trunk number as **Port Number**. There can be upto 120 members in a Group.

If you do not want any more members in a group, select **None** as the **Port Number**. For example, you want two members in a group, select the SIP Trunk numbers for member 1 and 2, and set the remaining members in the group to None.

- Define the **Member Selection Method**. To route a call, the system checks availability of a free port. There are two options for port selection, namely:
 - **First Free:** The first port which is free will be used for routing the call each time. For example, SIP Group Number 1 has four members SIP Trunk 1 (Member 1), 2 (Member 2), 3 (Member 3) and 6 (Member 4). For every incoming call, SETU VTEP will check the status of Member 1 (SIP Trunk 1) first. If free, the call will be routed using this port else system will check status of Member 2 (SIP Trunk 2) and so on.
 - **Rotation:** The first call will be routed through the first member port and the subsequent call through the next member port and so on. For example, SIP Group Number 2 has four members SIP Trunk 6 (Member 1), 7 (Member 2), 8 (Member 3) and 9 (Member 4). For the first incoming call, SETU VTEP will check the status of Member 1 (SIP Trunk 6). If free, the call will be routed using this port else system will check status of Member 2 (SIP Trunk 7) and so on.

If the first call has been routed through Member 1 (SIP Trunk 6), then for the next call, system will check the status of Member 2 (SIP Trunk 7) but if the first call has been routed through Member 2 (SIP Trunk 7), then the system will check the status of Member 3 (SIP Trunk 8) to route the call. Similarly, for the subsequent calls the system will check the next member port in the group.

Default: **First Free**.

- Click **Submit** to save the group.
- Select **Default**, to set the parameters of a particular group to default.
- Select **Default All**, to set the parameters of all the groups to default.
-

To create T1E1 Group,

- Click the **Advanced Settings** link to expand.
- Click **T1E1 - Group** under **Group**.

T1E1 Port - Group

T1E1 Group: 1

Member Selection Method: Rotation

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1	01	30	Ascending
2	2	01	30	Ascending
3	3	01	30	Ascending
4	4	01	30	Ascending

Submit Default Default All

- You can create as many as 8 T1E1 Groups with maximum 4 members in each group.
- Select a T1E1 Group Number from **1 to 8**.
- To configure **Members** in the Group,
- For each **Member Number**, select a T1E1 Port number as **Port Number**. There can be upto 4 members in a Group.
- Define the **Member Selection Method**. To route a call, the system checks availability of a free port. There are two options for port selection, namely:
 - **First Free:** The first port which is free will be used for routing the call each time. For example, T1E1 Group Number 1 has four members T1E1 Port 1 (Member 1), 2 (Member 2), 3 (Member 3) and 4 (Member 4). For every incoming call, SETU VTEP will check the status of Member 1 first. If free, the call will be routed using this port else system will check status of Member 2 and so on.
 - **Rotation:** The first call will be routed through the first member port and the subsequent call through the next member port and so on. For example, T1E1 Group Number 2 has four members T1E1 Port 1 (Member 1), 2 (Member 2), 3 (Member 3) and 4 (Member 4). For the first incoming call, SETU VTEP will check the status of Member 1 (T1E1 Port 3). If free, the call will be routed using this port else system will check status of Member 2 (T1E1 Port 4) and so on.

If the first call has been routed through Member 1 (T1E1 Port 1), then for the next call, system will check the status of Member 2 (T1E1 Port 2) but if the first call has been routed through Member 2 (T1E1 Port 2), then the system will check the status of Member 3 (T1E1 Port 3) to route the call. Similarly, for the subsequent calls the system will check the next member port in the group.

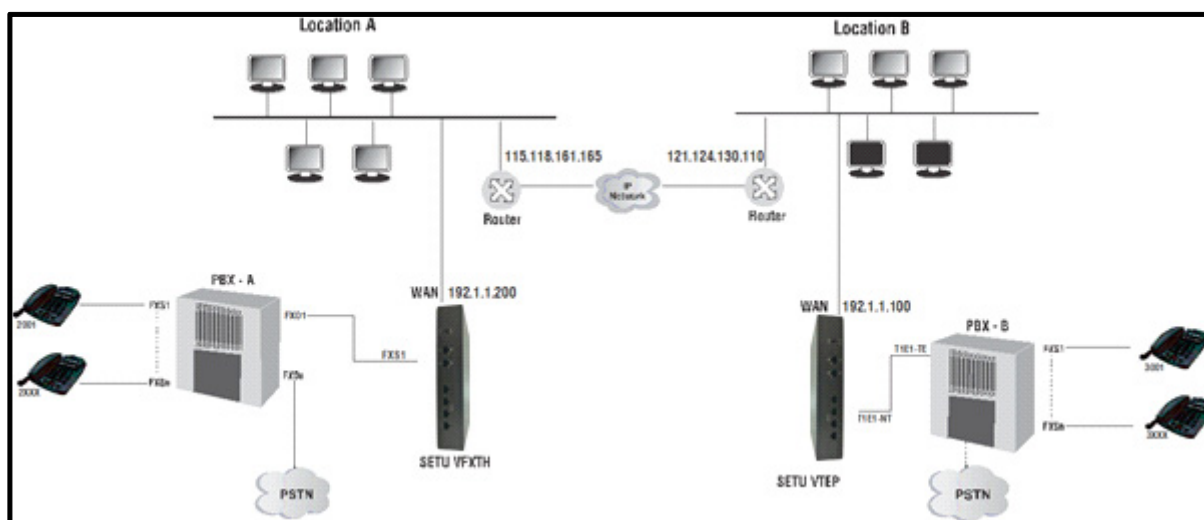
Default: **First Free**.

- Each Member can have multiple channels. For each Member,
 - Select the **Port Number**. If you do not want any more members in a group, select **None** as Port Number. For example, if you want two members, Member 1 and 2 in the Group, set Port Number for Member 3 and 4 to None.
 - Define the **Start Channel Number**. While determining the destination port, SETU VTEP will select this channel first for routing the calls originated on the T1E1 Port. Valid range is 1 to 30. Default: 1.
 - Define the **Total Channels** SETU VTEP should check while routing the call. Valid range is 1 or 30. Default: 30.
 - Set the sequence in which SETU VTEP should select the channel for routing the call as **Channel Selection Method**. You may select:
 - **Ascending**: When you select Ascending as Channel Selection Method, SETU VTEP will route call to first channel. If found busy the call will be routed to the next channel.
 - **Descending**: If you select Descending, SETU VTEP will route calls in the reverse sequence; starting from last channel to the first.
 - **Cyclic**: If you select Cyclic, SETU VTEP will route the first call to the first channel; if found busy the call will be routed to the next channel. If the first call has been routed through the first channel then the system will check the second channel for the next call but if the first call has been routed through the second channel, the system will check the third channel to route the call. Similarly, subsequent calls will be routed.
- Click **Submit** to save the group.
- Select **Default**, to set the parameters of a particular group to default.
- Select **Default All**, to set the parameters of all the groups to default.

Peer-to-Peer Dialing

Making an IP call without the intervention of a proxy server is called Peer-to-Peer Calling. As Peer-to-Peer calling does not require a proxy server, voice communication using this application can be done virtually free of cost. The major cost savings offered by this application makes it a very attractive mode of inter-branch or intra-office voice communication.

Let us understand how to use Peer-to-Peer Calling with the following illustration.



- Two offices are connected to the IP network.
- At Location A, a PBX (PBX A) and a Gateway (SETU VFXTH) is installed as shown above.
- SETU VTEP is installed at Location B.
- Peer-to-Peer calls can be made between the two locations with suitable configuration of SETU VTEP and the Gateway (SETU VFXTH).
- At **Location A**, you need to do the following configuration in SETU VFXTH:
 - Select a SIP Trunk to be used for this application and enable it. For example, SIP Trunk 1.
 - Set the **SIP Trunk Mode** of this trunk as **Peer-to-Peer**.
 - Keep the **SIP ID** of the SIP Trunk **blank**.



In the Router, you must configure the same SIP and RTP Ports as configured in the SETU VFXTH. In other words, you must configure Port Forwarding for SIP and RTP on the Router.

- By default, **Allowed IP Address for Incoming SIP Message** is set to **As per Peer to Peer table**. In the Peer to Peer table at Location A, you must configure the IP Address of the Router at Location B.
- Under **Handling of Incoming Calls** on the SIP Trunk, set the Incoming Call Routing option as **Route all incoming calls (with CLI) - to the Called Party Number**.

- For **SIP Trunk 1**, select the **Destination Port for Routing Calls** as **Fixed**, and create **Routing Group** as **FXS Port**.
- For **FXS Port**, select the **Destination Port for Routing Calls** as **Fixed**, and create **Routing Group** as **SIP Trunk 1** only.
- Now, configure the **Peer-to-Peer Table**.

In this example, you would have to configure the Peer-to-Peer table as follows:

- At Location A, in the Number field of the Peer-to-Peer table, enter the Number you want to dial to call the phone at Location B. In this case, 3001.
- For the number you entered, in the Destination Address field in the table, enter the IP Address of the Router connected at Location B. In this case, 121.124.130.110
- The Peer-to-Peer table you configure for SETU VFXTH at Location A would look like this:

Peer-to-Peer Dialing						
<input type="checkbox"/>	Edit	Destination Number	Minimum Digits	Maximum Digits	Destination Address	Name
<input type="checkbox"/>	➔	No Match Found	3	16		
<input type="checkbox"/>	➔	3001	3	16	121.124.130.110	Location B

Total Records : 2 1

+ Add
- Delete



Instead of configuring the complete number string, you may configure only the prefix of the number to be dialed as follows, the system will place all calls that start with '3' to the IP Address 121.124.130.110.

Destination Number	Destination Address	Name
No Match Found		
3	121.124.130.110	Location B

- At **Location B**, you need to do the following configuration in SETU VTEP:
 - Select a SIP Trunk to be used for this application and enable it. For example, SIP Trunk 1.
 - Set the **SIP Trunk Mode** of this trunk as **Peer-to-Peer**.
 - Keep the **SIP ID** field of the SIP Trunk **blank**.



In the Router, you must configure the same SIP and RTP Ports as configured in the SETU VTEP. In other words, you must configure Port Forwarding for SIP and RTP on the Router.

- By default, **Allowed IP Address for Incoming SIP Message** is set to **As per Peer to Peer table**. In the Peer to Peer table at Location B, you must configure the IP Address of the Router at Location A.

- Under **Handling of Incoming Calls**, set the Incoming Call Routing option as **Route all incoming calls (with CLI) - to the Called Party Number**.
- For **SIP Trunk 1**, select the **Destination Port for Routing Calls** as **Fixed**, and create **Routing Group** as **T1E1 Port** with **Start** and **End Channel** as **1** and **30**.
- For **T1E1 Port**, select the **Destination Port for Routing Calls** as **Fixed**, and create **Routing Group** as **SIP Trunk 1** only.

For instructions on configuring SIP Trunk parameters, see “[SIP Trunk](#)” under *Basic Settings*.

- Now, configure the **Peer-to-Peer Table**.

In this example, you would have to configure the Peer-to-Peer table as follows:

- At Location B, in the Number field of the Peer-to-Peer table, enter the Number you want to dial to call the phone at Location A. In this case, 2001.
- For the number you entered in the Destination Address field in the table, enter the IP Address of the Router connected at Location A. In this case, 115.118.161.165
- The Peer-to-Peer table you configure for SETU VTEP at Location B would look like this:

Peer-to-Peer Dialing				
<input type="checkbox"/>	Edit	Destination Number	Destination Address	Name
<input type="checkbox"/>		No Match Found		
<input type="checkbox"/>		2001	115.118.161.165	Location A

Total Records : 2 1

Testing
 Enter the destination number to know which entry would be selected for routing

- Configure PBX at location A such that calls received on the FXO Port of the PBX are routed to the FXS Port in sequential order, that is, calls to 2001 are routed to FXS 1 and so on. Similarly, when any FXS Port user dials a number starting with '3', it should be routed using the FXO Port of the PBX to the FXS Port of the SETU VFXTH.
- When user 2001 of Location A calls 3001, the call is routed using the FXO Port of the PBX to FXS Port of the SETU VFXTH. Further, it will be routed using the SIP Trunk of the SETU VFXTH to the IP address 121.124.130.110, as the system finds a matching entry for the dialed number in the Peer-to-Peer table.
- On receiving a call, the SETU VTEP at Location B routes this call through the T1E1 Port of the SETU VTEP to the T1E1 Port of the PBX B. Configure PBX at location B such that calls received on the T1E1 Port of the PBX are routed to the FXS Port in sequential order, that is, calls to 3001 are routed to FXS 1 and so on.
- Similarly, when the FXS Port user (3001) of Location B calls 2001, the call is received on the SIP Trunk of the SETU VTEP and is placed to the IP address 115.118.161.165, as the system finds a matching entry for the dialed number in the Peer-to-Peer table.

- On receiving a call, the SETU VFXTTH at Location A routes this call through the FXS Port of the SETU VFXTTH to the FXO Port of the PBX, which is further routed to 2001.

How to configure

For instructions on configuring the SIP Trunk parameters for the Peer to Peer application—SIP Trunk Mode, Peer to Peer Table, SIP ID, Handling of Incoming Call—see [“SIP Trunk”](#).

The Peer-to-Peer table stores upto 500 entries. Each entry consists of the parameters —Destination Number, Destination Address and Name.

To configure the Peer to Peer Table,

- Under Advanced Settings, click the **Peer-to-Peer Dialing** link.

The Peer-to-Peer table opens.

<input type="checkbox"/>	Edit	Destination Number	Destination Address	Name
<input type="checkbox"/>		No Match Found	192.168.1.100	

Total Records : 1 1

Testing

Enter the destination number to know which entry would be selected for routing

In the Peer-to-Peer table, the first entry is reserved for No Match Found.

- Click the **Add** button. A new window opens.

Add Entry

Destination Number

Destination Address

Name

- In **Destination Number**, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + [“Wildcard Characters”](#)) in this field. Valid characters: 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

If the number to be dialed out is <dialednumber@destination address>, for example, 1234@abc.com, you must enter 1234 in this field.

Wildcard Characters

SETU VTEP supports following characters.

Character	Description
X (letter X)	X represents any single digit from 0 to 9.
#	When # is configured in a number string, it will not be considered as End of Dialing.
*	When * is configured in a number string, it will not be considered as End of Dialing.
+	+ (plus) can be configured as a first character of the Destination Number string in the <i>SIP Trunk-Destination Port Determination-Destination Number Based</i> table only.
[-]	Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket.
[,]	Comma within a bracket is used as a separator between the groups of numbers.
[^]	Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret.
T (letter T)	Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing.

- In the **Destination Address** field, enter the domain name or IP Address to where the call is to be placed. The Destination Address may consists upto 40 characters (maximum). Default: Blank.

For example, if the peer-to-peer number to be dialed out is 1234@abc.com, enter abc.com as Destination Address. If the number is 1234@ 192.168.1.197, enter 192.168.1.197 as the Destination Address. The Destination Address can also be in the form of Address: Port number.

- In the **Name** field, enter a name to identify the number string you configured. It may be the name of your contact or any name you wish to assign to the number string. The name may consist of 24 characters (maximum). Default: Blank.

The name you configure here will not be used in SIP signaling.

- Click **Submit** to save your entries.



If there are multiple entries in the Peer to Peer table, to search a particular entry in the table, under Testing enter the desired number to know which entry would be selected for routing.

PIN Authentication

PIN Authentication is a necessary security feature to restrict access to the system and prevent possible misuse of the resources.

You can use PIN Authentication on the Source Port to establish the identity of callers before their call is processed by SETU VTEP.

PIN Authentication can be used on the Source Port only if the incoming call routing for the Source Port is set to ***Route calls After Answering the Call and Collecting the Digits***.

To be able to use PIN Authentication, this feature must be enabled on the Source Port and the PIN Authentication table must be configured.

The PIN Authentication table stores upto 500 PIN Numbers and their corresponding authentication Passwords.

When you enable PIN Authentication on the Source Port, SETU VTEP answers the incoming call on the port and plays the prompt tone. It waits for the caller to dial the PIN Number and the Password. It collects the digits dialed by the caller and matches them with the PIN Authentication table.

When a match is found in the table, SETU VTEP authenticates the caller and allows the call to be processed.

If the digits dialed by the caller do not match with any entry in this table, SETU VTEP allows the caller to make two more attempts to dial a valid PIN Number and Password. If the caller fails to dial the correct PIN and Password in all the attempts, the system disconnects the call.

Configuring PIN Authentication

To use this feature, you must enable PIN Authentication on the desired — SIP Trunks and T1E1 Ports (Terminal) — and configure the PIN Authentication Table.

To configure PIN Authentication table,

- Click the **Advanced Settings** link to expand.

- Click the **PIN Authentication** link.

Basic Settings
Advanced Settings

- System Parameters
- Dial Plan
- Number Lists
- Automatic Number Translation (ANT)
- SIP Profile
- Destination Number Determination
- Destination Port Determination
- Group
 - SIP - Group
 - T1E1 - Group
- Peer-to-Peer Dialing
- PIN Authentication**
- Digest Authentication
- Static Routing Table
- Access Code
- Emergency Number
- Certificate Manager
- Call Detail Records(CDR)

Maintenance
Status

Page Number 200 201-300 301-400 401-500

PIN Authentication

Index	PIN Number	PIN Password
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		
013		
014		
015		
016		
017		
018		
019		
020		

Submit Default All

- Now, configure the **PIN Authentication** table.
 - In **PIN Number**, enter the numbers with which callers will authenticate themselves. Default: Blank. The digits 0 to 9, * and # are allowed in PIN Numbers.



The length of the PIN Number must not exceed four digits. If you enter a PIN Number that is less than 4 digits, the system will add leading zeros. The caller must also dial the PIN Number with the leading zeros to authenticate.

- For each PIN Number you store, enter an authenticating password in **PIN Password**. The password can be of a maximum of four digits. The digits 0 to 9, * and # allowed. Default: Blank.
- Click **Submit** to save the entries.
- Now enable PIN Authentication on the desired — SIP Trunks and T1E1 Ports (Terminal) — port.

To do so, first you need to select **After Answering the Call and Collecting the Digits** as the Incoming Call Routing option under *Handling of Incoming Calls*. Now, enable **Prompt caller to enter PIN** on the respective port.

Under *Basic Settings*, see *SIP Trunk*, *T1 Port* and *E1 Port* for instructions.

Digest Authentication

Digest Authentication is a challenge-based authentication service of SIP to authenticate the identity of the originator of SIP request in the INVITE message. The recipient of the request can ascertain whether or not the originator of the request is authorized SETU VTEP to make the request. When the digest credentials of the originator — User Name and Password — in the INVITE message are authenticated and accepted by the recipient, the originator and the recipient are connected.

SETU VTEP supports Digest Authentication. The Digest Authentication feature works on the basis of the Digest Authentication Table in which the credentials — User Name and Password — of trusted/ authorised calling party SIP devices are stored. You must enable the Digest Authentication on the SIP Trunk and configure the Digest Authentication table.

SETU VTEP will check the Digest Authentication table,

- when you enable this feature on a SIP Trunk.
- when SIP Trunk mode is Peer to Peer and **Allowed IP Address for Incoming SIP Message** is set to **Any**.

For all incoming calls (SIP requests),

- SETU VTEP will challenge the identity of the calling party, that is, the SIP device initiating the request to send its digest credentials.
- When the calling party sends its credentials, SETU VTEP authenticates the credentials by matching it with its Digest Authentication Table.
- If a match is found, the calling party will be authenticated and the call will be allowed on the SIP Trunk.
- If no match is found, SETU VTEP will consider it as invalid authentication information and reject the call.

You may use Digest Authentication to:

- restrict access to SETU VTEP to specific callers.
- prevent unwanted or malicious calls.

Configuring Digest Authentication

To use this feature, you must enable **Digest Authentication** on the desired SIP Trunk and configure the Digest Authentication Table.

To configure Digest Authentication Table,

- Click the **Advanced Settings** link to expand.
- Click the **Digest Authentication** link.

The **Digest Authentication** Table window opens. You can configure upto 500 entries in this table. This Table is common for all SIP Trunks.

Index	User ID	User Password
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		
013		
014		
015		
016		
017		
018		
019		
020		

- Enter the user name assigned to the caller/ calling device in the **User ID**. SETU VTEP will use this User ID to match the digest credentials sent by the caller/ calling devices when challenged.

Make sure the User ID you enter here and the User ID assigned at the *calling end* are the same. The User ID may consist of a maximum of 40 characters. Default: Blank.

- Enter the password to authenticate the user ID in **User Password**. The password may consist of a maximum of 24 characters. Default: Blank.

Make sure the User Password you enter here and the User Password assigned at the calling end are the same.

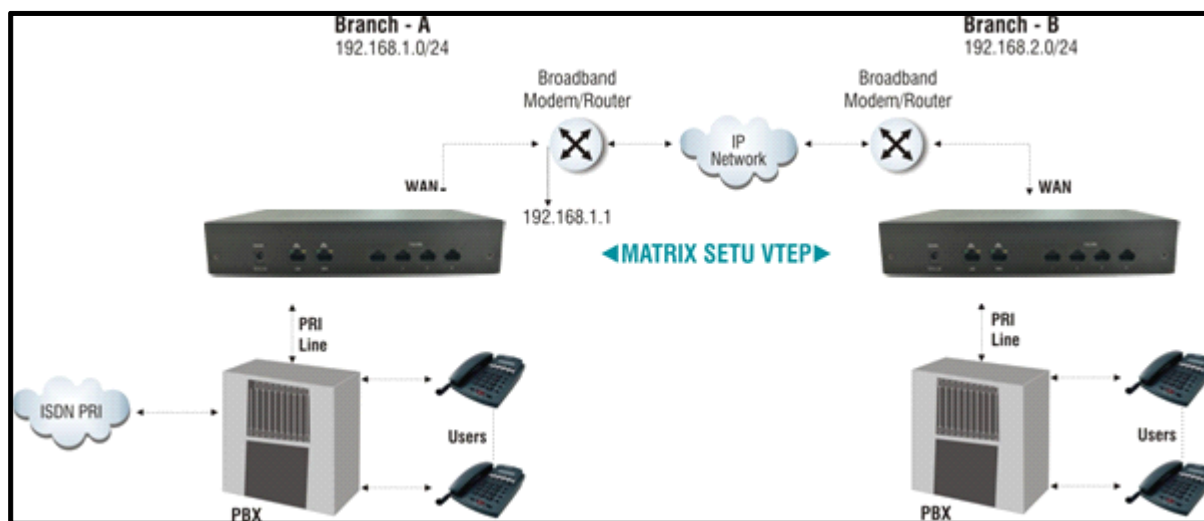
- Click **Submit** to save the entries.
- Make sure you enable Digest Authentication on the desired SIP Trunk. For instructions, see [“SIP Trunk”](#) under [“Basic Settings”](#).

Static Routing

Static Routing Table is required when you have more than one router (gateway) in your network and you want SETU VTEP to send packets to multiple routers/ gateways for different types of calls.

Static Routing Table helps route calls between point to point sites (connected through Multi Protocol Label Switching - MPLS, Frame Relay, etc.) and to public internet at the same time.

For example, two Local Area Networks, Network A and Network B, are connected through Frame Relay/ Multi Protocol Label Switching (MPLS) network to give access to local resources and also to make Peer-to-Peer calls. SETU VTEP is connected at both sites behind a router.



These sites are also connected to public IP network to:

- give internet access to local hosts.
- access DID service provided by ITSPs to make PSTN/ GSM calls over IP network.

Network A and Network B are in different subnets.

The Static Routing Table makes it possible to route different types of outgoing calls — Peer to Peer or Proxy — made to different subnets through different Gateways.

The Static Routing Table defines the appropriate Gateway Address (or Router's LAN Address) where the IP packets are to be sent.

In the Static Routing Table, you must configure:

- The address of the final Destination where the packets are to be sent.
- The Subnet Mask to be applied on the final destination address.
- The Gateway Address where the IP packets are to be sent.

When SETU VTEP sends packets, if the final destination IP Address and SETU VTEP are not in the same Subnet, the system will check the Static Routing Table.

If a perfect match is found, SETU VTEP will start sending the IP packets to the corresponding Gateway Address configured in the table.

If no match is found, SETU VTEP will send the IP Packets to the **Default Gateway Address** (Network Connection Type) you configured in the “[Network](#)” page.



- The Static Routing Table is common for all SIP Trunks.
- The Static Routing Table is applicable only when the Network Connection is established through WAN.

Configuring Static Routing Table

The Static Routing Table must be configured at each location where SETU VTEP is installed. To configure the Static Routing Table,

- Click the **Advanced Settings** link to expand.
- Click the **Static Routing Table** link.
- Static Routing Page opens.
- **IP v4 Addresses:**

Static Routing						
IPv4 Addresses						
Index	Destination Address	Subnet Mask	Gateway Address	Interface		Status
1	192.168.103.0	255.255.255.0	192.168.111.1	LAN	▼	Success
2	192.168.101.0	255.255.255.0	192.168.111.1	LAN	▼	Success
3				None	▼	NA
4				None	▼	NA
5				None	▼	NA
6				None	▼	NA
7				None	▼	NA
8				None	▼	NA
9				None	▼	NA
10				None	▼	NA
11				None	▼	NA
12				None	▼	NA
13				None	▼	NA
14				None	▼	NA
15				None	▼	NA
16				None	▼	NA
17				None	▼	NA
18				None	▼	NA
19				None	▼	NA
20				None	▼	NA

- **IPv6 Addresses:**

IPv6 Addresses					
Index	Destination Address	Prefix Length	Gateway Address	Interface	Status
1	2001::123	64	4001::1	WAN	Failed
2		64		None	NA
3		64		None	NA
4		64		None	NA
5		64		None	NA
6		64		None	NA
7		64		None	NA
8		64		None	NA
9		64		None	NA
10		64		None	NA
11		64		None	NA
12		64		None	NA
13		64		None	NA
14		64		None	NA
15		64		None	NA
16		64		None	NA
17		64		None	NA
18		64		None	NA
19		64		None	NA
20		64		None	NA

The Static Routing Table allows you to configure upto 20 entries for both IPv4 and IPv6 addresses. Each entry is stored against an Index number.

For each entry in IPv4 Addresses, you must configure the following:

- In **Destination Address**, enter the address of the final destination where the call is to be made. This can be a device IP Address or Network Address.
- In **Subnet Mask**, enter the subnet mask to be applied on the destination address.
- In **Gateway Address**, enter the IP address of the node where the IP packets are to be sent. Generally, it is the IP address of the LAN interface of the Router.

The Gateway Address must be in the same subnet as SETU VTEP.

- In **Interface**, choose from the given list of Interfaces which is to be applied on the particular destination address. The drop-down list includes LAN, WAN, Virtual WAN and None.
- Once all the details are entered in the Static Routing Table, then after checking all the details, **Status** will display either Success or Failed.
- Click **Submit** to save your entries.

For each entry in IPv6 Addresses, you must configure the following:

- In **Destination Address**, enter the address of the final destination where the call is to be made. This can be a device IP Address or Network Address.

- The Prefix Length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

The Prefix Length range is from 1 to 128 bits. Default: 64.

- In **Gateway Address**, enter the IP address of the node where the IP packets are to be sent. Generally, it is the IP address of the LAN interface of the Router.
- In **Interface**, choose from the given list of Interfaces which is to be applied on the particular destination address. The drop-down list includes LAN, WAN, Virtual WAN and None.
- Once all the details are entered in the Static Routing Table, then after checking all the details, **Status** will display either Success or Failed.
- Click **Submit** to save your entries.

As per the example, the Static Routing Table of SETU VTEP at Location A should be configured as:

Index	Destination Address	Subnet Mask	Gateway Address
1	192.168.2.0	255.255.255.0	192.168.1.1
2			
:			
8			

- The Destination Address 192.168.2.0 specifies the network address of Location B.
- The Subnet Mask is the mask to be applied on the Destination address.
- The Gateway Address 192.168.1.1 specifies the LAN address of the Router A which connects location A and location B.

The IP address of the LAN interface of the router which connects Location A to the public internet should be configured as Default Gateway in the Network Parameters of SETU VTEP at Location A.

With the Static Routing Table configured, all calls made by SETU VTEP to 192.168.2.0/ 24 will be routed through the router which connects Location A to Location B. Whereas, all calls made by SETU VTEP to addresses other than 192.168.2.0/ 24 will be routed through the Default Gateway.

Similarly, configure the Static Routing Table in SETU VTEP at location B to enable calling from Location B to Location A.

Access Code

Access Code is a string of digits dialed to use a feature. SETU VTEP users, can access the following features and facilities by dialing the Access Codes during call.

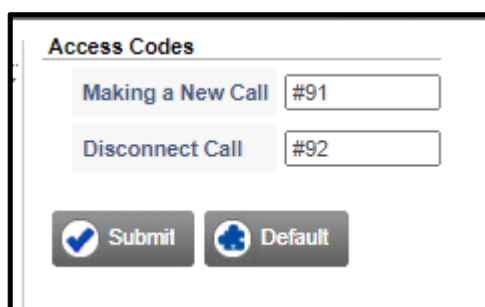
- Making a New Call (**#91**)
- Disconnect Call (**#92**)

You can change the default access codes assigned to the above features and facilities to suit your requirement.

Configuring Access Codes

To change the default Access Codes assigned to the features and facilities,

- Click the **Advanced Settings** link to expand.
- Click the **Access Code** link.

A screenshot of a web interface titled "Access Codes". It contains two rows of configuration options. The first row is "Making a New Call" with a text input field containing "#91". The second row is "Disconnect Call" with a text input field containing "#92". Below these fields are two buttons: "Submit" with a checkmark icon and "Default" with a globe icon.

- Change the default access code for the feature/ facility as per your requirement. Access Codes can be a maximum of 4 digits and digits 0-9, *, # and ^ are allowed.



Do not configure Access Codes that may conflict with the Emergency Numbers.

- Click **Submit** to save changes.

Emergency Number

SETU VTEP supports the dialing of Emergency Numbers from all ports. Emergency numbers and their respective Routing Groups (through which they are to be routed) must be configured in the Emergency Number Table.

When you select “*Region*”, the system loads the Emergency Numbers used in the country you selected as Region, in the Emergency Number Table.

For each of these numbers loaded, the system assigns a default Routing Group to route the number. You may reassign the Routing Group, as appropriate.

You may also add numbers of emergency services as per your requirement and assign Routing Group for the numbers in the Emergency Number Table.

You can configure up to 10 numbers of emergency services such as Ambulance, Fire Brigade, Police.



- *For a few Regions, the system may not load default Emergency numbers in the Emergency Table. You may add the numbers as per your requirement.*
- *Emergency number Dialing will not work if Mains power to SETU VTEP fails.*
- *Emergency Numbers have priority over Destination Number Table, PIN Number and Access Codes.*
- *The system does not apply End-of-Dialing when dialing Emergency Numbers.*
- *The system does not check Allowed-Denied Logic and Automatic Number Translation table when dialing an Emergency Number.*
- *Avoid configuring conflicting numbers as Access Code and Emergency Number.*

Configuring Emergency Numbers

To configure the Emergency Number Table,

- Click the **Advanced Settings** link to expand.
- Click the **Emergency Number** link.

The screenshot shows the 'Emergency Numbers' configuration page. On the left, the 'Advanced Settings' menu is expanded, and 'Emergency Number' is selected. The main content area features a table with the following structure:

	Edit	Emergency Number	Routing Group
<div><input type="button" value="Add"/> <input type="button" value="Delete"/></div>			

- To **Add** an Emergency Number in the table, click the **Add** button.
- Create the **Routing Group**.
- To create a routing group of *sequential T1E1 Port* as members,

The 'Add Entry' dialog box is shown. It includes an 'Emergency Number' input field. The 'Routing Group' section has four radio button options: 'T1E1 Port' (1), 'T1E1 Group' (1), 'SIP Trunk' (001 to 001 in Ascending order), and 'SIP Group' (1). The 'SIP Trunk' option is selected. At the bottom, there are 'Submit' and 'Close' buttons.

- Select the **T1E1 Port** Number. Default: 1.
- In Channel Number **From - to**, select the **Start Channel Number** and the **End Channel Number**, respectively.

- In **in - order**, select the order in which the system should hunt for a free member Channel to route the call.

Select **Ascending** to start hunting from the first to the last member channel. Select **Descending** to start hunting from the last to the first member channel. Default: Ascending.

- To create a group of *not-sequential T1E1 Channels* as members,
- Select **T1E1 Group**. Default: 1.

Add Entry

Emergency Number


Routing Group

☐ T1E1 Port and Channel Number from to in order

☒ T1E1 Group

☐ SIP Trunk to in order

☐ SIP Group

- Click **Settings** .
- The **T1E1 Port - Groups** window opens.


T1E1 Port - Group

T1E1 Group

Member Selection Method

Members

Member Number	Port Number	Start Channel Number	Total Channels	Channel Selection Method
1	1	01	30	Ascending
2	2	01	30	Ascending
3	3	01	30	Ascending
4	4	01	30	Ascending

- To **Edit** an Emergency Number and or assign a Routing Group, click **Settings**  of that number. A new window opens, to allow you to add/ edit the entry.
- The configurations are same as the procedure of adding a new Emergency number shown above.
- In **Emergency Number**, enter the emergency number used in your country/region.



Make sure that Access Codes you have configured do not conflict with the Emergency Numbers.

Certificate Manager

SETU VTEP supports certification for TLS, Web Server and Configuration Upgrade.

The two types of Certificates supported are: **Self-Signed Certificate** and **CA Signed Certificate**.

Self-Signed Certificate

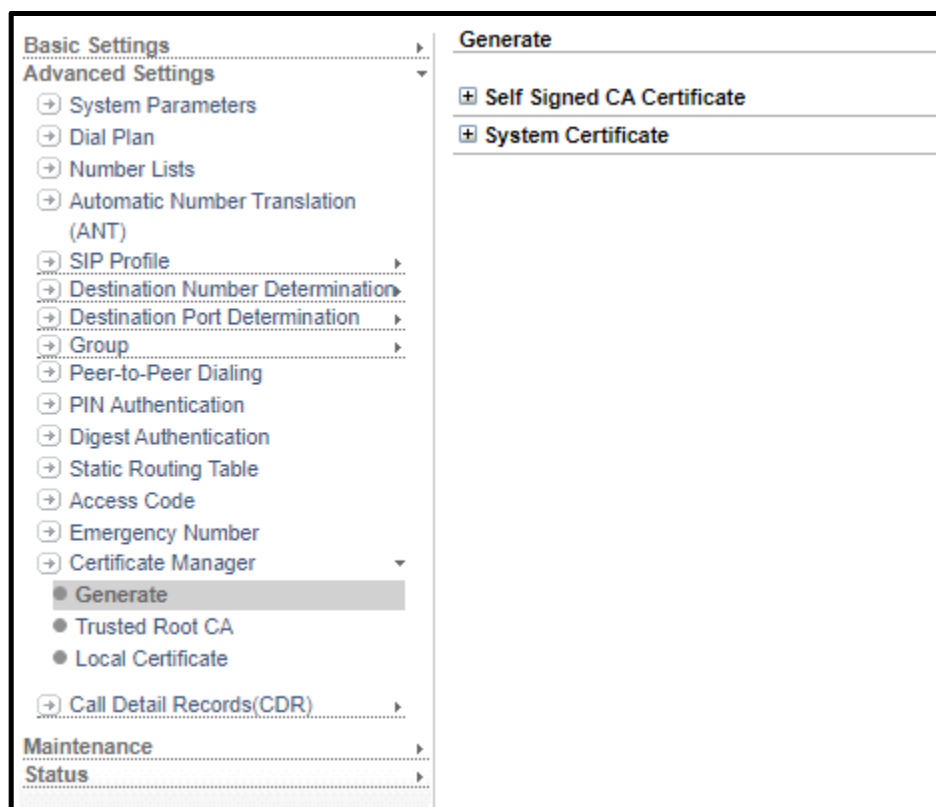
A self-signed certificate is created by the clients themselves or by the Servers and then given to their clients. It means that you yourself become the Certificate Authority (CA), create a CA Certificate and sign it. The self-signed certificate is faster to create but is not signed by a trusted CA Organization. The self-signed certificate must be installed in the trusted list of clients that connects over TLS with the Server. Because the certificate has been self-signed, the signature is not likely to be in the clients' trust file, hence, they need to add it.

If you select **Self-Signed Certificate**, you need to do the following:

1. Create a Self-Signed CA Certificate.
2. Create a System Certificate (Self-Signed Certificate).

Generating a Self-Signed CA Certificate

- Click **Generate** under the **Certificate Manager** link.



- Click **Self Signed CA Certificate** to expand and configure the following parameters.

Self Signed CA Certificate

Country Name - 2 letter code (eg. IN)	<input type="text"/>
State or Province Name - full name	<input type="text"/>
Locality Name (eg, city)	<input type="text"/>
Organization Name (eg, company)	<input type="text"/>
Organizational Unit Name (eg, section)	<input type="text"/>
Common Name (eg, System's hostname/IP Addr.)	<input type="text"/>
Email Address (eg. me@myhost.mydomain)	<input type="text"/>
Signature Algorithm	SHA-256 ▼

- In **Country Name - 2 letter code (e.g. IN)**, enter the name of your country.
- In **State or Province Name - full name**, enter the full name of your state or province.
- In **Locality Name (e.g. city)**, enter the name of your city.
- In **Organization Name (e.g. company)**, enter the name of your organization where SETU VTEP is installed.
- In **Organizational Unit Name (e.g. section)**, enter the name of the unit or section or domain of your organization, where SETU VTEP is installed.
- In **Common Name (e.g. System's hostname/IP Addr.)**, enter your Server's (SETU VTEP) host name or IP Address. This Common Name serves as the distinguishing factor.
- In **Email Address (e.g. me@myhost.mydomain)**, enter your host's e-mail address.
- Signature Algorithm:** SHA-1, SHA-256, SHA-512
- Click **Generate**, to generate this self-signed CA Certificate.

Once you generate self-signed certificate, you must send it to your clients so that they install it in their trusted list.

- To do this, click **Download**. Save the file at the desired location.

- Click the **Trusted Root CA** under **Certificate Manager** link. The CA Certificate you created appears in the **Root CA Certificate** table.

Trusted Root CA

Upload CA Certificate Choose File No file chosen (Valid format .cer, .crt & .pem)

Upload

Root CA Certificates

	Issued To	Issued By	Expiration Date	Friendly Name
<input type="checkbox"/>	192.168.101.220	192.168.101.220	Dec 31 2036	SelfSignedCaCertificate
<input type="checkbox"/>	www.MatrixComSec.com	www.MatrixComSec.com	Dec 31 2036	DefaultRootCertificate

Delete

- If you want to upload other CA Certificates, in **Upload CA Certificate** browse the location at which the certificate is saved and click **Upload**. The CA Certificate you uploaded appears in the **Root CA Certificate** table. Valid format are .cer, .crt and .pem.
- To delete a CA Certificate, select the check box of the respective Root CA Certificate and click **Delete**.

A sample Self-Signed CA Certificate is as follows:

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 2 (0x2)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=IN, ST=Gujarat, L=Vadodara, O=MATRIX COMSEC PVT. LTD., OU=R&D, CN=www.MatrixComSec.com/emailAddress=Support@MatrixComSec.com
Validity
  Not Before: Apr 30 07:42:32 2015 GMT
  Not After : Dec 31 07:42:32 2036 GMT
Subject: C=IN, ST=Gujarat, L=Vadodara, O=MATRIX COMSEC PVT. LTD., OU=R&D, CN=www.MatrixComSec.com/emailAddress=Support@MatrixComSec.com
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (2048 bit)
  Modulus:
    00:a2:93:45:0d:40:0b:97:90:a5:c5:83:ae:2a:25:
    d9:8d:55:05:06:09:d5:03:ed:b1:9f:53:34:b7:8f:
    2c:43:f6:d0:ff:a1:4e:30:ec:ed:8c:c8:b8:28:53:
    ad:25:19:19:a6:e4:da:3d:b1:75:79:c4:c7:e1:5f:
    58:ad:68:55:ae:f2:08:f8:82:f4:cc:be:cd:28:7a:
    8f:57:99:d7:41:e0:c4:57:a7:02:e9:7a:e1:95:1a:
    f2:9d:d0:66:49:17:60:a0:c9:51:eb:cd:ff:87:e0:
    1f:3f:5c:5d:34:46:67:67:22:99:2a:46:c6:16:3d:
    c1:3e:fc:f6:65:62:43:9e:d8:b1:99:96:c1:a3:47:
    03:53:78:17:77:22:fd:b5:c2:4a:94:9b:ec:b8:f3:
    52:c9:c7:cf:95:7c:a9:df:bc:c3:d2:2f:b7:26:1f:
    c5:0c:06:29:ae:c3:25:69:d2:eb:40:4a:0a:d4:cc:
    de:60:be:c2:73:33:3c:d1:cd:b7:a6:9f:37:0c:86:
    c8:28:52:b9:06:8f:3e:58:c1:e7:f4:7c:a0:0d:b9:
    91:40:53:b8:ac:42:99:2b:7c:12:ae:4c:57:34:c4:
    77:83:95:2b:be:3b:04:d7:58:3c:87:cf:f4:10:cf:
    80:15:44:f4:17:5d:c7:eb:73:42:01:88:b2:c8:10:
    9c:8b
  Exponent: 65537 (0x10001)
```

In the above Self-Signed CA Certificate:

- C = Country
- ST = State
- L = Location
- O = Organization
- OU = Organization Unit
- CN = Common Name
- **Issuer** represents the details of the CA issuing the Certificate. Here, the Organization itself is the CA (issuer), hence, the O, OU and CN of both Issuer and Subject is same.
- **Validity** represents the valid period of this certificate.
- **Subject** represents the credentials of the Server / User requesting for certification.
- **Public Key** represents the public key of the certificate.

Generating a System Certificate (Self-Signed Certificate)

After creating a Self-Signed CA Certificate, you can either,

- generate a System Certificate for your clients. These System Certificates can then be given to the respective clients.
- **or**
- the Clients can prepare their own System Certificates. For this you need to send them the CA Certificate created by you.
- **or**
- generate a Certificate Signing Request (CSR), if you want the Certificate to be signed by a third party.



If the clients prepare their own certificates, you need to send your CA Certificate to all the clients. The clients must upload the same in their system. Similarly, all the clients must send their CA Certificates to you and you must upload the same in your system. To avoid this, it is recommended that you create the Certificates and then provide it to your clients.

To create the System Certificate,

- Click the **Advanced Settings** link to expand.
- Click **Generate** under the **Certificate Manager** link to expand.

- Click **System Certificate** to expand and configure the following parameters.

System Certificate

Generate

☒ Self-Signed Certificate
 ☐ Certificate Signing Request (CSR)

Friendly Name

Country Name - 2 letter code (eg. IN)

State or Province Name - full name

Locality Name (eg, city)

Organization Name (eg, company)

Organizational Unit Name (eg, section)

Common Name (eg, System's hostname/IP Addr.)

Subject Alternate Name (eg. DNS:hostname,IP:ipaddr)

Email Address (eg. me@myhost.mydomain)

Validity upto

08 ▾

October ▾

2020 ▾

Signature Alogrithm

SHA-256 ▾

Generate

- In **Generate**, select the type of certificate you want to create. You must select **Self-Signed Certificate**.
- In **Friendly Name**, enter the name you want to assign to the certificate.
- In **Country Name - 2 letter code (e.g. IN)**, enter the name (two letter code) of your country.
- In **State or Province Name - full name**, enter the full name of your state or province.
- In **Locality Name (e.g. city)**, enter the name of your city.
- In **Organization Name (e.g. company)**, enter the name of your organization where SETU VTEP is installed.
- In **Organizational Unit Name (e.g. section)**, enter the name of the unit or section or domain of your organization, where SETU VTEP is installed.
- In **Common Name (e.g. System's hostname/IP Addr.)**, enter your Server's (SETU VTEP) host name or IP Address. This Common Name serves as the distinguishing factor.
- In **Subject Alternate Name (e.g. DNS:hostname,IP:ipaddr)**, enter the name of the multiple domain separated by comma (if the same certificate is to be issued for multiple domain of the organization).
- In **Email Address**, enter the your host's e-mail address.
- In **Validity Upto**, select the date till which this certificate will be valid.
- **Signature Algorithm:** SHA-1, SHA-256, SHA-512

- Click **Generate**, to generate this System Certificate.
- Under **Certificate Manager**, click the **Local Certificate** link. The generated certificate appears in the **Local Certificates** table.

Local Certificates

Upload Certificate No file chosen (Valid format .cer, .crt & .pem)

Upload Private Key No file chosen (Valid format .pem & .key)

Private Key Pass-Phrase (optional)

<input type="checkbox"/>	Issued To	Issued By	Expiration Date	Friendly Name	Download
<input type="checkbox"/>	www.MatrixComSec.com	192.168.101.220	Dec 31 2036	DefaultServerCert_Setu	
<input type="checkbox"/>	192.168.101.98	192.168.101.220	Dec 31 2036	IN_Setu	
<input type="checkbox"/>	192.168.101.98	192.168.101.220	Dec 31 2036	anmol_test_Setu	

- If you want to upload other System Certificates, in **Upload Certificate** browse the location at which the certificate is saved. Along with the certificate you also need to upload the Private Key, in **Upload Private Key** browse the location at which the key is saved and click **Upload**.

The System Certificate you uploaded appears in the **Local Certificates** table. Valid formats for certificate are .cer, .crt and .pem. Valid format for key are .pem and .key (Base64 encoded ASCII file).

- To delete a System Certificate, select the check box of the respective Certificate and click **Delete**.
- To download the System Certificate, click **Download**

A sample Default Server System Certificate is as follows:

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 1 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=IN, ST=Gujarat, L=Vadodara, O=MATRIX COMSEC PVT. LTD., OU=R&D, CN=www.MatrixComSec.com/emailAddress=Support@MatrixComSec.com
  Validity
    Not Before: Apr 30 07:59:06 2015 GMT
    Not After : Dec 31 07:59:06 2036 GMT
  Subject: C=IN, ST=Gujarat, L=Vadodara, O=MATRIX COMSEC PVT. LTD., OU=R&D, CN=www.MatrixComSec.com/emailAddress=Support@MatrixComSec.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:ae:e3:26:c7:54:a9:37:f7:11:42:19:0f:21:bd:
      3b:6e:9d:fe:9c:83:48:da:74:c9:d7:3f:2f:f3:bc:
      cb:33:e4:29:8c:e7:b5:5d:19:9d:e7:bd:27:e7:6e:
      16:60:60:35:13:cf:fb:e6:e4:48:e3:3a:a7:27:ae:
      4e:82:6a:05:9d:ec:e9:b6:bb:a1:80:56:73:39:28:
      a0:30:e3:23:f0:d9:31:19:57:cc:d7:a2:74:99:4d:
      cf:86:b6:d5:b8:0e:4e:5d:9c:ad:b4:56:dd:1e:37:
      1d:d0:49:03:32:a7:e7:02:64:bb:36:09:19:b0:43:
      34:f3:6b:83:61:9a:64:53:63:19:3d:e4:80:1b:39:
      f8:93:22:c6:f3:60:7a:1a:e2:de:81:eb:90:fa:f7:
      3b:88:4a:c6:38:62:32:93:b7:6b:d2:ea:87:6c:9f:
      7b:86:3f:fd:dd:0e:2b:a6:68:38:09:11:66:5f:e1:
      35:4c:d5:af:20:1a:b4:66:b9:30:f5:8b:0a:63:cc:
      30:4d:c6:e6:05:51:0e:62:ff:d7:b5:24:42:57:98:
      47:85:74:b8:7c:51:66:f7:42:9f:ce:62:f1:fb:07:
      b6:5b:74:3d:fe:a6:42:d1:80:1c:4a:10:51:9e:ee:
      e6:f1:7b:1b:31:05:35:fc:45:ed:1d:e1:5a:e2:e6:
      55:b5
    Exponent: 65537 (0x10001)
```

In the above Server Certificate,

- **Issuer** represents the details of the CA issuing the Certificate. Here, the Organization itself is the CA (issuer), hence, the O and CN of both Issuer and Subject is same.
- **Validity** represents the valid period of this certificate.
- **Subject** represents the credentials of the Server / User requesting for certification. Here, OU=R&D i.e. for whom the certificate is signed.
- **Public Key** represents the public key of the certificate.

CA Signed Certificate

Certificate Authority (CA) is a trusted organization which creates and sells TLS Certificates to websites. *CA Signed Certificates* are the TLS Certificates which are created by such trusted CAs, signed and sold to any applicant. These certificates contain a public key and the identity of the owner; and it is upto the CA to verify the owner's (applicant's) credentials. CAs issue a TLS Certificate to the organizations/websites after verifying their credentials. Generally, one TLS Certificate is issued for a particular server/website domain and it is valid for a certain period of time.

If you want to get a **CA Signed Certificate**, you need to do the following:

1. Generate and enroll the Certificate Signing Request (CSR).
2. Get the Certificate Signing Request (CSR) verified and signed by the Certified Authority (CA).

Generating the Certificate Signing Request

- Click the **Advanced Settings** link to expand.
- Click **Generate** under the **Certificate Manager** link.

- Click **System Certificate** to expand and configure the following parameters.

System Certificate

Generate

☐ Self-Signed Certificate
 ☒ Certificate Signing Request (CSR)

Country Name - 2 letter code (eg. IN)

State or Province Name - full name

Locality Name (eg, city)

Organization Name (eg, company)

Organizational Unit Name (eg, section)

Common Name (eg, System's hostname/IP Addr.)

Subject Alternate Name (eg. DNS:hostname,IP:ipaddr)

Email Address (eg. me@myhost.mydomain)

Signature Alogrithm

SHA-256

Private Key Pass-Phrase (optional)

Generate

Download CSR

- In **Generate**, select the type of certificate you want to create. You must select **Certificate Signing Request (CSR)**.
- In **Country Name - 2 letter code (e.g. IN)**, enter the name (two letter code) of your country.
- In **State or Province Name - full name**, enter the full name of your state or province.
- In **Locality Name (e.g. city)**, enter the name of your city.
- In **Organization Name (e.g. company)**, enter the name of your organization where SETU VTEP is installed.
- In **Organizational Unit Name (e.g. section)**, enter the name of the unit or section or domain of your organization, where your SETU VTEP is installed.
- In **Common Name (e.g. System's hostname/IP Addr.)**, enter your Server's (SETU VTEP) host name or IP Address. This Common Name serves as the distinguishing factor.
- In **Subject Alternate Name (e.g. DNS:hostname,IP:ipaddr)**, enter the name of the multiple domain separated by comma (if the same certificate is to be issued for multiple domain of the organization).
- In **Email Address (e.g. me@myhost.mydomain)**, enter your host's e-mail address.
- Signature Algorithm:** SHA-1, SHA-256, SHA-512
- Private Key Pass- Phase:**
- Click **Generate**, to generate this System Certificate.

- To send the certificate to the signing authority, click **Download CSR**. The Certificate and the Key downloads.

The Certificate Signing Request (CSR) to be sent to any trusted CA, appears as under:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDLDCCAhQCAQAwwaocCzAJBgNVBAYTAk1OMRAwDgYDVQQIEwdHdWphcmF0MREw
DwYDVQQHEWhWYWRvZGFyYTEgMB4GA1UEChMTUFUUK1YIENPTVNFQyBQV1QuIExU
RC4xDDAKBgNVBAsUA1ImRDEdMBsGA1UEAxMUd3d3Lk1hdHJpeENvbVNIYy5jb20x
JzAlBgkqhkiG9w0BCQEWGFN1cHBvcnRATWFOcm14Q29tU2VjLmNvbTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAPutA1/cZcz/qZe3soIITiVpPI8PIZ6d
9RvInx4haqVob7M110dYWvN2rLmFod3ZtEu9dX645crC4NXn9pxKXmkp5iNdBVca
rm1qedZ63S1cR3m4YhL2dUc7DQ9T1GNTFPbXLr1A4sQk+nVwO+C+XU/jPlpqiR0sn
Idh2/eLWVOauRgY3qdGjPaN8ndq8xVieY+v1/XpLQa4Oyd6aP+xn+z4pSWK4YLeP
36/CRh5q4f3vfMpuQTfegxGA+UB1V3qPMSqI0jBr7r1jptDxlmwzXkwz5w1rovh8
ZNP+1sIYPyZ9zrZm+eyhxpSX8o09jCcEm/R816x6GHEER7UGdZR1HvUCAwEAAaA8
MDoGCSqGSib3DQEJDjEtMCswCQYDVROTBAlwADALBgNVHQ8EBAMCBeAwEQYDVRO
BAowCIIIGTWF0cm14MA0GCSqGSIb3DQEBBQUAA4IBAQCQtMjNA13HAWYa9w1JGbKW
Yjoc/gbrhSUwgbR4Jh+13guInViTyJ5YDt9pLc8xzJe23MV2XDv4ImSSUSkRojcg
IpVTqNPgf91k50WmJHTIT0JJGEUXvzKE71V0kuf0XTelW0o81QYpjGn8GaSQQCDV
q746F0i84zwsejY+/jL+pDMpczxvbnnotWg+wCkMXwdkAk0InqL+DuSTEnuBEcW82
UF0rqoMdt90XpS9YZpjIsotRYgTRNIFaBFF4LxQa1bYQ15pZ79MxWJIZQZTnqHf
MbwSoss/QM7ZjE147b13m9Lk69jdzfSAPmCW4AdulBe7PENGGI+MMzfAVYYSwdkw
-----END CERTIFICATE REQUEST-----
```

Verification and Signing of the Certificate Signing Request by CA

On receiving the Certificate Signing Request (CSR), the CA verifies the Server's / User's credentials. After successful verification, the CA signs and sends the signed certificate.

After you receive the signed certificate, you must:

- Click the **Certificate Manager** link to expand.

- Click the **Local Certificate** link.

Local Certificates

Upload Certificate

Choose File

No file chosen

(Valid format .cer, .crt & .pem)

Upload Private Key

Choose File




No file chosen

(Valid format .pem & .key)

Private Key Pass-Phrase (optional)

Upload

Local Certificates


<input type="checkbox"/>	Issued To	Issued By	Expiration Date	Friendly Name	Download
<input type="checkbox"/>	www.MatrixComSec.com	192.168.101.220	Dec 31 2036	DefaultServerCert_Setu	
<input type="checkbox"/>	192.168.101.98	192.168.101.220	Dec 31 2036	IN_Setu	
<input type="checkbox"/>	192.168.101.98	192.168.101.220	Dec 31 2036	anmol_test_Setu	

Delete

- In **Upload Certificate** browse the location at which the certificate is saved. Along with the certificate you also need to upload the Private Key, in **Upload Private Key** browse the location at which the key is saved and click **Upload**

The System Certificate you uploaded appears in the **Local Certificates** table. Valid formats for certificate are .cer, .crt and .pem. Valid format for key are .pem and .key (Base64 encoded ASCII file).

To delete a System Certificate, select the check box of the respective Certificate and click **Delete**.

To download the System Certificate, click **Download** .

Call Detail Records (CDR)

SETU VTEP enables you to generate reports of Call Detail Records of calls using various filters such as:

- The port from which the calls originate (Source Port)
- The port on which the calls terminate (Destination Port)
- Calls made on particular dates
- Calls made at a particular time
- Calls of a certain duration
- Calls of certain Called Party Numbers
- Calls of certain Calling Party Numbers
- Calls made with PIN Authentication
- Calls made without PIN Authentication

You can set the different filters as required and generate Call Detail Record Report. The reports can be used for analyzing the call records for different purposes like cost savings, productivity enhancement, security and privacy.

The system stores records of matured calls only and it generates reports only of the filters that are set. For example, if you have not enabled the filter for *Calls Originated from SIP Trunks*, the system will not generate report for calls originated from SIP Trunks.

SETU VTEP supports upto 2000 call record entries and these entries are stored using the First In First Out (FIFO) method. Call records remain stored even when the system is set to default or the Firmware is upgraded.

Call records can be cleared manually or downloaded at any time.

Configuring Call Detail Record Filters

- Click the **Advanced Settings** link to expand.
- Click **Filters** under **Call Detail Record (CDR)** link.

Filter	Apply Filter	From	To
Calls originated from SIP Trunks	<input checked="" type="checkbox"/>	001	125
Calls originated from T1E1 Ports	<input checked="" type="checkbox"/>	1	4
Calls originated from T1E1 Channels	<input checked="" type="checkbox"/>	01	30
Calls terminated on SIP Trunks	<input checked="" type="checkbox"/>	001	125
Calls terminated on T1E1 Ports	<input checked="" type="checkbox"/>	1	4
Calls terminated on T1E1 Channels	<input checked="" type="checkbox"/>	01	30
Calls Made From	<input checked="" type="checkbox"/>	03 Jan 2020	29 Sep 2020
Calls Made Between	<input checked="" type="checkbox"/>	00:02	00:11
Called Party Numbers Matching with Number List	<input checked="" type="checkbox"/>	01	
Calling Party Numbers Matching with Number List	<input checked="" type="checkbox"/>	01	
Call Duration equal to and greater than (HH:MM:SS)	<input checked="" type="checkbox"/>	00:00:00	
Calls without PIN Number	<input checked="" type="checkbox"/>		
Calls with PIN Number	<input checked="" type="checkbox"/>	0001	9999

Clear Call Records Download Call Records

Submit Default

Setting Filters

- To set the filters, click the **Filters** link under Call Detail Records (CDR).

By default, all the filters are enabled. You may disable the filter you do not want to use by clearing the related **Apply Filter** check box.

Some of these filters are enabled by default, you cannot disable them, but you can set them.

- Set the following filters as required:



The filters you set are not applied on the downloaded report. The CSV and TXT files will contain all the records, irrespective of the filters you set.

- Calls originated from SIP Trunks:** The system will generate report of calls that were received on the SIP Trunks of SETU VTEP for further routing. To generate report using this filter for a range of SIP Trunks, select the range of the SIP Trunks in the **From** and **To** fields.

You can also generate report for a single trunk, by setting the same trunk number in the **From** and **To** fields.

- Calls originated from T1E1 Ports:** The system will generate report of calls that originated from the T1E1 Ports. To generate report using this filter for a range of ports, set the range of the T1E1 Ports in the **From** and **To** fields.

You can also generate report for a single T1E1 Port, by setting the same port number in the **From** and **To** fields.

- Calls originated from T1E1 Channels:** The system will generate report of calls that originated from each T1E1 Channel. To generate report using this filter for a range of channels, set the range of the T1E1 Channels in the **From** and **To** fields.

You can also generate report for a single T1E1 channel, by setting the same channel number in the **From** and **To** fields.

- **Calls terminated on SIP Trunks:** The system will generate report of calls terminated on the SIP Trunks. To generate report using this filter for a range of SIP Trunks, set the range of the SIP Trunks in the **From** and **To** fields.

To generate report for calls terminated on a single SIP Trunk, set the same trunk number in both fields.

- **Calls terminated on T1E1 Ports:** The system will generate report of calls that terminated the T1E1 Ports. To generate report using this filter for a range of ports, set the range of the T1E1 Ports in the **From** and **To** fields.

You can also generate report for a single T1E1 Port, by setting the same port number in the **From** and **To** fields.

- **Calls terminated on T1E1 Channels:** The system will generate report of calls that terminated on each T1E1 Channel. To generate report using this filter for a range of channels, set the range of the T1E1 Channels in the **From** and **To** fields.

You can also generate report for a single channel, by setting the same channel number in the **From** and **To** fields.

- **Calls made From:** The system will generate report of calls made between particular dates. Enter the start date and end date in the corresponding **From** and **To** fields.
- **Calls made Between:** The system will generate report of calls made between a particular time period. Enter the start time and end time in the corresponding **From** and **To** fields.
- **Called Party Number Matching with Number List:** The system generates report for calls made to specific numbers.

Select the Number List you want to assign to this filter. Make sure that you also configure this Number List with the Called Party Numbers which you want the system to match. See ["Number Lists"](#) for instructions.

- **Calling Party Numbers Matching with Number List:** The system generates report for calls received from specific numbers.
Select a Number List you want to assign to this filter. Make sure that you also configure this Number List with the Calling Party Numbers which you want the system to match. See ["Number Lists"](#) for instructions.
- **Call Duration equal to and greater than (HH: MM: SS):** The system generates report for calls of a specific time duration. Select the call duration in HH: MM: SS format.
- **Calls without PIN Number:** The system will generate report for calls without PIN Authentication.
- **Calls with PIN Number:** The system will generate a report for calls that were made using PIN Authentication. You can generate report of calls of specific PIN Numbers.

Enter the range of PIN Numbers in the **From** and **To** fields. PIN Numbers can be in the range of 0000 to 9999. The system will generate Report of all calls having PIN Numbers within the range you have set and display them under the 'PIN Numbers' column of the report.

If you want to generate report of a particular PIN Number, enter the same PIN Number in the **From** and **To** fields.

- Click **Submit** to save the settings.

Clear Call Records

- You can clear the call detail records any time you want by clicking the **Clear Call Records** button.

Calls Made From	<input checked="" type="checkbox"/>	03 ▾ - Jan ▾ - 2020 ▾	29 ▾ - Sep ▾ - 2020 ▾
Calls Made Between	<input checked="" type="checkbox"/>	00 ▾ : 02 ▾	00 ▾ : 11 ▾
Called Party Numbers Matching with Number List	<input checked="" type="checkbox"/>	01 ▾	
Calling Party Numbers Matching with Number List	<input checked="" type="checkbox"/>	01 ▾	
Call Duration equal to and greater than (HH:MM:SS)	<input checked="" type="checkbox"/>	00 ▾ : 00 ▾ : 00 ▾	
Calls without PIN Number	<input checked="" type="checkbox"/>		
Calls with PIN Number	<input checked="" type="checkbox"/>	0001	9999
<input type="button" value="Clear Call Records"/> <input type="button" value="Download Call Records"/>			

When call records are cleared, the **From** field of the filter **Calls Made Between** will change to the date of clearing of the records.

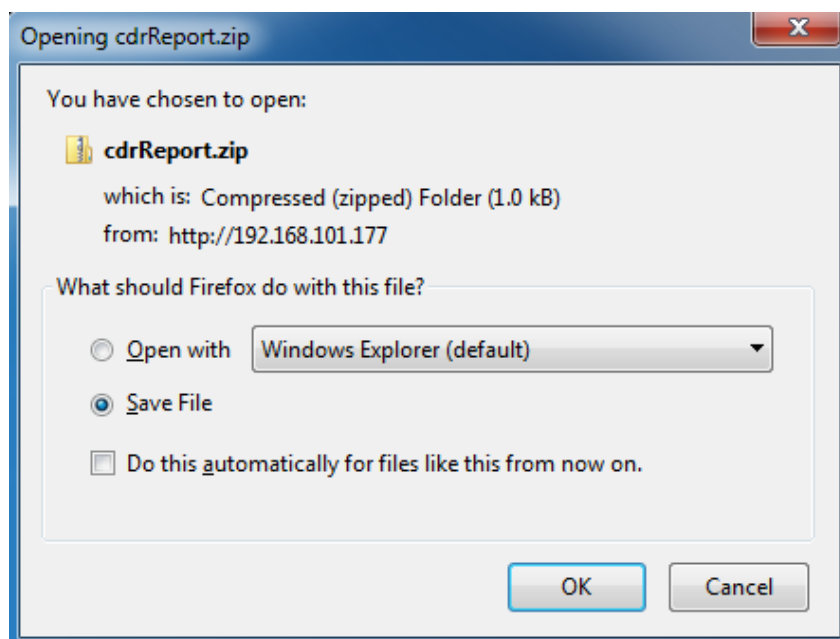
Download Call Records

- If you want to open/ save Call Detail Record Report on your computer, click the **Download Call Records** button.



*If you are using Mozilla Firefox (version 3.5 recommended), set the Downloads option of your browser as **Always ask me where to save the files**.*

- You will get a prompt with the option to open the **cdrReport.zip** file or save the file to a location. Save the file on the local disk.



- Open the cdrReport.zip file from the location you saved. The zip file contains the CDR report in Excel and Text format.

Printing Call Detail Record Report

- You can also print the Call Detail Record Report, if required.
- To print the CDR report in Excel format, open the file **CdrReport.csv**
- To print the CDR report in text format, open the file **CdrReport.txt**
- Print the file you opened. You may change the formatting of the text in the files before printing.



The filters you set are not applied on the downloaded report. The CSV and TXT files will contain all the records, without filters.

A sample **Call Detail Record Report** is presented at the end of this topic.

Viewing Call Detail Report

Click the **Report** link under Call Detail Record, to view the report generated by the system for the filters you have set.

Call Detail Record(CDR) Report				
Sr. No.	Date	Start Time	Calling Number	Called Number
0001	08-Oct-2020	23:17	2012@192.168.123.113	9999
0002	08-Oct-2020	23:18	2012@192.168.123.113	9999
0003	08-Oct-2020	23:18	2012@192.168.123.113	9999
0004	08-Oct-2020	23:19	2012@192.168.123.113	9999
0005	08-Oct-2020	23:19	2012@192.168.123.113	9999
0006	08-Oct-2020	23:19	2012@192.168.123.113	9999
0007	08-Oct-2020	23:19	2012@192.168.123.113	9999
0008	08-Oct-2020	23:20	2012@192.168.123.113	9999
0009	08-Oct-2020	23:20	2012@192.168.123.113	9999
0010	08-Oct-2020	23:20	2012@192.168.123.113	9999
0011	08-Oct-2020	23:20	2012@192.168.123.113	9999
0012	08-Oct-2020	23:20	2012@192.168.123.113	9999
0013	08-Oct-2020	23:21	2012@192.168.123.113	9999
0014	08-Oct-2020	23:21	2012@192.168.123.113	9999
0015	08-Oct-2020	23:21	2012@192.168.123.113	9999
Total Records : 2000 1 2 3 4 5 6 7 8 9 10 >>				

Call Detail Record(CDR) Report							
Sr. No.	Duration (sec)	Source Port	Destination Port	Disconnected By	Cause	PIN Number	Remarks
0001	00:00:05	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0002	00:00:05	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0003	00:00:05	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0004	00:00:06	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0005	00:00:02	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0006	00:00:05	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0007	00:00:02	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0008	00:00:06	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0009	00:00:03	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0010	00:00:05	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0011	00:00:02	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0012	00:00:05	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0013	00:00:02	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0014	00:00:06	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
0015	00:00:02	SIP-001	SIP-002	SIP-001	Normal Call Clearing (16)		N
Total Records : 2000 1 2 3 4 5 6 7 8 9 10 >>							

Call Detail Record Report generated as per the filters you set will appear in the following columns:

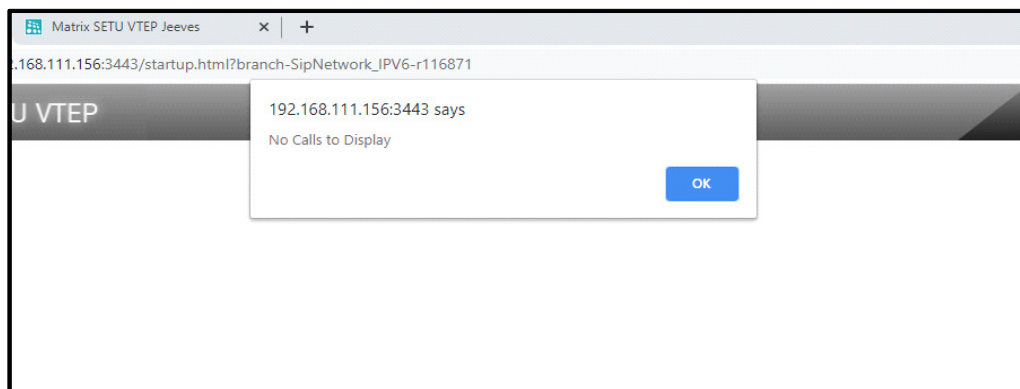
- **Date:** Calls made between particular dates.
- **Start Time:** Calls made during a particular time period.
- **Calling Number:** Calls received from specific numbers.
- **Called Number:** Calls made to specific numbers.

- **Duration:** Calls of a specific time duration.
- **Source Port:** Calls originated from the SIP Trunks/T1E1 Ports.
- **Destination Port:** Calls terminated on the SIP Trunks/T1E1 Ports.
- **Disconnected By:** The port that disconnected the call.
- **Cause:** The cause for disconnection.
- **PIN Number:** Calls made using PIN Authentication, the PIN Number dialed by the caller.
- **Remarks:** The type of call. A for Anonymous, U for Unanswered and N for Normal.

The total number of the records is displayed below the table.

On each page, 15 records are displayed. Click the page number at the bottom of the report to view the next 15 records.

The Alert message **No Calls to Display** will appear, if there are no records to be displayed.



SETU VTEP offers users the following features and facilities, which they can access by dialing the Access Codes assigned to them.

Making a New Call using Access Code

This feature enables callers to disconnect the current call and make a new call using SETU VTEP without getting disconnected from the system. This feature is useful when you want to allow users to make multiple calls without getting disconnected each time their call ends.

This feature is applicable only on the Source Port and only when **After Answering the Call and Collecting Digits** is selected as the **Destination Number Determination Method**. However, if you have enabled **Connect Source Port when Progress Indicator is received on T1/E1 Port** on the E1 Port or T1 Port or have enabled **Connect Source Port when 183 (Session Progress) is received on SIP** on the SIP Trunk, you will not be able to provide this feature to the users.

To provide this feature to users,

- you must enable **Allow making New Call using Access code** on the SIP Trunk and T1/E1 Port. See [“SIP Trunk”](#), [“E1 Port”](#) and [“T1 Port”](#) under *Basic Settings* for instructions.

To Make a New Call using Access Code,

- In speech during the current call.
- Dial **#91**. Current call will disconnect.
- Dial the new number you want to call.
- While in speech, dial **#91** again to make another call.

Disconnecting a Call using Access Code

SETU VTEP enables users to disconnect a call using an access code. When the call disconnect access code is dialed, SETU VTEP releases the port engaged in the call.

To provide this feature to users,

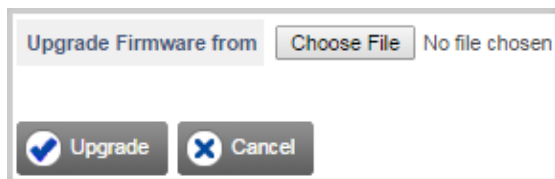
- you must enable **Allow Call Disconnection using Access code** on the SIP Trunk and T1/E1 Port. See [“SIP Trunk”](#), [“E1 Port”](#) and [“T1 Port”](#) under *Basic Settings* for instructions.

To Disconnect a Call using Access Code, dial **#92**.

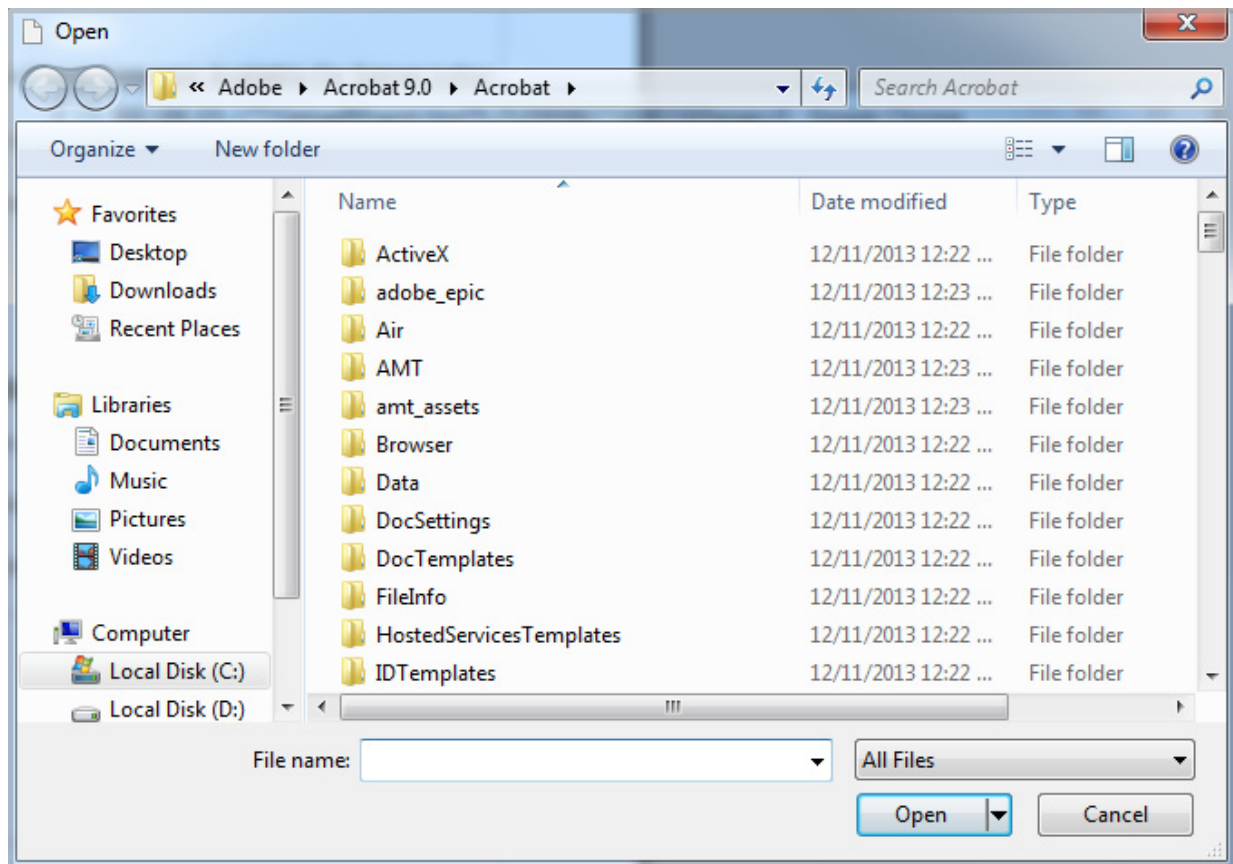
Firmware Upgrade

You can also upgrade firmware of SETU VTEP with the firmware files stored on your computer. To do so,

- Click the **Upgrade Firmware from PC** button. A new window - **Firmware Upgrade From** opens.
- Click the **Choose File** button to reach the location on the local disk on which the firmware files are stored.



- Select the required firmware files from the location on the local disk.



- The path to the file will appear in the **Firmware Upgrade From** box. Click the **Upgrade** button.

Configuration Upgrade

You can upgrade Configuration of SETU VTEP:

1. From the Auto Configuration Server
2. From a Personal Computer

Upgrading Configuration from the Auto Configuration Server

Auto Configuration Upgrade

Using Auto-Configuration, SETU VTEP can automatically download the configuration files stored at a central location: Auto Configuration Server (ACS).

This feature is useful for ITSPs that have deployed a large number of SETU VTEP. ITSPs can store the configuration files of each SETU VTEP that they have provided to their customers on the Auto Configuration Server (ACS).



*For the **Auto Configuration File** contact Matrix Support Team.*

To perform Auto Configuration,

1. Make sure that the configuration file of SETU VTEP is stored on the Auto-Configuration Server (ACS).
2. To ensure security, ITSP can encrypt the configuration file stored on the ACS. If the ITSP has encrypted the configuration file, the password to decrypt the file must be provided to you.
3. The following parameters must be configured in the SETU VTEP.
 - IP Address of the Auto Configuration Server (ACS).
 - Path of the Folder (containing the configuration file) on the Auto Configuration Server.
 - Password to decrypt the configuration file (if encryption is used).
 - The protocol to be used: TFTP, HTTP, HTTPS.
4. When SETU VTEP installed at a customer site connects to the ITSP network, it will automatically download its configuration file stored on the Auto-Configuration Server (ACS), without the intervention or assistance of a technician.

To configure Auto Configuration parameters,

- Click the **Maintenance** link to expand.

- Click the **Configuration** link.

Configuration

Auto Configuration Upgrade	<input checked="" type="checkbox"/> Enable
Protocol for Auto Configuration Upgrade	<input type="radio"/> TFTP <input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Server Address:Port	2001::192:168:111:20 : 443
Configuration Folder Path	
Upgrade Configuration Automatically at every Power ON	<input type="checkbox"/> Yes
Upgrade Configuration Automatically at Scheduled time	<input type="checkbox"/> Yes
Schedule Time	<input type="radio"/> Every 1440 Minutes <input type="radio"/> Everyday at time 00 : 00 <input checked="" type="radio"/> Every Month on Date 01 at time 00 : 00
Request Timeout	60 Seconds
Password to Decrypt Configuration File	

- By default, **Auto Configuration Upgrade** check box is enabled. You may clear this check box, if required.
- In **Protocol for Auto Configuration Upgrade**, select the protocol used by the Auto Configuration Server to upgrade the configuration. SETU VTEP generates file transfer request to the Auto-Configuration Server according to the protocol you select. You may select **TFTP**, **HTTP** or **HTTPS**. Default: HTTP.
- In **Server Address: Port**, enter the IP Address/Domain and the Port of the Auto Configuration Server on which the configuration files of SETU VTEP are stored.

The Auto Configuration Server Address can also be obtained by SETU VTEP using DHCP (using Option 224). To fetch Auto Configuration Server Address using DHCP, keep the Server Address: Port field blank.

Make sure that you also set the *Connection Type* on the [“Network”](#) page as *DHCP*.

The default Port differs as per the protocol you select. For TFTP, the Default Port is 69. For HTTP, the Default Port is 80. For HTTPS, the Default Port is 443. You can change the port as per your requirement. Valid range is 69/ 80/ 443/ 1031 to 65534.

- In **Configuration Folder Path**, specify the path of the folder on the Auto Configuration Server where the configuration files are stored. Default: Blank.
- Enable **Upgrade Configuration Automatically at Every Power ON** check box, if you want SETU VTEP to check for updates in the configuration file at each Power ON.



At Power ON, if both Auto Firmware upgrade and Auto Configuration upgrade are enabled, Auto Firmware upgrade has priority over Auto Configuration upgrade.

- Enable **Upgrade Configuration Automatically at Scheduled Time** check box, if you want SETU VTEP to check for updates in the configuration at a scheduled time. You may select any one of the following schedule options:
 - In **Every XX minutes**, enter the minutes after which you want SETU VTEP to check for configuration updates.
 - In **Everyday at HH:MM**, enter the time in **Hours(00-23)** and **Minutes(00-59)** after which you want SETU VTEP to check for configuration updates everyday.
 - In **Every Month on DD at HH:MM**, enter the **Date** (01-31) and **Time** in Hours (00-23) and Minutes(00-59) after which you want SETU VTEP to check for configuration updates every month.
- **Request Timeout** is the time for which SETU VTEP will try to connect to the Auto Configuration Server for TCP/TLS binding using HTTP or HTTPS. This timer specifies for how long SETU VTEP should wait for successful TCP/TLS binding.

Enter the required time in seconds. The range of Request Timeout is 01-99 seconds. Default: 60 seconds.

If SETU VTEP fails to connect to the Auto Configuration Server, it will make 10 attempts at a regular interval of 10 seconds to establish the binding. Even then, if it is unable to establish the binding, it will stop retrying and wait for next event of Auto Configuration upgrade.

- In **Password to Decrypt Configuration File**, enter the password as provided by your ITSP to decrypt the configuration file. During Auto Configuration, if SETU VTEP receives an encrypted configuration file, it will decrypt the file using this password.

The password may consist of 40 characters (maximum). Default: Blank.



The password is case-sensitive, make sure you enter the password in the same format as given to you by your ITSP.

- Click **Submit** to save.
- To view the status of Auto Configuration upgrade from Jeeves, see [“System Performance”](#) under [“Status”](#).

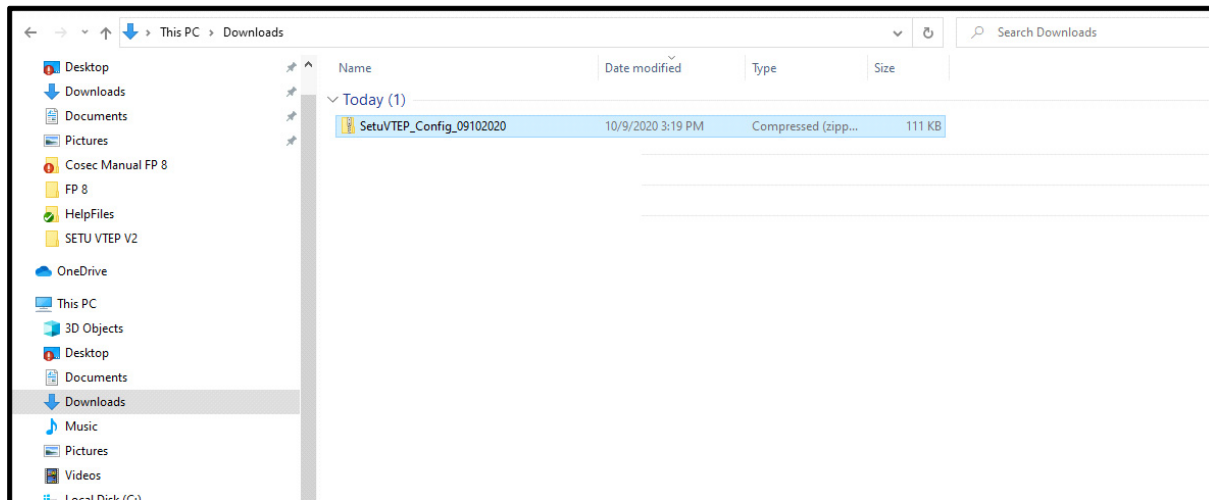
Manual Configuration Upgrade

To manually upgrade configuration of SETU VTEP, click the **Upgrade Configuration from Server** button.

Backup Configuration

- To save the existing configuration files as backup, click the **Backup Configuration** button.

The **SetuVTEP_Config_ddmmyyyy.zip** window will open; where ddmmyyyy signifies the current date.



- You can open the zip file.



The above window display depends upon the browser you are using. Check the **Download Settings** of your browser and set the Download path accordingly.

OR

If your browser does not ask you for the location you want to save your file, it saves it in the default location according to the download path specified for that browser.

If you are using Mozilla Firefox (version 3.5 recommended), before you save the configuration files, set the **Downloads** option of your browser as **Always ask me where to save files**.



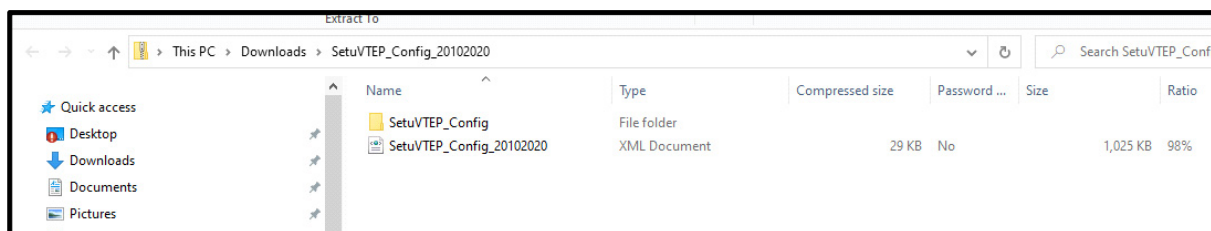
If you wish to upload the Backup Configuration of firmware V1R5.6 or later in system with firmware V1R5.5 or earlier, then make sure you upgrade the firmware to avoid system malfunction.

- Open the configuration file (.zip).

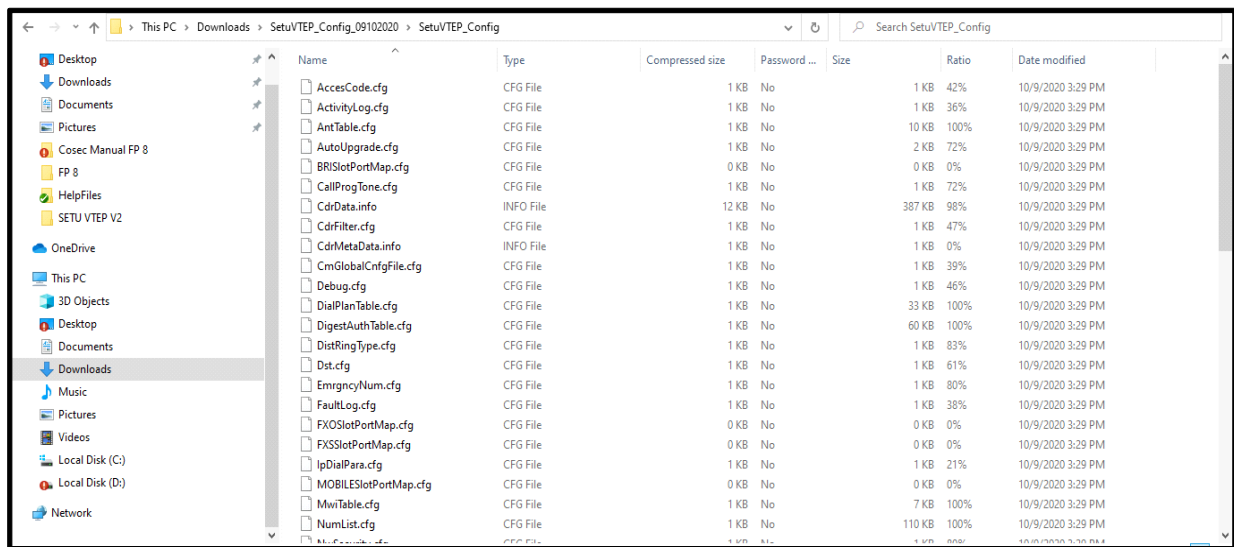


Save the back up configuration files by tagging the file name with the Version-Revision of the Firmware and tag the name of the backup folder on your computer with the date. This will help you at the time of restoring the back up configuration files.

The zip file contains all the system configuration files in .cfg format and xml format. You cannot edit the configuration files in .cfg format, however you can edit the configuration files in xml format and then upgrade the system with it.



- Open the **SetuVTEP_Config** folder to view the configuration files.



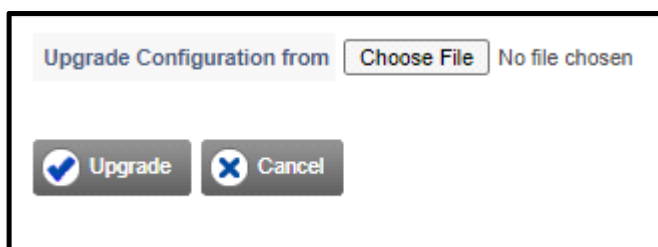
- Keep this folder as a backup. In case there is a problem with the system configuration files these backup files can be restored back in the system.
- Open **SetuVTEP_Config_09102020 XML** file.



Upgrading Configuration from a Personal Computer

You can upgrade configuration of SETU VTEP with the configuration files stored on your computer. To do so,

- Click the **Upgrade Configuration from PC** button. A new window - **Upgrade Configuration From** opens.



- Click the **Choose File** button to reach the location on the local disk on which the configuration file is stored.
- Select the required configuration files from the location on the local disk.
- The path to the file will appear in the **Configuration Upgrade From** box.
- Click the **Upgrade** button.



At a time, you can upgrade configuration either:

- manually or automatically from Auto Configuration Server*
- manually from a Personal Computer.*

Logs

Click on the **Logs** link if you want to check about all the activity performed in the respective Setu VTEP system.

Basic Settings

Advanced Settings

Maintenance

→ Firmware

→ Configuration

→ **Logs**

→ System Debug

→ System Activity Log

→ System Fault Log

→ Network Diagnosis

→ SNMP

→ System Port Activity

→ PCAP Trace

→ Manual Call Test

→ Default System

→ Soft Restart

→ T1E1 Port Alarms/Performance Monitoring

Status

Logs

File Name	Size	Last Modified
wdtCurLog.txt	270 Bytes	Sat Oct 10 10:53:38 2020
log_archive.zip	6.49 KB	Sat Oct 10 10:53:38 2020
service_run_history.log	1.00 KB	Sat Oct 10 10:53:38 2020
system_boot_up.log	16.40 KB	Sat Oct 10 10:53:38 2020
main_fs_booting.log	4.44 KB	Sat Oct 10 10:53:38 2020
snmp.log	2.98 KB	Sat Oct 10 10:53:38 2020
platform_upgrade.log	200 Bytes	Sat Oct 10 10:53:38 2020

Download all in zip

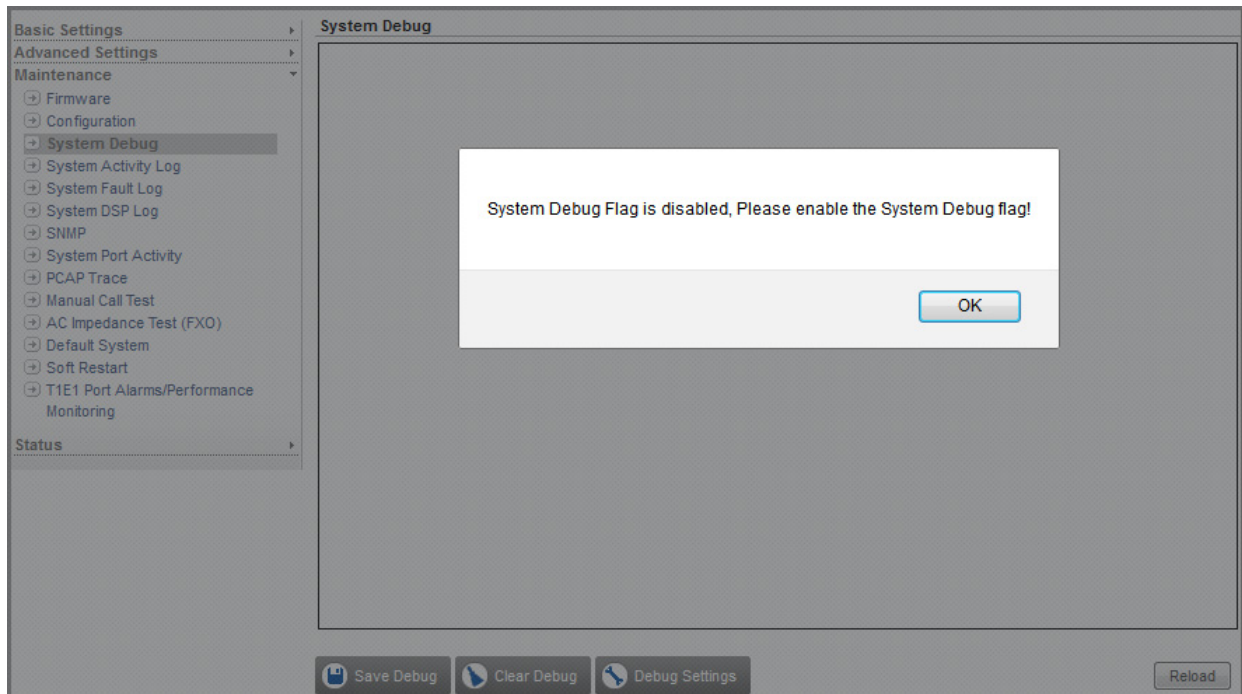
System Debug

Debugging is a method used for recording actions and events of the system. Debugs are the primary record keepers of the system and network activity. Debugging has several benefits which include troubleshooting, security and system administration.

SETU VTEP supports Syslog Client for sending debug messages to the remote syslog server on the IP network.

Configuring System Debug

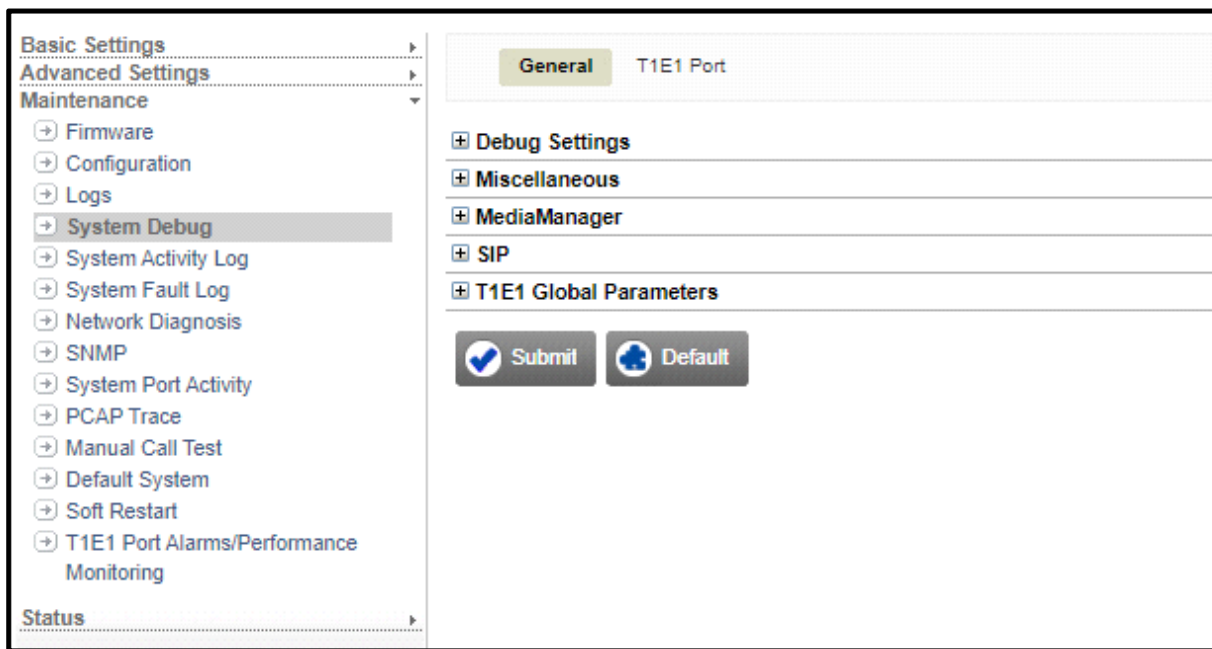
- Click the **Maintenance** link to expand.
- Click the **System Debug** link.



Debug details will be displayed only if you enable System Debug.

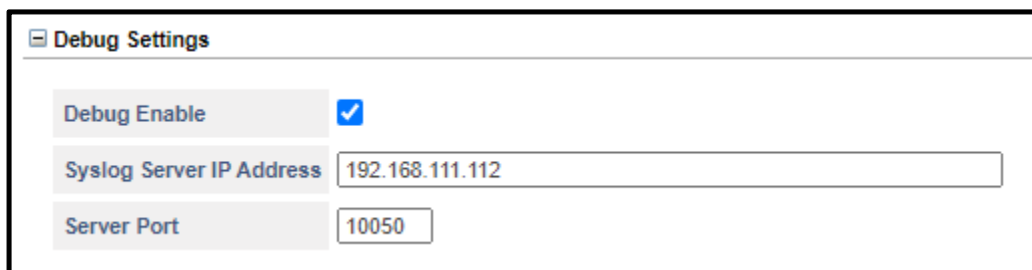
- The message appears to enable the Debug check box. Click **OK**.
- Click the **Debug Settings** button.

- The **Debug Settings** window opens.



The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu includes sections for Basic Settings, Advanced Settings, Maintenance, and Status. Under Maintenance, several options are listed with expandable arrows: Firmware, Configuration, Logs, System Debug (which is highlighted), System Activity Log, System Fault Log, Network Diagnosis, SNMP, System Port Activity, PCAP Trace, Manual Call Test, Default System, Soft Restart, and T1E1 Port Alarms/Performance Monitoring. The main content area has a 'General' tab selected, showing a list of expandable settings: Debug Settings, Miscellaneous, MediaManager, SIP, and T1E1 Global Parameters. At the bottom of this section are two buttons: 'Submit' (with a checkmark icon) and 'Default' (with a reset icon).

- Under the **General** tab, click **Debug Settings** to expand.



The screenshot shows the 'Debug Settings' window with a title bar and a close button. It contains three configuration items: 'Debug Enable' with a checked checkbox, 'Syslog Server IP Address' with a text input field containing '192.168.111.112', and 'Server Port' with a text input field containing '10050'.

- Select the **Debug Enable** check box to enable system debug. Default: Disabled.

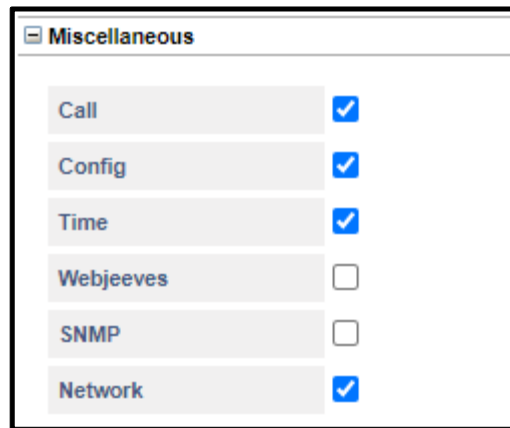
You will be able to configure the Debug Settings only after you enable this check box.

- Select the **Save Debug In File** check box, if you want to save the debug file in the system. Default: Disabled.
- In **Syslog Server IP Address**, enter the remote Syslog Server IP Address. Default: Blank.
- In Syslog **Server Port**, enter the port number. The range of the server port is 514, 1024 to 65535. Default: 514.



It is not possible to enable all these debugs at a time, only one of these can be enabled at a time.

- Click **Miscellaneous** to expand.



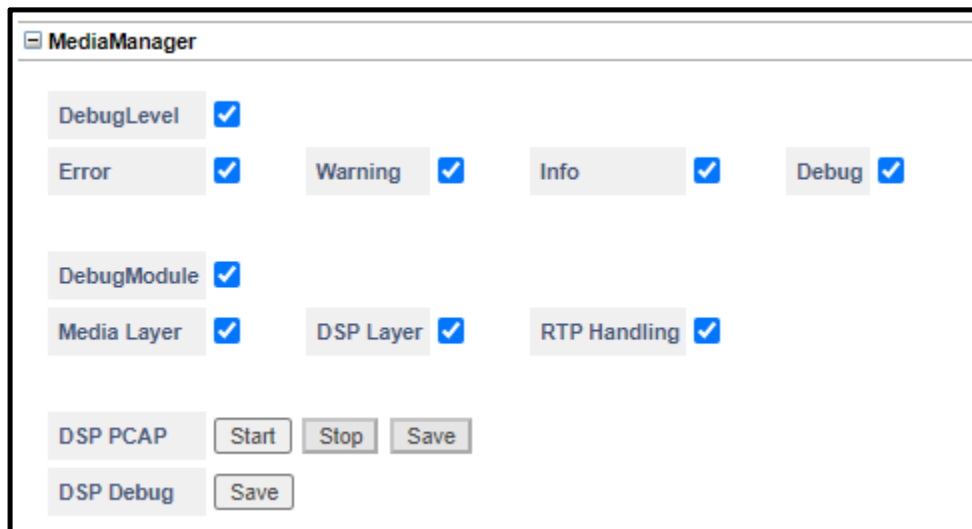
Miscellaneous	
Call	<input checked="" type="checkbox"/>
Config	<input checked="" type="checkbox"/>
Time	<input checked="" type="checkbox"/>
Webjeeves	<input type="checkbox"/>
SNMP	<input type="checkbox"/>
Network	<input checked="" type="checkbox"/>

- If you want the debug of these parameters, keep their — Call, Config, Time, SNMP and Network check boxes enabled.

Select the Webjeeves check box to enable, if required.

To disable a parameter, clear the respective check box.

- Click **MediaManager** to expand.



MediaManager			
DebugLevel	<input checked="" type="checkbox"/>		
Error	<input checked="" type="checkbox"/>	Warning	<input checked="" type="checkbox"/>
		Info	<input checked="" type="checkbox"/>
		Debug	<input checked="" type="checkbox"/>
DebugModule	<input checked="" type="checkbox"/>		
Media Layer	<input checked="" type="checkbox"/>	DSP Layer	<input checked="" type="checkbox"/>
		RTP Handling	<input checked="" type="checkbox"/>
DSP PCAP	Start	Stop	Save
DSP Debug	Save		

- Keep the **DebugLevel** check box enabled. All the debug levels — Error, Warning, Info, Debug — are enabled. To disable a debug level, clear the respective check box.
- Keep the **DebugModule** check box enabled. All debug modules — Media Layer, DSP Layer, RTP Handling — are enabled. To disable a debug module, clear the respective check box.
- In **DSP PCAP**, click the **Start** button to begin the capturing of the DSP Trace.

Click the **Stop** button to stop DSP Trace capture.

OR

Wait for the system to stop capturing. The system stops capturing once the maximum allotted memory is utilized.



Capturing of packets will not stop if you open any other page of Jeeves. So, you may continue using Jeeves for any other purpose while DSP Trace is being used.

- When the DSP capturing is stopped (by you or the system), click the **Save** button to save the files on your computer or on another computer.

A dialog box opens. You can select the path for saving the trace file.



The current packets captured will not be deleted after you have saved the trace file. The current packets will be deleted when you start the DSP capture again.

- After logging out of Jeeves, you can open the trace files using Wireshark/ Ethereal or any other software which supports opening of trace files.
- In **DSP Debug**, click the **Save** button to save the DSP Debug files on your computer or on another computer.
- Click **SIP** to expand.

SIP	
SIP	<input checked="" type="checkbox"/>
STUN	<input checked="" type="checkbox"/>
NAT	<input checked="" type="checkbox"/>
Call	<input checked="" type="checkbox"/>
Call Message	<input checked="" type="checkbox"/>
Register	<input checked="" type="checkbox"/>
OPTIONS	<input checked="" type="checkbox"/>

- If you want the debug of these parameters, keep the parameters — SIP, STUN, NAT, Call, Call Message, Register, OPTIONS and SUBSCRIBE check boxes enabled.
- To disable a parameter, clear the respective check box.
- Click **T1E1 Global Parameters** to expand.

T1E1 Global Parameters	
Level 1	<input checked="" type="checkbox"/>
Level 2	<input checked="" type="checkbox"/>

- Select the check box of the desired level — Level 1 or Level 2 — to enable.
- Click **Submit**.
- You can also enable debug for the desired Port — **T1E1**.
- To do so,

- Click the T1E1 port tab.

- Select the check boxes of the desired options — Level 1, Level 2 of the respective port numbers you wish to enable.

T1E1 Port		
Select All	<input checked="" type="checkbox"/>	
Port 1	Level 1 <input checked="" type="checkbox"/>	Level 2 <input checked="" type="checkbox"/>
Port 2	Level 1 <input checked="" type="checkbox"/>	Level 2 <input checked="" type="checkbox"/>
Port 3	Level 1 <input checked="" type="checkbox"/>	Level 2 <input checked="" type="checkbox"/>
Port 4	Level 1 <input checked="" type="checkbox"/>	Level 2 <input checked="" type="checkbox"/>

- Click **Submit**.



If debug is enabled, atleast one debug level should be selected. If no debug level is selected, SETU VTEP will prompt you to select a debug level.

System Activity Log

The SETU VTEP monitors all its activities and maintains records of these activities in the System Activity Log.

The System Activity Log has a buffer capacity of 500 records. The Activity Log stores records using the FIFO method.

The System Activity Log can be downloaded on a computer in form of a report. SETU VTEP also supports Syslog Client for System Activity Logs. The Syslog Client enables the system to send activity logs in syslog format to the remote 'Syslog Server'. You can view the logs on the remote server.

Index of the Type of Activities recorded in the System Activity Log:

Event Index	Activity	Description
1	Matrix SETU VTEP started:	When the application starts.
2	Default Jumper set	Jumper is set in default position.
3	Display Configuration Type:	Displays Configuration type used by the system.
4	Card Present: Slot Num:Card Type:	The Slot Number and Type of cards present in the system.
5	Card Status: Slot Num: Card Type:	Card Status during Power ON.
6	System Network functionality restarted	When network module restarts.
7	Network Connection Type change:	When the Network Connection Type is changed.
8	Network IP address change:	When the Network IP Address is changed.
9	Network Subnet Mask change:	When the Network Subnet is changed.
10	Network Gateway address change:	When the Network Gateway Address is changed.
11	DNS Server address change:	When the DND Server Address is changed.
12	Network VLAN/CoS Flag Enabled:	VLAN/CoS Flag status.
13	Network VLAN/CoS ID Change:	VLAN ID configured.
14	SIP Stack Destructed.	When the SIP Stack is Destructed.
15	SIP Stack Constructed.	When the SIP Stack is Constructed.
16	Stun Status:	Displays the STUN status.
17	Sync Date-Time with SNTP Server	SNTP Server sync with configured Server Address.
18	RTC Change	When Date-time is changed in the system.
19	System Default	When the system is set to default.
20	System Restart using:	Displays the reason for the system restart.
21	System Config file change:	Displays config file name when parameter is changed.
22	Network WAN Link UP	When WAN port is connected and network link is working.

Event Index	Activity	Description
23	Network WAN Link DOWN	When WAN port is connected and network link is not working
24	DynDNS status:	Displays the DynDNS Status.
25	WAN MAC address change:	When the system inits or MAC address of the system is changed (System to Clone or vice-versa).
26	T1E1 Layer 1 UP: Slot Num: Port Offset:	T1E1 Port Layer 1 link is up.
27	T1E1 Layer 2 UP: Slot Num: Port Offset:	T1E1 Port Layer 2 link is up.
28	T1E1 Layer 1 DOWN: Slot Num: Port Offset:	T1E1 Port Layer 1 link is down.
29	T1E1 Layer 2 DOWN: Slot Num: Port Offset:	T1E1 Port Layer 2 link is down.
31	Web Jeeves	When SE password is changed.
32	Command Password change	When command password is changed.
33	Server Port Change: HTTPS:	When Server port is changed.
34	Web Server Access from WAN:	Displays the status whether enable or disable.
35	Allow Server Access from specific IP Address:	Displays the status whether enable or disable.
36	Block ICMP on WAN:	Displays the status whether enable or disable.
37	Block PING on WAN:	Displays the status whether enable or disable.
38	Local Certificate for TLS:	Displays Local Certificate name used for TLS
39	Local Certificate for Firmware Upgrade:	Displays Local Certificate name used for Firmware Upgrade.
40	Local Certificate for Configuration Upgrade:	Displays Local Certificate name used for Configuration Upgrade.
41	Reserved	
42	Local Certificate for WebServer:	Displays Local Certificate name used for WebServer.
43	Trusted Root CA Certificate Uploaded:	Displays Trusted Root CA Certificate uploaded.
44	Trusted Root CA Certificate Upload Status:	Displays Trusted Root CA Certificate upload status.
45	Local Certificate Uploaded:	Displays Local Certificate uploaded.
46	Local Certificate Upload Status:	Displays Local Certificate upload status.
47	Trusted Root CA Certificate Deleted:	Displays Trusted Root CA Certificate deleted.
48	Local Certificate Deleted:	Displays Local Certificate deleted.
49	Auto Config process is started:	Displays the reason for which Auto Configuration Upgrade started.

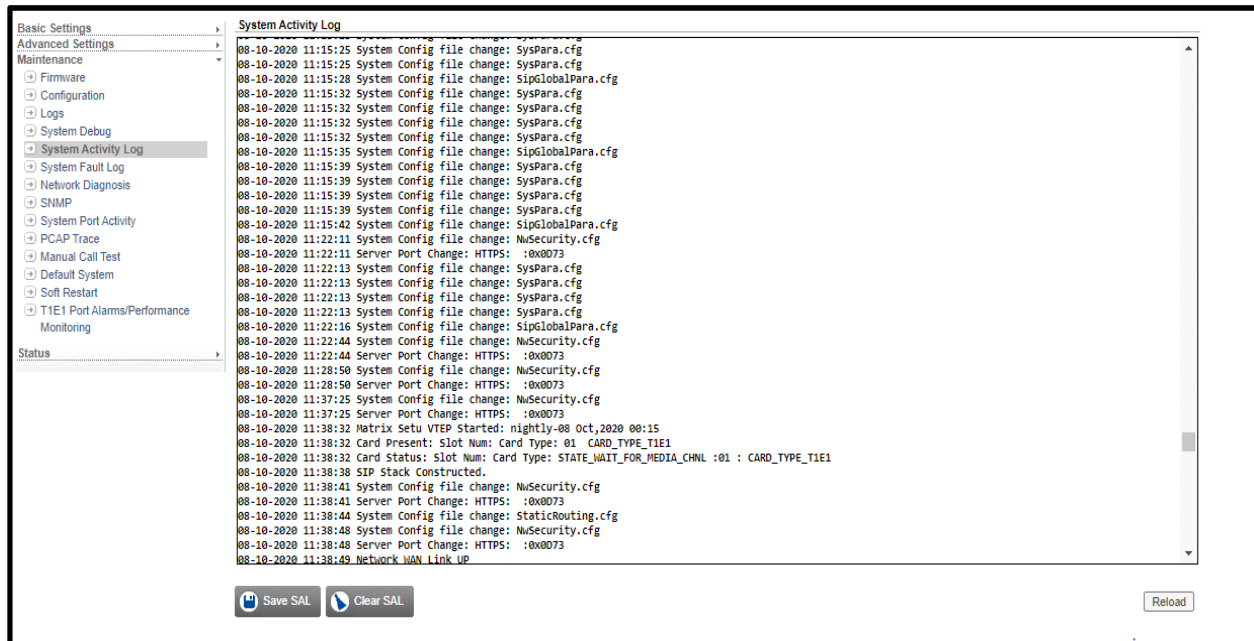
Event Index	Activity	Description
50	Auto Config process is stopped due to	Displays the reason for upgrade being stopped.
51	Auto Config file is successfully uploaded	Displays filename of the config file that has been uploaded successfully.
52	Auto Config process failed due to	Displays the reason for upload failure.
53	Auto Config file parsing failed	Displays the filename of the config file for which parsing got failed.
54	Auto Config file is parsing Done	Displays when the parsing gets completed.
55	MM::Maximum DSP CPU Usage Reached	When the maximum usage limit of DSP CPU is reached.
56	SE Login blocked for IP:	When an IP Address is blocked for SE Login due to continual invalid password entry.
57	MM::	Displays CMM Module status (when PCAP is start/stop).

How to configure

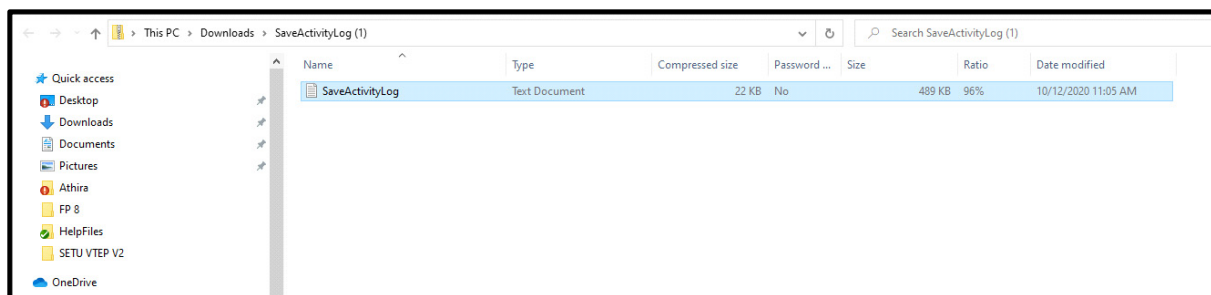
Activity Logs are stored in the system by default. For sending System Activity Log on remote server, Syslog Server setting needs to be done.

Configuring System Activity Log

- Click the **Maintenance** link to expand.
- Click the **System Activity Log** link.



- The list of activities appear on the screen.
- Whenever you want the system to fetch an updated activity report, click the **Reload** button.
- If you want to delete all the activities, click the **Clear SAL** button.
- If you want to Save the activities, click the **Save SAL** button. File will be saved under the name 'SaveActivityLog'.



- The list of activity log appears as shown:

```
SaveActivityLog - Notepad
File Edit Format View Help
Slot Num: Port Offset: 02 :001
11-10-2020 03:02:59 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:02:59 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:03:31 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:03:31 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:04:03 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:04:03 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:04:35 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:04:35 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:05:06 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:05:06 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:05:39 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:05:39 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:06:10 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:06:10 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:06:42 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:06:42 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:07:14 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:07:14 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:07:46 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:07:46 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:08:18 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:08:18 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:08:49 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:08:49 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:09:22 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:09:22 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:09:53 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:09:53 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:10:25 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:10:25 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:10:56 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:10:56 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:11:29 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
11-10-2020 03:11:29 T1E1 Layer 2 DOWN, Slot Num: Port Offset: 02 :001
11-10-2020 03:12:01 T1E1 Layer 1 UP, Slot Num: Port Offset: 02 :001
```

System Fault Log

The SETU VTEP maintains a log of all system faults. The system Fault Log has a buffer capacity of 500 records. The Fault Log stores records using the FIFO method.

The System Fault log can be downloaded on a computer in form of a report. SETU VTEP also supports Syslog Client for System Fault Logs. The Syslog Client enables the system to send fault logs in syslog format to the remote 'Syslog Server'. You can view the logs on the remote server.

The different fault events that are logged are summarized in this table:

Event ID	Event	Description
1	Failed to initialize Syslog Server. Syslog Type:	Failure in Syslog Server initialization.
2	Failed to initialize SNMP Server.	Failure in SNMP Server.
3	Failed to initialize IPC Message Queue	Internal system queue error.
4	Failed to initialize random number generator.	Random number generation failure.
5	Failed to download DSP, Slot Num: Card Type:	When the system fails to download DSP.
6	Keep alive not received Slot Num: Card Type:	Keep Alive failed for CPU DSP or Slave Card.
7	Failed to initialize Call Manager.	Call manager initialization failure.
8	Failed to initialize Port Config.	Config file initialization failure.
9	Failed to initialize Auto Upgrade.	Auto Upgrade failure.
10	SIP stack construct failed, error code:	Error response when SIP Stack construct fails.
11	SIP TLS initialize failed, error code:	Error response when SIP TLS initialize fails.
12	Outgoing Invite send failed, Trunk Num: reason:	When any INVITE message sending fails.
13	Invalid Slave Layer msg rcv:	When Invalid message is received from Slave Layer.
14	Invalid Slave Card msg rcv, Slot Num: Port Num:	When Invalid message is received from Slave Card.
15	DSP Frame sync error, Slot Num:	Internal system DSP error.
16	DSP DMA Drop error, Slot Num:	Internal system DSP error.
17	DSP DMA Time out error, Slot Num:	Internal system DSP error.
18	DSP DMA address error, Slot Num:	Internal system DSP error.
19	DSP HPI Queue Full error, Slot Num:	Internal system DSP error.
20	MM::Channel Allocation Failed	VoIP DSP channel allocation failure.
21	MM::DSP Command Failed	VoIP DSP command failure.
22	MM::DSP Firmware Download Failed	VoIP DSP Firmware download failure.
23	MM::Invalid Command from Master	VoIP DSP command error.
24	MM::Invalid Event from DSP Layer	VoIP DSP error.

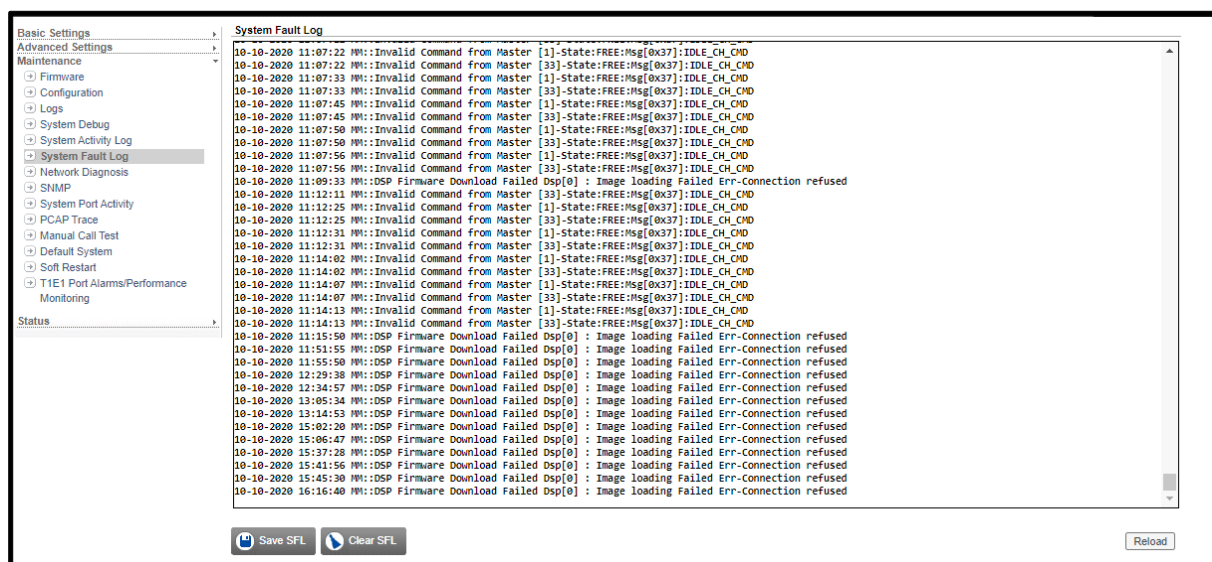
Event ID	Event	Description
25	DspLoader::Init Failed	When DSP loader failed to init.
26	DspLoader::CoffLoader Init Failed, Image: Appld:	Dsp Coff loader init failure.
27	DspLoader::Timer expired, State: Appld:	Dsp Loader timer expired.
28	DspLoader::Incorrect Read Result, State: Appld:	Dsp loader read status failure.
29	CardManager::Saved and Received Card Info not matched	Card status mismatched.
30	MMAccLayer::In Running state, received Invalid State:	When Media manager receives an invalid state.
31	Failed to Open RTC Driver	RTC failure.

How to configure

Fault Logs are stored in the system by default. For sending System Fault Log on remote server, Syslog Server setting needs to be done.

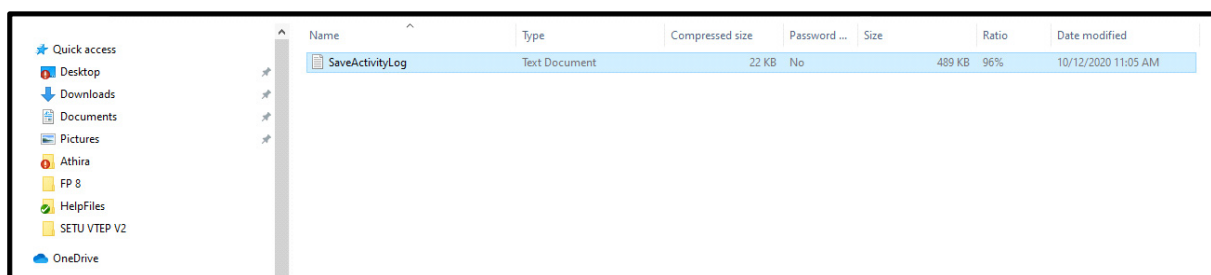
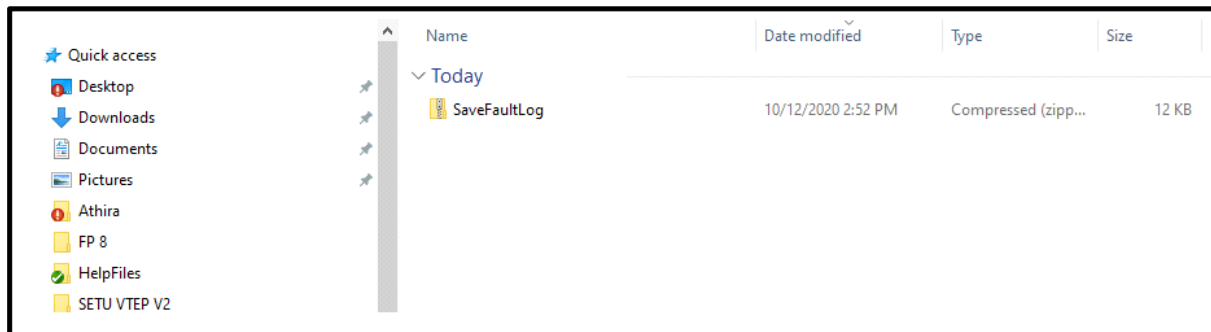
Configuring System Fault Log

- Click the **Maintenance** link to expand.
- Click the **System Fault Log** link.



- Whenever you want the system to fetch an updated fault report, click the **Reload** button.
- If you want to delete the entire list of faults, click the **Clear SFL** button.

- If you want to Save the list of faults, click the **Save SFL** button.
- The zip file contains the **SaveFaultLog.txt** file.



- The list of fault log appears as shown:

```
SaveFaultLog - Notepad
File Edit Format View Help

21-09-2020 15:20:12 MM::Invalid Command from Master [0]-State:FREE:Msg[0x46]:START_HOST_PCAP
21-09-2020 15:20:12 MM::Invalid Command from Master [0]-State:FREE:Msg[0x47]:STOP_HOST_PCAP
21-09-2020 19:21:50 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:23:00 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:23:16 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:28:20 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:29:32 MM::Invalid Command from Master [33]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:31:33 MM::Invalid Command from Master [33]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:33:35 MM::Invalid Command from Master [33]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:34:22 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:36:48 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:37:56 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
21-09-2020 19:39:28 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
22-09-2020 09:42:21 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
22-09-2020 09:54:18 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
22-09-2020 09:55:55 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
22-09-2020 13:57:10 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
23-09-2020 11:10:43 MM::Invalid Command from Master [319]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 10:20:39 MM::DSP Command Failed Dsp[0] Buf[15]: AllocateBufInDspRam Failed Err-cOCTVC1_MAIN_RC_BUFFER_MAX_REACHED
25-09-2020 10:36:32 MM::DSP Command Failed Dsp[0] Buf[15]: AllocateBufInDspRam Failed Err-cOCTVC1_MAIN_RC_BUFFER_MAX_REACHED
25-09-2020 11:09:55 MM::DSP Command Failed Dsp[0] Buf[15]: AllocateBufInDspRam Failed Err-cOCTVC1_MAIN_RC_BUFFER_MAX_REACHED
25-09-2020 17:22:52 MM::DSP Command Failed Dsp[0] Buf[15]: AllocateBufInDspRam Failed Err-cOCTVC1_MAIN_RC_BUFFER_MAX_REACHED
25-09-2020 17:37:54 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:37:54 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:38:14 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:38:32 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:38:33 MM::Invalid Command from Master [289]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:38:51 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:40:30 MM::Invalid Command from Master [257]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:40:30 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:44:21 MM::Invalid Command from Master [257]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:44:21 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:46:29 MM::Invalid Command from Master [1]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:46:29 MM::Invalid Command from Master [257]-State:FREE:Msg[0x37]:IDLE_CH_CMD
25-09-2020 17:47:34 MM::Invalid Command from Master [11]-State:FREE:Msg[0x37]:IDLE CH_CMD
```

Network Diagnosis

What's this?

Setu VTEP provides you an option to check the LAN/ WAN/ Virtual WAN connectivity using Ping and Traceroute as the diagnostic tools.

How to Configure

- Click the **Maintenance** link.
- Click the **Network Diagnosis** link

Basic Settings

Advanced Settings

Maintenance

- Firmware
- Configuration
- Logs
- System Debug
- System Activity Log
- System Fault Log
- **Network Diagnosis**
- SNMP
- System Port Activity
- PCAP Trace
- Manual Call Test
- Default System
- Soft Restart
- T1E1 Port Alarms/Performance Monitoring

Status

Network Diagnosis

Diagnostic Utility ☒ Ping ☐ Traceroute

Interface WAN

IP Address/Domain Name 1001::192:168:1:2

Ping Packet Size 32

Ping Count 4

Ping Timeout (sec) 3

```
PING 1001::192:168:1:2 (1001::192:168:1:2) from 1001::192:168:1:156: 32 data bytes
40 bytes from 1001::192:168:1:2: seq=0 ttl=64 time=2.382 ms
40 bytes from 1001::192:168:1:2: seq=1 ttl=64 time=0.514 ms
40 bytes from 1001::192:168:1:2: seq=2 ttl=64 time=0.518 ms
40 bytes from 1001::192:168:1:2: seq=3 ttl=64 time=0.740 ms

--- 1001::192:168:1:2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.514/1.038/2.382 ms
```

- In **Diagnostic Utility**, select the diagnostic tool — Ping or Traceroute — to check the Internet/WAN connectivity.
- Select the **Interface** as LAN, WAN, Virtual WAN.
- In **IP Address/Domain Name**, enter the IPV4 or IPV6 Address or the Domain Name of the system whose connectivity you wish to test. Default: Blank

If you have selected *Ping* as the *Diagnostic Utility* option, configure the following parameters:

- In **Ping Packet Size**, enter the number of bytes you want the system to send for Ping test. Valid Range: 4 to 1024. Default: 32 bytes.
- In **Ping Count**, enter the number of times you want system to send the request message for Ping test. Valid Range: 1 to 50. Default: 4 times.
- In **Ping Timeout (sec)**, enter the time for which you want the system to wait to get the response for each request message sent. Valid Range: 1 to 9. Default: 3 sec.

If you have selected *Traceroute* as the *Diagnostic Utility* option, configure the following parameters:

- In **Traceroute Max TTL**, enter the maximum number of hops (Time-To-Live value) you want the system to take in the path to find the IP Address configured. Valid Range: 1 to 255. Default: 30.
 - In **Traceroute Protocol**, select the protocol — ICMP or UDP — which you want the system to use for traceroute functionality.
- To start the Network Diagnosis, click **Start** button.

The Diagnostic result will appear on the screen.

To clear the Diagnostic result, click **Clear** button.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application-layer protocol used for exchanging management information between network devices. Using SNMP, you can manage and monitor network elements, audit network usage, detect network faults or inappropriate network access.

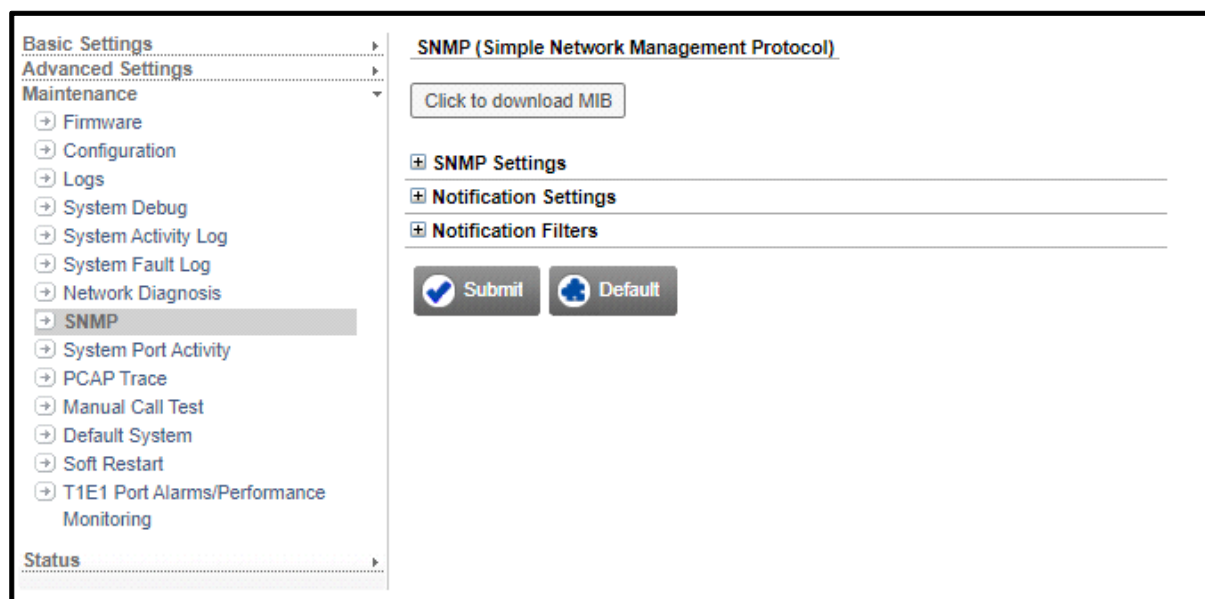
The SNMP architecture consists of:

- An **SNMP Agent** is a program that is bundled within the managed device. SNMP agent allows a managed device to collect the Management Information Base from the device and make it available to the SNMP Manager on request. It receives SNMP requests and generates SNMP responses or notifications (traps/informs). The SNMP Agents are SNMP Servers.
- **SNMP Manager**, usually the Network Management Station. The manager communicates with multiple SNMP Agents implemented in the network. It generates SNMP requests and receives SNMP responses and notifications (traps/informs). The SNMP Manager is an SNMP Client.
- **Managed device** or the network element is a part of the network that requires some form of monitoring and management. For example, switch, routers, servers.
- **Management Information Base** is the commonly shared database between the Agent and the Manager.

SNMP uses UDP (User Datagram Protocol) as the transport protocol for passing information between Managers and Agents. The Agent listens on UDP port 161 for requests from Manager and the Manager listens on UDP port 162 for notification from Agent.

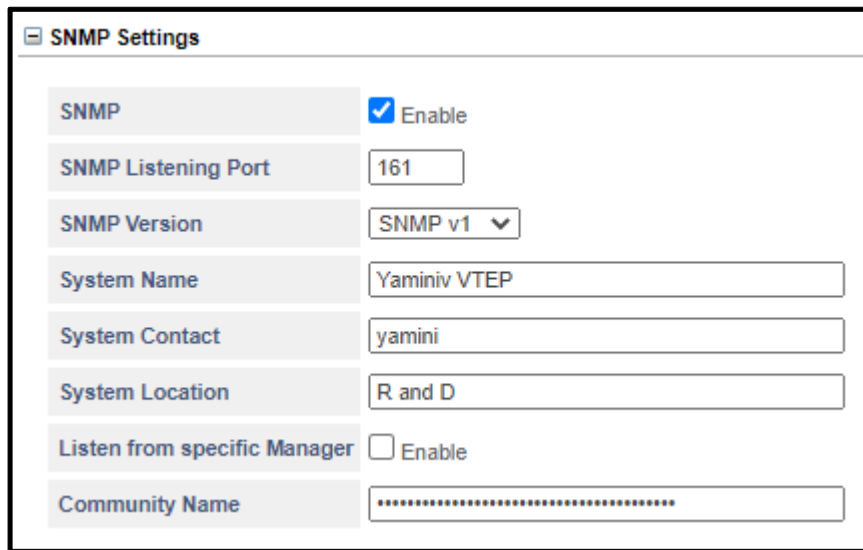
To configure SNMP parameters,

- Click the **Maintenance** link to expand.
- Click the **SNMP** link.



SNMP Settings

- Click **SNMP Settings** to expand.



SNMP	<input checked="" type="checkbox"/> Enable
SNMP Listening Port	161
SNMP Version	SNMP v1
System Name	Yaminiv VTEP
System Contact	yamini
System Location	R and D
Listen from specific Manager	<input type="checkbox"/> Enable
Community Name	*****

- Select the **SNMP** check box to enable. Default: Disabled.
- Configure the **SNMP Listening Port**. Valid range is 161/ 1031 to 65535. Default: 161.
- Select the **SNMP Version** as supported by your SNMP Manager. You can select— SNMPv1, SNMPv2c, SNMPv3.

For enhanced security, you must select SNMPv3.

- Configure the **System Name**. When there are multiple devices connected in the same network, the name configured helps to identify the SNMP Agent within the network. The System Name can be a maximum of 40 characters. Default: Blank.
- Configure the **System Contact**. It is the name and number of the person to be contacted, in case of notification. The System Contact can be of a maximum of 40 characters. Default: Blank.
- Configure the **System Location**. This is the physical location of SETU VTEP. This information is helpful to the administrator. The System Location may consist of a maximum of 40 characters. Default: Blank.
- Select the **Listen from Specific Manager** check box, if you want the system to listen to the incoming SNMP messages from a specific manager. Default: Disabled.
 - If you have enabled **Listen from Specific Manager** check box, you must configure the specific **Manager's Address**.

The Manager's Address can be a Domain Name or an IP Address. It can be a maximum of 64 characters. Default: Blank.

- If SNMP version is set as **SNMPv1** or **SNMPv2c**, configure **Community Name**.

Community Name identifies the SNMP community in which the sender and recipient of the message are located. It enables communication between SETU VTEP and the Manager. The Community Name can be a maximum of 40 characters. Default: Blank.

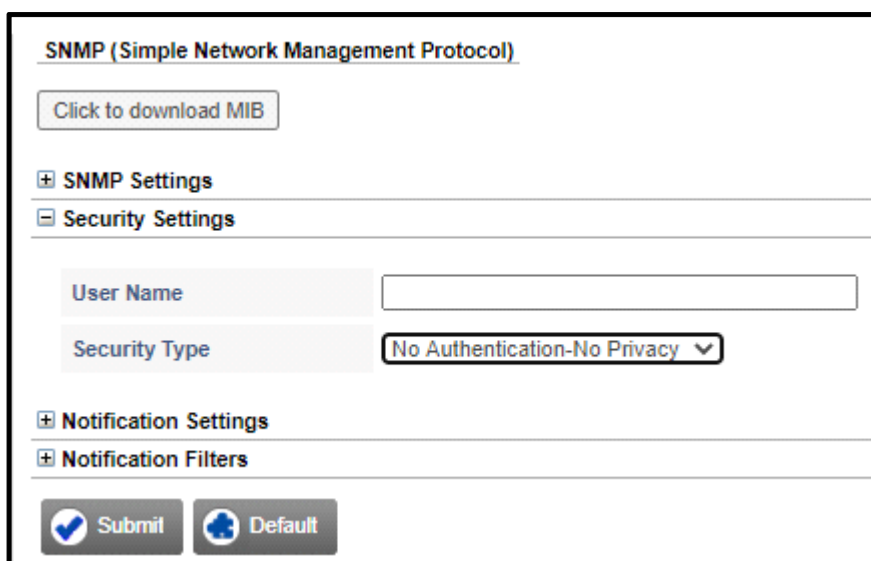
- If SNMP version is set as **SNMPv3**, the **System's Engine ID** is displayed in this field. This is a unique identification of the system. It is a hexadecimal field with length of 22 characters.

The ID consists of:

- Enterprise Number (800086df03 which is fixed)
- MAC Address of the system (MAC address of Network port)

Security Settings

- If SNMP version is set as **SNMPv3**, click **Security Settings** to expand and configure the following.



- Enter the **User Name**. The User Name can be a maximum of 40 characters. User Name will be used for authentication and privacy in SNMPV3.
- Select the appropriate **Security Type** as per your requirement. Security Type defines the level of security.
- When Authentication and Privacy are not required, select **No Authentication-No Privacy**.



- When only Authentication is required, select **Authentication without Privacy**. Incoming SNMP Messages will require authentication.

The screenshot shows the 'Security Settings' form with the following fields and values:

Security Settings	
User Name	<input type="text"/>
Security Type	Authentication without Privacy ▼
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>

If you select this method, select the **Authentication Algorithm** as **MD5** or **SHA**. Default: MD5.

In the **Authentication Password**, enter a password of your choice as Authentication Password for the User Name you have assigned. The Authentication Password must be a minimum of 8 characters and may have upto 24 characters. Default: Blank.

- When both Authentication and Privacy are required, select **Authentication with Privacy**. Incoming SNMP Message will require authentication and these messages will be encrypted, which will be decrypted at the receivers end only.

The screenshot shows the 'Security Settings' form with the following fields and values:

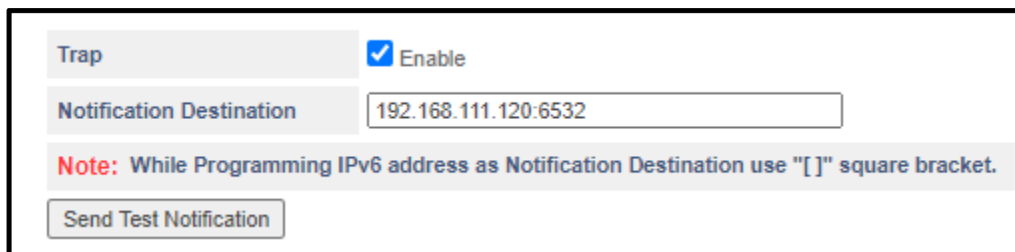
Security Settings	
User Name	<input type="text"/>
Security Type	Authentication with Privacy ▼
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Privacy Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES-128
Privacy Password	<input type="text"/>

If you select this method,

- Select the **Authentication Algorithm** as **MD5** or **SHA**. Default: MD5.
- Enter **Authentication Password** for the User Name you have assigned. The Authentication Password must be a minimum of 8 characters and may have upto 24 characters. Default: Blank.
- Select the **Privacy Algorithm** as **DES** or **AES-128**. Default: DES.
- Enter the **Privacy Password** of your choice. The Privacy Password must be a minimum of 8 characters and may have upto 24 characters. Default: Blank.

Notification Settings

- Click **Notification Settings** to expand.



The screenshot shows a web interface for configuring notification settings. It includes a 'Trap' checkbox which is checked and labeled 'Enable'. Below it is a 'Notification Destination' text field containing the IP address '192.168.111.120:6532'. A red note states: 'Note: While Programming IPv6 address as Notification Destination use "[" square bracket.' At the bottom is a 'Send Test Notification' button.

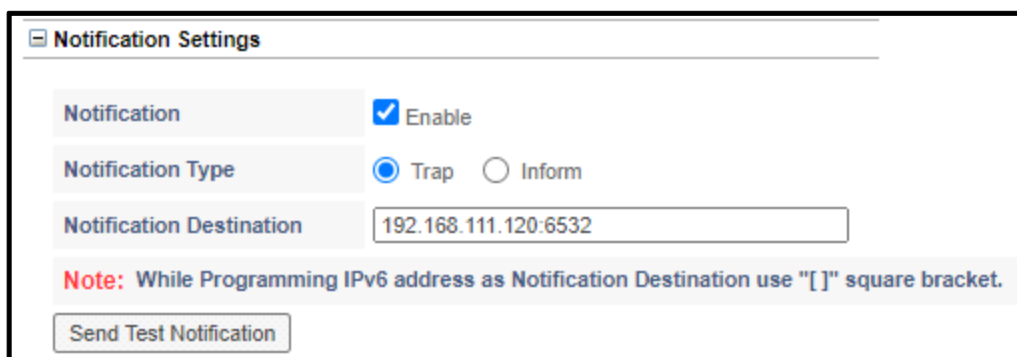
If SNMP version is set as **SNMPv1**, configure the following parameters.

- If you want SETU VTEP to generate Trap message for an error, select the **Trap** check box to enable. Default: Disabled.
- You must configure the **Notification Destination**. SETU VTEP will send the notification (error message) to the destination configured.

The Notification Destination can be an IP Address or a Domain Name and the Port of the Manager or of any other device where you want to receive the trap messages. IP Address/Domain Name can be a maximum of 64 characters. Valid range is 0 to 65535. Default: 162.

- Click **Submit** button to save the settings.

If SNMP version is set as **SNMPv2c** or **SNMPv3**, configure the following parameters.



The screenshot shows a web interface for configuring notification settings. It includes a 'Notification' checkbox which is checked and labeled 'Enable'. Below it is a 'Notification Type' section with two radio buttons: 'Trap' (selected) and 'Inform'. Below that is a 'Notification Destination' text field containing the IP address '192.168.111.120:6532'. A red note states: 'Note: While Programming IPv6 address as Notification Destination use "[" square bracket.' At the bottom is a 'Send Test Notification' button.

- Select the **Notification** check box to enable, if you want SETU VTEP to generate Trap or Inform message for an error.
- Select the **Notification Type**. You may select **Trap** or **Inform**.

If you want the system to send notification message without acknowledgement, select **Trap**.

If you want the system to send notification message with acknowledgement, select **Inform**.

- If you select **Inform** as the *Notification Type*, you must configure Retry Attempts and Retry Interval.

If acknowledgement is not received from the Manager for the notification sent, the system will keep retransmitting the message for the number of attempts you have configured as the **Retry Attempts**. Default: 3.

The system will retransmit the messages at regular time intervals you have configured as **Retry Interval**. Default: 10 seconds.

- Configure the **Notification Destination**. SETU VTEP will send the notification (error message) to the destination configured.

The Notification Destination can be an IP Address or a Domain Name and the Port of the Manager or of any other device where you want to receive the trap messages. IP Address/Domain Name can be a maximum of 64 characters. Valid range is 0 to 65535. Default: 162.

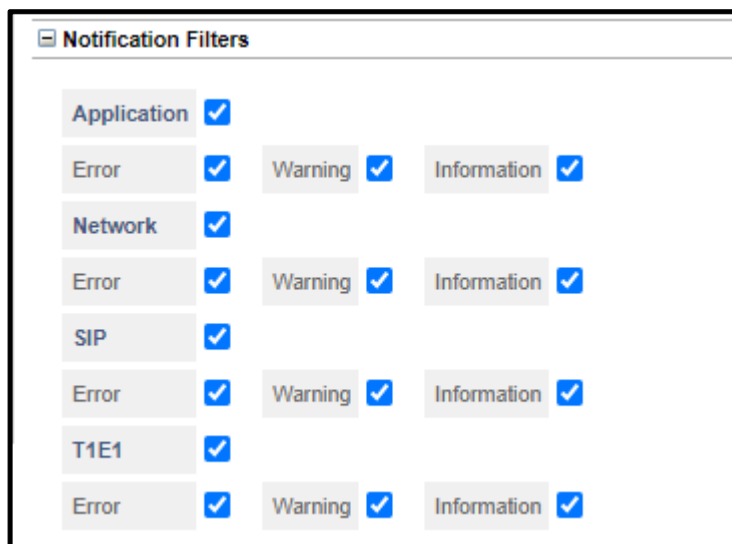
- Click **Submit** button to save the settings.

Notification Filters

By default, you get error notifications, information and warnings for events related to the Application, Network and all Port Types. See table at the end of this topic for the event list. You can choose the type of notification you want by setting the notification filters.

To set filters,

Click **Notification Filters** to expand.



Category	Error	Warning	Information
Application	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SIP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
T1E1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

To disable any filter, clear the respective check box.



Make sure that you have uploaded the MIB in your SNMP Manager to get the status and notifications for SNMP. Contact Matrix Support Team for the MIB files.

PCAP Trace

PCAP or packet capture consists of intercepting and logging the traffic passing over a digital network or a part of a network. PCAP intercepts each packet in the data streams that flow across the network, and can decode and analyze its contents.

PCAP can be used, among others, to monitor the network, analyze network problems, debug client/ server communications, debug network protocol implementations.

SETU VTEP supports PCAP Trace, which you can use to detect and diagnose network related problems; for example, when the SIP account is not getting registered, or a SIP related feature is not functioning.

Packets traveling over a network are captured and saved in the system. You can save these trace files (packets captured by the system) on a computer and open these trace files using a graphical packet capture and protocol analysis tool such as Wireshark or Ethereal.

A maximum of 10 MB of packets can be captured and stored in the system.

SETU VTEP also supports Filters and Promiscuous mode for capturing packets, which you can use to specify the types of data packets to be captured.

To use PCAP Trace,

- Click the **Maintenance** link to expand.
- Click the **PCAP** link.

PCAP

Filter Setting

Enable Promiscuous mode

☐

Last Status

Packets captured

7782

Total Bytes

2406280

Status

mpcap : running

Start

Stop

Save Trace File

Note:

To see what is going on on the network level, you can generate PCAP files on this page. This file can be read with various network tools, for example Ethereal, Wireshark. To start recording, press the start button and to stop, press the stop button.

Examples of Filter Setting

Filter Type	Filter Setting	Comment
src port port number	src port 5060	Capture packets if the packet has a source port value of 5060.
dst port port number	dst port 80	Capture packets if the packet has a destination port value of 80.
port port number	port 5060	Capture packets if the packet has either source or destination port value of 5060
src host ip address	src host 192.168.1.176	Capture packets if the source field of packet is 192.168.1.176
dst host ip address	dst host 192.168.1.176	Capture packets if the destination field of packet is 192.168.1.176
host ip address	host 192.168.1.176	Capture packets if either source or destination field of packet is 192.168.1.176
host ipv6 address	host fd00::1234	Capture packets if either source or destination field of packet is fd00::1234
src host ipv6 address	src host fd00::1234	Capture packets if the source field of packet is fd00::1234
dst host ipv6 address	dst host fd00::1234	Capture packets if the destination field of packet is fd00::1234

- Decide the type of packets to be captured and set the Filters accordingly. The **Filter Settings** must be within 60 characters. By default, this field is blank. So, all packets will be captured.

Few examples of the Filter Settings are provided to you on this page to help you set the Filters as per your requirement.



It is not mandatory to set Filters. When the Filter Settings left blank, the system will capture all packets.

- You may enable **Promiscuous Mode** by selecting the check box. Default: Disabled.

When you enable Promiscuous Mode, the SETU VTEP will capture all network traffic. However, this will work only in a non-switched environment.

When Promiscuous Mode is disabled, the system will capture only traffic that is directly related to it. Only traffic to, from or routed through the SETU VTEP will be picked up by the PCAP Trace.



'Filter Settings' and 'Promiscuous Mode' (enabled) will not be cleared during power down.

OR

Wait for the system to stop packet capturing. The system stops packet capturing once the maximum allotted memory of 10 MB (RAM) is utilized.

The Number of Packets and bytes captured as per the filter setting will be displayed in the fields **Packets Captured** and **Total Bytes** respectively.

The **Status** field displays the current activity of packet capturing.



Capturing of packets will not stop if you open any other page of Jeeves. So, you may continue using Jeeves for any other purpose while PCAP Trace is being used.

- When the packet capturing is stopped (by you or the system), click the **Save Trace File** button to save the files on your computer or on another computer.

A dialog box opens. You can select the path for saving the trace file.



The current packets captured will not be deleted after you have saved the trace file. The current packets will be deleted when you start the PCAP capture again.

- After logging out of Jeeves, you can open the trace files using Wireshark/ Ethereal or any other software which supports opening of trace files.

Manual Call Test

Manual Call Test enables you to check the quality of Speech between two ports — Source Port and Destination Port — of SETU VTEP without altering the existing call routing configuration.

To conduct Manual Call Test,

- Click the **Maintenance** link to expand.
- Click the **Manual Call Test** link.

The screenshot shows the 'Manual Call Test' web interface. It features a title bar, a 'Call on' dropdown menu, and two rows for 'Source Port' and 'Destination Port'. Each row contains dropdown menus for 'Port Type', 'Port Number', and 'Channel Number', followed by a text input field for the 'Phone Number'. A 'Call' button is located at the bottom left.

In **Call on**, choose either **Source and Destination** or **Destination** only.

In **Source Port**,

- Select the **Port Type** you want to test from the list.
- Select the **Port Number** you want to test from the list.
- Select the **Channel Number** for T1E1. Enter the **Phone Number** in the corresponding field. The phone number can be of maximum 16 characters. Valid characters are 0-9, *, #, + and dot (.).

In **Destination Port**,

- Select the **Port Type** you want to test from the list.
 - Select the **Port Number** you want to test from the list.
 - Select the **Channel Number** for T1E1.
 - Enter the **Phone Number** in the corresponding field. The phone number must be a valid number that the system can out-dial. It can be of maximum 16 characters. Valid characters are 0-9, *, #, + and dot (.).
- Click the **Call** button. SETU VTEP will out dial the phone number you entered to make a test call between the Source Port and the Destination Port.
 - As soon as the test call is made, the **System Port Activity** page will open. You can view the call states and status of the ports you are testing on this page.

For more information on Call States and Port Status, see [“System Port Activity”](#).

Default System

You can restore the system configuration to default values:

- using the Web Jeeves.
- by changing the Jumper position.

Restoring Default Settings using Web Jeeves

When you restore default settings using the Web Jeeves, all the parameters will be assigned default values **except** the following:

- Real Time Clock
- Call Detail Records
- Region
- Network
 - Connection Type
 - DNS Settings
 - DYN DNS
- System Parameters - NAT
 - Route Public IP Address
 - STUN Server Address
 - STUN Server Port
- System Parameters - Server Ports
 - HTTPS Web Server Port
- SIP Trunk
 - Allowed IP Address for Incoming SIP Message.
 - NAT Type
- Configuration Parameters
- Login Password

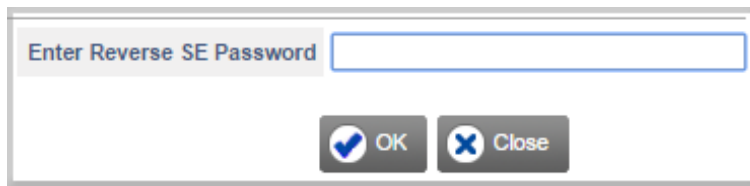
To restore the default settings using the Web Jeeves,

- Click the **Maintenance** link to expand.
- Click the **Default System** link.



- An alert message will appear, "**This option will assign default values to all the programmable parameters and will Restart. Do you want to continue?**".

- Click **OK**.



- You will be prompted to enter the reverse SE password. Enter reverse SE password. For example, if your password is Matrix@1234, enter 4321@xirtam. Click **OK**. The system will restart.

Restoring Default Settings by changing the Jumper Position

By changing the position of **Jumper J13** on the PCB, you can restore the following parameters to default values:

- SE Password
- LAN Port Parameters
 - IP Address
 - Subnet Mask
- System Parameters - Server Ports
 - HTTPS Web Server Port

To restore the Default Jeeves/Command Password by changing the Jumper (**J13**) Settings on the Setu VTEP,

- Make sure you are wearing an electrostatic discharge preventive wrist strap or belt and have a grounding mat.
- Switch off the power supply
- Remove the top cover of the enclosure.
- Locate and change the position of the Jumper **J13** from **AB** to **BC** i.e. from 'Normal' to 'Reset Login Password'
- Switch ON the system and wait for 15 seconds.
- Switch OFF the system.
- Change the Jumper position from **BC** to the original position **AB**.
- Replace the enclosure cover.
- Switch ON the system.

The LAN IP Address will be restored to default, **192.168.2.100**

Soft Restart

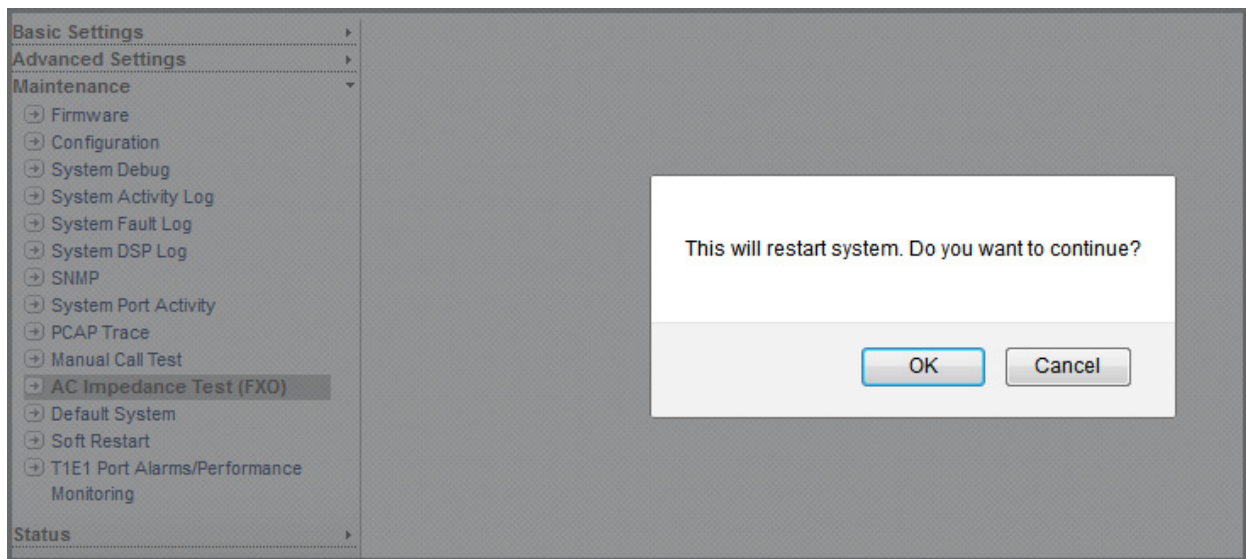
If you need to restart SETU VTEP, you may do it

- using *Soft Restart* from Jeeves

When you restart the system, all active calls will be disconnected and the ports in use will be released. The system configuration however, will remain unaffected.

To use Soft Restart,

- Click the **Maintenance** link to expand.
- Click the **Soft Restart** link.



- An alert message will appear, "**This will Restart System. Do you want to continue?**"
- Click **OK** to restart the system.

T1E1 Port Alarm/ Performance Monitoring

T1E1 Port Alarms

SETU VTEP supports the following alarms to detect the errors occurring on the T1E1 Port.

- RED Alarm (Loss of Signal)
- YELLOW Alarm (Remote Alarm Indication)
- BLUE Alarm (Alarm Indication Signal)

RED Alarm

- This alarm is generated if Loss of Signal persists for 2.5 seconds.
- When RED Alarm is declared, Yellow Alarm is sent to the far end within 12ms of detection of Loss of Signal.
- RED Alarm is declared if,
 - received signal is more than 20 dB or 40 dB below nominal for at least 1ms.
 - 10 consecutive zeroes are received.
 - Loss of frame alignment occurs.
- This alarm is cleared when the signal is acquired back and persists for 10 seconds.

YELLOW Alarm

- This Alarm is also known as Remote Alarm Indication.
- This Alarm is generated when Yellow Alarm is sent by the far end (Yellow Alarm is sent by the far end to indicate that it has lost the incoming signal).
- Yellow Alarm is declared when the signal corresponding to Yellow Alarm persists for 0.5 seconds.
- This alarm is cleared when No Yellow Alarm signal persists for 0.5 seconds.

BLUE Alarm

- It is also known as Alarm Indication Signal (AIS).
- This alarm is generated when AIS persists for 2.5 seconds.
- Blue Alarm (AIS) is declared if less than six zeroes are received on the incoming line data during a 3 msec interval. AIS is cleared if the above condition does not exist for 3 msec. This interval of 3 msec can extend upto a maximum of 75 msec.
- When BLUE Alarm is declared, Yellow Alarm is sent to the far end.
- This alarm is cleared when clearance of AIS is detected for continuous 10 seconds.

You can view the status of these alarms in the Jeeves. To view the status,

- Click the **Maintenance** link to expand.
- Click the **T1E1 Port Alarms/Performance Monitoring** link.

- Click the tab of the desired T1E1 port.

- Whenever, any alarm is detected by the system, it will increment the counter for that alarm and display its status as **Present**. When that alarm is cleared, the system will change the status of that alarm to **Absent**.

By default, the value of each counter is 0. The maximum value for each counter is 255. Once the counter value reaches 255, the system will continue to display this value until you clear it.

- Click the **Clear Alarms/Counters** button to clear the counter value. You must clear the counter value, if you change any settings of the system or the line connection.



The page refreshes automatically after every 10 seconds to display the new status.

Performance Monitoring Counter

All errors do not generate an alarm. A few severe errors generate alarms while for others, error counters are supported by the ISDN chip in the system hardware. This error counter is used for Performance Monitoring.

Various Error Counters supported by the ISDN chip in E1 Mode are given in the table below.

Counter	Meaning
Frame Alignment Signal Error Counter	This counter is incremented on receipt of each errored FAS.
Far End Block Error Counter	This counter is incremented when either E1 or E2 bit is set in the transmit frame.
CRC-4 Error Counter	This counter is incremented when the received frame has CRC-4 errors.
Line Code Violation	This counter is incremented when a line code violation error occurs.
Positive Slip Counter	This counter is incremented every time a positive slip occurs.

Counter	Meaning
Negative Slip Counter	This counter is incremented every time a negative slip occurs.

Various Error Counters supported by the ISDN chip in T1 Mode are given in the table below.

Counter	Meaning
Framing Alignment Bit Error Counter	This counter is incremented on receipt of any error in the framing pattern. In D4, Ft errors are counted. (Fs errors are counted if enabled) In ESF, any error in the 001011 framing pattern increments this counter.
Out of Frame Synchronization Error Counter	Out Of Frame (OOF) - Out of Frame is the occurrence of a particular density of framing error events. For D4 framing, OOF is declared when the receiver detects two or more framing errors within 0.75 msec or two or more errors out of five or fewer consecutive framing bits. It ends when there are fewer than two frame bit errors within a 0.75 msec period. For ESF framing, OOF is declared when the receiver detects two or more framing errors within 3ms or two or more errors out of five or fewer consecutive framing bits. It ends when there are fewer than two frame bit errors within a 3 msec period.
CRC-6 Error Counter	This counter is incremented when the received frame has CRC-6 errors. This is applicable for ESF framing only.
Line Code Violation	This counter is incremented when a bipolar violation error occurs or when excessive zeroes event occurs.
Positive Slip Counter	This counter is incremented every time a positive slip occurs.
Negative Slip Counter	This counter is incremented every time a negative slip occurs.

You can view these Error Counters in the Jeeves for monitoring the performance of T1E1 Port.

- Click the **Maintenance** link to expand.
- Click the **T1E1 Port Alarms/Performance Monitoring** link.

Performance Monitoring Counter	
CRC-4 Error Counter	<input type="text" value="0"/>
FAS/NFAS Bit/Pattern Error Counter	<input type="text" value="0"/>
Far End Block Error Counter	<input type="text" value="0"/>
Line Code Violation	<input type="text" value="0"/>
Positive Slip Counter	<input type="text" value="0"/>
Negative Slip Counter	<input type="text" value="241"/>

- Whenever an error is detected by the system, it will increment the counter for that error.

By default, the value of each counter is 0. The maximum value for each counter is 255. Once the counter value reaches 255, the system will continue to display this value until you clear it.

- Click the **Clear Alarms/Counters** button to clear the counter value. You must clear the counter value, if you change any settings of the system or the line connection.



The page refreshes automatically after every 10 seconds to display the new status.

You can view the System Details, NX DBM Vocoder Details and the status of Auto Configuration upgrade, LAN Port, WAN Port, SIP Trunks, and T1E1 Ports from Jeeves.

To view status,

- Click the **Status** link to expand.

System Detail

- Click the **System Detail** link.

Basic Settings	System Detail
Advanced Settings	
Maintenance	
Status	
+ System Detail	
+ NX DBM Vocoder Detail	
+ System Performance	
+ Configuration	
+ Network	
+ SIP Trunk	
+ T1E1 Port	

System Detail	
Product Name	SETU VTEP4P
Software Version-Revision	nightly-07 Oct,2020 00:15
Platform Version-Revision	trunk-r116553 (Sep 30 2020 20:55:39)
Kernel Date	#1 Tue Oct 6 09:46:31 IST 2020
CPLD Version-Revision	V1R1
Serial Number of the Product	1
Hardware Design of Main Board	2
Call Manager Firmware Version	branch-SipNetwork_IPV6-r116871 (Oct 7 2020 00:18:44)
Slave Layer Firmware Version	trunk-r116619 (Oct 7 2020 00:19:55)
Media Server Firmware Version	branch-Sip_IPV6_Support-r116872 (Oct 7 2020 00:19:59)
T1E1 Port	4
NX DBM Vocoder 1 Status	Present (64 channels) - Temperature (30 °C)
NX DBM Vocoder 2 Status	Present (64 channels) - Temperature (38 °C)
WAN Port MAC Address	00:1b:09:07:fa:78
LAN Port MAC Address	00:1b:09:07:fa:77

The following **System Details** will be displayed on this page.

- Product Name:** This displays the name of the Product.

- **Software Version-Revision:** This displays the current version and revision of the firmware of SETU VTEP.
- **Platform Version-Revision:** This displays the version revision of the platform along with date and time.
- **Kernel Date:** This displays the Kernel compilation date.
- **WAN Port MAC Address:** This displays the factory set MAC Address of the WAN Port.



If you have cloned the MAC Address of the WAN Port, you can view it in Network Status.

- **LAN Port MAC Address:** This displays the factory set MAC Address of the LAN Port.



If you have cloned the MAC Address of the LAN Port, you can view it in Network Status.

NX DBM Vocoder

The NX DBM Vocoder displays the status of the Vocoder modules present in the system.

NX DBM Vocoder 1 Status: This displays the status of NX DBM Vocoder 1.

NX DBM Vocoder 2 Status: This displays the status of NX DBM Vocoder 2.

NX DBM Vocoder Detail

NX DBM Vocoder 1 status is displayed on this page.

NX DBM Vocoder 1

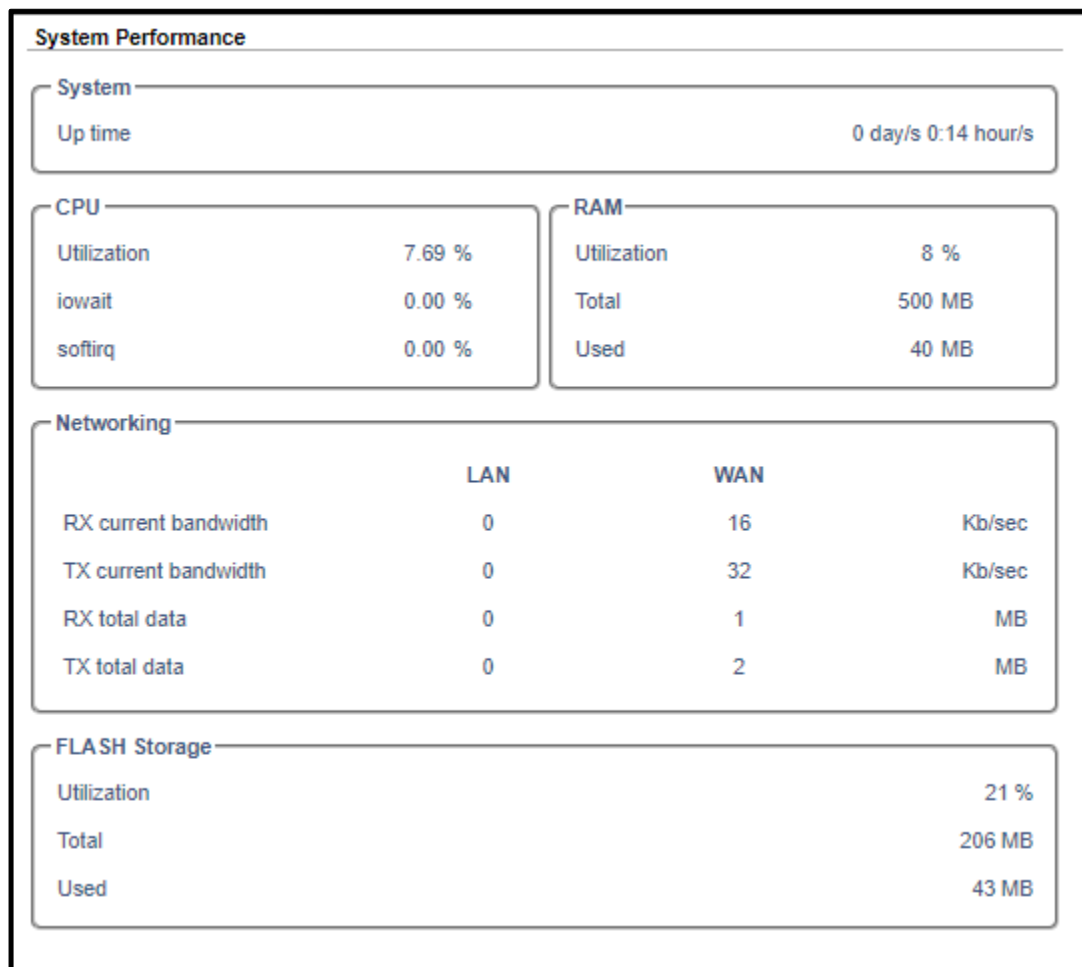
Status	Running
Firmware Version	Vocallo 02.01.10-B5-PR
Main API Version	Main API 2.1.10.5
Cpp API Version	Cpp API 2.1.10.5
Vspmp Voc API Version	VspMp Voice API 2.1.10.5
Vspmp Vid API Version	VspMp Video API 2.1.10.5
Net API Version	Net API 2.1.10.5
Device Information	<div>DEVICE_TYPE=0x2 DEVICE_VERSION_ID=0x4 DEVICE_SERIAL_NUMBER=0x000012D5 DEVICE_PROJECT_NUMBER=0x4BDAD DEVICE_DSP_CORE_TYPE=0x2 DEVICE_DSP_CORE_NUMBER=0x18 DEVICE_EXT_MEM_BYTE_SIZE=0x20000000 DEVICE_IO_ETH_PORT_NUMBER=0x2 DEVICE_IO_ETH_MAC_ADDRESS_PORT_0=000C90493E71 DEVICE_IO_ETH_MAC_ADDRESS_PORT_1=000C90493E73 DEVICE_IO_TDM_STREAM=0x8 DEVICE_IO_TDM_FREQUENCY=0x0 DEVICE_IO_TDM_OUTPUT_ENABLE_SUPPORT=0x0 DEVICE_IO_TDM_OUTPUT_ENABLE=0x1 DEVICE_LAST_SYSLOG=0x00 DEVICE_STAGE1_VERSION=0x0210</div>

NX DBM Vocoder 2:

NX DBM Vocoder 2

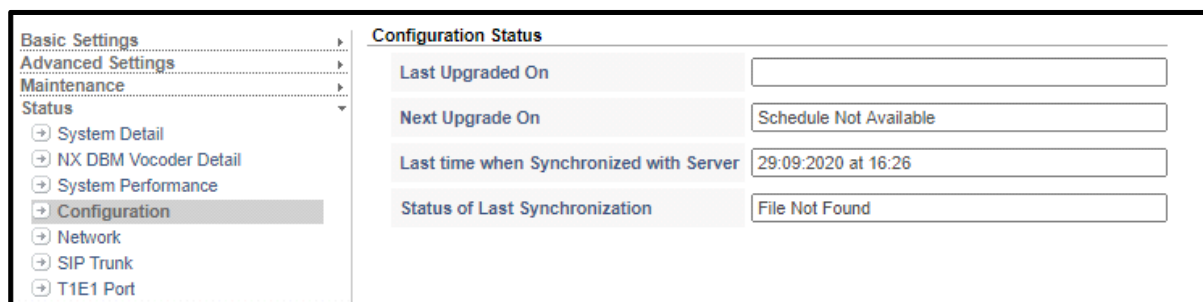
Status	Not Present
Firmware Version	
Main API Version	
Cpp API Version	
Vspmp Voc API Version	
Vspmp Vid API Version	
Net API Version	
Device Information	

System Performance



Configuration

- Click the **Configuration** link.



The following information related to Auto-Configuration upgrade will appear on your screen.

- Last Upgraded On:** This displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VTEP last upgraded its configuration through the server.

- **Next Upgrade On:** This displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VTEP will again check for new configuration on the server.
- **Last time when Synchronized with Server:** This displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VTEP last resynchronized with the server for new configuration.
- **Status of Last Synchronization:** This displays the status of last synchronization. The possible status messages that may appear are listed in the table below.

Possible Responses	Event
Invalid Parameters	When parameters are not valid.
Local Failure	When internal error occurs, like Thread Creation failed.
Resolving Server Address	When IP Address is not found using DNS query.
Server Not Found	When server is not connected after the expiry of Retry Timer and Retry Counter.
Send Request Failed	When there is Curl Internal Error
Connecting to Server	When system is establishing TCP connection with server until the expiry of Retry Timer and Retry Counter.
TCP/TFTP Connection Failed	When no response is received for TCP/TFTP connection until expiry of Retry Timer and Retry Counter.
Connection Failed	When no response is received for TCP connection after expiry of Retry Timer and Retry Counter. When there is an open SSL error. When the maximum file size is exceeded. When there are too many Redirect or illegal operation from curl response.
Permission Denied	When access is denied. When there is permission problem on the server. When login fails.
Downloading Config File	When the system is retrieving config file.
File Not Found	When the remote file is not found.
Config Decryption Failed	When the config decryption has failed.
Config Parsing Failed	When the file parsing has failed. When the root tag is not found.
Successfully Updated	When configuration is updated successfully.

Network

- Click the **Network** link.

Network Status	
IP Addressing mode for LAN	IPv4 and IPv6
IP Addressing mode for WAN	IPv4 and IPv6
LAN	
Ethernet Link	Down
MAC Address	00:1b:09:07:fa:7b
IPv4 Status	
Stack State	Static - Success
IP Address	192.168.123.186
Subnet Mask	255.255.255.0
IPv4 Network Reinitialization	
IPv6 Status	
Stack State	Static - In Progress
IP Address	
Prefix length	64
IPv6 Network Reinitialization	
WAN	
Ethernet Link	Up
Default MAC Address	00:1b:09:07:fa:7c
MAC Address in use	00:1b:09:07:fa:7c
Dynamic DNS Status	Updaters Error

IPv4 Status	
Stack State	Static - Success
VoIP Stack State	Up - UDP, TCP, TLS
IP Address	192.168.111.186
Subnet Mask	255.255.255.0
Gateway	192.168.111.1
DNS Address	192.168.123.112
IPv4 Network Reinitialization	
IPv6 Status	
Stack State	Static - Success
VoIP Stack State	Up - UDP, TCP, TLS
IP Address	4001::186
Prefix length	64
Gateway	4001::1
DNS Address	
IPv6 Network Reinitialization	
NAT	
NAT Type	Stun Adr Rslv Fail
Router's Public IP Address for WAN	192.168.123.10
System IP Address fetched using STUN	0.0.0.0
IP Address fetched using STUN	
SIP Port fetched using STUN	0

The current values of the following parameters will appear on your screen:

Network Status

- IP Addressing mode for LAN:** IPv4 and IPv6
- IP Addressing mode for WAN:** IPv4 and IPv6

LAN Port

- Ethernet Link:** This displays the status of Ethernet link of LAN Port of SETU VTEP..
- MAC Address:** This displays the MAC Address assigned to the LAN Port of SETU VTEP.

IPv4 Status

- Stack State:** This displays the SIP Stack Status.
- IP Address:** This displays the current IP address assigned to the LAN Port of SETU VTEP.

- **Subnet Mask:** This displays current Subnet Mask assigned to the LAN Port of SETU VTEP.
- **IPv4 Network Reinitialization:**

IPv6 Status

- **Stack State:** This displays the SIP Stack Status.
- **IP Address:** This displays the current IP address assigned to the LAN Port of SETU VTEP.
- **Prefix length:** This displays current Prefix length of LAN Port of SETU VTEP.
- **IPv4 Network Reinitialization:**

WAN Port

- **Ethernet Link:** This displays the status of Ethernet link of LAN Port of SETU VTEP..
- **Default MAC Address:** This displays the default MAC Address assigned to the LAN Port of SETU VTEP.
- **MAC address in use:** This displays the MAC Address which is in use assigned to the LAN Port of SETU VTEP.
- **Dynamic DNS Status:** This displays the response received from DDNS server while sending the IP Address update request to the server. The following are the responses which you may receive:

Possible Responses	Event
Please Wait....!!	When system is waiting for error/ successful response from DDNS server
Updated Successfully - IP Address	IP Address updated successfully in DDNS server
Host has been blocked	When 'abuse' is received
Authentication Fail	When authentication check is failed either problem in user id or password
No such host in the system	When 'no host' is received
Invalid hostname format	When 'notfqdn' is received
Host not in this account	When '!Yours' is received
DNS error encountered	When 'dnserr' is received
Server goes under schedule maintenance	When '911' is received
No Response	No response is received from DDNS server due to any reason
DDNS Failed	For all remaining cases
In all remaining cases, the default messages supported by DDNS client will appear in this.	

IPv4 Status

- **Stack State:** This displays the SIP Stack Status.
- **VoIP Stack State:** This displays the VoIP Stack Status.
- **IP Address:** This displays the IP address assigned to the WAN Port of SETU VTEP.
- **Subnet Mask:** This displays the Subnet Mask assigned to the WAN Port of SETU VTEP.
- **Gateway IP Address:** This displays the Gateway Address assigned to the WAN Port of SETU VTEP.
- **DNS Address:** This displays the DNS address.
- **IPv4 Network Reinitialization:**

IPv6 Status

- **Stack State:** This displays the SIP Stack Status.
- **VoIP Stack State:** This displays the VoIP Stack Status.
- **IP Address:** This displays the IP address assigned to the WAN Port of SETU VTEP.
- **Prefix length:** This displays current Prefix length of WAN Port of SETU VTEP.
- **Gateway:** This displays the Gateway Address assigned to the WAN Port of SETU VTEP.
- **DNS Address:** This displays the DNS address.
- **IPv6 Network Reinitialization:**

NAT

- **NAT Type:** This displays the NAT Type, if STUN is enabled in SETU VTEP. The commonly used NAT types are:
 - Unknown
 - Open
 - Conenat
 - Restrictednat
 - Portrestrictednat
 - Symmetricnat
 - Symmetricfirewall
 - Blocked
- **Router's Public IP Address for WAN:** This displays the Router's Public IP address of WAN programmed in the System Parameters. See ["NAT"](#) under *System Parameters*.
- **System IP Address fetched using STUN:** This displays the IP address fetched using STUN, if STUN server address is programmed in the system.

- **IP Address fetched using STUN:** This displays the IP address fetched using STUN, if STUN server address is programmed in the system.
- **SIP Port fetched using STUN:** This displays the SIP Port fetched using STUN, if STUN server address is programmed in the system.

SIP Trunk

- Click the **SIP Trunk** link.

SIP Trunk Status				
<div> <div>1-32</div> <div>33-64</div> <div>65-96</div> <div>97-125</div> </div>				
SIP Trunk Number	Status	Registration Time	Registration Retry Count	Failed Reason
1	Active	0	0	
2	Active	0	0	
3	Disabled	0	0	
4	Active	0	0	
5	Active	0	0	
6	Disabled	0	0	
7	Disabled	0	0	
8	Disabled	0	0	
9	Disabled	0	0	
10	Disabled	0	0	
11	Disabled	0	0	
12	Disabled	0	0	
13	Disabled	0	0	
14	Disabled	0	0	
15	Disabled	0	0	
16	Disabled	0	0	
17	Disabled	0	0	

The following status indications will appear for the SIP Trunks.

- **SIP Trunk Number:** This displays the SIP Trunk number.

- **Status:** The possible status indications that will be displayed in this column for the respective SIP Trunk numbers are described in the table below.

Status Message	Meaning
Disable	The SIP Trunk is disabled.
Registering	The SIP Trunk is enabled and is waiting for response from the SIP server.
Active	The SIP Trunk is registered with the SIP server.
Failed	Some error has occurred in the SIP Trunk and no calls can be made using the SIP Trunk (applicable only if the SIP Trunk mode is configured as 'Proxy').
Network Connection Disable	The SIP Trunk is enabled but the active <i>Network Connection</i> does not match the option selected for <i>Use SIP Trunk for Network Connection</i> parameter.
Inactive	The Proxy Server is unavailable (no response is received from the server).

- **Registration Time:** The SIP Trunk is registered with the Registrar Server for a particular time period, after which it has to be re-registered. The registrar server indicates the time remaining for re-registration of the SIP Trunk. The same is displayed in this field as Registration Time.
- **Registration Retry Count:** This displays the total number of register messages which are sent to the registrar server for registering the SIP Trunk.
- **Failed Reason:** This displays the reason for failure of SIP Trunk registration with the registrar server. The different reasons for registration failure that may appear are:

Failure Message	Description
Message send fail	This reason is displayed when registration request sent to registrar server fails.
Failed to create Register client	This reason is displayed when SIP stack has memory constraints, or resource limitation or the number of SIP clients to register is greater than the number programmed in the stack.
Failed to detach register client	This reason is displayed when SIP stack has memory constraint/ resource limitation/ the number of SIP clients to register is greater than the number programmed in the stack.
Failed to send request	This reason is displayed when DNS server is not programmed.
Local Failure	This reason is displayed when DNS query fails.
Response timeout	This reason is displayed on the expiry of the General Request Timer.
Error Response- 4xx to 6xx	This is the error response code.
No contact header in 2xx	This reason is displayed when no contact address is received in the 2xx response from the SIP server.
Authentication Failed	This reason is displayed when the SIP server does not authenticate the client.
STUN address is not programmed	This reason is displayed when STUN is enabled but address is not configured.
STUN query fail	This reason is displayed when a query to the STUN server fails.

Failure Message	Description
Outbound address is not programmed	This reason is displayed when Outbound is enabled but Outbound address is not configured.
Router's IP address is not programmed	This reason is displayed when Router's IP Address is to be used in signaling but the address is not programmed.
Remote Peer Not Alive	This reason is displayed when no response is received from the remote peer for the OPTIONS message.



If for a SIP Trunk, you have enabled **Fallback Server** and **Registration Behavior** is set to **Register with all Servers**, the SIP Trunk Status page will display status of all the servers for that SIP Trunk as shown below.

T1E1 Port

- Click the **T1E1 Port** link.

T1E1 Port Status		
T1E1 Port Number	Layer 1	Layer 2
1	UP	UP
2	UP	UP
3	DOWN	DOWN
4	DOWN	DOWN

The following parameters will be displayed for the T1E1 Port.

- Layer 1:** Displays if the link is up or down.
- Layer 2:** Displays if the link is up or down.

Appendix

Acronyms

AIS	Alarm Indication Signal
ANT	Automatic Number Translation
ANSI	American National Standard Institute
BRI	Basic Rate Interface (2 B-Channels@64Kbps + D-Channel@64Kbps)
CAS	Channel Associate Signaling
CDR	Call Detail Record
CLI	Caller Line Identification
CLIP	Caller Line Identification and Presentation
CLIR	Calling Line Identification Restriction
CO	Call Outgoing
COS	Class of Service
CPT	Call Progress Tone
CPTG	Call Progress Tone (Generation)
CRC	Cyclic Redundancy Check
CUG	Closed User Group
DDI	Direct Dialing In
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Service
DTMF	Dual Tone Multi-Frequency
E1	E-Carrier1 (30B+D)
FCBC	Float cum Boost Charger
FIFO	First In First Out
FoIP	Fax over IP
FSK	Frequency Shift Keying
FTP	File Transfer Protocol

GMT	Greenwich Mean Time
GSM	Global System for Mobile
IC	Incoming call
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ITSP	Internet Telephony Service Provider
ITU	International Telecommunication Union
LAN	Local Area Network
LCD	Liquid Crystal Display
LCR	Least Cost Routing
LED	Light Emitting Diodes
LOS	Loss of signal
MAC	Media Access Control
MDF	Main Distribution Frame
MFA	Multi-Frame Alignment
MOH	Music on Hold
MSN	Multiple Subscribers Numbers
NAT	Network Address Translation
NPI	Numbering Plan Identification
NT	Network Terminal
PBX	Private Branch Exchange
PC	Personal Computer
PCM	Primary Interface Compounding
PIN	Personal Identification Number
PMS	Property Management Software
POTS	Plain Old Telephone Systems
PPM	Primary Protection Module
PPPoE	Point-to-Point Protocol over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSTN	Public Switched Telephone Network
PUK	Personal Unlock Key
RBS	Robbed Bit Signaling
RCOC	Returned Call to Original Caller
RF	Radio Frequency
RTC	Real Time Clock

<i>RTP</i>	Real Time Protocol
<i>SAL</i>	System Activity Log
<i>SE</i>	System Engineer
<i>SFL</i>	System Fault Log
<i>SIP</i>	Session Initiation Protocol
<i>SIM</i>	Subscriber Identity Module
<i>SLT</i>	2 wire Analog Station, Single Line Telephone
<i>SMDR</i>	Station Message Detail Recording
<i>SMPS</i>	Switch Mode Power Supply
<i>SNMP</i>	Simple Network Management Protocol
<i>SNTP</i>	Simple Network Time Protocol
<i>T1</i>	T-Carrier (23B+D)
<i>TE</i>	Terminal Equipment / Device
<i>TCP/IP</i>	Transmission Control Protocol/Internet Protocol
<i>TON</i>	Type of Numbering Plan
<i>UDP</i>	User Datagram Protocol
<i>UPS</i>	Un-interrupted Power Supply
<i>URI</i>	Uniform Resource Identifier
<i>VoIP</i>	Voice over IP
<i>WAN</i>	Wide Area Network

Default Region Table

The country-specific default settings of various parameters that will be loaded on changing the **Region** are presented in the table below.

Region Code	Country/ Region	Default Language	Default Time Zone	Default DST Type	Default CPTG	Default Ring Type	Country Code	Companding Type	T1E1 Carrier Type	System Clock Synchronization
1	Afghanistan	English	GMT+04:30				93			
2	Algeria	English	GMT+01:00				213	A-law		
3	Antigua and Barbuda	English	GMT-04:00				1 268			
4	Argentina	Spanish	GMT-03:00		4		54	A-law		
5	Australia (Perth)	English	GMT+08:00		5	8	61			
6	Australia (Adelaide)	English	GMT+09:30	2	5	8	61			
7	Australia (Brisbane, Canberra, Melbourne, Sydney)	English	GMT+10:00		5	8	61			
8	Austria	German	GMT+01:00	1			43			
9	Bahamas	English	GMT-05:00				1 242			
10	Bahrain	English	GMT+04:00	3			973			
11	Bangladesh	English	GMT+06:00				880			
12	Belarus	English	GMT+02:00				375			
13	Belgium	French	GMT+01:00	2	39	11	32	A-law		
14	Bhutan	English	GMT+06:00				975			
15	Bolivia	Spanish	GMT-04:00				591			
16	Bosnia and Herzegovina	English	GMT+01:00				387			
17	Botswana	English	GMT+02:00				267			
18	Brunei	English	GMT+08:00				673			
19	Brazil (Fernando De Noronha)	Portuguese	GMT-02:00		6	6	55	A-law		
20	Brazil (Brasilia, Rio de Janeiro, Sao Paulo)	Portuguese	GMT-03:00	4	6	6	55	A-law		
21	Brazil (Manaus)	Portuguese	GMT-04:00		6	6	55	A-law		
22	Brazil (Acre)	Portuguese	GMT-05:00		6	6	55	A-law		
23	Bulgaria	English	GMT+02:00				359			
24	Cambodia	English	GMT+07:00				855			
25	Cameroon	English	GMT+01:00				237			
26	Canada (St. John's)	English	GMT-03:30	5	7	7	1	U-law	T1	1.54MHz
27	Canada (Halifax)	English	GMT-04:00	5	7	7	1	U-law	T1	1.54MHz
28	Canada (Montreal, Ottawa, Toronto)	English	GMT-05:00	5	7	7	1	U-law	T1	1.54MHz
29	Canada (Winnipeg)	English	GMT-06:00	5	7	7	1	U-law	T1	1.54MHz
30	Canada (Calgary)	English	GMT-07:00	5	7	7	1	U-law	T1	1.54MHz
31	Canada (Vancouver)	English	GMT-08:00	5	7	7	1	U-law	T1	1.54MHz
32	Chile	Spanish	GMT-04:00	6			56			
33	China	English	GMT+08:00		8	11	86	A-law		
34	Colombia	Spanish	GMT-05:00				57			
35	Costa Rica	Spanish	GMT-06:00				506			
36	Croatia	English	GMT+01:00				385			
37	Cuba	Spanish	GMT-05:00	18			53	A-law		
38	Cyprus	English	GMT+02:00				357			
39	Czech Republic	English	GMT+01:00				420			
40	Denmark	English	GMT+01:00	7			45	A-law		
41	Egypt	English	GMT+02:00	11	9	7	20	A-law		
42	Fiji	English	GMT+12:00				679			
43	Finland	English	GMT+02:00	8			358	A-law		

Region Code	Country/ Region	Default Language	Default Time Zone	Default DST Type	Default CPTG	Default Ring Type	Country Code	Companding Type	T1E1 Carrier Type	System Clock Synchronization
44	France	French	GMT+01:00	2	10	14	33	A-law		
45	Germany	German	GMT+01:00	2	11	6	49	A-law		
46	Greece	English	GMT+02:00	2	12	6	30			
47	Guyana	English	GMT-04:00				592			
48	Hong Kong	English	GMT+08:00				852			
49	Hungary	English	GMT+01:00	2			36			
50	India	English	GMT+05:30		13	8	91	A-law		
51	Indonesia	English	GMT+07:00		14		62			
52	Iran	English	GMT+03:30		15		98			
53	Iraq	English	GMT+01:00	9	16		964			
54	Ireland	English	GMT	7			353			
55	Israel	English	GMT+02:00		17	15	972			
56	Italy	Italian	GMT+01:00	2	18	6	39			
57	Japan	English	GMT+09:00		19	10	81	U-law		
58	Jordan	English	GMT+02:00				962	A-law		
59	Kazakhstan	English	GMT+05:00				7			
60	Kenya	English	GMT+03:00		20		254			
61	Korea – North	English	GMT+09:00		21	11	850			
62	Korea – South	English	GMT+09:00		21	11				
63	Kuwait	English	GMT+03:00				965			
64	Kyrgyzstan	English	GMT+06:00	10			996			
65	Lebanon	English	GMT+02:00	12			961			
66	Libya	English	GMT+02:00				218			
67	Malaysia	English	GMT+08:00		22	15	60			
68	Maldives	English	GMT+05:00				960			
69	Mauritius	English	GMT+04:00				230			
70	Mexico (Mexico City)	Spanish	GMT-06:00	3	23		52	A-law		
71	Mexico (Chihuahua)	Spanish	GMT-07:00	3	23		52	A-law		
72	Mexico (Tijuana)	Spanish	GMT-08:00	3	23		52	A-law		
73	Mongolia	English	GMT+08:00				976			
74	Mozambique	Portuguese	GMT+02:00				258			
75	Myanmar	English	GMT+06:30				95			
76	Namibia	English	GMT+01:00	13			264			
77	Nepal	English	GMT+05:45				977			
78	Netherlands	English	GMT+01:00				31	A-law		
79	New Zealand	English	GMT+12:00	14	24	15	64			
80	Nigeria	English	GMT+01:00				234			
81	Norway	English	GMT+01:00	15			47	A-law		
82	Oman	English	GMT+04:00				968			
83	Pakistan	English	GMT+05:00				92			
84	Paraguay	Spanish	GMT-04:00	16			595			
85	Peru	Spanish	GMT-05:00				51			
86	Philippines	English	GMT+08:00		25		63	A-law		
87	Poland	English	GMT+01:00	1	26	15	48			
88	Portugal	Portuguese	GMT	7	27	12	351			
89	Qatar	English	GMT+03:00				974			
90	Romania	English	GMT+02:00				40			
91	Russia (Moscow, St. Petersburg)	English	GMT+04:00	1	28	11	7			
92	Russia (Novosibirsk)	English	GMT+07:00	1	28	11	7			
93	Russia (Vladivostok)	English	GMT+11:00	1	28	11	7			

Region Code	Country/ Region	Default Language	Default Time Zone	Default DST Type	Default CPTG	Default Ring Type	Country Code	Companding Type	T1E1 Carrier Type	System Clock Synchronization
94	Singapore	English	GMT+08:00		30	8	65	A-law		
95	Slovakia	English	GMT+01:00				421			
96	South Africa	English	GMT+02:00		31	8	27			
97	Spain	Spanish	GMT+01:00	1	32	13	34	A-law		
98	Sri Lanka	English	GMT+05:30				94			
99	Sudan	English	GMT+03:00				249			
100	Sweden	English	GMT+01:00	2			46	A-law		
101	Switzerland	German	GMT+01:00	2			41			
102	Syria	English	GMT+02:00	17			963			
103	Taiwan	English	GMT+08:00				886			
104	Tajikistan	English	GMT+05:00				992			
105	Thailand	English	GMT+07:00		33	15	66	A-law		
106	Turkey	English	GMT+02:00		34		90			
107	Uganda	English	GMT+03:00				256			
108	Ukraine	English	GMT+02:00				380			
109	United Arab Emirates	English	GMT+04:00		35	15	971	A-law		1.54MHz
110	United Kingdom	English	GMT	7	36	8	44	A-law		1.54MHz
111	United States (Atlanta, Augusta, Boston, Charlotte, Columbus, Detroit, Indianapolis, Miami, NY, Philadelphia, Washington)	English	GMT-05:00	3	37	7	1	U-law	T1	1.54MHz
112	United States (Chicago, Dallas, Des Moines, Memphis, Minneapolis, New Orleans, Oklahoma, Omaha, St. Louis)	English	GMT-06:00	3	37	7	1	U-law	T1	1.54MHz
113	United States (Albuquerque, Boise, Cheyenne, Denver, Salt Lake City)	English	GMT-07:00	3	37	7	1	U-law	T1	1.54MHz
114	United States (Las Vegas, Los Angeles, Phoenix, San Francisco, Seattle)	English	GMT-08:00	3	37	7	1	U-law	T1	1.54MHz
115	United States (Juneau)	English	GMT-09:00	3	37	7	1	U-law	T1	
116	United States (Hawaii)	English	GMT-10:00		37	7	1	U-law	T1	
117	Uzbekistan	English	GMT+05:00				998			
118	Venezuela	Spanish	GMT-04:30				58			
119	Vietnam	English	GMT+07:00				84			
120	Yemen	English	GMT+03:00				967			
121	Yugoslavia	English	GMT+02:00				381			
122	Zambia	English	GMT+02:00				260		T1E1 Carrier Type	
123	Zimbabwe	English	GMT+02:00				263			

Call Progress Tones

Call Progress Tones (CPT) are audible tones sent by switching systems such as PSTN or PBX, to calling parties to show the status of the phone call.

Each CPT has a distinctive tone frequency and cadence assigned to it, for which some standards have been established by the ETSI.

On the basis of specific frequency, modulating frequency and cadence, the CPTs generated by SETU VTEP are categorized as:

- Dial Tone
- Ring Back Tone
- Busy Tone
- Error Tone 1
- Confirmation Tone
- Feature Tone/ Programming Tone
- Intrusion Tone
- Error Tone 2
- Routing Tone

CPT standards are applied differently in different situations and in different countries. You can match call progress tones of SETU VTEP to that of the country standard where it is installed.

See the table for the **CPTG Type** (frequency and cadence of the different tones) supported by SETU VTEP. The table shows the CPTG Types supported for different countries.

When you select 'Region', the Call Progress Tones matching the country standards of the selected Region/Country will be automatically loaded. However, you may select a different CPTG Type, if required. You can also customize the frequency and cadence. For instructions, see ["Region"](#) under *Basic Settings*.



Remote Hold Tone is fixed for all the countries; it is non-programmable.

CPTG Types (as per ETSI standard) supported by SETU VTEP

CPTG Type	Country	Feature / Programming / Prompt Tone		Routing Tone		Intrusion Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
1	Type1	350+440	0.1on 0.9off	350+440	0.1on 1.9off	440	0.1on 2.9off
2	Type2	400	1.5on 0.1off	400	0.1on 1.9off	400	0.1on 2.9off
3	Type3	350+440	0.1on 0.9off	350+440	0.1on 1.9off	440	0.1on 2.9off
4	Argentina	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
5	Australia	425*25	0.1on 0.9off	425*25	0.1on 1.9off	425*25	0.1on 2.9off
6	Brazil	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
7	Canada	350+440	0.1on 0.9off	350+440	0.1on 1.9off	350+440	0.1on 2.9off
8	China	450	0.1on 0.9off	450	0.1on 1.9off	450	0.1on 2.9off

CPTG Type	Country	Feature / Programming / Prompt Tone		Routing Tone		Intrusion Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
9	Egypt	425*50	0.1on 0.9off	425*50	0.1on 1.9off	450	0.1on 2.9off
10	France	440	0.1on 0.9off	440	0.1on 1.9off	440	0.1on 2.9off
11	Germany	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
12	Greece	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
13	India	400*25	0.1on 0.9off	400*25	0.1on 1.9off	400*25	0.1on 2.9off
14	Indonesia	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
15	Iran	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
16	Iraq	400	0.1on 0.9off	400	0.1on 1.9off	400	0.1on 2.9off
17	Israel	400	0.1on 0.9off	400	0.1on 1.9off	400	0.1on 2.9off
18	Italy	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
19	Japan	400	0.1on 0.9off	400	0.1on 1.9off	400	0.1on 2.9off
20	Kenya	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
21	Korea	350+440	0.1on 0.9off	350+440	0.1on 1.9off	350+440	0.1on 2.9off
22	Malaysia	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
23	Mexico	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
24	New Zealand	400	0.1on 0.9off	400	0.1on 1.9off	425	0.1on 2.9off
25	Phillippines	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
26	Poland	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
27	Portugal	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
28	Russia	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
29	Saudi Arabia	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
30	Singapore	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
31	South Africa	400*33	0.1on 0.9off	400*33	0.1on 1.9off	400*33	0.1on 2.9off
32	Spain	425	0.1on 0.9off	425	0.1on 1.9off	425	0.1on 2.9off
33	Thailand	400*50	0.1on 0.9off	400*50	0.1on 1.9off	400*50	0.1on 2.9off
34	Turkey	450	0.1on 0.9off	450	0.1on 1.9off	450	0.1on 2.9off
35	UAE	350+440	0.1on 0.9off	350+440	0.1on 1.9off	350+440	0.1on 2.9off
36	UK	350+440	0.1on 0.9off	350+440	0.1on 1.9off	350+440	0.1on 2.9off
37	USA	350+440	0.1on 0.9off	350+440	0.1on 1.9off	350+440	0.1on 2.9off
38	Type4	400	1.75on 0.1off	400	0.1on 1.9off	400	0.1on 2.9off

CPTG Type	Country	Feature / Programming / Prompt Tone		Routing Tone		Intrusion Tone	
		Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)	Freq.(Hz)	Cadence (Seconds)
39	Belgium	350+440	0.1on 0.9off	425	0.1on 1.9off	350+440	0.1on 2.9off
40	Type5	350+440	0.1on 0.9off	350+440	0.1on 1.9off	350+440	0.1on 2.9off

Remote Hold

- **Frequency:** 400 Hz (applicable for all Regions)
- **Cadence (msec):** 500-1500 (applicable for all Regions)

Product Specifications

System Resources

System Resources	SETU VTEP 4P	SETU VTEP 3P	SETU VTEP 2P	SETU VTEP 1P
T1/E1 PRI Ports	4	3	2	1
SIP Trunks	125	125	125	125
No. of simultaneous calls	120	90	60	30
No. of Built-in VoIP Modules	2	2	1	1

Technical Specifications

VoIP

VoIP Protocols	SIP v2, SDP, RTP (RFC 2883),SRTP
Network Protocol	IPv4, TCP, UDP, DHCP, PPPoE, SNTP, NAT, STUN, HTTP, TLS, DynDNS
SIP	Maximum 125 SIP Accounts per system, Outbound Proxy Support, Display Name, User Name, Password, URL, Proxy URL, Register URL, Register Interval
NAT	STUN and NAT Keep Alive
Voice CODECS	G.729, G.723, GSM FR, iLBC (30ms), iLBC (20ms), GSM EFR, G.711 (u-Law), G.711 (ALaw)
Line Echo Cancellation	G.168 with variable Tail Length
Call Progress Tones	Dial Tone, Ring Back Tone, Busy Tone, Error Tone
Voice	Dynamic Jitter Buffer (Adaptive), Comfort Noise Generation and Voice Activity Detection
Fax	T.38(UDPTL), T.38(RTP) and Pass Through
Quality of Service	Layer 3 DiffServe and ToS
Security	Password Protection Administration

ISDN PRI

Channels	23B+D and 30B+D
Personality	Network (NT) and Terminal (TE)
Line Coding	AMI/B8ZS for T1 and HDB3 for E1
Framing	ESF for T1 and CEPT1 (with/without CRC) for E1
Switch Variant	AT&T 5ESS, DMS, US NI2 (National ISDN 2), ETSI NET5

Protection	Solid State (Over Voltage and Over Current) Built-in Secondary Protection
------------	--

E1 CAS

Bit Rate	2048 kbps
High Precision Clock Source	0.025 ppm
Line Coding	HDB3
Framing	CEPT1 (with/without CRC) with CAS MF
Line Signaling	ITU-T Q.400 - Q. 490
Register Signaling	MFC-R2
Alarms	I.431. G.732, ETSI 300-233
Protection	Solid State (Over Voltage and Over Current) Built-in Secondary Protection

T1 RBS

Bit Rate	1544 kbps
High Precision Clock Source	0.025 ppm
Line Coding	AMI and B8ZS
Line Signaling	FXS Loop Start, FXO Loop Start, FXS Ground Start, FXO Ground Start, E&M (Immediate, Wink Start, Wink Start FGD)
Framing	D4, ESF
Digit Dialing	DTMF
Alarms	ANSI T1.231
Performance	ANSI T1.403, ANSI T1.231, AT&T TR54016
Protection	Solid state (Over Voltage and Over Current) Built-in Secondary Protection

Power Supply

Input	12V DC, 2A
Power Consumption	22.37 W (Maximum)

Mechanical

Dimensions (WxHxD)	250.6 X 155.7 X 46 MM (Without Side Clamp) 491 X 155.7 X 46 MM (With Side Clamp)
Mounting	1U Rack Mount & Table-Top

Weight

Unit Weight	Gross Weight: 2.035 Kg 1.067 Kg (Without side clamps) 1.245 Kg (With side clamps)
-------------	---

Environmental

Operating Temperature	0°C to 45°C
Operating Humidity	5-95% RH, Non-Condensing
Storage Temperature	-20°C to +70°C
Storage Humidity	0-95% RH, Non Condensing

Features at Glance

Feature Description	Feature Code
For Making a New Call	#91
To Disconnect Call	#92

a. *Dial # as end of dialing, if it has been configured by you or the system will wait till the expiry of the inter digit wait timer.*

Warranty Statement

Matrix warrants that its products will be free from defects in material and workmanship, under normal use and service for a period of twelve (12) months from the date of installation.

Matrix warrants the replacement or repair of any product or component(s) found to be defective during the applicable period and return the same, or grant a reimbursement credit with respect to the product or component. Parts repaired or replaced will be under warranty throughout the remainder of the original warranty period only. In case of software program design defect(s) that prevents the program from performing the specified functionality, affecting service and beneficial use of the product, Matrix reserves the right to incorporate solutions in its new release of the software and make it available to the customer within a reasonable period of time. The above said with regard to the software design defect, constitutes the sole obligation of Matrix and its authorized installer with respect to the product.

Matrix does not, however, affirm or stand for that the functions or features contained in the system will satisfy its end-user's particular purpose and /or requirements or that the operation of the program will be uninterrupted or error free.

This warranty is voidable by Matrix:

1. If the product is used other than under normal use and is not properly serviced and maintained by qualified technicians.
2. If the product is not maintained under proper environmental conditions.
3. If the product is subjected to abuse, damage, misuse, neglect, fire, power flow, acts of God, accident.
4. If the product is installed or used in combination or in assembly with the products that are not supplied or authorized by Matrix or are of inferior quality or design than Matrix supplied products, which may cause reduction or degradation in functionality.
5. If the product is operated outside the product's specifications or used without designated protections.
6. If the completely filled warranty cards have not been received by Matrix within 15 days of the installation.

In no event will Matrix be liable for any damages, including lost profits, lost business, lost savings, downtime or delay, labor, repair or material cost, injury to person, property or other incidental or consequential damages arising out of use of or inability to use such product, even if Matrix has been advised of the possibility of such damages or losses or for any claim by any other party.

Except for the obligations specifically set forth in this Warranty Policy Statement, in no event shall Matrix be liable for any direct, indirect, special, incidental or consequential damages, whether based on contract or any other legal theory, and where advised of the possibility of such damages.

Neither Matrix nor any of its channel partners makes any other warranty of any kind, whether expressed or implied, with respect to Matrix products. Matrix and its distributors, dealers or sub-dealers specifically disclaim the implied warranties of merchantability and fitness for a particular purpose.

This warranty is not transferable and applies only to the original user of the Product. All legal course of action subjected to Vadodara (Gujarat, India) jurisdiction only.

Disposal of Products/Components after End-Of-Life

Main components of Matrix products are given below:

- **Soldered Boards:** At the end-of-life of the product, the soldered boards must be disposed through e-waste recyclers. If there is any legal obligation for disposal, you must check with the local authorities to locate approved e-waste recyclers in your area. It is recommended not to dispose-off soldered boards along with other waste or municipal solid waste.
- **Batteries:** At the end-of-life of the product, batteries must be disposed through battery recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved batteries recyclers in your area. It is recommended not to dispose off batteries along with other waste or municipal solid waste.
- **Metal Components:** At the end-of-life of the product, Metal Components like Aluminum or MS enclosures and copper cables may be retained for some other suitable use or it may be given away as scrap to metal industries.
- **Plastic Components:** At the end-of-life of the product, plastic components must be disposed through plastic recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved plastic recyclers in your area.

After end-of-life of the Matrix products, if you are unable to dispose-off the products or unable to locate e-waste recyclers, you may return the products to Matrix Return Material Authorization (RMA) department.

Make sure these are returned with:

- proper documentation and RMA number
- proper packing
- pre-payment of the freight and logistic costs.

Such products will be disposed-off by Matrix.

"SAVE ENVIRONMENT SAVE EARTH"

E-Waste Management and Handling Rules

E-waste is a popular, informal name for electronic products nearing the end of their useful life. E-wastes are considered dangerous, as certain components of some electronic products contain materials that are hazardous, depending on their condition and density. The hazardous content of these materials pose a threat to human health and environment. Discarded electronics products such as circuit boards, batteries, wires and other electronic accessories if improperly disposed can leach lead and other substances into soil and groundwater. Many of electronic products can be reused, refurbished or recycled in an environmentally sound manner so that they are less harmful to the ecosystem.

Benefits of E-waste Recycling

Electronics Recycling Conserves Natural Resources

There are many materials that can be recovered from old electronic products. These materials can be used to make new products, thus reducing the need for the new raw materials. For instance, various metals can be recovered from circuit boards and other electronics can be recycled.

Electronics Recycling Supports the Community

Donating your old electronics plays an important role in the provision of refurbished products which can be of great help to certain industries, small organizations and non-profitable organizations. It also helps individuals gain access to technology that they could not have otherwise afforded.

Electronics Recycling Creates Employment Locally

Considering that around 90 percent of electronic equipment is recyclable, electronics recycling can play a significant role in creating employment. This is because new firms dealing with electronics recycling will form and existing firms will look to employ more people to recover recyclable materials. This can be triggered by the increase in the demand for electronics recycling.

Electronics Recycling Helps Protect Public Health and the Environment

Many electronics have toxic or hazardous materials such as mercury and lead, which can be harmful to the environment if disposed in trashcans. Reusing and recycling electronics safely helps in keeping the hazardous materials from harming humans or the environment. For example, certain electronic components and batteries are hazardous since they have lead in them. Printed circuit boards contain harmful materials such as cadmium, lead, mercury and chromium.

Instead of keeping old electronics or dumping them in landfills, recycling or reusing them is an appropriate option that should be supported by individuals and organizations. Considering the benefits of electronics recycling, it is very important that people in various parts around the world embrace this concept.

Creates Jobs

E-waste recycling creates new jobs for professional recyclers and creates a second market for the recycled materials.

Do's & Don'ts

Do's:

- Always look for information on the catalogue with your product for end-of-life equipment handling.
- Ensure that only Authorized Recyclers/Dismantler handle your electronic products.
- Always call at our toll-free No's to Dispose products that have reached end-of life.
- Always drop your used electronic products, batteries or any accessories, when they reach the end of their life at your nearest Authorized E-Waste Collection Points.
- Always disconnect the battery from product and ensure any glass surface is protected against breakage.

Don'ts:

- Do not dismantle your electronic Products on your own.
- Do not throw electronics in bins having "Do not Dispose" sign.
- Do not give e-waste to informal and unorganized sectors like Local Scrap Dealer/ Rag Pickers.
- Do not dispose your product in garbage bins along with municipal waste that ultimately reaches landfills.

E-Waste Management Plan

M/s. MATRIX COMSEC PVT LTD has partnered with **E-Waste Recyclers India (EWRI)** to comply with the new India E-Waste management and handling rules in providing drop-of centers and environmentally sound management of end of life electronics.

EWRI has obtained authorizations from the appropriate governmental agency for their processing facilities. EWRI will receive and recycle customer returned equipment, including all the e-waste. Customers can drop their e-waste in the drop-box provided at various collection centers of EWRI.

A list of collection centers along with the address is mentioned below.

The customers can also call on the following toll free number (1800-102-5679) from Monday to Friday between 10:00 AM to 5:30 PM to get details about the collection centers.

Collection Centers:

State/ City	Location	Logistic	Address	Toll-Free Number
Delhi	Rangpuri	Professional Logistics	Rangpuri, Milakpur Kohi Rangpuri, Rangpuri, New Delhi - 110037	1800-102-5679
Gurugram	Gurugram	Professional Logistics	295, LIG Colony, Sector 31, Gurugram, Haryana - 122022	1800-102-5679
Jharkhand	Dhanbad	Professional Logistics	Sardar Patel Nagar, Dhanbad, Jharkhand - 826004	1800-102-5679
Noida	Salarpur Khadar	Professional Logistics	2, Gejha Rd, Goyal Colony, Salarpur Khadar, Sector 102, Noida, Uttar Pradesh - 201304	1800-102-5679
Mumbai	Vashi	Professional Logistics	Plot-92,gala no 01,Sector 19C Vashi Navi, Mumbai - 400705	1800-102-5679

State/ City	Location	Logistic	Address	Toll-Free Number
Pune	Vallabh Nagar	Professional Logistics	No.3/20,Near Ashok Sah Bank, Vallabh Nagar, S.T.Stand Road, Pimpri, Pune - 302021	1800-102-5679
Odisha	Cuttack	Professional Logistics	Cuttack, Odisha	1800-102-5679
Hyderabad	Secunderabad	Professional Logistics	4,Block-3,4th Shatter at 179, MPR Estates Near Old Check Post Old Bowaenpally Secunderabad, Hyderabad - 500011	1800-102-5679
Bangalore	Yeshwanthpur	Professional Logistics	No.44 1st floor 2nd main D.D.U.T.T.L. Yeshwanthpur, Bangalore - 560022	1800-102-5679
Mangalore	Bhathery Road Bloor	Professional Logistics	Opp. Hindustan Lever Ltd, Sulthan, Bhathery Road Bloor, Mangalore (KA) - 575003	1800-102-5679
Jharkhand	Ranchi	Professional Logistics	Ranchi, Jharkhand	1800-102-5679
Chennai	Sennerkuppam	Professional Logistics	27,Sakthi Nagar Phase-II, Sennerkuppam, Near Bisleri Water Plant, Chennai - 600056	1800-102-5679
Rajasthan	Jaipur	Professional Logistics	A-81, 200 ft. By Pass, Heerapura, Jaipur, Rajasthan - 302021	1800-102-5679
Bokaro	Odisha	Professional Logistics	Cuttack, Odisha, India	1800-102-5679
Guwahati	Kundil	Professional Logistics	HN-34, Kundil Nagar Basistha Chariali, Near Parbhat Apartment, Guwahati - 781029	1800-102-5679
Lucknow	Kanpur Road	Professional Logistics	S-175,1st Floor Transport Nagar Near RTO Kanpur Road Lucknow - 226004	1800-102-5679
Madhya Pradesh	Indore	Professional Logistics	284 AS-3 Scheme No.-78,Vijay Nagar, Indore, Madhya Pradesh	1800-102-5679
Ahmedabad	Pushp Penament	Professional Logistics	Shop No D-18, Pushp Penament, Behind Mony Hotel, Isanpur, Ahmedabad	1800-102-5679
Patna	Malyanil buddha	Professional Logistics	Dr. A.K Pandey (IPS) Malyanil buddha Colony, Patna (Bihar) - 800001	1800-102-5679
Andhra Pradesh	Vishakapatnam	Professional Logistics	Shop No.8, New Gajuwaka, Opp. High School Road, Vishakapatnam, Andhra Pradesh - 530026	1800-102-5679
Chandigarh	Pharbhat Road	Professional Logistics	Shop no:-19, Pharbhat Road, Opp:- Tennis Academy, Zirakpur, Chandigarh, Punjab	1800-102-5679

State/ City	Location	Logistic	Address	Toll-Free Number
Kolkata	B.T. ROAD DUNLOP	Professional Logistics	156A/73, Northern Park, B.T. Road Dunlop, Kolkata -700108	1800-102-5679
Odisha	Bhubaneswar	Professional Logistics	Acharya Vihar - jaydev Vihar Rd, Bhubaneswar, Odisha	1800-102-5679
West Bengal	Asansol	Professional Logistics	Shop No-4 Asansol Station Bus Stand Road, Munshi Bazar, Asansol, West Bengal - 713301	1800-102-5679

Open Source Licensing Terms and Conditions

- The firmware of this product also includes some of the Open-Source software released under GNU General Public License (GPL) Version 2. Terms of this license is printed in full below.
- The source of the open source software used in this product is available on CD, upon written request from:

R&D Team
Matrix Comsec Pvt Ltd
394, Makarpura GIDC,
Vadodara - 390 010
Gujarat
India.

Customer shall bear the shipping and handling charges.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion

of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your

cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>
```

```
This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.
```

```
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
```

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.
```

```
<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Index

A

Access Code 259
Advanced Settings 119, 168, 216
Allowed - Denied Logic 65, 110, 158, 196
Applications 6
Auto Configuration Upgrade 284
Automatic Number Translation (ANT) 201

B

B - channel 80, 128
Backup Configuration 286
Battery 8
Black Listed Callers 67, 197

C

CA Signed Certificate 270
Call Detail Record Filters 198, 275
Call Detail Records(CDR) 274
Call Detail Report 279
Call Progress Tones 20, 339
Called party 3
Called-Numbering Plan Identification (NPI) 79, 127
Called-Type of Numbering Plan (TON) 79, 127
Callee 3
Caller 3
Caller-Numbering Plan Identification (NPI) 79, 127
Caller-Type of Numbering Plan (TON) 79, 127
Calling party 3
CAS Settings 80
Certificate 192
Certificate Manager 264

Certificate Signing Request 270
Channel Selection Method 244
Check Proxy Address for Incoming SIP Message 210
Check Proxy Port for Incoming SIP Message 210
Clock Synchronization 184
Clone MAC Address 40
Codec Profile 212, 224
Comm Manager Failure Cause 303
Configuration Status 325
Configuration Upgrade 284, 290
Connecting SETU VTEP
 Computer 15
 ISDN Network 11
 Power Supply 13
 VoIP Network 10
Connection Type 26
Copy Channel Based Routing Parameters 113, 162
Copy E1-CAS Parameters 84
Copy MSN Based Routing Parameters 116, 165
Copy SIP Trunk Parameters 74
Copy T1E1 Port Parameters 122, 171
Copy T1-RBS Parameters 131
Country Code 21
Custom Pulse 121, 171

D

D - Channel 80
Date-Time Settings 175
Daylight Saving Time 176
Debug Settings 291
Default Region Table 336

Default System 315

Destination Number Determination 44, 86, 134

Route after Answering the Call and Collecting the Digits 51, 93, 142

Route Calls without any Destination Number 45, 87, 134

Route on the basis of Calling Party Number 46, 87, 135

Route on the basis of DDI Number 48, 91, 139

Route to a Fixed Destination Number 45, 87, 134

Route to the Called Party Number 50, 93, 140

Destination Port 3

Destination Port Determination 53, 97, 144, 226

Fixed 54, 97, 144

On the basis of Calling Party Number 61, 105, 153

On the basis of Destination Number 57, 101, 148

Dial Plan 193

Digest Authentication 208, 210, 253

Disconnecting a Call using Access Code 281

DNS Setting 28

DTMF for VoIP 221

DTMF Settings 119

Dynamic DNS 29, 35

E

E1 Port 75, 173

E1-CAS R2 MFC Parameters 82

Emergency Number 260

Error Tone Delay Timer 183

Error Tone Timer 183

Ethernet Port 3

F

FAX 222

Fax Protocol 44

FDL Protocol 131

Firmware Status 325

Firmware Upgrade 282

First Free 243

Framing 125

Framing Mode 77

G

General Request Timer 188

Group 241

H

Handling of Calls 118, 168

Handling of Incoming Calls 44, 79, 126

Channel Number Wise 111, 159

MSN/DDI Number Wise 115, 163

Port Wise 85, 133

Handling of Outgoing Calls 68, 117, 166

L

LAN 24

Line Coding 77, 125

Line Signal Parameters 82

Line Signaling Variants 130

M

Maintenance 282

Making a New Call using Access Code 281

Management/Security Settings 189

Manual Call Test 314

Manual Configuration Upgrade 286

Media Manager 293

Member Selection Method 243

Message Wait Indication (MWI) 74

N

NAT 185

Network 22, 327

Ethernet Port 328

LAN Port 327

NAT 329

Network Port 3

Notification Filters 311

Notification Settings 309

Number Lists 196

O

Originating Port 3

Overview of SETU VTEP 4

P

Package Contents 9

Pass-Through FAX Parameters 223

PCAP Trace 312

PCM Companding Type 20

Peer-to-Peer Dialing 245

Performance Monitoring Counter 319

PIN Authentication 250

Presentation Indicator 80, 128
PRI Settings 122, 130
Progress Indicator (PI) 79, 127
Protecting SETU VTEP 7

Q

QoS (Layer 3) 40

R

RBS Settings 128
Real Time Clock 175
Redundancy Settings 211
Region 20
Register Signal Parameters 82
Register Signaling Variant 131
Registrar Settings 208
Reset Cycle 13
Ring Type 21
Rotation 243
RTP 220

S

Screening Indicator 80, 128
Security Settings 308
Self-Signed CA Certificate 264
Self-Signed Certificate 264
SIP INVITE Timer 188
SIP Network Profile 205
SIP Over TCP 187
SIP Over TLS 187
SIP Provisional Timer 188
SIP TCP Port 188
SIP TLS Port 188
SIP Trunk 41
SIP UDP Port 188
SIP VoIP Profile 220
SMTP Errors 303
SNMP 306
SNMP Settings 307
SNTP Settings 180
Soft Restart 317
Source 3
SRTP 221
Static Routing 255
Static Routing Table 256
Status 322
 FXO Port 330
 SIP Trunk 330
STUN Server Address and Port 185

System Activity Log 296
System Certificate (Self-Signed Certificate) 267
System Debug 291
System Detail 322
System Engineers 1
System Fault Log 301
System Parameters 181

T

T.38 FAX Parameters 222
T1 Port 123
T1E1 Port Alarms 318
 BLUE Alarm 318
 RED Alarm 318
 YELLOW Alarm 318
TCP NAT Keep Alive 186
Terminating Port 3
Trusted Root CA 266

U

UDP NAT Keep Alive 186
Users 1

V

VLAN/CoS 40
VMS Debug 348
VoIP Profile 215

W

WAN 25
Wildcard Characters 58, 102, 150, 194, 234, 237



MATRIX COMSEC

Head Office

394-GIDC, Makarpura, Vadodara - 390010, India.

Ph: (+91)1800-258-7747

E-mail: Customer.Care@MatrixComSec.com

www.MatrixTeleSol.com